AUTARQUIA ASSOCIADA À UNIVERSIDADE DE SÃO PAULO

**Metodologia de especificação e projeto aplicado a usinas nucleares
móveis**

LUCIANO ONDIR FREIRE

**Tese apresentada como parte dos
requisitos para obtenção do Grau de
Doutor em Ciências na Área
de Tecnologia Nuclear - Reatores**

Orientador:

Prof. Dr. Delvonei Alves de Andrade

São Paulo

2018

INSTITUTO DE PESQUISAS ENERGÉTICAS E NUCLEARES
Autarquia associada à Universidade de São Paulo

**Metodologia de especificação e projeto aplicado a usinas nucleares
móveis**

LUCIANO ONDIR FREIRE

**Tese apresentada como parte dos
requisitos para obtenção do Grau de
Doutor em Ciências na Área
de Tecnologia Nuclear - Reatores**

Orientador:

Prof. Dr. Delvonei Alves de Andrade

Versão Corrigida

Versão Original disponível no IPEN

São Paulo

2018

Autorizo a reprodução e divulgação total ou parcial deste trabalho,
para fins de estudo e pesquisa, desde que citada a fonte

Como citar:

ONDIR FREIRE, L. **Metodologia de especificação e projeto aplicado a usinas nucleares móveis**. 2018. 180 p. Tese (Doutorado em Tecnologia Nuclear), Instituto de Pesquisas Energéticas e Nucleares, IPEN-CNEN/SP, São Paulo. Disponível em: <www.teses.usp.br> (data de consulta no formato: dd/mm/aaaa)

Ficha catalográfica elaborada pelo Sistema de geração automática da Biblioteca IPEN/USP,
com os dados fornecidos pelo(a) autor(a)

Ondir Freire, Luciano

Metodologia de especificação e projeto aplicado a usinas nucleares móveis / Luciano Ondir Freire; orientador Delvonei Alves de Andrade. -- São Paulo, 2018.
180 p.

Tese (Doutorado) - Programa de Pós-Graduação em Tecnologia Nuclear (Reatores) -- Instituto de Pesquisas Energéticas e Nucleares, São Paulo, 2018.

1. Método de projeto. 2. Lei Construtal. 3. Usina nuclear móvel. 4. Reator Naval. 5. Engenharia de Sistemas. I. Alves de Andrade, Delvonei, orient. II. Título.

DEDICATÓRIA

Este trabalho é dedicado à minha mulher Sueide com amor e gratidão por sua presença e compreensão das minhas ausências e pelo incessante apoio e incentivo em todos os momentos ao longo dessa jornada.

AGRADECIMENTOS

Ao Prof. Dr. Delvonei agradeço imensamente pela competente orientação deste trabalho. Atuou com muita dedicação e responsabilidade na condução desse processo, em especial, na busca de apoio para a pesquisa, que sem o qual, este trabalho não seria possível. Os seus conselhos e recomendações foram fundamentais para o desenvolvimento deste trabalho. Sou muito grato ao Dr. Delvonei pela confiança depositada em mim e por sempre ter acreditado no potencial desse projeto.

RESUMO

FREIRE, Luciano Ondir. **Metodologia de especificação e projeto aplicado a usinas nucleares móveis**. 2018. 180p. Tese (Doutorado em tecnologia nuclear) – Instituto de Pesquisas Energéticas e Nucleares – IPEN-CNEN/SP. São Paulo.

A importância de métodos de projeto vem crescendo nos últimos anos à medida que sistemas sócio-técnicos complexos se tornam mais numerosos. Além da complexidade, o tamanho e o investimento financeiro destes sistemas amplificam a gravidade dos erros de projeto. O objetivo geral deste trabalho foi desenvolver uma metodologia de especificação e projeto que reduza o tempo e energia para desenvolver um sistema complexo cujas funções sejam conhecidas a priori, gerenciando em paralelo os riscos. O objetivo específico foi verificar a viabilidade econômica de usinas nucleares móveis de pequeno porte. Este trabalho adotou como princípio a lei construtal que prevê o sucesso de sistemas que facilitem os fluxos necessários à sua existência. Após a identificação dos fatores chave para facilitar o fluxo de informações, esta tese desenvolveu um conjunto de conceitos para facilitar o trabalho de engenharia. Aplicando tais conceitos, este trabalho desenvolveu sequências de atividades que descrevem o método proposto, sendo cada atividade detalhada por uma lista de requisitos. A demonstração das vantagens do método proposto foi feita por meio de análise de árvore de eventos e árvore de falhas. Usando o método, esta tese desenvolveu especificações e projetos em vários níveis (empresarial, usina, caldeira nuclear, circuito primário e gerador de vapor). Baseando-se em dados da marinha americana, esta tese desenvolveu um modelo de custo para reatores de pequeno porte. Concluiu que a energia nuclear pode ser competitiva se a potência elétrica média efetiva ao longo da vida útil ficar acima de 30MWe e se o tempo de vida útil for igual ou maior do que 60 anos. Tal fato decorre dos altos custos de aquisição que requerem uma vida longa para compensar o investimento e dos efeitos de economia de escala especialmente pronunciados para reatores a água pressurizada.

Palavras-chave: Método de projeto, Lei Construtal, Usina nuclear móvel, Segurança energética, Reator Naval, Engenharia de Sistemas

ABSTRACT

FREIRE, Luciano Ondir. **Specification and design methodology applied to mobile nuclear power plants**. 2018. 180p. Tese (Doutorado em tecnologia nuclear) – Instituto de Pesquisas Energéticas e Nucleares – IPEN-CNEN/SP. São Paulo.

The importance of design methodologies has been growing in recent years as complex socio-technical systems become more common. In addition to complexity, the size and financial investment of these systems amplifies the severity of design errors. The general goal of this work was to develop a specification and design methodology that reduces the time and energy to develop a complex system whose functions are known *a priori*, managing the risks in parallel. The specific goal was to verify if small modular reactors could be economically possible. This work adopted as principle the Constructal law, that predicts the success of systems that ease the necessary flows to its existence. After finding the key factors to ease the flow of information, this work developed a set of concepts to ease the engineering work. Applying such concepts, this work developed sequences of activities that describe the proposed methodology. Lists of requirements gave guidance for each activity. Event tree and fault tree analyses showed the advantages of the proposed methodology. Using the methodology, this work developed specifications and designs at many product breakdown levels (enterprise, nuclear power plant, nuclear steam supply system, reactor coolant system and steam generator). Using data from US Navy, this work developed a cost model for small reactors. This work concluded that nuclear power may be competitive if average electrical power extracted during the life is larger than 30 MWe and if life time is superior to 60 years. The first condition is consequence of the high overnight costs of nuclear power. The second is consequence of the strong scale economy effects of pressurized water reactors.

Keywords: Design methodology, Constructal Law, Mobile nuclear power plants, Energy security, Naval Reactors, System Engineering

LISTA DE TABELAS

Tabela 1 – Dados do sistema de refrigeração do primário do NS Savannah.....	33
Tabela 2 – Dados do núcleo do reator do NS Savannah.....	33
Tabela 3 – Dados do núcleo do NS Sevmorput	40
Tabela 4 – Analogia entre as funções de um canal físico e um canal de informação.....	45
Tabela 5 – Requisitos do sistema para o exemplo didático	72
Tabela 6 – Identificando nexos causais entre funções de serviço e funções técnicas	74
Tabela 7 – Classificação de funções do sistema S5 – Inversor	74
Tabela 8 – Identificação dos status de cada subsistema	75
Tabela 9 – identificação de fases do exemplo didático	76
Tabela 10 – Declinando requisitos entre níveis hierárquicos	76
Tabela 11 – Requisitos para caracterizar as funções técnicas dentro de cada status	77
Tabela 12 – Escolha do método de realização	77
Tabela 13 – Caracterização de interfaces do exemplo didático.....	78
Tabela 14 – Compatibilização de interfaces	79
Tabela 15 – Definição de modos de operação do exemplo didático.....	79
Tabela 16 – Configuração de referência	79
Tabela 17 – Desempenhos calculados para o exemplo didático.....	80
Tabela 18 – Definição de procedimentos do produto do exemplo didático	80
Tabela 19 – Revisão da compatibilização de interfaces	81
Tabela 20 – Projetando interfaces.....	82
Tabela 21 – Analisando riscos	82
Tabela 22 – Revisão da compatibilização de interfaces	83
Tabela 23 – Revisão do projeto de interface.....	84
Tabela 24 – Cálculo de propriedades.....	84
Tabela 25 – Verificação de atendimento	84
Tabela 26 – Atividades nas interfaces por estado da empresa.....	89
Tabela 27 – Características das classes mais numerosas por grupo	91
Tabela 28 – Atividades por status de uma usina nucleares móvel.....	97
Tabela 29 – Status da caldeira nuclear.....	101

Tabela 30 – Status do circuito primário.....	105
Tabela 31 – Status do sistema de geração de vapor.....	107
Tabela 32 – Configuração física por modo de operação do circuito primário.....	114
Tabela 33 – Hipóteses de características do reator	118
Tabela 34 – Configuração física por modo de operação do circuito primário.....	120
Tabela 36 – Características não funcionais do Circuito primário.....	121
Tabela 36 – Propriedades estimadas da caldeira nuclear.....	125
Tabela 37 – Configuração física por modo de operação da caldeira nuclear	126
Tabela 38 – Propriedades da usina nuclear móvel.....	128
Tabela 39 – Configuração física por modo de operação da usina	129
Tabela 40 – Comparação com UML.....	133
Tabela 41 – Relação com alguns processos PMBOK.....	136
Tabela 42 – Hipóteses adotadas na estimativa de custo	144

LISTA DE FIGURAS

Figura 1 – Ilustração da composição de um sistema sócio-técnico complexo.....	16
Figura 2 – Definição de Sistema cibernético neste trabalho	20
Figura 3 – Arranjo do NS Savannah	32
Figura 4 – Visão superior da contenção nuclear do NS Savannah.	34
Figura 5 – Arquitetura do reator do NS Otto Hahn.....	36
Figura 6 – Arranjo geral do NS Mutsu	37
Figura 7 – Vista superior do núcleo do reator do NS Mutsu	37
Figura 8 – Fluxograma de processo do NS Mutsu.....	38
Figura 9 – Mudanças feitas no NS Mutsu	39
Figura 10 – Seção reta do reator KLT-40.	40
Figura 11 – Sistema de resfriamento do reator KLT-40	41
Figura 12 – Análise funcional de um canal.....	44
Figura 13 – Dilema da redução do risco – adaptado de [34]	46
Figura 14 – Conceito de separação formal entre problema e solução.....	48
Figura 15 – Modelo de Sistema	49
Figura 16 – Conceito de diferentes estados de um Sistema genérico	51
Figura 17 – Equivalência e não equivalência funcional entre sistemas	53
Figura 18 – Exemplo de mapeamento dos modos de operação nos status	54
Figura 19 – Qualificadores dos modos de operação no espaço de estados.....	61
Figura 20 – Árvore de eventos de especificação.....	62
Figura 21 – Árvore lógica para cálculo da probabilidade P1	64
Figura 22 – Árvore lógica para cálculo da probabilidade P2 e P3.....	64
Figura 23 – Diferença conceitual entre especificação (sistema) e solução (produto)..	66
Figura 24 – Comparação das abordagens atuais com a abordagem proposta.....	67
Figura 25 – Relação entre equipe de projeto e decomposição do sistema	68
Figura 26 – Fluxos de informação de uma equipe de projeto.....	69
Figura 27 – Fluxos de informação nas interfaces de um arquiteto	70
Figura 28 – Diagrama de estados de um arquiteto.....	71
Figura 29 – Diagrama de blocos do exemplo didático.....	71
Figura 30 – Modelo de comportamento do exemplo didático	72

Figura 31 – Identificação de subsistemas do exemplo didático.....	73
Figura 32 – Identificação de funções técnicas	73
Figura 33 – Revisão da especificação dos subsistemas	81
Figura 34 – Revisão da especificação	83
Figura 35 – Diagrama de status da empresa	88
Figura 36 – Diagrama de blocos do navio	91
Figura 37 – Status dos navios	91
Figura 38 – Diagrama funcional da empresa nuclear móvel.....	94
Figura 39 – Diagrama de status da usina nuclear móvel.....	97
Figura 40 – Diagrama funcional de uma usina nuclear móvel	98
Figura 41 – Diagrama de estados da caldeira nuclear.....	101
Figura 42 – Diagrama funcional da caldeira nuclear	102
Figura 43 – Diagrama de status do Sistema de Resfriamento do Reator.....	103
Figura 44 – Diagrama funcional do Circuito primário	106
Figura 45 – Diagrama de estados do Sistema de geração de vapor	107
Figura 46 – Diagrama funcional do gerador de vapor híbrido.....	109
Figura 47 – Trocador de calor do tipo casco e placa	111
Figura 48 – Comparação de tamanho para uma mesma potência.....	111
Figura 49 – Vista superior do arranjo de pilhas de placas no gerador de vapor	112
Figura 50 – Arranjo proposto para o trocador de calor (não está em escala).....	112
Figura 51 – Arranjo dos geradores de vapor.....	113
Figura 52 – Arquitetura do Circuito primário proposto	117
Figura 53 – Esquema físico do Circuito primário proposto.....	117
Figura 54 – Diagrama de pressão versus temperatura do circuito primário	119
Figura 55 – Esquema físico da contenção após acidente de perda de refrigerante	122
Figura 56 – Resfriamento de emergência e despressurização automática	123
Figura 57 – Arquitetura do sistema de remoção de calor residual.....	123
Figura 58 – Esquema do circuito primário auxiliar	124
Figura 59 – Diagrama unifilar do sistema de alimentação elétrica (de segurança) ...	124
Figura 60 – Arranjo geral da usina nuclear móvel.....	127
Figura 61 – Comparação de tamanho da usina proposta com um navio.....	128
Figura 62 – Efeito da potência sobre o custo da energia	143

Figura 63 – Comparação do custo de transporte das opções	145
Figura 64 – Comparação do diesel e de um navio nuclear com módulo nuclear	146

LISTA DE ABREVIATURAS E/OU SIGLAS

ABEN	Associação Brasileira de Energia Nuclear
AISI	American Iron and Steel Institute
ANS	American Nuclear Society
ANSI	American National Standards Institute
ASME B & PVC	American Society of Mechanical Engineers Boiler and Pressure Vessel Code
Bar	Unidade de pressão (10^5 Pascals)
CNEN	Comissão Nacional de Energia Nuclear
CO₂	Dióxido de carbono
dB	Decibéis
EDF	Électricité de France (Empresa)
EPRI	Electric Power Research Institute
FR	Função Recebida
FS	Função de Serviço
FT	Função Técnica
g	Gravidade ($9,81\text{m}^2/\text{s}$)
GESMEX	GESMEX Exchangers GmbH (Empresa)
Hz	Hertz
IAEA	International Atomic Energy Agency
IBM	International Business Machines (Empresa)
IEEE	Institute of Electrical and Electronics Engineers
IEN	Instituto de Engenharia Nuclear
INAC	International Nuclear Atlantic Conference
IPEN	Instituto de Pesquisas Energéticas e Nucleares
IRD	Instituto de Radioproteção e Dosimetria
JAERI	Japanese Atomic Energy Research Institute
kV	Quilovolts
kW	Quilowatts
m	Metro
MAM	MAN Diesel & Turbo (Empresa)
MW	Mega Watts

MWe	Mega Watts elétricos
MWth	Mega Watts térmicos
NASA	National Aeronautics and Space Administration
NEA	Nuclear Energy Agency
NM	Nautical Miles
NOx	Família de óxido de nitrogênio
NPSH	Net Positive Suction Head
NRC	Nuclear Regulatory Commission
NS	Nuclear Ship
OOSE	Object-Oriented System Engineering
PFD	Probabilidade de Falha sob Demanda
PMBOK	Project Management Body Of Knowledge
SOx	Família de óxidos de enxofre
SysML	System Modeling Language
TMI	Three Mile Island
ULCC	Ultra Large Crude Carrier
UML	Unified Modeling Language
USP	Universidade de São Paulo
V&V	Validação e Verificação
VLBC	Very Large Bulk Carrier
VLCC	Very Large Crude Carrier

SUMÁRIO

1 INTRODUÇÃO	14
1.1 Contexto do tema da pesquisa.....	14
1.2 Relevância e contribuição original do trabalho.....	24
1.3 Objetivos da pesquisa.....	25
1.3.1 Objetivo geral.....	25
1.3.2 Objetivo específico	25
1.4 Estrutura da tese	25
2 REVISÃO DA LITERATURA	27
2.1 Bases fundamentais da engenharia de sistemas e histórico	27
2.2 Revisão dos métodos de engenharia de sistemas	28
2.3 Revisão dos navios mercantes nucleares	31
3 METODOLOGIA	42
3.1 Delineamento da pesquisa.....	42
3.2 Embasamento teórico	42
3.3 Desenvolvimento da metodologia.....	49
4 DESENVOLVIMENTO	85
4.1 Proposta de uma empresa provedora de usinas nucleares móveis	85
4.2 Análise de cima para baixo em um navio mercante.....	89
4.3 Análise de cima para baixo em uma empresa de usinas nucleares móveis....	94
4.4 Análise de cima para baixo em uma usina nuclear móvel	98

4.5 Análise de cima para baixo em um sistema de refrigeração do reator.....	101
4.6 Análise de cima para baixo em um sistema de geração de vapor	106
4.7 Análise de cima para baixo nos componentes do gerador de vapor	107
5 RESULTADOS.....	110
5.1 Análise de baixo para cima no gerador de vapor	110
5.2 Análise de baixo para cima no circuito primário	114
5.3 Análise de baixo para cima na caldeira nuclear.....	121
5.4 Análise de baixo para cima na usina nuclear móvel	127
6 ANÁLISE E DISCUSSÃO DOS RESULTADOS	130
7 CONCLUSÃO	148
8 REFERÊNCIAS BIBLIOGRÁFICAS.....	151
ANEXO 1 – Lista de requisitos e suas justificativas	157

1 INTRODUÇÃO

1.1 Contexto do tema da pesquisa

O avanço tecnológico vem impondo a concepção cada vez mais frequente de sistemas cibernéticos e complexos. Exemplos são usinas nucleares, submarinos nucleares, navios aeródromos e navios mercantes. Tais sistemas são cibernéticos devido à existência malhas fechadas para regular seu comportamento. Mesmo que as máquinas não tenham nenhum tipo de inteligência intrínseca, a presença do homem como tomador de decisões confere essa característica de malha fechada. Vale ressaltar que é incomum nos dias de hoje achar sistemas cujas máquinas sejam desprovidas de computadores e de certo grau de inteligência.

A natureza parece privilegiar soluções que favoreçam o fluxo de massa e energia, tal como sintetizado pela lei construtal. Sistemas grandes e complexos facilitam mais os fluxos do que sistemas pequenos e simples, fato que é chamado de economia de escala. Grandes navios conseguem transportar mercadorias a um custo energético menor do que pequenos navios. Grandes usinas termelétricas são mais eficientes do que usinas pequenas. Evidentemente, tais gigantes só podem sobreviver se houver grandes demandas e ofertas. A globalização acaba gerando tais ofertas e demandas, criando um ambiente no qual gigantes são favorecidos.

Isso significa que a evolução tecnológica, acompanhada da integração econômica mundial, chamada de globalização, favorece o aumento de sistemas complexos. Tais sistemas não podem mais ser concebidos por um único homem. Requerem equipes numerosas trabalhando muitos anos antes de ver o resultado. A equipe de projeto em si é um sistema cibernético complexo.

O gigantismo desses sistemas faz com que qualquer falha se torne um risco potencialmente muito grande. Por outro lado, evitar falhas torna-se quadraticamente mais difícil com o aumento da complexidade. Existem riscos de projeto, que causam o aumento de custos e estouro do orçamento, levando a danos ao patrimônio. Existem também riscos à segurança das pessoas e do meio ambiente. Risco é o dano financeiro esperado causado por um perigo. Consequentemente, um risco causa um aumento no custo de ciclo de vida que

ocorre de maneira estocástica e não determinística, decorrente da imperfeição das informações e concorre para a ineficiência.

Para controlar tais riscos, a adoção de metodologias se faz necessária. Atualmente, tais metodologias são reunidas em uma disciplina chamada de engenharia de sistemas. Metodologias são compostas de processo, ferramentas e métodos.

Ferramentas são instrumentos que facilitam ou possibilitam a execução de uma tarefa. Ferramentas requerem pessoas propriamente treinadas e habilitadas para que se tornem produtivas. Ferramentas reduzem o tempo ou energia requerida para a execução de uma tarefa. Ferramentas podem ser ideias, processos, métodos, software, computadores ou equipamentos.

Processo é uma sequência lógica de tarefas a serem executadas para atingir um objetivo particular. Um processo define o que deve ser feito, sem especificar como as tarefas devem ser feitas. A estrutura de um processo prevê vários níveis de decomposição para permitir a realização de análises e definições em vários níveis de detalhe. Essas análises e definições dão base à tomada de decisão.

Método é a definição de como realizar uma tarefa, consistindo de técnicas. Nesse contexto, as palavras método, técnica, prática e procedimento são comumente usadas como sinônimos. A cada nível, as tarefas de um processo são realizadas usando um método. Cada método também é um processo em si, com uma sequência de tarefas a serem executadas. Em outras palavras, cada método em um nível de abstração é visto como um processo no nível mais detalhado.

Metodologia é uma coleção de ferramentas, processos e métodos usados de maneira coordenada e lógica para resolver uma classe específica de problemas. Existe também o ambiente de desenvolvimento. Ambiente são objetos externos, condições e fatores que permitam a atividade de projeto. O ambiente integra e dá suporte aos métodos e ferramentas necessários à atividade de projeto.

O modelo de um sistema é a divisão do universo percebido em dois lados, um interno e outro externo, que se relacionam por meio de entradas e saídas [1]. O comportamento do sistema é inicialmente representado por meio de estados que é o que ocorre dentro do

sistema. Para Wymore, estado é um vetor de variáveis numéricas, podendo pertencer a um conjunto finito (0 ou 1, por exemplo) ou a um conjunto infinito (números reais, por exemplo) [1].

Embora pessoas trabalhem em sistemas, o ser humano em si não faz parte de um sistema. O componente do sistema é o capital humano, que é um bem imaterial que está sempre contido em pessoas, mas não é as pessoas. O capital humano é a combinação de competência e motivação dos indivíduos de realizarem os papéis necessários à consecução dos objetivos do sistema. Um sistema sócio-técnico complexo é um conjunto de ferramentas e capital humano operando sob o controle de um processo, tal como exibido na Figura 1.

Figura 1 – Ilustração da composição de um sistema sócio-técnico complexo

O projeto de sistemas complexos geralmente usa processos de ciclos de vida para balizar a concepção, o projeto detalhado, a construção, a operação e o descarte. Os processos mais usuais são: cascata, espiral e “Ve”. Existem também processos de aquisição de sistemas complexos, tais como o da NASA e do Departamento de Defesa dos Estados Unidos. O processo da NASA divide o ciclo de vida em fases numeradas por letras: A (concepção), B (projeto básico), C (projeto detalhado), D (construção), E (operação) e F (descarte). O processo de aquisição do Departamento de Defesa é similar, mas usa letras para indicar eventos e não fases.

Os processos de desenvolvimento podem ser baseados em documentos ou em modelos. Em um processo baseado em documentos, cada participante executa suas tarefas e

comunica os resultados de seu trabalho por meio de documentos. A informação total fica na mente de cada participante, sendo que cada documento é uma faceta desse conjunto de informações. Por exemplo, um arquiteto pode fazer um documento para mostrar as características de sua solução, outro para mostrar os cálculos, outro para dar detalhes das interfaces e outro para descrever o modo de operação.

Evidentemente, os dados de saída de um participante servirão de entrada para outro. À medida que o projeto evolui e os dados mudam, garantir a consistência entre cada documento se torna um problema. Para isso, são necessárias reuniões entre os participantes para certificar de que os dados dos diversos documentos estejam consistentes.

Em um processo baseado em modelos, existe um ambiente digital no qual os participantes inserem seu trabalho usando uma linguagem específica, tal como UML ou SysML. Nesse ambiente, mudanças em um trabalho gerarão avisos imediatos a todos os envolvidos. A replicação de dados é cuidadosamente evitada, criando um banco de dados único a partir do qual a documentação é gerada de maneira automática. A consistência entre documentos é assim assegurada por software. Documentos em linguagem comum precisam ser gerados para lidar com o público externo, que geralmente não é treinado na linguagem empregada no ambiente de desenvolvimento.

Processos baseados em modelos podem alcançar uma produtividade elevada, mas requerem uma equipe treinada em uma linguagem incomum nos dias de hoje. Existem vários fornecedores de soluções que integram um ambiente de desenvolvimento, um processo, métodos e ferramentas, tais como a IBM com o ambiente Rhapsody e o processo Harmony.

Apesar da importância da modelagem comportamental para o projeto de sistemas, a literatura ainda deu menos atenção a esse aspecto do que à modelagem física de sistemas. Atualmente, no campo de modelagem comportamental, vários autores apresentam muitas definições diferentes usando as mesmas palavras, fato que pode gerar confusão. Por exemplo, em engenharia de controle, estado é um vetor de variáveis pertencentes ao conjunto dos números reais, como posição, velocidade e aceleração. O conjunto dos possíveis valores do vetor de estado é chamado de espaço de estados [2].

Por outro lado, Wasson define modo como uma maneira de operar relacionada a objetivos dentro de uma fase na vida de um sistema [3]. Estado seria um modo de existência

no qual um sistema pode estar, tal como também definido pela norma IEEE-Std-610.12 [4], e está dentro de um modo de operação. Adicionalmente, cada estado tem um conjunto de configurações físicas que consistem na maneira como um sistema está arranjado (Sistema ou item de arquitetura, interfaces e configurações).

Por outro lado, Wymore define modos de um sistema como um sistema próprio, com suas próprias entradas, saídas e estados [1]. Para Wymore, estado é o que ocorre dentro do sistema e todo sistema tem um conjunto não vazio de estados. Cada estado é uma variável que pode assumir um valor dentro de um conjunto finito, como em máquinas de estado finitos ou dentro de um conjunto infinito, tal como números reais. Wymore [1] usa a mesma palavra estado para denominar o vetor de variáveis e cada variável dentro deste vetor. A metodologia “Análise de Estados” [5] adota uma definição similar de estado, afirmando que um vetor de variáveis de estado representa o conhecimento completo do estado de um sistema. Tal como para Wymore, na “Análise de Estados” as variáveis de estado podem ser discretas, tais como modos de operação de uma câmera (ligada ou desligada) ou contínuas, como a temperatura interna da câmera.

Existem ainda definições baseadas na linguagem gráfica chamada SysML, discutidas a seguir. Para Weillkiens [6], um estado representa um conjunto nomeado de combinações de valores para o sistema, que pode ter comportamentos ativados em certos eventos. Para a OOSE [7], um estado representa uma condição significativa na vida do sistema, representando como o sistema responde a eventos e quais comportamentos ele executa.

Atualmente, muitos sistemas complexos artificiais adotam estados tais como representados em diagramas de máquinas de estado, representando uma síntese de informação. Por exemplo, países usam estados de exceção (Guerra, calamidade pública, sítio), dando um conjunto de comandos predefinidos aos vários agentes públicos. Outro exemplo é o de uma usina nuclear, que tem um conjunto de estados definidos de acordo com calor residual, pressão e temperatura do circuito primário e fornecimento de energia. Belonaves também adotam conceitos similares, mas usando em português, as palavras regime ou postos.

Esses exemplos mostram que as pessoas vêm adotando usualmente a palavra estado para denominar um grupo de comportamentos desejáveis a serem executados simultaneamente. Essa abordagem tem um potencial inexplorado para gerenciar a complexidade do projeto de sistemas complexos, bem como sua operação.

Ainda que existam similaridades nos conceitos de modelagem comportamental, existem muitas diferenças e discrepâncias. Para vários autores, estado é um vetor de variáveis enquanto para outros, estado é uma única variável que pode assumir um número finito de valores (noção usada nos diagramas de máquinas de estado da SysML). Essa falta de definição clara usando as mesmas palavras pode criar confusão e conflitos dentro de uma equipe de projeto. Outros problemas é a redundância de estados (ter dois estados idênticos representados no diagrama) ou falta de estados que atendam às necessidades.

Um problema advindo da definição de estado como vetor de variáveis é a grande quantidade de estados possíveis, conhecida como explosão de estados. Assumindo um vetor com dez variáveis binárias como estado de um sistema, existem 1024 possíveis combinações no espaço de estados. Esse número elevado torna análises ou testes por estado impraticáveis.

Outro problema relacionado aos estados é a dificuldade de estimar com confiança o estado atual de um sistema complexo, sendo que tais erros podem causar acidentes. Esse trabalho adota a palavra estimar porque o valor real de uma variável não pode nunca ser obtido com exatidão, sendo obtido por meios indiretos. Um exemplo de tal dificuldade foi a sequência de eventos do acidente de Three Miles Island [8] e os problemas de procedimento da abordagem baseada em eventos nas usinas nucleares [9] [10].

Outra família de dificuldades vem dos problemas de coordenação ou integração quando um sistema pode receber ordens ou perturbações de várias fontes diferentes. Se o estado do sistema não for reconhecido no momento anterior ao comando, podem haver acidentes devido ao início de uma transição inadequada.

Este trabalho adota algumas definições enumeradas a seguir. Sistema é uma divisão do mundo percebido em duas partes, sendo uma interna e outra externa [1]. Da parte externa a parte interna recebe serviços ou funções (funções recebidas) e a parte interna fornece serviços (funções de serviço). Vale ressaltar que o fluxo de massa nem sempre segue o fluxo funcional, pois quando um sistema presta o serviço de remover um fluido de outro, o fluxo de massa fica contrário ao funcional. Sistemas cibernéticos são sistemas que possuem características intrínsecas de malha fechada. Atualmente, malha fechada é caracterizada pela realimentação dos sinais das interfaces no comportamento dinâmico do sistema, tal como mostrada na Figura 2.

Figura 2 – Definição de Sistema cibernético neste trabalho

Funções são ações que um sistema deve desempenhar, transformando algum tipo de entrada em outra entidade ou mudando o estado do sistema. Por exemplo, a função de uma turbina é gerar energia mecânica usando entalpia de vapor recebida de uma caldeira. Funções de serviço são os objetivos de um sistema, cuja representação é feita com um verbo e um substantivo opcional, sendo aceitável adicionar qualificadores para completar o sentido. Desempenho é uma definição de faixa de quanto uma função deve fazer em termos de uma propriedade física, que deve ter uma unidade. Por exemplo, o desempenho de uma função de bombeamento pode ser “vazão de 15 a 20 metros cúbicos de água por hora”.

Sistemas podem ter perigos, que são falhas e acidentes em potencial que podem ter efeitos adversos, tais como perdas patrimoniais, perdas de reputação, mortes e perdas de oportunidades. Riscos são danos financeiros esperados por unidade de tempo devido à existência de um perigo.

Quanto à parte naval, no mundo em 2007, os navios mercantes são responsáveis por 2,7% das emissões de CO₂, por 4 a 9% das emissões de SO_x e 15% das emissões de NO_x [11]. Tal fato levou a mudanças nas leis ambientais, restringindo os tipos de óleo combustível, que pode levar à elevação de custos. Juntamente à escassez de combustíveis fósseis, tal mudança legal pode ter significativos impactos nos custos de transporte e no comércio mundial. Atualmente, o transporte marítimo é responsável por 95% do comércio mundial e tem papel central na economia e prosperidade dos povos [12].

A energia nuclear é a única forma de energia já posta à prova no mar que não emite poluentes na atmosfera. Apesar da existência dos riscos da energia nuclear, a sua adoção reduziria a frequência de derramamento de óleo no mar, que é muito mais frequente. Do

ponto de vista econômico, os preços do combustível nuclear são estáveis e baixos, reduzindo custos de operação e a volatilidade do mercado.

Atualmente, existe uma experiência acumulada de cerca de 700 reatores nucleares em todo o mundo [12] para uso militar e cerca de 200 reatores nucleares estavam em operação em 2012 [13]. Essa experiência indica que reatores nucleares tem melhor confiabilidade operacional do que motores Diesel [14]. O uso de energia nuclear confere maior flexibilidade ao projeto naval por possuir um volume reduzido. Além disso, a operação de navios nucleares é mais flexível devido à menor frequência de reabastecimento.

Para propulsão naval, a solução de reator nuclear mais bem-sucedida é o reator a água pressurizada, que provou ser simples, segura e compacta. Tais características são interessantes para navios mercantes porque permitem mais espaço para carga útil. Quanto à segurança, hoje em dia as usinas nucleares atingem níveis de segurança muito mais elevados do que as da primeira geração. Graças à adoção de segurança passiva e simplificações da planta, os custos de aquisição das usinas nucleares foram reduzidos, se comparados aos custos de construção dos anos 1990.

Por outro lado, usinas nucleares tem algumas desvantagens, como o alto custo de capital, problemas de proliferação nuclear e padrões rigorosos de qualidade nuclear. Se navios empregarem energia nuclear, eles estarão sujeitos às inspeções de autoridades nucleares de vários países, sendo que cada uma pode ter requisitos diferentes ou até conflitantes entre si.

Mesmo que haja em um futuro próximo a adoção de um padrão internacional único de segurança nuclear, a empresa transportadora ainda teria que adquirir e manter competências do campo nuclear. Além da manutenção de competências especializadas, instalações com classificação de segurança nuclear precisam ser construídas e mantidas para executar reparos e recarga de combustível. Por fim, existe ainda o problema da posse do combustível usado, que aumenta ainda mais o custo da opção nuclear. Para um número pequeno de reatores, todos esses custos fixos deixam a solução nuclear relativamente custosa se comparada a outras opções.

Outra dificuldade é o medo da população em relação à energia nuclear, que aumentou depois dos acidentes de Chernobyl e Fukushima, levando vários países a abandonar a energia

nuclear. Alguns navios nucleares, como o NS Otto Hahn (da Alemanha) e NS Sevmorput (da Rússia), encontraram dificuldades de obter permissão de entrar em vários portos [15].

Apesar de todos os problemas, é possível que, para grandes navios, a aplicação de energia nuclear possa ser economicamente competitiva. Existem propostas técnicas que poderiam resolver o problema do custo, tal como a linha de estudos sobre reatores pequenos e modulares [16] [17] [18]. O problema da proibição da energia nuclear nos portos poderia ser resolvido com arquiteturas modulares de navios, tal como proposta por Gravina [13]. O problema dos custos fixos poderia ser resolvido por meio da criação de uma empresa operadora de usinas nucleares móveis que deteria todas as competências nucleares. Sendo dona de muitas usinas, os custos fixos seriam diluídos, reduzindo o custo total. Tal empresa seria fiscalizada continuamente pela autoridade de segurança nuclear e libertaria as empresas de transporte de qualquer responsabilidade quanto à segurança nuclear.

No campo militar, a marinha dos Estados Unidos concluiu que a energia nuclear seria mais econômica para navios de combate de porte médio [19]. Os custos do ciclo de vida são similares e a propulsão nuclear tem muitas vantagens, como melhor mobilidade, presença, discrição acústica, discrição infravermelha e independência de navios-tanque. Esse mesmo estudo concluiu que, para navios grandes, a propulsão nuclear se torna mais econômica. Apesar do sentimento anti-nuclear, os navios com propulsão nuclear são aceitos em 150 portos em 50 países [19], o que mostra que a proibição de entrada não é um problema generalizado, mas local.

Vale ressaltar que a produção deve ser mantida para evitar a perda de competências, sendo mais barato manter uma pequena produção por um tempo longo do que desenvolver outra vez [20]. Assim, poderia ser interessante construir usinas nucleares móveis para navios mercantes para manter a produção dos reatores militares, diluindo os custos com a maior escala de produção. Assim, seria possível aproveitar a credibilidade dos reatores militares para introduzir a energia nuclear nos navios mercantes. Também seria possível fornecer energia a custos baixos, já que a maior parte das despesas fixas já estariam pagas pelos investimentos militares. O fornecimento de energia barata para propulsão dos navios mercantes aumentaria a competitividade do país. Na mesma linha de raciocínio, a infraestrutura nuclear criada para defesa poderia ser usada para reabastecer e executar

serviços de manutenção nas usinas nucleares móveis, evitando a necessidade de grandes investimentos em portos.

É fundamental ressaltar que, em tempo de guerra, forças inimigas tentarão bloquear o comércio marítimo para causar danos materiais devido à interrupção de suprimentos. Tal ato visa submeter o país à sua vontade, obtendo acordos comerciais favoráveis, por exemplo. Assim sendo, o tráfego mercante não é algo inocente que possa ser ignorado do ponto de vista da defesa nacional. É, pois, imprescindível uma estratégia nacional envolvendo forças armadas e transporte marítimo.

Antes de entrar em ideias mais detalhadas sobre o uso de energia nuclear para propulsão de navios mercantes, é fundamental investigar experiências passadas. Seus sucessos, suas falhas e dificuldades precisam ser compreendidas antes de propor soluções. Neste trabalho, quatro navios construídos para navegação em águas quentes foram escolhidos para revisão bibliográfica (NS Savannah, NS Otto Hahn, NS Mutsu, NS Sevmorput), excluindo os navios quebra-gelo porque eles são uma aplicação muito específica e sua história pode não ter muitas lições aplicáveis aos navios mercantes típicos.

Recentemente, o professor Adrian Bejan propôs a lei construtal, que afirma que na natureza, todos os sistemas evoluem de maneira a melhorar os fluxos [21]. Tal lei é aplicável a vários domínios, incluindo desde sistemas físicos, tais como bacias hidrográficas, até sistemas de informação, passando por seres vivos. Tal lei identifica o sentido geral da evolução das espécies, que é facilitar o acesso aos fluxos que os organismos precisam para sobreviver. No âmbito deste trabalho, a lei construtal será a base para a tomada de decisão, sendo que todo elemento do método a ser proposto deverá facilitar o fluxo de informação.

Voltando ao tópico da engenharia de sistemas, a proposta deste trabalho é focar no pensamento sistêmico, que é essencialmente pensar problemas antes de pensar em soluções. Cada problema é visto como uma caixa preta, à qual são impostas funções e restrições. Somente após a determinação completa do problema é que uma solução poderá ser buscada. Dentro deste espírito, serão identificados os nichos nos quais a energia nuclear pode oferecer vantagens superiores às outras opções energéticas. Tal trabalho será uma maneira de demonstrar a efetividade do método de engenharia de sistemas proposto.

1.2 Relevância e contribuição original do trabalho

A limitação desses processos é que eles são evoluções de métodos anteriores e são destinados a vender a clientes que já tem uma certa estrutura de trabalho. Tais soluções não pensam a relação de poder entre as pessoas. Elas facilitam o trabalho e são bem-sucedidas comercialmente. Mas são soluções parciais e obtidas por tentativa e erro. Tais soluções são desenvolvidas a partir da experiência de muitos anos de prática de alguns engenheiros.

Esse trabalho é ortogonal a essas ferramentas, podendo ser empregado com qualquer tipo de processo, baseado em modelo ou em documentos. Ele foca em restrições sobre as pessoas, desenvolvidos a partir de um modelo físico (lei construtal). Tais restrições ao mesmo tempo funcionam como um protocolo de comunicação e como uma ferramenta de raciocínio.

A originalidade do trabalho está em buscar na física as diretrizes para a concepção de um processo de desenvolvimento de sistemas cibernéticos complexos. Outro ponto de originalidade está na apresentação de uma arquitetura de uma usina nuclear móvel. Os possíveis usos seriam para propulsão de navios, para dessalinização e para produção de energia elétrica.

A relevância deste trabalho está na redução do custo e do risco de projetos cuja importância econômica vem aumentando progressivamente. Quanto à usina nuclear móvel, sua relevância fica evidente pela importância estratégica de seus possíveis clientes. O comércio marítimo transporta cerca de 95% dos produtos. A agricultura, devido ao aumento populacional e aumento da demanda, deverá requerer cada vez mais água doce. Devido às mudanças climáticas, parte da água de irrigação terá que ser obtida por dessalinização da água do mar. Pequenas ilhas precisam de geradores geralmente movidos a motores diesel, que poderiam ser substituídos por uma usina nuclear móvel. Em caso de guerra, usinas nucleares móveis podem restabelecer o fornecimento de energia elétrica para indústrias ou serviços vitais.

Os combustíveis fósseis são finitos e oriundos de países politicamente instáveis. Logo, o uso de energia nuclear para tais funções (agricultura, transporte marítimo e fornecimento de energia) pode proporcionar segurança energética. Além disso, as mudanças climáticas imporão novos desafios à humanidade, que podem ser suavizados por meio do

uso racional da energia nuclear. A energia nuclear é compacta, permitindo a formação de estoques de longo prazo, requer pequenas superfícies de terreno e é independente do clima. Tais características tornam a energia nuclear uma candidata para o emprego em uma grande gama de aplicações.

1.3 Objetivos da pesquisa

Realizada a introdução contextual do tema e apresentadas a relevância e a contribuição original da tese, definem-se, então, os objetivos que orientaram o presente trabalho.

1.3.1 Objetivo geral

Orientado pela lei construtal, desenvolver um método de desenvolvimento de sistemas cibernéticos complexos cujas funções sejam conhecidas.

1.3.2 Objetivo específico

Empregando o método desenvolvido, tentar conceber uma usina nuclear móvel comercialmente viável que atenda um mercado amplo.

1.4 Estrutura da tese

Esta tese está organizada em seis capítulos. Neste capítulo é realizada a introdução do trabalho contextualizando o tema da pesquisa, apresentando a relevância e a contribuição original do trabalho e definindo os seus objetivos.

No Capítulo 2 é realizada uma revisão da literatura relacionada ao tema da pesquisa. Primeiro é abordado o estado da arte dos métodos de engenharia de sistemas, citando as ferramentas comerciais mais conhecidas e os conceitos fundamentais. Depois, é feita uma revisão da experiência com navios mercantes nucleares.

A metodologia empregada para que os objetivos propostos fossem atingidos é desenvolvida no Capítulo 3. Inicialmente é apresentado o delineamento do trabalho. Na seção seguinte é realizado um embasamento teórico acerca dos conceitos oriundos da lei construtal. Em seguida, essa tese define um conjunto de conceitos fundamentais de

engenharia de sistemas que são usados na definição do método proposto. Finalmente, um exemplo simples mostra como tal método funciona.

O Capítulo 4 apresenta o desenvolvimento de especificações de sistema em vários níveis de decomposição do produto, partindo de uma empresa nuclear. O Capítulo 5 apresenta algumas soluções técnicas para atender as especificações desenvolvidas.

O Capítulo 6 faz a discussão das limitações do método e das soluções institucionais ou técnicas propostas. São também feitas comparações com os métodos existentes.

Por fim, no Capítulo 7 são apresentadas as conclusões finais do trabalho, as limitações verificadas no desenvolvimento do modelo e as recomendações para futuros desenvolvimentos.

2 REVISÃO DA LITERATURA

Este capítulo tem por finalidade apresentar o resultado de uma ampla pesquisa realizada na literatura sobre engenharia de sistemas e navios nucleares mercantes.

2.1 Bases fundamentais da engenharia de sistemas e histórico

A engenharia de sistemas é um campo interdisciplinar da engenharia com foco na maneira de gerenciar e projetar sistemas complexos ao longo de todo o seu ciclo de vida [22]. Questões como logística, coordenação de diferentes equipes e automação se tornam exponencialmente mais difíceis com o aumento da complexidade. A engenharia de sistemas lida então com métodos de trabalho e ferramentas para gerenciar riscos e envolve disciplinas tanto técnicas quanto centradas no ser humano, como engenharia de controle, engenharia industrial, estudo de organizações e gerenciamento de projeto.

O termo engenharia de sistemas pode ser encontrado já na década de 1940, nos laboratórios Bell Telephone [23]. A necessidade de identificar e gerenciar as propriedades de um sistema como um todo, o que em projetos complexos pode apresentar uma grande diferença com relação à soma das partes, motivaram o departamento de defesa dos Estados Unidos e a NASA a empregar a engenharia de sistemas [24].

A engenharia de sistemas prega o uso de ferramentas e métodos para compreender e gerenciar a complexidade de sistemas, tais como modelagem, simulação, arquitetura de sistemas, otimização, dinâmica de sistemas, análise de sistemas, análise estatística, análise de confiabilidade e tomada de decisão [25].

Para dominar a complexidade e dividir as tarefas para cada pessoa ou equipe, o sistema global precisa ser dividido em partes menores, denominadas subsistemas [22]. Assim, é possível desenvolver em paralelo as diversas partes e chegar à conclusão do projeto dentro de um prazo menor do que se houvesse um desenvolvimento em série. Além disso, é possível agrupar famílias de competências dentro de cada subsistema, reduzindo a necessidade de um elevado número de competências diferentes dentro de cada módulo, o que reduz a quantidade de pessoal necessária para levar a cabo o projeto.

Wymore produziu uma formulação formal do que é um sistema e do problema de seu projeto [1]. Um sistema é uma interpretação humana por meio dos sentidos, usando um

modelo mental. Um modelo de um sistema é uma descrição que separa o universo em duas partes, interior e exterior. Do exterior, o sistema recebe fluxos por meio de canais chamados de entradas. Do interior para o exterior ocorrem fluxos por meio de canais chamados de saídas. A parte interna de um sistema é descrita inicialmente por meio de estados [1].

O gerenciamento de projetos possui uma norma chamada PMBOK [26] que estabelece os conceitos fundamentais para o gerenciamento bem-sucedido de projetos. O PMBOK, por outro lado, não é uma metodologia por não definir como fazer, apenas estabelece requisitos de alto nível do que fazer. O detalhamento fica a cargo da instituição usuária.

2.2 Revisão dos métodos de engenharia de sistemas

O projeto de sistemas complexos geralmente usa processos de ciclos de vida para balizar a concepção, o projeto detalhado, a construção, a operação e o descarte. Os processos mais usuais são: cascata, espiral e “Ve”. Existem também processos de aquisição de sistemas complexos, tais como o da NASA [22] e do Departamento de Defesa dos Estados Unidos [27]. O processo da NASA divide o ciclo de vida em fases numeradas por letras: A (concepção), B (projeto básico), C (projeto detalhado), D (construção), E (operação) e F (descarte). O processo de aquisição do Departamento de Defesa é similar, mas usa letras para indicar eventos e não fases.

Os processos de desenvolvimento podem ser baseados em documentos ou em modelos [28]. Em um processo baseado em documentos, cada participante executa suas tarefas e comunica os resultados de seu trabalho por meio de documentos. A informação total fica na mente de cada participante, sendo que cada documento é uma faceta desse conjunto de informações. Por exemplo, um arquiteto pode fazer um documento para mostrar as características de sua solução, outro para mostrar os cálculos, outro para dar detalhes das interfaces e outro para descrever o modo de operação.

Evidentemente, os dados de saída de um participante servirão de entrada para outro. À medida que o projeto evolui e os dados mudam, garantir a consistência entre cada documento se torna um problema. Para isso, são necessárias reuniões entre os participantes para certificar de que os dados de interface estejam consistentes.

Em um processo baseado em modelos, existe um ambiente digital no qual os participantes inserem seu trabalho usando uma linguagem específica, tal como UML ou SysML. Nesse ambiente, mudanças em um trabalho gerarão avisos imediatos a todos os envolvidos. A replicação de dados é cuidadosamente evitada, criando um banco de dados único a partir do qual a documentação é gerada de maneira automática. A consistência entre documentos é assim assegurada por projeto. Documentos em linguagem comum precisam ser gerados para lidar com o público externo, que geralmente não é treinado na linguagem empregada no ambiente de desenvolvimento.

Processos baseados em modelos podem alcançar uma produtividade elevada, mas requerem uma equipe treinada em uma linguagem incomum nos dias de hoje. Existem vários fornecedores de soluções que integram um ambiente de desenvolvimento, um processo, métodos e ferramentas.

A IBM fornece o ambiente Rhapsody e o processo Telelogic Harmony-SE, que é baseado no clássico modelo em V [29], que é derivado do processo de desenvolvimento de software Harmony®.

A IBM também tem outro método, chamado Processo Unificado Racional para engenharia de sistemas (Rational Unified Process for Systems Engineering -RUP SE). É a extensão do Processo Unificado Racional (Rational Unified Process -RUP) para suporte de desenvolvimento de sistemas baseados em modelos [30]. Seus elementos principais são: papéis (“quem?”), produtos (“o que?”) e tarefas (“como?”). Um papel define um conjunto de competências, habilidades e responsabilidades. Produtos representam resultados de uma tarefa, incluindo documentos e modelos produzidos. Uma tarefa descreve uma unidade de trabalho alocada a um papel que produz um resultado. Nesse método, um projeto tem quatro fases: Concepção, Elaboração, Construção e Transição.

A engenharia de sistemas orientada a objetos – OOSE – é baseada em técnicas de software, sendo uma mistura de orientação a objetos e métodos de engenharia de sistemas [7]. Introduz novas técnicas, como análise causal e modelo de negócio. Adota desenvolvimento integrado de produtos e um modelo de ciclo de vida em V com recursão a cada nível hierárquico [28].

A empresa Vitech Corporation oferece uma metodologia de engenharia de sistemas baseada em modelos [31]. Essa metodologia define uma linguagem gráfica para modelar e definir sistemas. Essa metodologia baseia-se em quatro atividades concorrentes que são ligadas e gerenciadas em um repositório compartilhado. As quatro atividades são: análise de requisitos básicos; análise funcional e comportamental; síntese e arquitetura; e validação e verificação do projeto. Essa metodologia adota um modelo de casca de cebola, trabalhando completamente cada camada antes de entrar na próxima camada para reduzir riscos de projeto [31]. Nesse método, três modelos são necessários e suficientes para especificar completamente um sistema: modelo de controle (comportamento funcional), modelo de interfaces, e modelo de arquitetura física.

Ingham e aliados apresentam uma metodologia para engenharia de sistemas espaciais embarcados chamada de análise de estados [5]. O laboratório de propulsão de jatos (jet propulsion laboratory - JPL) desenvolveu essa metodologia, que nivela o modelo e arquitetura de controle baseada em estados. Estado é definido como “representação instantânea da condição de um sistema dinâmico”. Modelos descrevem como estados evoluem no tempo.

Wasson fornece um método que primeiro identifica as partes da vida útil de um sistema [3]. Para cada parte da vida de um sistema, modos de operação são definidos de acordo com objetivos genéricos. Dentro de cada modo de operação existem estados operacionais que são conjuntos de objetivos específicos que ocorrem simultaneamente. Dentro de cada estado operacional existem estados de configuração física, que são as possíveis combinações de atividade ou inatividade dos componentes, criadas para atender os objetivos. Assim, os objetivos globais do cliente serão transformados em comportamento do sistema de maneira formal e exaustiva. Blanchard introduz engenharia e análise de sistemas em seu livro. Ele mostra conceitos, metodologias, modelos e ferramentas necessários à análise e implementação de um levando em conta todo o ciclo de vida [25].

A limitação desses processos é que eles são evoluções de métodos anteriores e são destinados a vender a clientes que já tem uma certa estrutura de trabalho. Tais soluções não pensam a relação de poder entre as pessoas. Elas facilitam o trabalho e são bem-sucedidas comercialmente. Mas são soluções parciais e obtidas por tentativa e erro. Tais soluções são desenvolvidas a partir da experiência de muitos anos de prática de alguns engenheiros.

Esse trabalho é ortogonal a essas ferramentas, podendo ser empregado com qualquer tipo de processo, baseado em modelo ou em documentos. Ele foca em restrições sobre as pessoas, desenvolvidos a partir de um modelo físico (lei construtal). Tais restrições ao mesmo tempo funcionam como um protocolo de comunicação e como uma ferramenta de raciocínio.

2.3 Revisão dos navios mercantes nucleares

Foi feito um levantamento inicial sobre os navios mercantes nucleares já construídos. Esse levantamento deu origem a um artigo [15], que faz uma revisão bibliográfica sobre a experiência com navios mercantes nucleares do passado. Existem agora novas regras contra a emissão de gases poluentes, tais como CO₂, SO_x e NO_x. Novas opções, menos poluentes, para obter energia para propulsão naval precisam ser estudadas. Uma potencial fonte de que não emite grandes quantidades de gases poluentes é a energia nuclear. Reatores do tipo PWR já foram postos à prova no mar com sucesso. Esse trabalho traz alguma informação sobre a história e arquiteturas desses projetos. O NS Savannah foi o primeiro deles, sendo feito pelo governo dos Estados Unidos. A Figura 3 mostra o arranjo do NS Savannah.

O navio NS Savannah foi aceito em 1962 e foi construído por ordem do então presidente dos Estados Unidos dentro do programa “Atoms for Peace”. O conceito era demonstrar boa vontade e não ser economicamente viável. A administração marítima queria um laboratório para estudar o projeto, operação e tripulação de um navio nuclear e não o lucro.

O navio atingiu os objetivos de projeto e a operação de um reator naval com urânio de baixo enriquecimento foi um sucesso. O reator respondia mais rápido do que uma planta convencional (duas a quatro vezes mais rápido). Gastou 90 milhões e ganhou 12 milhões em 5 anos de operação.

Figura 3 – Arranjo do NS Savannah

Fonte: [15]

A Tabela 1 apresenta os principais dados sobre o sistema primário do NS Savannah.

O NS Savannah foi abandonado em 1971 por problemas de viabilidade econômica, confiabilidade dos sistemas e disputas salariais entre os condutores da planta nuclear e dos oficiais de convés. Foi um navio considerado muito importante para a aceitação pública da energia nuclear, até então restrita às armas e navios de guerra.

Era um navio de 21800 toneladas de deslocamento, com capacidade de 10000 toneladas e 60 passageiros. A linha de eixo tinha uma potência de 16MW. Foi luxuosamente decorado por Jack Heaney, com um piso exclusivo para os passageiros decorados com pinturas e esculturas de artistas norte-americanos.

Tabela 1 – Dados do sistema de refrigeração do primário do NS Savannah

Parâmetros do sistema de resfriamento do reator	Valor	Unidade
Pressão	120,7	Bar
Temperatura média	264	°C
Vazão	1009	Litro/s
Potência térmica	70	MW
Diâmetro dos tubos dos Geradores de vapor	1,905	cm
Vazão de vapor	32,76	Kg/s
Pressão de vapor na potência nominal	31,72	Bar
Pressão de vapor sem carga	50,33	Bar
Diâmetro das pernas do circuito primário	31,8	cm
Subresfriamento na perna quente	37,8	°C
Vazão normal de purificação	1,26	Litro/s
Vazão máxima de purificação	3,79	Litro/s
Vida útil da resina de purificação	50	Dias

Fonte: [15]

Diferentemente dos outros reatores usados pela marinha americana, o NS Savannah usava urânio comercial de baixo enriquecimento e um projeto completamente civil, executado pela Westinghouse. A Tabela 2 mostra os principais dados sobre o núcleo do reator.

Tabela 2 – Dados do núcleo do reator do NS Savannah

Parâmetros do núcleo do reator	Valor	Unidade
Altura do núcleo	1,68	m
Diâmetro do núcleo	1,57	m
Diâmetro das varetas	1,00	cm
Enriquecimento do combustível (UO ₂)	4,4	%
Largura dos elementos de controle	20	cm
Espessura dos elementos de controle	1,00	cm
Comprimento dos elementos de controle	1,68	m

Fonte: [15]

O reator nuclear era protegido por uma barreira de contenção de 10,67m de diâmetro e 15,24m de comprimento, com terminações esféricas. Era constituída de aço carbono de até 10cm de espessura e era projetada para resistir até a 12,8 bar absolutos em caso de acidentes de perda de refrigerante. Tinha uma escotilha de 4,3m de diâmetro no topo para efetuar a recarga de combustível e quatro escotilhas para acesso de pessoal, sendo duas na parte de cima e duas na parte de baixo. A 30,5 m de profundidade as escotilhas de baixo se romperiam para evitar o colapso da contenção em caso de afundamento do navio. Após meia hora do desligamento, a radiação dentro da contenção ficava abaixo de 200 milirem por hora.

A metade de baixo da contenção ficava apoiada em uma estrutura de aço cercada por uma parede de concreto de 1,22m. A metade de cima da contenção era revestida por uma camada de chumbo de 15,2cm e outra camada de 15,2cm de polietileno. Adicionalmente, ambos os lados da contenção eram protegidos por camadas alternadas de madeira e aço, em um total de 61 cm de escudo de colisão. Assim, considerava-se o navio seguro contra abalroamentos e pouso no fundo.

Havia recursos para acumular rejeitos radioativos por 100 dias. O treinamento para a tripulação consistia de 31 semanas de teoria, 30 semanas de prática em campo, 4 partidas e 4 paradas de reator [31].

A Figura 4 apresenta a vista superior da contenção. Os números têm os seguintes significados: 1 – Feixe de tubos em U do gerador de vapor; 2 – Refrigerador da sangria do sistema de purificação; 3 – Tambor do gerador de vapor; 4 – Tanque de condensação dos efluentes das válvulas de alívio; 5 – Tanque de drenos da contenção; 6 – Pressurizador; 7 – válvula de retenção; 8 – Bombas do refrigerante do primário; 9 – Válvulas de isolamento.

Figura 4 – Visão superior da contenção nuclear do NS Savannah.

Fonte: [15]

O segundo navio estudado foi o transportador de minério alemão Otto Hahn, que foi encomendado em 1962 pela empresa GKSS. Depois de 10 anos de operação, o reator foi descomissionado e substituído por motores diesel.

Seu reator era do tipo integrado e auto pressurizado. A pressão do primário era a pressão de saturação relativa à temperatura da perna quente. Os três geradores de vapor eram do um só passe, helicoidal e contracorrente. Seus tubos eram compostos pela liga NiCr16Fe8. Sua potência térmica nominal era 38MWth. Seu Segundo núcleo operou com os seguintes parâmetros: temperatura de saída do núcleo de 269°C; temperatura de entrada do núcleo de 258°C; vazão mássica de 653 kg/s; pressão do vapor secundário de 3MPa; vazão mássica no secundário de 17,78 kg/s; temperatura de saída do vapor de 267°C (33°C de superaquecimento); e temperatura da água de alimentação de 185°C. A Figura 5 mostra a arquitetura do reator do NS Otto Hahn.

Figura 5 – Arquitetura do reator do NS Otto Hahn

Fonte: [15]

O terceiro navio estudado foi o NS Mutsu. O instituto de pesquisa em energia atômica do Japão gerenciou a construção de um protótipo de navio comercial para transporte de cargas especiais e treinamento da tripulação. A Figura 6 apresenta o arranjo geral desse navio.

Figura 6 – Arranjo geral do NS Mutsu

Fonte: [15]

A potência térmica nominal do reator do NS Mutsu era 36MW. Havia 32 elementos combustíveis. Os 12 elementos internos eram enriquecidos em ^{235}U a 3,24% e os 20 elementos externos eram enriquecidos a 4,44%. A Figura 7 mostra o núcleo do NS Mutsu.

Figura 7 – Vista superior do núcleo do reator do NS Mutsu

Fonte: [15]

O circuito primário do NS Mutsu tinha dois loops com uma bomba de circulação cada um. Possuía sistemas de injeção de segurança, tal como previsto por normas internacionais. A Figura 8 mostra o fluxograma simplificado do NS Mutsu.

Figura 8 – Fluxograma de processo do NS Mutsu. 1 – Vaso do reator; 2 – geradores de vapor; 3 – Pressurizador; 4 – trocador de calor regenerativo; 5 – trocadores de calor residual; 6 – bombas de remoção de calor residual; 7 – bombas de circulação de refrigerante; 8 – leitos de resina; 9 – tanque de compensação; 10 – bombas de injeção; 11 – turbina; 12 – condensador; 13 – bombas de extração do condensado; 14 – ejetor de ar; 15 – aquecedor de baixa pressão; 16 – desaerador; 17 – bombas de alimentação principal; 18 – bombas de alimentação auxiliar; 19 – aquecedor de alta pressão; 20 – desvio de vapor

Fonte: [15]

Esse navio foi completado em 1972, mas quando foi realizar testes de mar, os pescadores locais bloquearam o porto por medo da radiação. Após obter um acordo, quando o reator começou a operar em potência, houve vazamento de radiação através da blindagem.

Esse fato, junto com o erro da mídia local reportar vazamento de radionuclídeos ou radioatividade, gerou muita resistência popular contra o projeto. Foram feitas modificações

na blindagem que ficaram prontas em 1982. O problema de vazamento de radiação foi resolvido. Após um conjunto de testes, o navio foi descomissionado em 1992. A Figura 9 mostra as mudanças feitas na blindagem primária e secundária do NS Mutsu.

Figura 9 – Mudanças feitas no NS Mutsu

Fonte: [15]

O quarto navio estudado foi o NS Sevmorput. A união soviética já tinha uma tradição em reatores para navios quebra gelo, que foram essenciais para abastecer a população pela rota do mar do Norte. O primeiro reator foi o OK-150 de 90MW térmicos, empregado no NS Lenin, que era um quebra-gelo.

O NS Sevmorput empregou reatores de terceira geração, o KLT-40, e entrou em operação em 1988. Apesar de um histórico impecável, várias autoridades portuárias proibiram seu acesso devido ao medo pós Chernobyl. A Tabela 3 apresenta alguns dados do núcleo.

Tabela 3 – Dados do núcleo do NS Sevmorput

Parâmetro	Valor
Potência térmica nominal	135 MWth
Altura do núcleo ativo	1 m
Diâmetro do núcleo	1,21 m
Massa de U-235 no núcleo	150,7 kg
Enriquecimento	90%
No. de elementos combustíveis	241
Arranjo das varetas	Triangular
Espaçamento entre elementos	72 mm
No. de varetas por elemento	53
Espaçamento entre varetas	7,2 mm
Diâmetro das varetas	5,8 mm
Encamisamento	Zr-alloy
Combustível	U-Zr-alloy

Fonte: [15]

O KLT-40 tem quatro loops, cada um com uma bomba e gerador de vapor. Um arranjo de tubo dentro de tubo foi adotado, reduzindo a probabilidade de acidentes de perda de refrigerante. Vale notar que a pressurização do circuito primário é feita por ar comprimido. A Figura 10 mostra uma vista em corte do KLT-40.

Figura 10 – Seção reta do reator KLT-40.

Fonte: [15]

A Figura 11 apresenta uma vista esquemática do sistema de resfriamento do reator KLT-40. Junto com a Figura 10, ela permite entender como o fluido primário flui da saída do núcleo para os geradores de vapor pelo tubo interno. Depois o fluido primário retorna ao vaso do reator pelo tubo externo. Subdivisões dentro do vaso do reator conduzem o fluido à entrada da bomba pelo tubo externo. Após passar pela bomba, o fluido retorna à câmara descendente pelo tubo interno.

Figura 11 – Sistema de resfriamento do reator KLT-40

Fonte: [15]

Uma análise foi feita sobre as razões para o sucesso ou falha de cada projeto. Foi observado que é fundamental manter os aspectos econômicos no centro do projeto. A experiência mostra que, exceto imediatamente após acidentes catastróficos, a confiança do público pode ser obtida por meio do diálogo aberto e boas práticas de engenharia.

3 METODOLOGIA

Este capítulo apresenta os métodos empregados para que os objetivos propostos para esse trabalho fossem atingidos.

3.1 Delineamento da pesquisa

Esse trabalho é inteiramente conceitual e não envolve experimentos. Partindo de uma lei física mais geral (lei construtal [21]), uma extrapolação é feita para processos mentais. Para facilitar os fluxos de informação, essa tese define conceitos estendendo a engenharia de sistemas e demonstra a utilidade da aplicação de tais conceitos em um projeto. Tal aplicação leva a uma série de requisitos a serem considerados durante o projeto de sistemas, requisitos esses que são justificados à luz da lei construtal. Esta tese aplica esses requisitos a uma pessoa de uma equipe de projeto e propõe um método de desenvolvimento de sistemas.

Posteriormente, esta tese aplica o método a um país genérico e identificando suas funções, necessidades e riscos. Em seguida, esta tese desenvolve uma solução institucional para uma parte de seus problemas, que é o fornecimento de energia a lugares remotos, navios mercantes ou em estados de exceção. Sempre usando o método, esta tese desenvolve sistemas em vários níveis da decomposição do produto, chegando até um sistema de resfriamento do reator.

Tal desenvolvimento será feito em nível de projeto conceitual, fazendo apenas cálculos em regime permanente. Será levada em conta a norma ANSI/ANS51.1 (ANSI/ANS, 1988) na definição da arquitetura e das funções de segurança. Também será feita a restrição de trabalhar somente com materiais e componentes de prateleira.

3.2 Embasamento teórico

No campo da física e da biologia, Bejan propôs a lei construtal. Essa lei afirma que um sistema de fluxos evolui no sentido de facilitar os fluxos que ele precisa para sobreviver e persistir no tempo [21]. A lei construtal expande as ciências térmicas (leis termodinâmicas e transferência de calor) incluindo um modelo de projeto natural [21]. A seguir, esta tese lança mão de uma série de hipóteses, identificadas a seguir.

Hipótese 1: Um dos principais fluxos institucionais é informação [33].

Este trabalho assume que instituições também evoluem de acordo com a lei construtal, mesmo sendo entidades mentais. Instituições que evoluem no sentido de facilitar o fluxo de informação crescem e se tornam poderosas. Instituições que restrinjam o fluxo de informação tendem a desaparecer no tempo. Assim, um modelo objetivo para prever o futuro de qualquer instituição é definido.

Neste trabalho, informação são dados necessários à tomada de decisões. Por exemplo, ordens e relatórios são tipos de informação tipicamente trocadas dentro de instituições. A transmissão de informação requer um protocolo comum ao emissor e ao receptor (linguagem) e um meio físico, como papel ou internet. O fluxo de informação é essencial para que as pessoas ajam de acordo com as necessidades de outrem, produzindo trabalho.

Hipótese 2: Um canal precisa de três funções para assegurar a passagem de fluxos: facilitar escoamento, reduzir contaminação e preservar integridade [33].

Para que fluxos possam ocorrer, existe a necessidade de canais. Canal neste trabalho é uma abstração da realidade. É um caminho para um fluxo qualquer, seja um fluido, calor, eletricidade, tensão mecânica ou informação. A primeira função de um canal é facilitar o escoamento. Essa é a razão pela qual tubos, artérias, traqueias e caules tem a forma circular, pois trata-se da melhor relação de superfície sobre perímetro, reduzindo a perda de carga.

A segunda função de um canal é reduzir a contaminação. Em outras palavras, evitar a entrada de outros materiais que não o de interesse para o fluxo em questão. Assim, o volume livre para o fluxo em questão é assegurado, evitando o bloqueio. Outros materiais são contaminantes e podem entupir ou dificultar o fluxo. Na natureza, essa função é feita por uma barreira física, como em traqueias. Em outros canais, tal função é feita por uma combinação de forças naturais, como a gravidade e as propriedades físicas do solo que mantém as partículas de terra fixas no leito de um rio. Tal combinação de forças impede que a terra seja carregada com a água, bloqueando o rio. Em uma artéria, a pressão interna realiza essa função, assegurando o volume interno livre.

A terceira função é preservar a integridade do fluxo. Se uma parte do fluxo for perdida no caminho, a destinação começa a receber menos fluxo. Se a destinação não receber o fluxo necessário, ela define e pode até deixar de existir. Em animais, um exemplo disso é a perda de sangue. Essa função pode ser feita por uma entidade física ou por uma conjunção de forças naturais. Em uma mangueira, o material à prova d'água faz essa função. Em condutores elétricos, a ausência de um meio condutor evita a perda de carga elétrica. A Figura 12 apresenta uma representação gráfica de um canal.

Figura 12 – Análise funcional de um canal

Fluxos mentais, tais como crédito e informação, também necessitam de um canal de transmissão. Tal espaço pode ser criado por meio de disciplina mental criada por meio de regras sociais. Um conjunto coerente de regras sociais sendo aplicadas em paralelo pode ser chamado de instituição. Instituições são orientadas a objetivos comuns aos membros do grupo e tais objetivos levam à cooperação em um sentido genérico. A cooperação permite a soma com sinergia dos esforços individuais, produzindo trabalho, que é a transformação do mundo em algo melhor.

Por outro lado, informações (por exemplo, planos, projetos, ordens) são necessárias para a realização de trabalho cooperativo. As pessoas precisam saber o que é esperado delas para que possam agir corretamente.

Fazendo uma analogia entre canais físicos e mentais, pode ser afirmado que as instituições precisam construir canais para que a informação flua na direção necessária. A analogia consiste em afirmar que as mesmas três funções dos canais físicos precisam ser realizadas para que o canal mental funcione.

Para facilitar o fluxo de dados, um canal de informação precisa reduzir o tempo e a energia gasta para comunicar uma ideia. Em um texto escrito, isso significa reduzir tempo e esforço cerebral do leitor para entender um texto. Parte da solução é usar sentenças concisas, simples e com vocabulário trivial.

Para evitar a contaminação de um canal de dados com informações falsas ou irrelevantes (ruído), filtros precisam ser empregados. Somente dados de interesse devem ser inseridos no canal. Informações adicionais, auto expressão ou ideias sem fundamento empírico devem ser eliminadas para não induzir as pessoas a perderem o foco nos aspectos relevantes.

Para preservar a integridade da informação, uma solução é impor protocolos, que precisam ser conhecidos tanto pelo transmissor como pelo receptor. Protocolos ajudam a manter a integridade dos dados, contribuindo para que o receptor receba toda a informação necessária para agir.

A Tabela 4 mostra a analogia entre as funções de um canal físico e um canal de informação.

Tabela 4 – Analogia entre as funções de um canal físico e um canal de informação

Canal físico	Canal de informação
Facilitar escoamento	Facilitar comunicação
Reduzir contaminações	Reduzir ruído
Preservar integridade	Preservar integridade

Esta hipótese é usada na própria definição dos axiomas da seção 3.2 e nos requisitos do anexo 1.

Hipótese 3: A maximização dos fluxos ocorrerá no ponto de menor custo esperado na curva custo total versus investimento em segurança.

Este trabalho também lança mão de uma hipótese, também baseada na lei construtal, de que o aumento da segurança tem um custo, bem como a falta de segurança incorre em custos devidos aos acidentes. Existe um ponto ótimo onde o investimento em segurança torna a solução mais eficiente, tal como mostrado na Figura 13. De acordo com a lei construtal, o objetivo é atingir ou aproximar desse ponto.

Figura 13 – Dilema da redução do risco

Fonte: adaptado de [34]

Reduzir o ruído e preservar a integridade da informação reduzem riscos a um custo significativo, que se for demasiadamente elevado, tornam o sistema inviável. Então, existe a necessidade de comprovar que as soluções de redução de ruído e preservação da integridade tragam um benefício líquido à equipe de projeto. Tal princípio norteia as justificativas da tabela de requisitos no anexo 1.

Hipótese 4: Necessidade de operar em malha fechada.

Outra hipótese usada neste trabalho é a presença inevitável de ruído na monitoração e perturbações sobre o sistema, o que virtualmente impossibilita a condução do sistema em malha aberta. Isto significa que um sistema deve ser conduzido em malha fechada a partir da medida das variáveis de processo. Nem sempre um sistema comercial tem um controlador que faça um processo em malha fechada, mas sempre haverá interfaces para permitir a entrada de comandos e reportar o estado do sistema. Na prática, a maioria dos sistemas sem um controlador interno operam em malha fechada onde o controlador está fora do sistema, seja um computador ou um operador humano. A referência a ser seguida pelo sistema pode ser um conjunto de regras organizacionais ou até a vontade do operador, tal como ocorre com equipamentos de entretenimento. Grosso modo, pode-se afirmar que a imensa maioria

dos sistemas complexos construídos opera seguindo uma referência para atingir objetivos, pois do contrário eles não seriam comprados.

Esta hipótese justifica a decisão de aplicar a abordagem por estados à pessoa encarregada de um trabalho de engenharia, pois a mesma deve realizar um trabalho de acordo com os objetivos institucionais. Para assegurar que isso ocorra, é necessário ter meios de mensurar e avaliar o trabalho realizado.

Hipótese 5: Ignorância do autor da especificação sobre o estado da arte e melhor capacidade do fornecedor (assimetria de informação).

Tipicamente, a pessoa encarregada de fazer uma especificação de sistema não tem conhecimento razoável acerca das possibilidades atuais das tecnologias mais modernas. Evidentemente, conhecimento total é impossível e nem mesmo fabricantes detém tal nível de conhecimento. Porém, fornecedores lidam com muitos equipamentos similares ao longo de sua vida profissional e detém um conhecimento relativamente preciso das capacidades e limitações de seu produto.

Pessoas encarregadas de encomendar um sistema, por outro lado, tem um conhecimento muito mais superficial, tipicamente como usuários, não como fabricantes. Tais pessoas tendem a ter um conhecimento superficial de muitos tipos de sistemas diferentes, atuando na integração de sistemas boa parte de sua vida. Assim, não é usual que quem escreve especificações tenha conhecimentos profundos sobre as possibilidades e limitações de todo tipo de produto.

Hipótese 6: Especificações inviáveis representam um perigo.

Caso uma dada especificação contenha requisitos que tornem inviável achar um produto que a satisfaça, o projeto será atrasado até que a especificação seja revista. A redação da especificação, a leitura da especificação e a redação de uma proposta requerem muito trabalho. Tal trabalho implica que a descoberta de inviabilidade requer tempo, bem como a revisão da especificação. Considerando que um projeto mobiliza muita gente, atrasos costumam causar prejuízos, sendo um perigo à sobrevivência de uma equipe de projeto. Essa hipótese é empregada na definição de alguns requisitos do anexo 1.

Hipótese 7: Separação formal entre necessidades e soluções técnicas.

Esta hipótese advém da organização industrial típica de empresas ou instituições que realizam sistemas complexos, pois elas tipicamente fazem especificações de subsistemas e compram de outras empresas especializadas. Devido à hipótese 5, identifica-se a necessidade de expressar necessidades e somente necessidades, sem as poluir com opiniões (acerca da melhor solução técnica) de indivíduos sem qualificação técnica.

As necessidades a serem satisfeitas por um sistema devem ser enunciadas em uma especificação, que traz somente informação sobre os objetivos do sistema, ou o problema a ser resolvido. Por outro lado, soluções técnicas são descrições de arquiteturas físicas, tecnologias, desempenhos, propriedades e comportamentos relativos a um produto.

Essa separação implica que especificações não devem fazer qualquer menção à arquitetura, preservando a liberdade do projeto e permitindo a inovação. Adicionalmente, tal separação reduz os riscos de projeto por inibir a adoção de soluções técnicas por gente sem capacitação para tal ou antes de completar a especificação.

Em engenharia de sistemas, a palavra sistema está associada a uma divisão do mundo criada para definir um problema. Por outro lado, o objeto físico (construído para resolver o problema definido por um sistema e seus requisitos) é denominado solução tecnológica ou simplesmente produto. A Figura 14 ilustra o conceito de separação formal entre problema e solução. Idealmente, o produto deve atender a todas as necessidades associadas ao sistema.

Figura 14 – Conceito de separação formal entre problema e solução

3.3 Desenvolvimento da metodologia

Na engenharia de sistemas, um sistema é idealizado para realizar funções (de serviço) e precisa receber serviços do exterior. Assim sendo, esta tese propõe a seguinte definição de sistema (Figura 15): um sistema é a divisão do universo em duas partes (interior e exterior), sendo que o interior realiza funções de serviço para exterior e precisa receber serviços do mesmo. Além de realizar as funções de serviço, um sistema deve abster de causar inconvenientes além de certos limites, definidos em requisitos não-funcionais. Assim, todo sistema tem um conjunto de requisitos não funcionais que restringem as propriedades dos produtos que possam vir a ser adotados como solução. Propriedades são substantivos relacionados a grandezas físicas com unidades. Exemplos de propriedade são massa (Kg), volume (m³), preço (\$), dimensões (m).

Figura 15 – Modelo de Sistema

A realização de uma dada função de um sistema para outro requer um número igual ou superior a um de interfaces. Esta tese propõe a seguinte definição de interface: “Interfaces são superfícies de contato (materiais ou não) entre sistemas que permitem a transferência de massa, energia e informação de um sistema a outro. Interfaces tem um conjunto igual ou maior do que 0 de propriedades, um conjunto igual ou maior do que um de funções, um sistema responsável e um sistema coadjuvante”. Interfaces podem ser criadas de maneira intencional para cumprir um fim, tal como um flange, um conector elétrico ou transmissão de dados sem fio. Interfaces também podem ser meios de ocorrências postuladas indesejáveis que não podem ser evitadas totalmente. Exemplos são fissuras em vasos de pressão e a propagação de ruídos eletromagnéticos.

Esta tese também define o conceito de status de uma função, já que ao longo da vida de um sistema, suas funções variam de comportamento. “Status de uma função é uma

situação possível de execução com determinado conjunto de desempenhos ou prontidão com determinado tempo de resposta, assumindo a cada momento um único valor dentro de uma lista finita”. Por exemplo, uma função pode estar ativa quando a respectiva ação está ocorrendo com os desempenhos nominais e inativa quando parada sem um prazo determinado para retomar a atividade. Uma função pode também estar em prontidão, o que significa que a sua ação deve iniciar dentro de um prazo determinado. Outro status típico é inibido, empregado quando a ativação da função pode causar acidentes, sendo que a frequência de atuação inadvertida deve ser expressa. Existem também status de desempenho parcial, quando o sistema pode prover apenas parte do desempenho nominal, por exemplo: ativa-50%, ativa-75%. Em um produto concebido para realizar uma dada função “A”, um conjunto de um ou mais sensores tipicamente determina o status da função A. Por exemplo, sensores de tensão (opcionalmente corrente) podem determinar o status de fornecimento de energia a um sistema. Essa definição é a base da definição a seguir.

Acontece que, durante a vida de um sistema, ocorrem combinações específicas de atividade no conjunto de funções recebidas ou realizadas. Ou seja, todo sistema precisa de status distintos e identificáveis de funcionamento, que são decorrentes das necessidades funcionais (do exterior e do interior do sistema) e das leis da física. Esta tese propõe a seguinte definição para a palavra status (para não confundir com o conceito de estado da teoria de controle moderno): “Status de um sistema é uma combinação simultânea dos status de todas as funções trocadas entre o interior e o exterior de um sistema”. Em um modelo relacional, um status de sistema é um registro contendo:

1. Referência ou identificação do sistema em questão;
2. Nome do status; e
3. Lista de status de funções do sistema (de serviço e recebidas).

A Figura 16 apresenta um exemplo de sistema genérico em três status diferentes. Cada status é único no sentido de que, se o mesmo modo de interação ocorre em mais de uma situação, trata-se do mesmo estado sendo empregado. Ou seja, se na tabela de definição de status de um sistema houverem duas linhas com todos os status de funções iguais, existe um erro, já que será impossível distinguir os dois status.

Figura 16 – Conceito de diferentes estados de um Sistema genérico

Cada status está relacionado a um conjunto de casos de uso, que são contextos dentro dos quais o sistema é empregado, do ponto de vista do usuário.

Esta tese também define fase da maneira a seguir: “Fase de um sistema é um evento de mudança de um dado status A para outro dado status B dentro de um período finito e determinado de tempo”. Tipicamente funções internas (feitas pelos subsistemas do sistema, tais como motores, pistões, relés) junto com funções recebidas do exterior (eletricidade, ar comprimido) realizam as fases de um sistema. Para sistemas físicos, as fases têm sempre uma duração considerável, decorrendo a necessidade de usar uma palavra diferente de transição. Transições discretas (duração nula) são usadas em máquinas de estado e redes de Petri. Vale ressaltar que toda fase requer uma combinação de funções internas e externas para ocorrer, o que costuma acarretar problemas de integração na construção de sistemas complexos. Isso ocorre porque as pessoas encarregadas do projeto tendem a não pensar com cuidado em todas as fases do sistema durante o trabalho de engenharia. Problemas típicos são tempos de resposta inadequados, falta de funções (e respectivos atuadores) para realizar fases, falta de recebimento de funções externas, ou mesmo arquiteturas que impeçam a realização de uma dada fase.

O conceito de qualificador de fase também é útil. Uma fase é “ativa” quando o sistema precisa mudar o status de alguma função técnica para que a fase ocorra. Uma fase é “passiva” se o sistema não precisa realizar qualquer ação para que a fase ocorra, dependendo somente da ação dos sistemas externos (função recebida).

Um conceito também introduzido nesta tese é o de relevância de uma função. “Uma dada função de serviço ou recebida é relevante para a determinação do status se ela muda de status durante a operação do sistema e pelo menos uma das condições abaixo for verdadeira:

1 – O custo adicional que esta função cria ao projeto do sistema em termos de dimensionamento ou equipamento é significativo;

2 – O custo esperado causado pelos acidentes devido à sua falha ou atuação inadvertida é significativo”.

Por exemplo, uma função de suporte mecânico tipicamente não precisa de mudanças de estado. Em uma rede elétrica, pequenas cargas podem ser irrelevantes para o dimensionamento da maior parte dos componentes. Por fim, uma chave de alimentação geral pode ter um custo pequeno perto do sistema, não afeta dimensionamento de componentes, mas tem papel importante na segurança. Outro exemplo são as portas, que quando são internas dentro de uma casa, seu status é irrelevante, mas quando existem preocupações de segurança, tipicamente existem meios ou procedimentos para monitorar seu status. Em suma, relevância é definida em relação ao impacto global esperado em termos monetários que uma função deve causar durante o projeto de um produto que atenda à especificação do sistema.

Esse conceito pode ser interessante para remover criteriosamente um conjunto de status de funções da definição do status do sistema. O interesse de retirar funções com relevância abaixo de certo nível é simplificar o modelo comportamental sem incorrer em riscos de projeto consideráveis. Implicitamente, gerentes de projeto precisam definir o que é significativo em termos de impacto monetário e o aumento do limiar significa tolerar mais risco.

Esta tese também define a propriedade de equivalência funcional entre sistemas, a seguir. Um dado sistema A é funcionalmente equivalente ao sistema B se, e somente se, A recebe e fornece as mesmas funções, tem os mesmos status e as mesmas fases do sistema B. Essa propriedade não é comutativa, ou seja, um sistema com mais status e mais fases pode ser equivalente a um sistema mais simples, enquanto o oposto não é verdade. Figura 17 apresenta um exemplo no qual ambos têm os mesmos status (e necessariamente as mesmas funções de serviço e recebidas). O sistema à direita é equivalente ao sistema da esquerda, mas a recíproca não é verdade. Este conceito é importante porque idealmente toda especificação de sistema deve definir o sistema ao qual as soluções candidatas devem ser equivalentes. Outro aspecto é a possibilidade de trocar (a qualquer momento da vida do sistema) a solução de um subsistema com mais facilidade se tivermos conhecimento do subsistema equivalente requerido. Uma especificação que falha em definir os status e fases mínimos de um sistema pode incorrer em dois tipos de risco. O primeiro risco é a falta de

status e fases necessários à operação do sistema de nível superior, o que leva a problemas de integração e retrabalhos custosos. O segundo risco é a pessoa encarregada do projeto do sistema assumir uma postura exageradamente conservadora e incluir mais status e fases do que o necessário. Isto significa mais componentes, serviços recebidos, mais esforço de projeto, menor confiabilidade, mais massa, mais volume, mais custo, mais tempo para terminar o projeto e mais risco.

Figura 17 – Equivalência e não equivalência funcional entre sistemas

É importante também definir o conceito de modo de operação de uma solução tecnológica ou produto, que resultará de uma atividade de projeto. “Modo de operação de produto é uma região do espaço de estados das variáveis internas de um dado produto”. Em um modelo relacional, um modo de operação de um produto é um conjunto de registros contendo:

- 1 – Nome do modo de operação;
- 2 – Referência ao produto;
- 3 – Para cada componente do produto, uma lista dos possíveis modos de operação de do componente dentro do modo de operação do produto;
- 4 – Uma lista de faixas de variáveis de processo, sendo uma faixa para cada variável de processo.

Variáveis de processo são medidas como temperatura, pressão, vazão e outras. Um modo de operação se distingue de um status por se referir a um produto existente descrito em uma descrição de sistema, enquanto status se refere a um problema definido em uma especificação. Enquanto status são baseados em funções, modos são baseados em modos de operação dos componentes e variáveis de processo medidas pela instrumentação. Uma dada combinação de modos dos componentes e de valores das variáveis de processo constitui um estado do produto (um ponto dentro do espaço de estados), também chamado de

configuração física. Um modo constitui uma região do espaço de estados e cada status de um sistema idealmente tem um conjunto não vazio de modos de operação do produto que o materializam. Como o número de estados pode ser astronômico, o projeto deve estudar só estados necessários para atingir os objetivos do sistema (evitando a explosão de estados). Esta tese adota a palavra modo de operação para componentes porque vários autores usam essa nomenclatura [1] [5] [3]. Além disso, é fundamental atender a distinção entre a necessidade e a solução (hipótese 7), distinguindo status (parte do problema) de modo de operação (parte da solução). A Figura 18 apresenta um exemplo gráfico de relação entre status e modos.

Figura 18 – Exemplo de mapeamento dos modos de operação nos status

Todo modo de operação é uma resposta técnica a pelo menos um status do sistema. As variáveis internas de um produto formam um vetor que inclui os modos de operação dos seus componentes e outras variáveis geradas por sensores ou funções de software. Embora modos e status pareçam similares, eles são conceitos radicalmente diferentes porque funções (objetivos abstratos de um sistema) são a base dos status enquanto leituras de variáveis físicas são a base dos modos. A importância dessa definição deriva da separação formal entre necessidades (expressas pelo sistema, suas funções e status) e soluções técnicas (produtos, propriedades e modos). Além disso, os modos de operação são a base para uma série de conceitos úteis para projeto e análise de produtos.

A primeira definição é o conceito equivalente de fase no domínio da solução – procedimento de produto. “Procedimento de produto é a lista de eventos, nos componentes ou em produtos adjacentes, necessários à mudança de um modo de operação a outro em um tempo determinado e finito”.

Enquanto as fases são mudanças de comportamento em entidades imaginárias e abstratas (sistemas), procedimentos são um conjunto de:

- a. Chamadas de procedimentos nos componentes do produto ou em produtos adjacentes, feitas para causar mudanças físicas no comportamento do produto;
- b. Leituras de variáveis internas ou externas ao produto;
- c. Tomadas de decisão (exemplo: abortar o procedimento se algum componente falhar em mudar seu modo de operação);
- d. Períodos de espera (exemplo: esperar que um dado componente mude seu modo de operação).

Enquanto as fases de um sistema contêm apenas informação do sistema enquanto caixa preta, procedimentos de produto também tem informação de eventos dentro do produto (abordagem de caixa branca). Tipicamente, atuadores (por exemplo, motores, pistões e relés) com funções recebidas (por exemplo, eletricidade, ar comprimido) realizam ações que contribuem para o procedimento do produto. Cada procedimento deve responder a pelo menos uma fase do sistema que especifica o produto, sendo que todas as fases devem ser implementadas por pelo menos um procedimento. A descrição detalhada dos eventos de cada procedimento é fundamental para o gerenciamento dos riscos de projeto e prevenção de acidentes. A falta de alternativas viáveis para realizar um procedimento para uma dada solução (por exemplo, por falta de atuadores ou serviços de outros sistemas) pode causar atrasos em um projeto. Procedimentos mal definidos podem causar acidentes previsíveis, principalmente quando não existem soluções técnicas ou instruções no manual para evitar condições perigosas. Nos estágios iniciais do projeto, a obrigação de descrever detalhadamente cada procedimento reduz riscos com baixo custo, justificando a adoção desse conceito.

Outro conceito que precisa de definição é o de confiabilidade aplicada a um modo de operação. “Confiabilidade do modo de operação é a probabilidade de que um produto possa atingir dentro de um dado prazo e manter um modo de operação por um dado período, assumindo que todas as funções recebidas pelo sistema correspondente estejam em condições nominais”.

Fica implícito que todas as funções de serviço do status correspondente atingem os desempenhos definidos. Alguns autores definem confiabilidade como a probabilidade de que uma única função atinja os desempenhos por um tempo determinado. Outros autores definem confiabilidade como a probabilidade de que o produto cumpra todas as funções e relativos desempenhos por um certo intervalo de tempo. Essa definição é importante porque nem

sempre todas as funções são necessárias ao mesmo tempo e duas ou mais funções podem ser necessárias em um dado modo de operação.

Implicitamente, as confiabilidades de cada modo de operação não são necessariamente iguais para um dado produto. Por exemplo, um produto pode ter um modo com baixos desempenhos e alta confiabilidade e outro modo com alto desempenho e confiabilidade inferior. A hipótese de condições nominais nas funções recebidas é importante porque o projetista tipicamente não tem autoridade para mudar outros produtos. Outro ponto é a necessidade de conhecer a contribuição individual de cada componente para a taxa de falha do produto. Por fim, do ponto de vista do cliente, o que importa é o cumprimento de uma missão, que implica também na capacidade de entrar em operação.

Similar ao conceito de confiabilidade é o conceito de disponibilidade do modo de operação. Esta tese define disponibilidade de um dado modo de operação como “probabilidade de que um produto, ao longo de sua vida operacional, possa atingir e manter o dado modo de operação por um período definido, assumido que todas as funções recebidas pelo produto estejam em condições nominais”. O tempo disponível exclui os períodos de manutenção preventiva e corretiva.

Esta tese também propõe uma adaptação do conceito de observabilidade de modos de operação de produtos, focando nas funções do sistema associado e não nas variáveis. “A observabilidade de um dado modo A de operação de um produto é a probabilidade de que a instrumentação definida pelo projeto estime que o produto está no modo A quando o produto está fisicamente no modo A, em um dado período”.

É importante notar que cada status de sistema deve ser distinto dos demais para permitir que os modos de operação (do produto que atende o sistema) sejam observáveis. Para criar um status para um sistema, pelo menos uma função precisa ter um status diferente. Essa propriedade de unicidade é também importante para reduzir o número de status de um sistema, reduzindo também o esforço de engenharia. Em outras palavras, se houver vários status iguais, haverá confusão na construção do diagrama de máquina de estados, estudos desnecessários, confusão na comunicação de requisitos e erros na estimativa do modo de operação. Tais efeitos aumentam o custo de projeto e riscos de atraso e retrabalho, podendo causar, de maneira indireta, até acidentes. É importante notar também que os modos de operação não são iguais em termos de risco e essa definição permite que haja diferentes observabilidades para cada modo. Assim, o projeto de um produto pode aumentar a observabilidade quando for crítico para a segurança. É o caso para condições acidentais ou

modos de operação que podem causar acidentes, requerendo soluções mais confiáveis estimar o modo de operação do que modos inofensivos.

Esse conceito é fundamental para a definição da instrumentação e para a análise de risco, já que a capacidade de identificar corretamente o status pode afetar a segurança. Se o projetista não monitorar todas as funções, ocorrem dois riscos. O primeiro, de deixar o operador sem as informações necessárias à condução da planta, especialmente em situações de acidente, tal como ocorreu em Three Mile Island [8]. O outro risco é o projetista tentar incluir várias medições internas aos componentes sem fazer uma síntese, incorrendo em explosão de estados e introduzindo ruído. Ambos os riscos estavam ocorrendo nas plantas da EDF, empresa de distribuição de energia francesa, que tinha manuais de operação extremamente complexos, com cerca de 30 procedimentos. A EDF [35] introduziu a abordagem por estados onde as decisões são tomadas com base em medidas de instrumento e não por diagnóstico humano ou hipótese sobre a falha ocorrida. Por exemplo, foi criado o medidor de nível do vaso do reator para monitorar a função de remoção de calor residual do núcleo. Assim, os reatores franceses passaram a ser conduzidos como na Figura 2, ou seja, passaram a ser um sistema cibernético, reduzindo os procedimentos a apenas 6.

Além da observabilidade, a controlabilidade precisa de uma definição em função dos conceitos da engenharia de sistemas, distinta da controlabilidade da teoria de controle. Esta tese propõe a seguinte definição: “Controlabilidade de um procedimento (de um produto) é a probabilidade de sua realização, sem incorrer em perigos, dentro de um prazo determinado após a demanda, assumindo que todas as funções recebidas pelo produto estejam em condições nominais”. A importância deste conceito advém do fato de que um procedimento pode ser uma sequência complexa de ativação de funções internas ou externas a um sistema, cuja ordem pode ter efeitos sobre a segurança. Além disso, o sistema de controle e monitoração precisa manter a identificação do modo de operação do produto enquanto a fase é executada, bem como dos passos já executados e dos próximos a executar. Por fim, é interessante manter um registro do nível de risco ao qual o produto está exposto. Durante procedimentos, um produto pode passar por riscos maiores do que aqueles em seus modos de operação. Um exemplo de aumento de risco é um circuito de água do mar que precisa ser esvaziado e preenchido com água doce quando estiver inativo (a água do mar é muito corrosiva quando parada). O período entre a parada da bomba e o término do preenchimento

com água doce é um período com riscos maiores do que o normal se o trabalho for interrompido.

Esta tese também propõe que podem existir riscos relacionados a cada modo de operação de um produto. “Riscos de status são riscos que surgem exclusivamente em função do modo de operação do produto”. Existem três famílias principais de fontes de risco, entre outras.

- A primeira são os riscos de que subsistemas sofram perturbações (ação humana inadvertida, falha de equipamento, agressão externa como incêndio) que gerem perigos adicionais;
- A segunda são os riscos de atuação inadvertida de funções que devem estar inibidas para evitar danos; e
- A terceira família são os riscos relacionados aos erros de estimação do modo de operação do produto, permitindo que uma disfunção cause danos progressivamente maiores. Por exemplo, a falta do acionamento de um procedimento de segurança está inclusa nesta família.

Esta definição é importante porque às vezes os riscos vêm dos materiais que compõe o sistema e estão presentes em todos os status, não sendo riscos de qualquer status. Mas existem riscos que surgem a partir da operação incorreta e a análise de risco fica mais racional se conduzida por status, reduzindo o esforço médio de uma análise do tipo HAZOP. A redução de esforço ocorre pelo uso apenas de hipóteses realistas de emprego, aumentando a probabilidade de que a análise seja exaustiva nos modos de operação previstos.

Para especificações, existe um conceito muito importante que é a flexibilidade de requisitos. No contexto desta tese, a flexibilidade de um requisito pode ser: opcional, desejável, negociável ou mandatório. Um requisito opcional é aquele que o cliente aceita uma dada característica ou função, mas não está disposto a pagar mais por isso. Também podem ser permissões ou ideias que servem para guiar o trabalho de projeto, mas sem compromisso contratual. Requisitos desejáveis são aqueles pelos quais o cliente está disposto a pagar, mas podem ser ignorados de maneira unilateral pelo fornecedor. Em uma concorrência, o atendimento a tais requisitos pode ser usado como critério de desempate. Requisitos negociáveis podem ser parcialmente ignorados mediante uma negociação com o cliente, deixando-o ciente dos desvios. Requisitos mandatórios são aqueles cujo atendimento

integral é absolutamente necessário, sendo suficientes para condenar uma solução em caso de não atendimento. A importância da flexibilidade vem do fato de que ninguém tem conhecimento total sobre o que é possível ou não na prática. Dado um espaço de desempenhos e propriedades de um sistema, existe uma região de certeza, onde uma dada pessoa tem certeza de que é possível atingir, dadas as experiências anteriores. Existe também uma região que essa pessoa tem certeza de que não é possível atingir devido às leis naturais. Entre essas duas regiões existe uma região de incerteza. Assim sendo, tentar buscar apenas aquilo que certamente possível é permanecer estagnado no tempo, o que pode ser fatal nos dias de hoje, com a rápida evolução tecnológica. Por outro lado, existe o risco de o projeto sofrer reveses por apostar em uma promessa tecnológica que não atinja o desempenho esperado ou tenha inconvenientes inaceitáveis. Assim, a declaração de flexibilidade leva a instituição contratante a receber menos ofertas inadequadas e mais ofertas adequadas.

Um conjunto de conceitos importantes para o projeto de produtos são os qualificadores nominal, degradado, reduzido e proibido para os modos de operação.

Em modos de operação nominais, o produto realiza as funções relativas ao status correspondente com capacidade de atingir todos os requisitos de desempenho sem incorrer em riscos anormais.

Modos nominais são condições ideais que o projeto prevê para a operação do produto e incluem regiões relativamente reduzidas dentro do espaço de estados.

Em modos de operação degradados, o produto realiza as funções do status correspondente, mas nem todos os requisitos de desempenho são cumpridos ou existem riscos anormais.

Um exemplo pode ser um sistema de resfriamento a água do mar em um navio após parar as bombas de circulação e antes de isolar a rede e remover a água salgada. Neste caso, existe um risco anormal devido ao fato de a água salgada estacionária ser muito corrosiva, pois os sais tendem a sedimentar gerando diferenças de potencial. Permanecer com água salgada estacionária na rede por longo período aumenta muito a frequência de alagamentos a bordo. Em condições degradadas os operadores precisam fazer algo para reduzir riscos ou restabelecer os desempenhos nominais, mas sem necessidade de ação imediata (algo como uma luz amarela em um sinal de trânsito).

Em modos rebaixados, o produto realiza as funções do status correspondente sem riscos anormais, mas nem todos os desempenhos são atingidos.

Tais modos são interessantes para atingir altas confiabilidades para baixos desempenhos, sacrificando a confiabilidade para desempenhos elevados. Assim, o produto pode atingir soluções de compromisso interessantes em termos de custo, desempenho e segurança em casos onde uma interrupção total da função pode causar grandes danos. Um exemplo é a propulsão de um navio elétrico com várias fontes de potência em paralelo. Se uma fonte falhar, a velocidade máxima fica um pouco prejudicada, mas a possibilidade de perder todas as fontes em uma única viagem é muito pequena se comparada a uma arquitetura com um único motor. A perda completa da propulsão pode causar acidentes, tais como afundamento, encalhe, abalroamento, acompanhados de desastres ambientais e perda da carga.

Modos proibidos são regiões do espaço de estados que o produto não deve entrar ou deve sair tão logo quanto possível.

Um exemplo é um reator nuclear com calor residual e sem refrigerante no vaso do reator, situação que deve ser evitada, mas que pode ocorrer após uma grande ruptura na barreira de pressão. Modos proibidos requerem procedimentos e soluções para evitá-los e, após entrar neles, o produto requer ações imediatas para evitar a progressão dos danos.

A definição dos qualificadores dos modos de operação (nominal, degradado, rebaixado, proibido) é importante para apoiar a definição de procedimentos. É desejável que o sistema de controle (computadores ou seres humanos) possa estimar sem interrupção o modo de operação durante a execução de um procedimento. Durante um procedimento (idealmente saindo de um modo nominal e chegando a outro modo nominal), o produto deve passar por modos degradados, evitando regiões desconhecidas do espaço de estados. Assim, o sistema de controle mantém o entendimento do status do sistema e a percepção de que ainda existem ações a serem tomadas. Adicionalmente, um procedimento deve evitar o ingresso em um modo proibido, sendo que projeto deve documentar e comunicar os modos proibidos por todo o ciclo de vida do produto. Enquanto o status do sistema depende apenas das interações com o exterior (funções de serviço e recebidas), os modos e seus qualificadores (nominal, degradado, rebaixado, proibido) precisam de variáveis internas para sua definição (projeto) e posterior cálculo (operação). Em geral, modos nominais tem regiões mais restritas do que modos reduzidos, que são mais restritos do que modos degradados, como mostra a Figura 19. Nesta figura, os procedimentos são representados por flechas, bem como eles devem evitar a passagem por um modo proibido.

Figura 19 – Qualificadores dos modos de operação no espaço de estados

Essa proposição de status é ao mesmo tempo a mais simples e completa. É a mais simples porque se baseia diretamente na definição matemática de sistema, permitindo a definição dos status de um sistema antes do projeto de um produto. É completa porque o conjunto de funções, status e fases identificados abrange toda a informação funcional e comportamental requerida ao projeto de produtos. Tal simplicidade contribui para reduzir dados falsos ou irrelevantes durante o projeto. A completude contribui para mitigar perdas de dados, preservando a integridade da informação importante.

Todas as definições apresentadas são axiomas, ou seja, não são afirmações falseáveis, ou seja, com possibilidade de serem provadas erradas. Então esta tese apresenta a sua afirmação central (falseável): “Se aplicadas sistematicamente em todos os níveis de decomposição do produto, as definições desta tese levam à redução do custo total de projeto, construção e integração de um sistema complexo em relação às práticas correntes.”

A demonstração empírica da tese, a rigor, requer um experimento com um número estatisticamente significativo de equipes desenvolvendo projetos iguais, parte usando os conceitos desta tese e parte como grupo de controle usando métodos atuais. Tal demonstração seria extremamente custosa, além de ser demorada. Logo esta tese apresenta uma demonstração analítica e uma série de resultados do emprego dos conceitos como demonstração.

A demonstração analítica envolve a adoção de algumas hipóteses, a seguir. A primeira é que a pessoa encarregada de especificar um sistema (de qualquer nível da decomposição do produto) consiga identificar todas as funções, status e fases do sistema. A segunda hipótese é a de que a pessoa inclua apenas funções, status e fases necessárias ao sistema do nível acima. Abrindo em uma árvore de eventos, temos sequências tais como mostradas na Figura 20 quando uma pessoa desenvolve um sistema sem levar as definições propostas em conta. Na Figura 20, P1, P2 e P3 são as probabilidades associadas à hipótese ser verdadeira, ou seja, ocorrer o sim no losango.

Figura 20 – Árvore de eventos de especificação

Para o caso 1, a adoção das definições propostas nesta tese não traz benefício, sendo que elas podem incorrer em custos adicionais, ainda que pequenos. Por outro lado, no caso 2, o emprego das definições propostas pode reduzir a adição de componentes supérfluos no âmbito do sistema em questão. Vale lembrar que componentes supérfluos adicionam material, fontes de risco, esforço inútil de projeto e podem dificultar a viabilidade global de projetos tais como submarinos. Não só ocorrem custos no sistema, mas também podem ocorrer impactos em outros sistemas. Nos casos 3 e 4, o risco fica mais explícito, pois fatalmente ocorrerá a necessidade de retrabalho e consequentes atrasos no projeto. Um projeto complexo mobiliza muitas pessoas e empresas e atrasos implicam em aumentos de custo em percentual do projeto, não em relação ao subsistema que sofreu atrasos. Neste caso,

o fornecedor do subsistema sabe que seu cliente está disposto a pagar valores muito altos pela solução rápida do problema. Por exemplo, se um componente, feito sob encomenda custando \$10.000, for crítico para um projeto de \$1 bilhão, provavelmente o cliente estará disposto a pagar \$100.000 por uma alteração rápida. Essa inflação ocorre porque o cliente provavelmente está gastando \$50.000 por dia com pessoal, e mudar de fornecedor implicaria em um atraso de vários meses. Ou seja, o preço nestas condições embute a conveniência de obter um retrabalho rápido por parte do fornecedor. Resumindo, um projeto incompleto incorre em custos de retrabalho, custos de atraso do projeto e custos de conveniência.

Não parece possível estabelecer números ou ordens de grandeza para as probabilidades P1, P2 e P3, mas vale a pena avaliar os fatores dos quais elas dependem. A Figura 21 apresenta a árvore lógica para o cálculo da probabilidade P1. Esta tese assume que se o sistema em questão for reusado de um projeto anterior, o risco de falta de modelagem comportamental é desprezível, já que o sistema e o produto associado são bem conhecidos. Por outro lado, excluindo o caso de reuso ou comportamento trivial, uma modelagem comportamental completa só será possível por meio de simulações virtuais ou pelo emprego do conceito de status (proposto por essa tese). Por outro lado, somente identificar o comportamento necessário não é suficiente para que a especificação fique completa. Para atingir a completude da especificação, o projeto precisa traduzir todas as informações relativas aos status e fases do sistema em requisitos objetivos e verificáveis. Existe ainda o risco de ocorrer um fenômeno desconhecido (não necessariamente pela humanidade, mas somente pelas pessoas do projeto) que impossibilite o funcionamento de um produto tal como esperado.

Figura 21 – Árvore lógica para cálculo da probabilidade P1

As probabilidades P2 e P3 são logicamente idênticas e a Figura 22 apresenta sua árvore lógica.

Figura 22 – Árvore lógica para cálculo da probabilidade P2 e P3

Na falta de informação sobre o comportamento necessário, é razoável que a pessoa encarregada da especificação inclua status ou fases adicionais como uma espécie de margem. Analogamente, o projeto de um produto sem requisitos de comportamento e sem um produto de referência (reuso) tende a incluir modos e procedimentos desnecessários. Outra possibilidade é a inclusão arbitrária de status e fases na especificação (ou modos e procedimentos no projeto) e não haver rastreabilidade das decisões tomadas. Enquanto a adoção dos conceitos propostos pode reduzir a adição de status e fases por conservadorismo, a inclusão arbitrária só pode ser coibida por meio da rastreabilidade.

Se por um lado o conceito de status ajuda a compreender o comportamento de um sistema, o conhecimento do conceito não é suficiente para obter resultados. São necessários meios de controle de qualidade baseados neste conceito, impostos consistentemente em todos os níveis de decomposição do sistema e do produto.

Vale ressaltar que a definição de status proposta usa apenas as funções ou objetivos do sistema, que são elementos da especificação do sistema. Ou seja, o conceito proposto permite definir um modelo do comportamento necessário sem entrar em detalhes da arquitetura física do produto.

As metodologias atuais de engenharia de sistema empregam variáveis que pertencem ao projeto de uma solução para definir o modelo comportamental. As abordagens do estado da arte [29] [30] [28] [5] [7] [1] [6] baseadas em modelos tem o inconveniente de precisar estabelecer uma solução descrita por equações dinâmicas antes de verificar problemas de integração. Para essas metodologias, somente após resolver os problemas de integração é seguro passar o modelo comportamental como especificação. Passar o modelo como especificação também tem alguns inconvenientes tais como a falta de informação de flexibilidade para cada elemento do modelo. Essa falta de flexibilidade na especificação encontra frequentemente resistência por parte dos fornecedores de equipamentos que veem risco em aceitar um contrato excessivamente rigoroso. A Figura 23 apresenta a diferença entre especificações e soluções. Enquanto especificações devem delimitar um domínio viável amplo, uma solução é um ponto dentro de tal domínio viável. Assim sendo, passar uma solução como especificação reduz drasticamente a probabilidade de achar um fabricante disposto a desenvolver algo muito diferente de seus produtos habituais.

Figura 23 – Diferença conceitual entre especificação (sistema) e solução (produto)

Resumindo, as metodologias atuais identificam sistemas, suas funções e suas características (inconvenientes aceitáveis) na especificação. A partir da especificação, a atividade de projeto desenvolve o modelo comportamental, a arquitetura funcional e o modelo físico de um produto.

Os conceitos propostos implicam em incluir na especificação requisitos de comportamento, que são os status e fases do sistema. Consequentemente, a atividade de projeto desenvolve a arquitetura funcional e o modelo físico, e apenas refina o comportamento. Tal abordagem reduz o esforço médio porque o comportamento requerido do sistema fica definido antes do projeto do produto. A proposta desta tese muda o escopo das atividades de projeto e especificação, ou seja, o sistema enquanto problema é definido até o nível de comportamento. O projeto com dados de entrada incluindo o comportamento fica mais simples e direto, dispensando o lançamento de hipóteses e parte dos testes virtuais ou reais de integração (projeto por tentativa e erro). Assim, o número de iterações para resolver problemas de integração fica reduzido porque parte da lógica de coordenação entre sistemas foi resolvida durante a especificação. A Figura 24 apresenta a comparação das abordagens atuais e proposta de maneira gráfica.

Figura 24 – Comparação das abordagens atuais com a abordagem proposta

Por outro lado, não basta declarar que os conceitos propostos precisam ser aplicados e controlar a qualidade de seu emprego, pois não é trivial entender como aplicar tais conceitos. Por isso, esta tese desenvolve um método simplificado de especificação e projeto de sistemas genéricos. Tal método genérico não pode ser ótimo para nenhum tipo de sistema em particular, mas serve como base para desenvolver métodos otimizados para casos específicos.

Contextualizando, esse trabalho assume que haja uma hierarquia funcional dentro da equipe de projeto que tenha relação com a decomposição do sistema sendo projetado, tal como mostrado na Figura 25.

Figura 25 – Relação entre equipe de projeto e decomposição do sistema

Líderes de sistema criam especificam um sistema para atender um conjunto de necessidades. Em caso de sistemas complexos, haverá composição de subsistemas também complexos que precisam atender uma série de requisitos criados pelo líder de sistema. O conjunto de requisitos para cada subsistema é denominado especificação e cada especificação produzida pelo líder de sistema é entregue a líderes de subsistema.

Em resposta, tais líderes também produzem descrições de soluções (produtos) que são comunicados por meio de documentos (metodologias baseadas em documentos) ou de um modelo relacional em um banco de dados (metodologias baseadas em modelos). Os líderes de subsistema também devem criar especificações de cada (sub) subsistema, a serem passadas a líderes do nível hierárquico imediatamente abaixo ou a fornecedores.

Pode-se afirmar que especificações são o meio de comunicação de níveis hierárquicos superiores para inferiores, em todos os níveis. No sentido contrário, descrições são o instrumento de comunicação dos níveis inferiores para os superiores. Este trabalho chama de análise de cima para baixo a atividade de decompor um sistema descrito por uma especificação em um conjunto coerente de subsistemas, cada um descrito por uma especificação. A análise de cima para baixo é o movimento descendente da informação na árvore hierárquica e na decomposição do sistema.

Por outro lado, análise de baixo para cima é a atividade de definir uma solução (produto) a partir de informação (ou hipóteses) sobre componentes (produtos disponíveis). A análise de baixo para cima é o projeto de um produto e tem como objetivo final o

atendimento aos requisitos e verificar os impactos das discrepâncias de cada componente no produto. Se por um lado a análise de cima para baixo estabelece onde chegar, a análise de baixo para cima define como e até onde é possível chegar.

A Figura 26 mostra os fluxos de informação entre os níveis hierárquicos. Quando se trata de um fornecedor externo, a especificação de sistema também costuma ser chamada de consulta e a descrição de produto, de proposta.

Figura 26 – Fluxos de informação de uma equipe de projeto

Os requisitos funcionais de um sistema incluem as funções ou ações que ele realiza para sistemas clientes e as transições entre status, sendo as declarações dos objetivos do sistema. Requisitos não funcionais impõem limites para propriedades intrínsecas do sistema como peso, volume e custo, sendo declarações dos limites aceitáveis dos inconvenientes do sistema. Esta tese sustenta que uma lista completa de requisitos funcionais e não funcionais relacionados aos status do sistema permite decompor adequadamente em subsistemas menores. Cada subsistema realiza um conjunto de funções internas, tem seus status e correspondentes requisitos funcionais e não funcionais. Cada função interna usa pelo menos uma interface, sendo que cada interface pode ser usada por várias funções. A diferença entre funções de serviço e funções internas é o contexto. Funções de serviço são realizadas pelo sistema como um todo para clientes externos e são dados de entrada para o trabalho de engenharia. Funções internas são realizadas por subsistemas, dentro do sistema, contribuindo para a realização das funções de serviço. Funções internas são definidas pela pessoa responsável pela especificação dos subsistemas, ou seja, funções internas são um dado de saída do trabalho de especificação em um dado nível.

É interessante aplicar o conceito de sistema à pessoa encarregada de realizar especificações e projeto de sistemas, pois de acordo com a hipótese 4, essa pessoa deve seguir como referência os objetivos da organização. Além da pessoa seguir tais objetivos, a gerência precisa avaliar constantemente se os objetivos estão sendo seguidos, pois podem haver erros, dificuldades, mal-entendidos e desobediência. Aplicando a metodologia de abordagem por estados nas interfaces a um arquiteto dentro de uma equipe de projeto, identifica-se uma entidade adicional que é o trabalho de engenharia. O trabalho pode ser materializado em diversos meios físicos, tais como documentos em papel, sistemas informatizados ou bancos de dados. O arquiteto interage com o trabalho por meio de múltiplos ciclos de criação (modificações no trabalho) e análise (cálculos, demonstrações lógicas e verificações). A Figura 27 mostra os fluxos de informação entre os níveis hierárquicos e entre um arquiteto e sua obra (trabalho), ignorando as informações gerenciais de projeto.

Figura 27 – Fluxos de informação nas interfaces de um arquiteto

Para que haja observabilidade, toda troca de informação entre os níveis hierárquicos deve ser registrada formalmente por escrito. Do ponto de vista gerencial, o registro formal é uma ferramenta de observabilidade, pois permite identificar o status do trabalho por meio da análise dos dados.

A partir dos fluxos de informação de um arquiteto, identifica-se dois status gerais de um arquiteto em uma equipe de projeto: especificando e projetando. Por outro lado, tais

status se dividem em vários passos dependendo da interação do arquiteto com o trabalho em desenvolvimento. Na

Figura 28, à esquerda são apresentados os status dentro da análise de cima para baixo (especificação) e à direita, os status da análise de baixo para cima (projeto).

Figura 28 – Diagrama de estados de um arquiteto

Para ilustrar o método, juntamente com a descrição será apresentado um pequeno exemplo didático de especificação e projeto de um sistema, representado pelo sistema S1 na Figura 29.

Figura 29 – Diagrama de blocos do exemplo didático

O modelo de comportamento do exemplo didático é apresentado na Figura 30.

Figura 30 – Modelo de comportamento do exemplo didático

Os requisitos não funcionais e de desempenho são apresentados na Tabela 5.

Tabela 5 – Requisitos do sistema para o exemplo didático

Alvo	Texto	Flexibilidade
FS1	A potência removida deve ser > 200kW	Negociável
FS1	As taxas de falhas com taxa de reparo <1/hora devem ser <1e-5/hora	Mandatário
S1	A massa deve ser <1ton	Desejável

O primeiro passo da especificação é a identificação de subsistemas da solução, que pode ser gerenciada pelo controle de qualidade de diagrama de blocos. Neste diagrama devem ser incluídas as funções externas do sistema, tal como exemplificado na Figura 31.

Figura 31 – Identificação de subsistemas do exemplo didático

O segundo passo da especificação é identificar as funções técnicas de cada bloco e definir quais são os alvos ou clientes de cada função, tal como mostrado na Figura 32. Quando um bloco faz uma função para fora do sistema em estudo, assume-se que o cliente é um subsistema de mesmo nível hierárquico.

Figura 32 – Identificação de funções técnicas

De posse de todas as funções técnicas relativas a cada subsistema, a especificação deve identificar nexos causais entre as funções técnicas e as funções de serviço. Tal passo permitirá estabelecer a rastreabilidade de requisitos, assegurando que todas funções técnicas sejam necessárias. Assim fica mais difícil incluir funções de maneira arbitrária em um

projeto, já que o nexo causal é uma justificativa da existência de cada função. Além da rastreabilidade, os nexos causais facilitam a transmissão de requisitos entre os níveis hierárquicos, facilitando a compreensão da especificação. Após o estabelecimento dos nexos causais, requisitos de desempenho das funções de serviço podem ser facilmente traduzidos em requisitos de desempenho das funções técnicas. A Tabela 6 apresenta o exemplo didático de identificação de nexos causais.

Tabela 6 – Identificando nexos causais entre funções de serviço e funções técnicas

Funções técnicas	FS1	F2	F3	F4	F5	FR1	FR2
FT1 - Fornece 440Vac		•			•	•	
FT2 - Fornece 127Vac		•			•	•	
FT3 - Insere comandos			•	•			•
FT4 - Alimenta motor	•						
FT5 - Impele fluido	•						
FT6 - Remove calor	•						
FT7 - Conduz Fluido	•						

Tendo definido e justificado as funções técnicas, falta classificar as mesmas, já que nem todas serão relevantes para a definição dos status dos subsistemas. Neste ponto, vale ressaltar que essa classificação é relativa a cada subsistema, pois uma função pode ser irrelevante para quem realiza e relevante para quem recebe, e vice-versa. Essa etapa serve para simplificar o modelo de comportamento e mitigar o problema de explosão de status. A Tabela 7 mostra a classificação de funções do sistema S5 – Inversor.

Tabela 7 – Classificação de funções do sistema S5 – Inversor

Funções técnicas	Muda status?	Dimensionamento	Risco	Relevante?
FT1-Fornece 440Vac	Sim	Alto impacto	Nenhum	Sim
FT2-Fornece 127Vac	Sim	Médio impacto	Nenhum	Sim
FT3-Insere comandos	Sim	Pequeno impacto	Nenhum	Não
FT4-Alimenta motor	Sim	Alto impacto	Nenhum	Sim

A partir das funções técnicas relevantes, o arquiteto pode definir os status de operação para cada subsistema da solução, o que pode ser verificado pelo controle da qualidade da tabela de definição de status. Esta tabela identifica as funções internas ativas para cada status do sistema, definindo as necessidades de cima para baixo de combinações de atividade nas interfaces para cada um dos subsistemas. **A Erro! Fonte de referência não encontrada.** mostra essa tarefa para o exemplo didático.

Tabela 8 – Identificação dos status de cada subsistema

Funções técnicas	Operação	Pronto	Desligado
FT1 - Fornece 440Vac	Ativa	Pronta	Inativa
FT2 - Fornece 127Vac	Ativa	Ativa	Inativa
FT4 - Alimenta motor	Ativa	Pronta	Inativa
S5 - Inversor	Alimentando	Ligado	Desligado
FT4 - Alimenta motor	Ativa	Pronta	Inativa
FT5 - Impele fluido	Ativa	Inativa	Inativa
S6 Bomba	Girando	Pronta	Parada
FT5 - Impele fluido	Ativa	Inativa	Inativa
FT6 - Remove calor	Ativa	Inativa	Inativa
FT7 - Conduz Fluido	Ativa	Inativa	Inativa
S7 - Rede	Fluindo	Parada	
FT6 - Remove calor	Ativa	Inativa	Inativa
S8 Trocador de calor	Resfriando	Em equilíbrio	

A partir dos status, o arquiteto deve detalhar cada fase de seu sistema, identificando fases ou até novos status de subsistemas para viabilizar cada fase do sistema. Quando um sistema realiza uma fase ativa, pelo menos um de seus subsistemas realiza uma fase. Isso significa que um sistema pode precisar de uma série de fases de seus subsistemas para que uma mudança de status ocorra. Detalhando cada fase do sistema, a especificação identifica a lista completa de fases de cada subsistema. Pode ocorrer até a inclusão de um novo subsistema, tal como um motor de partida. Essa etapa pode ser verificada pelo controle de qualidade da tabela de descrição de fases, que emprega funções técnicas de seus subsistemas ou funções externas ao sistema. É fundamental distinguir as fases que o próprio subsistema efetua (ativas) das fases que são totalmente efetuadas por funções recebidas (passivas). Fases ativas usam verbos no presente do indicativo e fases passivas usam verbos no particípio. Fases ativas requerem funções de transição enquanto fases passivas não precisam. A Tabela 9 apresenta o exemplo didático de descrição das fases.

Tabela 9 – identificação de fases do exemplo didático

Funções técnicas	F2	F3	F4	F5
FT1-Fornece 440Vac	Prepara	-	-	Desliga
FT2-Fornece 127Vac	Liga	-	-	Desliga
FT3-Insere comandos	Guarnece	Comanda partida	Comanda parada	Desguarnece
S5-Inversor				
FT4-Alimenta motor	-	Liga	Desliga	-
S6-Bomba				
FT5-Impele fluido	-	Ligada	Desligada	-
S8-Trocador de calor				
FT6-Remove calor	-	Ligada	Desligada	-
S7-Rede				
FT7-Conduz Fluido	-	Ligada	Desligada	-

Tendo definido o comportamento dos subsistemas, é necessário declinar os requisitos de sistema para os subsistemas. A especificação deve traduzir os requisitos de desempenho das funções de serviço para requisitos de desempenho das funções técnicas com nexo causal. Os requisitos não-funcionais do sistema devem ser traduzidos em requisitos não funcionais para cada subsistema. Tal passo serve para preservar a integridade das informações. A Tabela 10 apresenta um exemplo didático de declinação de requisitos.

Tabela 10 – Declinando requisitos entre níveis hierárquicos

Requisito Pai	Requisito Filho
FS1: A potência removida deve ser > 200kW	FT4: A potência deve ser > 3,6kW FT5: A vazão deve ser > 17m ³ /h FT7: A velocidade média do fluido deve ser <3 m/s FT6: A potência trocada deve ser >220kW
S1: A massa deve ser < 1ton	S5: A massa deve ser inferior a 300kg S6: A massa deve ser inferior a 300kg S8: A massa deve ser inferior a 200kg S7: A massa deve ser inferior a 200kg

Após definir os requisitos de desempenho, a especificação deve caracterizar cada status de subsistema, em função dos status de cada função técnica definidos em “identificando status”. A Tabela 11 apresenta os tipos de requisitos necessários para cada status de função técnica e seus requisitos de refino. Tais requisitos são determinantes no custo da solução, sendo mais barato obrigar todos as especificações a incluí-los do que arriscar a obter uma solução inadequada. Ou seja, esse passo serve para preservar a integridade das informações necessárias ao projeto de cada subsistema.

Tabela 11 – Requisitos para caracterizar as funções técnicas dentro de cada status

Estado da FT	Tipo de requisito	Refinado por requisitos de:
Ativa	Performance	Taxa de falha e de reparo, método de V&V, cronograma
Pronta	Tempo de resposta, Performance	PFD, frequência de atuação inadvertida, método de V&V, cronograma
Proibida	Frequência de atuação inadvertida	-
Inativa	-	-
Indiferente	-	-

Tendo os requisitos funcionais, comportamento e desempenhos definidos, a pessoa encarregada da especificação deve escolher o método de realização de cada subsistema. As opções mais comuns são comprar, fazer um projeto interno ou reusar um produto já pronto [21]. Cada um desses métodos tem vantagens e desvantagens, mas tal discussão fica fora do escopo deste trabalho.

Tabela 12 – Escolha do método de realização

Subsistema	Método de realização
S5-Inversor	Reuso
S6-Bomba	Compra
S8-Trocador de calor	Compra
S7-Rede	Projeto Interno

Caso haja subsistemas reusados, para os subsistemas adjacentes, a especificação deve incorporar as especificações de interface [36]. Esse passo serve para preservar as informações necessárias ao projeto dos subsistemas, já que sistemas reusados já tem interfaces completamente definidas. Tipicamente, alterar a interface de um sistema cujo projeto já está pronto é mais caro do que desenvolver uma interface adequada em um novo subsistema. A Tabela 13 mostra um exemplo de atribuição de requisitos de interface em função do reuso do inversor.

Tabela 13 – Caracterização de interfaces do exemplo didático

Função técnica ou subsistema	Requisito de interface
FT1-Fornece 440Vac	Deve atender os requisitos enunciados no manual do inversor
FT2-Fornece 127Vac	Deve atender os requisitos enunciados no manual do inversor
FT3-Inserir comandos	Não aplicável
S6-Bomba	A alimentação da bomba deve ser compatível com a saída do inversor, descrita no manual

Depois, o arquiteto deve identificar as interfaces necessárias (criadas por projeto, como conectores) e inevitáveis (decorrentes da física, como emissão eletromagnética). O gerenciamento da equipe de projeto pode monitorar tal passo por meio da inspeção de diagramas de interface.

Vale ressaltar que tanto a atividade de especificação como a de projeto são iterativas, e, em dado passo, pode-se concluir que o sistema precisa de uma mudança arquitetural. Como a arquitetura é a base para todo tipo de análise, isso impõe o retrabalho de todos os passos anteriores.

Após definir e justificar regras para análises de cima para baixo e especificações, é preciso apresentar regras para análises de baixo para cima e descrições de sistema. Descrições de sistema podem ser transmitidas por meio de documentos (desenvolvimento baseado em documentos) ou por meio de um modelo compartilhado pela equipe de projeto (desenvolvimento baseado em modelos). Este trabalho apresenta regras aplicáveis aos dois tipos de metodologias.

A análise de baixo para cima começa com a obtenção de dados dos subsistemas ou hipóteses realistas sobre os mesmos. O primeiro passo é checar as interfaces, revisando a arquitetura do sistema adicionando adaptadores ou mudando as especificações de interface dos subsistemas. A Tabela 14 apresenta um exemplo didático de tabela de controle de interfaces.

Tabela 14 – Compatibilização de interfaces

Nome da interface	Subsistema 1	Funções / direção	Subsistema 2	Status da interface
I1	S3	FT1→ FT2→	S5	Analisada
I2	S5	FT4→	S6	Testada
I3	S6	FT5→	S7	Pendente
I4	S7	FT6←	S8	Pendente
I5	Operador	FT3→	S5	Pendente

O segundo passo é identificar os modos de operação para cada status. O status definido na especificação é um desejo, enquanto os modos de operação são o resultado do projeto. Deve haver pelo menos um modo para cada status. A Tabela 15 apresenta a definição dos modos de operação e sua relação com os status do sistema.

Tabela 15 – Definição de modos de operação do exemplo didático

Modo	Status associado	S5	S6	S7	S8
Operação	Operação	Alimentando	Girando	Fluindo	Resfriando
Pronto	Pronto	Ligado	Parada	Parada	Em equilíbrio
Desligado	Desligado	Desligado	Parada	Parada	Em equilíbrio
Manutenção	Desligado	Travado	Seca	Aberta	Seco

Após a definição dos modos de operação, é preciso escolher as configurações físicas de referência para verificar o dimensionamento. O projeto deve ter pelo menos uma configuração física de referência para cada modo de operação relativo a um status no qual funções de serviço estão ativas. Configurações físicas são pontos de operação dentro de um modo (os modos de operação são regiões do espaço de estados), o que as torna mais adequadas para verificações. A Tabela 16 apresenta uma configuração de referência para o exemplo didático.

Tabela 16 – Configuração de referência

Configuração	Modo	S5	S6	S7	S8
Config1	Operação	Alimentando	Girando	Fluindo	Resfriando

De posse das configurações físicas de referência, pode-se calcular desempenhos, confiabilidade e reparabilidade. Para cada configuração física, calcula-se o desempenho do produto atingido em relação a cada requisito de desempenho, tal como mostrado na Tabela 17.

Tabela 17 – Desempenhos calculados para o exemplo didático

Configuração	Estado relacionado	Requisito	Valor efetivo
Config1	Operação	FS1: A potência removida deve ser > 200kW	225kW

A seguir, o projeto deve descrever os procedimentos para realizar as transições de um modo a outro, usando estritamente os comandos disponíveis dos subsistemas, como na Tabela 18.

Tabela 18 – Definição de procedimentos do produto do exemplo didático

Modo inicial	Modo final	Processo	Obs.
Operação	Pronto	Operador comanda ‘parar inversor’	
Pronto	Desligado	Operador desalimenta o inversor	
Desligado	Manutenção	Operador comanda ‘travar inversor’ Operador drena tubulação	Não existe função para drenar
Manutenção	Desligado	Operador enche a tubulação Operador comanda ‘destravar inversor’	Não existe função para encher
Desligado	Pronto	Operador alimenta o inversor	
Pronto	Operação	Operador comanda ‘partir inversor’	

Em face da necessidade de novas funções para realizar os procedimentos, foi necessário revisar a especificação de todos subsistemas, tal como mostrado na Figura 33.

Figura 33 – Revisão da especificação dos subsistemas

As novas funções necessitam de novas interfaces, que são mostradas na Tabela 19.

Tabela 19 – Revisão da compatibilização de interfaces

Nome da interface	Subsistema 1	Funções / direção	Subsistema 2	Status da interface
I1	S3	FT1→ FT2→	S5	Analisada
I2	S5	FT4→	S6	Testada
I3	S6	FT5→	S7	Pendente
I4	S7	FT6←	S8	Pendente
<i>I5</i>	<i>S4-Operador</i>	<i>FT3→</i>	<i>S5</i>	<i>Pendente</i>
<i>I6</i>	<i>S4-Operador</i>	<i>FT8→</i> <i>FT9→</i>	<i>S7</i>	<i>Pendente</i>

Após a definição dos procedimentos e devida revisão do trabalho de engenharia, falta definir as funções de interface do sistema. No caso, as únicas interfaces que requerem funções são as interfaces do sistema com as pessoas, que precisam de funções de controle e monitoração e funções de manipulação manual de válvulas. A Tabela 20 apresenta as funções da interface humana com o sistema.

Tabela 20 – Projetando interfaces

Função de interface	Nome	Interface – Função pai	Local
FI1	Partir inversor	I5 – FT3	Painel do inversor
FI2	Parar inversor	I5 – FT3	Painel do inversor
FI3	Travar inversor	I5 – FT3	Painel do inversor
FI4	Destruir inversor	I5 – FT3	Painel do inversor
FI5	Esvaziar circuito	I6 – FT8	Válvula de dreno
FI6	Encher circuito	I6 – FT9	Válvula de suspiro

Em seguida, uma análise de risco deve ser conduzida para identificar necessidade de possíveis mudanças arquiteturais. Juntamente com as funções de controle, é importante verificar se as interfaces são adequadas para efetuar as transições. A Tabela 21 mostra uma análise de perigos simplificada com ações corretivas.

Tabela 21 – Analisando riscos

Sis.	Nº	Descrição	λ	μ	Consequência	Ação corretiva
S5	fm1	Falha cartão	1e-5	1	S1 para por um tempo incerto – não cumpre requisito de taxa de falha e reparo	Monitorar estado do inversor
S5	fm2	Falha barramento	1e-7	1e-3	S1 para até a troca do inversor	-
S6	fm3	Desgasta impelidor	1e-6	1e-1	S1 tem desempenho abaixo do mínimo por tempo indeterminado – arrisca descumprir requisito de taxa de falha e reparo em caso de imprevistos	Monitorar pressão diferencial da bomba Monitorar NPSH

Devido aos resultados da análise de perigos, houve necessidade de incluir novas funções na rede, tais como monitorar a pressão na sucção da bomba e a pressão diferencial. O inversor passou a ter um papel de disponibilizar informações para a pessoa que opera o sistema, que por sua vez precisa fazer a manutenção do inversor. A Figura 34 apresenta o diagrama de blocos revisado.

Figura 34 – Revisão da especificação

Devido à revisão do diagrama de blocos e da especificação, as interfaces precisam também de uma revisão, tal como mostrada na Tabela 22.

Tabela 22 – Revisão da compatibilização de interfaces

Nome da interface	Subsistema 1	Funções / direção	Subsistema 2	Status da interface
I1	S3	FT1→ FT2→	S5	Analisada
I2	S5	FT4→	S6	Testada
I3	S6	FT5→	S7	Pendente
I4	S7	FT6←	S8	Pendente
I5	Operador	FT3→ FT12→ FT13←	S5	Pendente
I6	Operador	FT8→ FT9→	S7	Pendente
I7	S5	FT10← FT11←	S7	Pendente

Uma vez que as interfaces mudaram, novas funções de interface também são necessárias para efetivar as novas funções técnicas. A Tabela 23 mostra as novas funções de interface adicionadas em função da análise de risco.

Tabela 23 – Revisão do projeto de interface

Função de interface	Nome	Interface – Função pai	Local
FI1	Partir inversor	I5 – FT3	Painel do inversor
FI2	Parar inversor	I5 – FT3	Painel do inversor
FI3	Travar inversor	I5 – FT3	Painel do inversor
FI4	Destruir inversor	I5 – FT3	Painel do inversor
FI5	Esvaziar circuito	I6 – FT8	Válvula de dreno
FI6	Encher circuito	I6 – FT9	Válvula de suspiro
FI7	Monitorar estado do inversor	I5 – FT3	Painel do inversor
FI8	Monitorar pressão dif. da bomba	I7 – FT10	Sensor de pressão dif.
FI9	Monitorar NPSH da bomba	I7 – FT11	Sensor de pressão abs.
FI10	Mostrar pressão dif. da bomba	I5 – FT13	Painel do inversor
FI11	Mostrar NPSH da bomba	I5 – FT13	Painel do inversor

Finalizada a arquitetura, a análise de baixo para cima deve calcular as propriedades do produto para subsidiar a verificação de atendimento aos requisitos, tal como mostrado na Tabela 24.

Tabela 24 – Cálculo de propriedades

Memorial de cálculo	Requisito	Valor efetivo
xxxxxxxxx.pdf	S1: A massa deve ser <1ton	0,87 ton

Por fim, mas não menos importante, é fundamental preencher a matriz de atendimento aos requisitos, que deve relacionar todos requisitos de sistema, os resultados e as análises que comprovam tais resultados. A Tabela 25 apresenta um exemplo didático de tabela de atendimento.

Tabela 25 – Verificação de atendimento

Requisito	Valor efetivo	Prova
S1: A massa deve ser <1ton	0,87 ton	xxxxxxxxx.pdf
FS1: As taxas de falhas com taxa de reparo <1/hora devem ser < 1e-5 /hora	$\lambda=1e-6$ e $\mu=0,1$ $\lambda=1e-7$ e $\mu=1e-3$	yyyyyyyyy.pdf
FS1: A potência removida deve ser > 200kW	225kW	zzzzzzzzz.pdf

Concluindo, o resultado da análise de baixo para cima é uma descrição de sistema, que pode ser um conjunto de documentos (projeto baseado em documentos) ou um modelo (projeto baseado em modelos). Tanto a análise de cima para baixo como a análise de baixo para cima precisam satisfazer uma série de requisitos, que esta tese lista no Anexo 1 para facilitar a leitura. Os requisitos listados no Anexo 1 são aplicáveis aos dois tipos de metodologias (baseadas em documentos ou em modelos).

4 DESENVOLVIMENTO

Esta seção apresenta uma sequência de análises de cima para baixo a partir de uma empresa provedora de usinas nucleares móveis e chegando até os componentes de um gerador de vapor.

4.1 Proposta de uma empresa provedora de usinas nucleares móveis

Essa empresa teria uma função crítica do ponto de vista do desenvolvimento nacional, pois ela asseguraria energia barata em regiões remotas e reduziria o custo do frete dos navios mercantes. Além disso, essa empresa teria um papel destacado em situações de calamidade pública, por exemplo, restabelecendo energia para clientes prioritários, tais como hospitais. Por fim, em situação de conflito, essa empresa poderia permitir restabelecimento da energia ou facilitar a realocação de indústrias.

A energia nuclear é a melhor solução em termos de segurança energética devido às suas características intrínsecas. Essas características são: densidade energética do combustível, densidade de potência da planta, robustez às mudanças climáticas, diversidade e dispersão geográfica dos fornecedores de combustível e estabilidade do preço de combustível.

Considerando que sua emissão de carbono é reduzida, tem a vantagem de causar impactos ambientais menores do que combustíveis fósseis. Por outro lado, as tecnologias atuais de conversão de energia nucleares são custosas e precisam ter grande potência instalada para serem competitivas. Assim, os combustíveis fósseis permanecem inevitavelmente no curto prazo como a solução dominante para motores de caminhões e pequenos navios. Como exercem papel crítico na distribuição de alimentos e são limitados, as jazidas dos combustíveis fósseis devem ser economizadas ao máximo por meio do uso de energias renováveis e nuclear. Uma aplicação que poderia reduzir consideravelmente o consumo de óleo e gás natural seriam os motores de grandes navios mercantes, que requerem potências da ordem de 50 MWe.

Este trabalho propõe a criação de uma empresa provedora de usinas nucleares móveis que poderiam ser usadas para fornecer energia elétrica a uma ampla gama de clientes. Tais clientes seriam a rede de distribuição elétrica, navios mercantes, forças armadas e o setor agropecuário. Devido ao seu reduzido tamanho, usinas nucleares móveis não poderiam ser

economicamente competitivas com grandes usinas fixas. Por outro lado, tais usinas móveis teriam flexibilidade, mobilidade, força nos números e aplicação dual.

A flexibilidade de deslocar até o cliente torna o fornecimento de energia por usinas móveis mais confiável. Uma usina pode ser trocada rapidamente e não depende instalações fixas, como linhas de transmissão. A flexibilidade permite que clientes que tem demanda inopinada por tempo limitado possam ser atendidos em locais remotos, como em caso de grandes obras. Em caso de eventos imprevisíveis, tais como agressões militares ou fenômenos meteorológicos, a flexibilidade das usinas móveis reduz o tempo para restabelecer serviços de fornecimento de energia.

Devido à mobilidade, as usinas móveis seriam particularmente competitivas em lugares remotos ou isolados, que exigem altos custos com linhas de transmissão ou transporte de combustível. Ilhas, lugares remotos e navios mercantes, que pagam um preço mais elevado pela energia, seriam clientes potenciais. A mobilidade também tem vantagens estratégicas bélicas, pois em caso de guerra, usinas móveis poderiam ser deslocadas para evitar a captura pelo inimigo.

Como seriam construídas em grande quantidade, tais usinas teriam seu custo unitário abaixado, pois os custos não recorrentes (projeto, infraestrutura, tecnologias, pessoal) seriam diluídos. Além disso, como usariam componentes em grande quantidade, seria possível obter redução de custos. Por outro lado, dado o alto custo de aquisição de um reator de potência, é desejável empregar reatores com a maior potência nominal possível para reduzir o custo da energia.

Por fim, tais usinas teriam aplicação dual, sendo usadas tanto pelas forças armadas e por clientes civis. Assim, em caso de guerra, haveria muitas usinas para ajudar no esforço de guerra, o que torna os custos de mobilização relativamente baixos. Após o fim do conflito, as mesmas usinas produzidas para fins militares poderiam ser usadas para fornecer energia a preço de custo, o que reduz o custo de desmobilização da guerra. Outra vantagem da aplicação dual é a continuidade da produção, que torna mais barata a manutenção das competências técnicas necessárias à fabricação do material bélico.

Vale ressaltar que tais usinas estariam sujeitas a muitos tipos de ameaças, como colisão com navios, encalhamento, furacões, maremotos, tornados e queda de aviões.

Também teriam que satisfazer requisitos militares, como choque militar, discríção acústica, discríção térmica e discríção magnética. As condições ambientais também seriam bastante amplas, já que tais usinas móveis podem estar em qualquer ponto dos oceanos, mares ou rios, o que implica em margem de fluutuabilidade.

Essa empresa teria várias interfaces de fornecimento de energia. Para fornecer energia para indústrias, comércio ou residências, as usinas nucleares móveis se conectariam à rede de distribuição elétrica. As interfaces com as empresas transportadoras, proprietárias dos navios mercantes, serão contratos de fornecimento de energia com uma dada confiabilidade e tempo de restabelecimento. Esses contratos exigem as transportadoras de quaisquer responsabilidades em termos de segurança nuclear ou tratamento de rejeitos nucleares. Em status de exceção, tais contratos poderiam ter cláusulas que, sob decisão do poder político, obriguem as empresas transportadoras a ceder seus navios para uso com fins estatais, mediante uma indenização pré-estabelecida. O fornecimento de energia, feito por uma organização sob controle estatal, torna virtualmente impossível a desobediência por parte das empresas transportadoras.

As interfaces com as forças armadas seriam contratos prioritários de fornecimento de energia, cujos clientes finais podem ser bases, navios de guerra ou mesmo submarinos. O setor agropecuário receberia energia para dessalinização de água ou alimentar suas instalações por meio da rede de distribuição de energia elétrica.

Vale ressaltar que o principal tipo de cliente seriam os navios mercantes devido ao seu grande número e alto consumo de energia. Existem no mundo centenas de navios porta-contêineres que requerem mais do que 50MW de potência mecânica de propulsão [37].

Decorrente do papel prestado nos status de exceção, esta empresa precisa ter status análogos aos dos serviços essenciais, prevendo transições de mobilização para a guerra e desmobilizações. A Figura 35 apresenta o diagrama de status proposto para a empresa.

Figura 35 – Diagrama de status da empresa

A empresa provedora de usinas nucleares móveis também receberia combustível nuclear para recarregar os reatores. Tal fornecimento teria que mudar de acordo com o estado do país, construindo maiores estoques em status de exceção para reduzir o risco de perder a capacidade de reabastecer as usinas. A Tabela 26 apresenta as atividades na interface da empresa.

Tabela 26 – Atividades nas interfaces por estado da empresa

Função	Direito	Calamidade	Sítio	Guerra	Guerra total
FR1 - Prover combustível nuclear	Estoque para 6 meses	Estoque para 6 meses	Estoque para 1 ano	Estoque para 5 anos	Estoque para 10 anos
FR2 - Distribuir energia elétrica	Ativa	Inativa	Ativa	Ativa (baixa confiabilidade)	Ativa (baixa confiabilidade)
FR3 - Prover mão de obra	Ativa	Possível reconvocação	Possível reconvocação	Reconvocação de pessoal crítico	Reconvocação de toda mão de obra possível
FR4 - Prover equipamentos	Ativa	Ativa	Ativa (baixa confiabilidade)	Ativa (baixa confiabilidade)	Ativa (baixa confiabilidade)
FR5 - Regular atividade	Ativa (exigências nominais)	Ativa (possíveis flexibilizações)	Ativa (possíveis flexibilizações)	Ativa (exigências reduzidas)	Ativa (maximização do poder combatente)
FS1 - Prover energia elétrica	Todos clientes	Redirecionamento eventual para regiões afetadas	Redirecionamento eventual para belonaves	Redirecionamento parcial para belonaves	Somente clientes úteis ao esforço de guerra
FS2 - Alimentar belonaves	Mínimo número para belonaves	Redirecionamento eventual para regiões afetadas	Reforço eventual do número de belonaves	Aumento do número de belonaves	Máximo de belonaves
FS3 - Prover energia de propulsão	Todos clientes	Redirecionamento eventual para regiões afetadas	Redirecionamento eventual para belonaves	Redirecionamento parcial para belonaves	Somente clientes úteis ao esforço de guerra

4.2 Análise de cima para baixo em um navio mercante

Dado que o tipo de cliente mais numeroso é o navio mercante, segue uma análise de suas necessidades e restrições. Além de ser o principal cliente, é também o mais exigente devido ao seu ambiente inóspito e variável. Outros clientes têm limitações bem menos severas, à exceção das forças armadas. Navios mercantes devem resistir ao pior estado de mar encontrado a cada 100 anos [38]. Além disso, em guerra, explosões causadas por minas ou torpedos inimigos ameaçam esses navios, ao passo que acidentes nucleares continuam a ser indesejáveis. Isso impõe requisitos de resistência a choque militares no projeto dos componentes da parte nuclear da usina. A qualquer tempo, colisões podem ocorrer (assume-se uma frequência média da ordem de 1 vez a cada 100 anos por navio [39]) o que reforça a necessidade de algum nível de resistência a choques para evitar acidentes nucleares. Para

este trabalho, assumiu-se que uma resistência a um choque de 10g em todos os eixos será suficiente para evitar a grande maioria dos problemas enquanto mantém-se um nível razoável de resistência para componentes eletrônicos. Assim, as usinas atingem um nível de segurança razoável sem demandar o emprego de componentes de alto custo.

Para melhorar a disponibilidade e a flexibilidade operacional, a autonomia do combustível nuclear deve ser compatível com o ciclo de manutenção típico dos navios, que é de cerca de 2,5 anos [40]. Para manter a disponibilidade alta em caso de manutenção corretiva (falha da usina), deve ser possível destacar a usina do navio dentro de 6 horas. Assim, outra usina pode substituir a usina em pane em poucas horas, mantendo a disponibilidade alta. Além disso, a tripulação do navio deve ser composta de funcionários da companhia de transporte enquanto a tripulação da usina deve trabalhar para a empresa provedora de usinas (talvez militares). Assim, somente tripulação da usina precisa ter competências nucleares, bem como os equipamentos do navio não precisam aderir a padrões nucleares, já que a usina é capaz de resolver o problema da segurança nuclear sozinha.

Quando estiver navegando em alto mar, o navio tipicamente demandará a potência nominal da usina para atingir sua velocidade de cruzeiro. Porém, quando se aproxima de um porto, o navio precisa reduzir a velocidade para reduzir riscos de colisão e encalhe, bem como a propulsão deve parar quando o navio atraca. No cais, o navio pode precisar de energia elétrica caso a eletricidade vendida no porto seja muito cara, sendo que esse trabalho assume um valor de até 10MWe.

Este trabalho assume que um navio mercante tem tipicamente os blocos mostrados na Figura 36, onde a usina provê energia elétrica em média voltagem alternada para propulsão e auxiliares. O casco do navio e suas estruturas dão uma solução para fixar fisicamente a usina durante a navegação. A tripulação do navio dá ordens à tripulação da usina por meio do sistema de comunicações interiores, que podem envolver o acoplamento ao navio, destacar do navio, e atingir níveis de potência.

Figura 36 – Diagrama de blocos do navio

Um navio deve operar nos status apresentados na Figura 37, bem como realizar as fases indicadas, sendo que a remoção e recolocação da usina devem ocorrer no início e no fim da manutenção, respectivamente.

Figura 37 – Status dos navios

Existem três grandes grupos de navios mercantes: graneleiros, navios-tanque e porta-contêiner. A Tabela 27 apresenta uma classe numerosa por grupo (cada grupo tem várias classes de acordo com o deslocamento).

Tabela 27 – Características das classes mais numerosas por grupo

Grupo – Classe	Deslocamento [t]	Potência no eixo [MW]
Navios-tanque – VLCC	280,000	25 MW
Porta-contêineres – Post Panamax	97,000	60 MW
Graneleiros – Capesize	150,000	15 MW

Não foram escolhidas as maiores classes dentro de cada grupo porque o número de navio é pequeno, o que tornaria o mercado restrito. Por exemplo, VLCC é a segunda classe

em tamanho atrás da classe ULCC e respondia, em 2009, por 36,7% do total da tonelagem dos navios-tanque, enquanto ULCC responde por apenas 0,8% [41]. Outro exemplo é a classe Post Panamax, que tinha, em 2009, 32% da capacidade de carga do grupo de porta-contêineres, enquanto as classes maiores têm apenas 1% da capacidade [37]. A causa pode ser a falta de portos apropriados e rotas para navios muito grandes. Por outro lado, ordens recentes indicam o avanço da classe New Panamax, mas este trabalho não conta com o sucesso desta tendência no curto prazo, escolhendo a terceira classe em tamanho. O mesmo raciocínio orientou a escolha da classe Capesize, que é a segunda em tamanho, atrás da classe VLBC, mas que responde por 31,7% da tonelagem em 2007 [42].

Porta-contêineres, apesar de menores, precisam de mais potência de propulsão do que outras classes devido à sua alta velocidade de 25 nós (outras classes navegam de 14 a 16 nós). Além disso, o emprego de contêineres frigoríficos requer altas potências para máquinas auxiliares, atingindo uma ordem de 10 MWe.

Uma vez que a energia nuclear precisa de economia de escala para ser competitiva, este trabalho propõe o uso de energia nuclear apenas para porta-contêineres. Para ter um mercado amplo, este trabalho propõe focar na classe Post-Panamax (requer um total de 70MWe), o que pode ser mudado no médio prazo, o que melhoraria a competitividade das usinas nucleares móveis.

Atualmente, porta-contêineres usam tanques de combustível de cerca de 9000m^3 [43], o que significa que a solução nuclear não deve ter um volume superior a esse para ser competitiva.

Uma vez que componentes de qualidade nuclear são mais caros e levam mais tempo para serem construídos, é desejável estender a vida das usinas por pelo menos 60 anos (bem maior do que a vida de um navio, que é de 25 anos [37]). Tal fato também sugere o emprego de arquiteturas modulares que permitam destacar a usina nuclear de um navio no fim da vida e coloca-la em um navio novo. Além da melhoria da disponibilidade operacional, o requisito de destacar dentro de 6 horas também tem o efeito de permitir que navios nucleares atendam portos que baniram a energia nuclear [13].

Com o uso de acoplamentos de três pontos modernos, é possível destacar e colocar usinas em um navio mercante com baixo risco tecnológico [13]. Para o caso de destacamento

rápido no meio do mar, a usina nuclear móvel precisa de uma propulsão limitada (com velocidades da ordem de 5 nós) mas confiável. Tal propulsão ajudaria nas operações de acoplamento e desacoplamento e permitiria a usina manter a posição enquanto o navio entra no porto com ajuda de rebocadores. A propulsão da usina precisa ser retrátil para reduzir o arrasto durante a operação normal. Uma vez que a falha da propulsão da usina pode resultar em encalhe em uma praia e consequente perda de resfriamento, sua probabilidade de falha sob demanda deve ser inferior a 10^{-4} .

De acordo com a MAM [44], um navio mercante fica a maior parte de sua vida em mar aberto na velocidade de cruzeiro, precisando da potência nominal da propulsão em cerca de 280 dias por ano. Este trabalho assume que a três quartos dos outros dias do ano são gastos nas operações de carga e recarga nos portos (63 dias). O resto dos dias do ano seriam gastos em navegação a baixa velocidade, em canais, entradas de portos ou áreas de tráfego muito intenso, demandando cerca de 25% da potência nominal. O fator de uso adotado para o cálculo do índice de eficiência de energia de projeto é 75% [44].

A perda total de fornecimento de energia elétrica pode ter efeitos catastróficos para o navio ou para o meio ambiente, ainda que a segurança passiva assegure a segurança nuclear. Assim sendo, a perda completa da função de fornecimento de energia deve ter uma frequência inferior a uma vez a cada 100 anos por usina nuclear móvel, para ficar compatível com a resistência às condições de mar da Bureau Veritas [38]. Obviamente, objetivos de proteção do capital podem limitar ainda mais tal frequência se for economicamente viável.

Para alargar o mercado alvo, a usina nuclear móvel deve prover energia em um formato compatível com padrões internacionais, tais como 13kV/60Hz ou 11kV/50Hz. Assim, ilhas, cidades costeiras, plataformas de petróleo, navios mercantes, belonaves e usinas de dessalinização de água do mar podem todos vir a comprar energia.

Do ponto de vista militar e ecológico, as usinas devem irradiar níveis de ruído inferior a 110dB (com referência a 1 micro Pascal a 1 metro de distância) em todas as frequências. Em caso de afundamento, as barreiras devem permanecer intactas até tocar o fundo, requerendo soluções para equilibrar as pressões internas e externas para prevenir implosão, tal como no NS Savannah [45].

4.3 Análise de cima para baixo em uma empresa de usinas nucleares móveis

Essa empresa teria os seguintes componentes: centro de controle, fábrica de usinas, estaleiro naval, navios de transporte das usinas nucleares móveis, e um conjunto de usinas nucleares móveis. A Figura 38 apresenta o diagrama funcional da empresa.

Figura 38 – Diagrama funcional da empresa nuclear móvel

O centro de controle executa as tarefas administrativas, de planejamento e de operação das usinas nucleares móveis. Também faz novos projetos de desenvolvimento de novos modelos de usinas nucleares. Em caso de acidente em uma usina, o centro de controle coordena as ações de salvamento ou mitigação do acidente. O centro de controle integra o sistema de comunicações para trocar informações com outros componentes da empresa.

A fábrica produz e testa novas usinas e faz toda a qualificação técnica nuclear dos componentes, entregando à frota usinas prontas para uso. Essa fábrica faz uma produção em série para reduzir custos, adotando procedimentos padronizados de produção e de controle de qualidade. O estaleiro é uma estrutura, com diques secos, usada para fazer rotinas de manutenção e reabastecimento dos reatores das usinas nucleares móveis. Deve ser resistente a terremotos e eventos meteorológicos extremos, pois lidará com reatores com calor residual considerável.

Os navios de transporte são cascos alagáveis, similares a diques flutuantes, capazes de transportar pelo menos uma usina nuclear móvel, sendo ideal transportar três. Sua alimentação também seria feita por uma usina nuclear móvel. Assim, idealmente, um navio indo realizar trocas de usinas teria quatro usinas, sendo três transportadas e uma fornecendo energia. Teriam também recursos de salvamento para acudir uma usina após um acidente de perda de refrigerante e fontes de energia própria baseadas em combustíveis fósseis. Teria motores elétricos para propulsão em velocidades compatíveis às de navios porta-contêineres, com o objetivo de reduzir o tempo de substituição das usinas em caso de falha.

As usinas nucleares móveis seriam similares às usinas nucleares de terra, mas mais simplificadas. Devem suportar choques devido a colisões com navios, queda de aeronaves, terremotos quando nos diques, mares agitados e fenômenos meteorológicos extremos. Uma vez que ainda existe pirataria, essas usinas devem possuir armamento suficiente para repelir piratas ou milícias buscando a obtenção de material nuclear.

Seu projeto deve levar em conta restrições de descrição acústica e térmica, já que serão possivelmente usadas para guerra. Além disso, idealmente precisam resistir a choque devido a explosões a nível similar àqueles de submarinos. A função de geração de energia nuclear deve continuar enquanto os movimentos e atitude da usina não ultrapassarem valores que são observados em menos de 1% da vida de um navio. As usinas nucleares móveis deverão ter pelo menos 12% de fluabilidade positiva, de modo a ficar, em sua maior parte, imerso para trocar calor com a água em caso de acidente.

Um aspecto importante é que a tripulação deve ser militar pelas seguintes razões: assegurar obediência em caso de guerra; vedar a ocorrência de greves; oferecer proteção contra sequestro; prover confiança pública.

Deve também ser compatível com muitas pequenas cidades e ilhas para competir em um mercado o mais amplo possível. O formato da energia elétrica fornecida deve ser compatível com padrões típicos de voltagem e frequência. O vínculo mecânico da usina com o navio cliente deve eliminar movimentos relativos em relação ao navio. As operações de acoplamento e desacoplamento devem durar menos de 6 horas cada para conferir agilidade na troca de usinas. As usinas devem ter uma capacidade própria de propulsão e posicionamento que as permita entrar e sair dos navios cliente.

Tais usinas devem ter todos os recursos de segurança nuclear de maneira a tornar aceitável o risco de contaminação nuclear. Seu projeto deve ser realizado conforme as recomendações da EPRI [46] para reatores avançados e passivos. Adicionalmente, devem resistir a todos os acidentes básicos de projeto sem receber ajuda externa por 14 dias, que seria o tempo de um navio de transporte chegar ao local. Cada usina deve ter sua própria tripulação, treinada pela empresa em todas as competências nucleares necessárias à operação em segurança. Em caso de uma falha única, as usinas devem ser capazes de manter a produção de energia nuclear, mesmo que mantendo uma fração da potência nominal. Em caso de afundamento do navio, a usina nuclear móvel deve evitar vazamento de produtos radioativos mesmo que não haja qualquer ação humana nesse sentido. As únicas operações requerendo infraestrutura nuclear serão reabastecimento, inspeção detalhada a cada 10 anos e desincorporação. Em caso de um acidente básico de projeto ocorrer em um porto, a dose de radiação ao público em geral deve atender às restrições estabelecidas para as usinas nucleares de terra.

Por fim, o custo da energia fornecida deve ser competitivo com o preço de mercado. Isso é considerado viável para grandes navios, já que um estudo para a marinha dos Estados Unidos [19] afirmou que, para navios militares de médio e grande porte, a opção nuclear é mais econômica. Um projeto com restrições econômicas poderia atingir preços ainda mais competitivos, lembrando que os reatores militares são hoje concebidos sem preocupações econômicas, usando combustível com alto enriquecimento. Para reduzir custos, a vida útil das usinas devem ser pelo menos 50 anos, sendo desejável 60 anos. O nível de automação da usina deve buscar a minimização do custo global do ciclo de vida, levando em conta os riscos de erros dos operadores.

Usando o método, foram identificados os seguintes status para essas usinas: Recarga de combustível, Docada, Atracada, Gerando energia elétrica no cais, Transportada em navio, Navegando e Propelindo um navio. A Tabela 28 apresenta os status da usina e a Figura 39 apresenta o diagrama de status proposto.

4.4 Análise de cima para baixo em uma usina nuclear móvel

Uma usina nuclear móvel teria os seguintes sistemas internos: sistema de gerenciamento, casco e estruturas, sistema elétrico, sistemas da plataforma, sistema de conversão de energia e caldeira nuclear.

Figura 40 – Diagrama funcional de uma usina nuclear móvel

O sistema de gerenciamento envolve os operadores, computadores, regras de processo, a documentação e recursos de manutenção preditiva para realização da manutenção das instalações e componentes da usina. Suas funções são: monitorar o estado da planta; tomar decisões; e executar comandos. Deve tornar a operação previsível e controlada, reduzindo danos devidos a variações de processo, tais como erros dos operadores. Outra função é conectar com o ambiente externo por meio de satélites e rádio, mantendo a comunicação com o centro de controle da empresa provedora de usinas nucleares móveis. Por fim, também contém. O sistema de gerenciamento é centralizado em uma sala na parte de ré da usina, denominada sala de controle. Na sala de controle ficam os operadores do horário, que tem a visão geral da usina. As interfaces desse sistema com os outros sistemas da usina são: cabos analógicos; cabos digitais; e cabos de dados seriais com sensores ou atuadores inteligentes. As interfaces com a tripulação são: consoles para controle remoto a partir da sala de controle; painéis de controle locais; telefones para comunicações interiores; e telefones para comunicações exteriores.

Na parte de vante ficam as instalações de habitáveis, como cozinha, dormitórios, sala de estar, banheiros, onde fica a maior parte da tripulação. Em caso de acidente, os operadores fora do horário se reúnem na sala de estar para avaliar a evolução do acidente e verificar se as decisões do pessoal do horário tiveram os efeitos esperados. A sala de estar constitui então um centro de resposta a emergências, que deverá ser equipado com a documentação da usina e meios de monitoração. Conterá também com um controle remoto alternativo para efetuar as funções de segurança nuclear em caso de perda da sala de controle.

O casco e estruturas tem as funções de prover um volume estanque para a carga útil, proteger de choques devido a explosões, proteger contra colisões, suportar o peso e forças de aceleração de todos equipamentos, isolar fontes de ruído, segregar equipamentos redundantes e permitir a passagem de equipamentos para rotinas de manutenção. As interfaces do casco e estruturas com os equipamentos são os calços, berços, escotilhas, portas e escotilhões de manutenção. Na interface de arranjo, assume-se que o casco seja cilíndrico e com diâmetro externo de até 11 metros e comprimento de até 90 metros, ficando com um deslocamento um pouco menor do que o limite de 9000 metros cúbicos. Tal volume é imposto pelo principal tipo de cliente, que é o navio mercante.

O sistema elétrico inclui toda distribuição interna de energia elétrica e as interfaces externas de fornecimento de energia e de recebimento de energia. O sistema elétrico tem uma parte com classificação nuclear que fornece energia para os sistemas de segurança nuclear. Outra parte fornece energia elétrica em 360 V corrente contínua para todos os equipamentos de grande porte usados para operação normal. O uso de corrente contínua permite a continuidade da operação dos sistemas durante os processos de conexão e desconexão das fontes de energia. Por fim, existe uma rede de distribuição para pequenas cargas em 115V e 60 Hz, bem como uma rede de segurança de mesmo formato que fornece energia para equipamentos que não possam sofrer interrupções. As interfaces desse sistema com seus clientes internos à usina são os quadros de distribuição secundários onde cada carga deve ser conectada. A interface com clientes externos é o cabo de média voltagem para fornecimento da energia elétrica. Existe as seguintes interfaces para recebimento de energia elétrica: duas tomadas de recebimento de energia elétrica do cais; um disjuntor para receber energia de média voltagem do sistema de conversão de energia; e dois disjuntores para receber energia de baixa voltagem do sistema de conversão de energia. Existe também uma interface para receber combustível dos diesel geradores. O sistema elétrico tem geradores e

combustível para fornecer um mínimo de energia para o navio por 14 dias em caso de perda total da geração de energia nuclear.

Os sistemas da plataforma são um conjunto de instalações que operam de maneira independente e são distribuídos por vários locais dentro da usina. Eles providenciam os seguintes serviços: condicionam a temperatura e umidade da atmosfera interna; ventilam os compartimentos; proveem água de resfriamento; combatem incêndios; gerenciam a segurança náutica (por exemplo, esgoto de porões, monitoração de nível no fundo, fechamento de válvulas de casco); aplicam propulsão ao casco; atracam o casco ao cais; e engastam o casco à nave mãe.

O sistema de conversão de energia converte a energia do vapor em energia elétrica que será usada pela própria usina e entregue aos clientes. O sistema de conversão de energia realiza as seguintes funções: entrega energia elétrica de média voltagem ao sistema elétrico para que este possa atender aos clientes via conexão externa; entrega energia de baixa voltagem em corrente contínua ao sistema elétrico para que este possa distribuir pelos sistemas da usina; fornece água de alimentação a baixa pressão para a caldeira nuclear; fornece água desmineralizada para a caldeira nuclear; e resfria a caldeira nuclear após o desligamento em operação normal.

As interfaces com a caldeira nuclear são: a válvula de isolamento da linha de água de alimentação; a válvula externa de isolamento da linha de vapor principal; e o flange no tanque de água desmineralizada.

A caldeira nuclear tem a única função de gerar vapor. Ela deve gerenciar as funções de segurança nuclear de modo a atingir os objetivos de segurança nuclear de vazamento de radioatividade e derretimento de núcleo. Para reduzir os custos mantendo os níveis adequados de segurança, as soluções usadas para mitigar acidentes devem utilizar princípios físicos e equipamentos simples e que não dependam de energia. A caldeira nuclear tem algumas interfaces passivas, que não nunca mudam de estado, como suporte mecânico e interface de arranjo. Tais interfaces são importantes porque trazem requisitos que não podem ser ignorados, como requisitos de geometria e requisitos de resistência a choque.

A Figura 41 apresenta os estados e transições identificados para a caldeira nuclear e a Tabela 29 descreve as atividades nas interfaces da caldeira nuclear.

Figura 41 – Diagrama de estados da caldeira nuclear

Tabela 29 – Status da caldeira nuclear

Função	Em potência	Seguro	Prontidão 6h	Resfriando	Prontidão 72h	Recarga	Manutenção
FR1 - Fazer manutenção	Ativa (1º escalão)	Ativa (1º escalão)	Ativa (1º escalão)	Ativa (1º escalão)	Ativa (cais)	Ativa	Ativa
FR2 - Prover água de alimentação	Ativa	Inativa	Inativa	Ativa	Inativa	Inativa	Inativa
FR3 - Prover água desmineralizada	Standby	Inativa	Standby	Standby	Standby	Inativa	Inativa
FR4 - Resfriar circuito primário	Inativa	Inativa	Inativa	Ativa	Inativa	Inativa	Inativa
FR5 - Distribuir eletricidade 360Vcc	Ativa	Inativa	Ativa	Ativa	Inativa	Inativa	Inativa
FR6 - Distribuir eletricidade 115Vca	Ativa	Inativa	Ativa	Ativa	Ativa	Ativa	Ativa
FR7 - Resfriar a contenção	Ativa (normal)	Ativa	Ativa (normal)	Ativa (normal)	Ativa (normal)	Inativa	Inativa
FR8 - Reabastecer combustível	Inativa	Inativa	Inativa	Inativa	Inativa	Ativa	Inativa
FS1 - Produzir vapor	Ativa	Inativa	Inativa	Ativa_7%	Inativa	Inativa	Inativa

4.5 Análise de cima para baixo em um sistema de refrigeração do reator

De acordo com a norma ANSI-ANS51.1 [45], uma usina nuclear tem um conjunto de sistemas com as respectivas funções. No caso particular deste trabalho, apesar de baseado

na norma, alguns sistemas não existem e suas funções são realizadas por outros subsistemas da usina nuclear móvel. A caldeira nuclear tem os seguintes subsistemas: núcleo do reator e internos, sistema de controle de reatividade, sistema de proteção, sistema de resfriamento do reator, sistema de remoção de calor residual, sistema auxiliar do refrigerante do reator, sistema de água de resfriamento, sistema de resfriamento em emergência do núcleo, sistema de contenção primária, sistema de remoção do calor do secundário em emergência, sistema auxiliar da contenção, sistema ar condicionado de segurança, sistema elétrico, sistema de combate a incêndio, sistema de processamento dos rejeitos radioativos. As funções desses sistemas são definidas pela norma e não serão revistas nesse trabalho, exceto pelo sistema de resfriamento do reator.

Figura 42 – Diagrama funcional da caldeira nuclear

De acordo com a norma ANSI-ANS51.1 [47], o sistema de resfriamento deve conter produtos de fissão, remover calor em qualquer emergência e remover calor do núcleo em operação normal. Neste trabalho, o sistema de resfriamento do reator tem as seguintes funções de serviço: transferir calor do núcleo para o sistema de conversão de energia; conter o fluido refrigerante e produtos de fissão; abrir passagem para a troca de combustível; e refrigerar o núcleo em qualquer situação. Para transferir calor para o sistema de conversão de energia, existem duas interfaces: a linha de vapor principal e a linha de condensado principal. Para conter o fluido refrigerante e produtos de fissão, também existem duas

interfaces: a barreira de pressão e o casco do tanque de alívio. Este último contém um disco de ruptura para aliviar a pressão para a contenção em último caso. Para refrigerar o núcleo, existem as seguintes interfaces: o conjunto de linha de vapor principal e linha de condensado principal; e os flanges para acoplamento mecânico com o sistema de remoção do calor do secundário em emergência.

Vale ressaltar que a função de transferir calor para conversão de energia não é de segurança nuclear, mas relacionada à função principal de produção de energia. Assim sendo, pelos requisitos propostos neste trabalho, essa função deve ser segregada das outras duas funções de segurança nuclear (conter refrigerante e produtos de fissão e refrigerar o núcleo em qualquer situação).

Outro aspecto relevante é que o sistema de resfriamento está sujeito a agressões militares, tais como explosões, o que requer robustez mecânica e desacoplamento do casco. Por fim, existe também a necessidade de reduzir o ruído produzido para evitar a detecção por forças inimigas.

Os status de operação identificados estão descritos na Figura 43, juntamente com as transições necessárias.

Figura 43 – Diagrama de status do Sistema de Resfriamento do Reator

A Tabela 30 apresentam as atividades na interface do sistema de resfriamento do reator. Vale ressaltar que o status de “Resfriando em emergência” tem como objetivo apenas

a segurança nuclear, ignorando a proteção do capital. Para que esse status não venha a ocorrer frequentemente devido a falhas no sistema de conversão de energia, que é complexo e dificilmente confiável, foi criado um status adicional (“Resfriando anormal”). Nesse status, o sistema de remoção de calor residual assume a tarefa de resfriamento do Primário via gerador de vapor, o que deve ocorrer poucas vezes na vida da usina.

Tabela 30 – Status do circuito primário

Funções	Operando	Pronto	Resf. normal	Resf. anormal	Quente	Recarga	Resf. de emergência	Despres-surizando	Seguro	Frio	Vazio	Desgazei-ficando
FR1 - Aquecer fluido refrigerante	Ativa	Ativa_7%	Inativa	Inativa	Inativa	Inativa	Inativa	Inativa	Inativa	Inativa	Inativa	Inativa
FR2 - Remover calor do secundário	Pronta	Pronta	Pronta	Ativa	Pronta	Inativa	Pronta	Inativa	Inativa	Pronta	Inativa	Inativa
FR3 - Remover calor do primário	Inativa	Inativa	Inativa	Inativa	Ativa	Ativa	Inativa	Inativa	Inativa	Ativa	Inativa	Ativa
FR4 - Compensar contração de refrigerante	Pronta	Inativa	Ativa	Ativa	Pronta	Pronta	Inativa	Inativa	Inativa	Inativa	Inativa	Inativa
FR5 - Prover alimentação auxiliar do GV	Pronta	Pronta	Pronta	Pronta	Pronta	Inativa	Inativa	Inativa	Inativa	Inativa	Inativa	Inativa
FR6 - Gerar vácuo no tanque de alívio	Inativa	Inativa	Inativa	Inativa	Inativa	Inativa	Inativa	Inativa	Inativa	Inativa	Inativa	Ativa
FR7 - Injetar refrigerante	Pronta	Pronta	Pronta	Pronta	Pronta	Pronta	Inativa	Inativa	Ativa	Pronta	Inativa	Pronta
FR8 - Evaporar fluido	Pronta	Pronta	Pronta	Pronta	Pronta	Inativa	Ativa	Inativa	Inativa	Pronta	Inativa	Pronta
FR9 - Despressurizar circuito primário	Pronta	Pronta	Pronta	Pronta	Pronta	Inativa	Pronta	Ativa	Inativa	Pronta	Inativa	Pronta
FR10 - Alimentar GV	Ativa	Inativa	Ativa	Inativa	Inativa	Inativa	Inativa	Inativa	Inativa	Inativa	Inativa	Inativa
FR11 - Resfriar circuito primário	Inativa	Inativa	Ativa	Inativa	Inativa	Inativa	Inativa	Inativa	Inativa	Inativa	Inativa	Inativa
FS1 - Transferir vapor	Ativa	Inativa	Ativa_7%	Inativa	Inativa	Inativa	Inativa	Inativa	Inativa	Inativa	Inativa	Inativa
FS2 - Abrir passagem para recarga	Inativa	Inativa	Inativa	Inativa	Inativa	Ativa	Inativa	Inativa	Inativa	Inativa	Inativa	Inativa

4.6 Análise de cima para baixo em um sistema de geração de vapor

A Figura 44 apresenta o diagrama funcional do circuito primário proposto sem o sistema de controle, que tem presta funções para todos e deixaria o diagrama muito poluído. Esse diagrama apresenta os subsistemas como caixas pretas e cada flecha é um serviço prestado, sendo que sua ponta indica o cliente. Esses serviços descritos nas flechas são também chamados de função técnica ou função interna do circuito primário. Os quadrados brancos pequenos são as interfaces externas dos sistemas. Nem todas as funções técnicas estão ativas em todos os status do sistema.

Figura 44 – Diagrama funcional do Circuito primário

As necessidades do sistema de resfriamento impõem o comportamento do gerador de vapor. Quando o circuito primário está em status normais e resfriamento anormal, o gerador de vapor opera normalmente. Quando o sistema de resfriamento entra no status de resfriamento em emergência, o gerador de vapor precisa entrar em um status homônimo. Se o sistema de resfriamento despressurizar, o gerador de vapor precisa injetar fluido refrigerante para manter o núcleo do reator alagado. A Figura 45 apresenta o diagrama de estados do gerador de vapor e as transições requeridas.

Figura 45 – Diagrama de estados do Sistema de geração de vapor

A Tabela 31 apresenta a descrição dos status do sistema de geração de vapor.

Tabela 31 – Status do sistema de geração de vapor

Funções	Pronto	Operando	Resfriando	Resf. Alt.	Manutenção	Resf. emerg.	Injetando	Quente
FS1 - Gerar vapor	Pronta	Ativa	Inativa	Inativa	Inativa	Inativa	Inativa	Inativa
FS2 - Remover calor residual	Pronta	Pronta	Ativa	Pronta	Inativa	Ativa	Inativa	Pronta
FS3 - Injetar refrigerante	Pronta	Pronta	Pronta	Pronta	Pronta	Pronta	Ativa	Pronta
FR1 - Abrir passagem para trocadores	Inativa	Inativa	Inativa	Inativa	Ativa	Inativa	Inativa	Inativa
FR2 – Gerar calor	Pronta	Ativa	Inativa	Inativa	Inativa	Inativa	Inativa	Inativa
FR3 – Refrigerar secundário	Pronta	Pronta	Pronta	Ativa	Inativa	Inativa	Inativa	Pronta
FR4 - Prover água de alimentação auxiliar	Pronta	Pronta	Pronta	Pronta	Inativa	Inativa	Inativa	Pronta
FR5 - Fornecer refrigerante	Pronta	Pronta	Pronta	Pronta	Pronta	Pronta	Ativa	Pronta
FR6 - Resfriar em emergência	Pronta	Pronta	Pronta	Pronta	Inativa	Ativa	Inativa	Pronta
FR7 – Manter nível	Pronta	Ativa	Ativa	Inativa	Inativa	Inativa	Inativa	Inativa

4.7 Análise de cima para baixo nos componentes do gerador de vapor

Os geradores de vapor são um componente importante de um circuito primário e afetam a disponibilidade, eficiência, volume e segurança da usina como um todo. De acordo com a ANSI/ANS 51.1 [47], geradores de vapor tem papéis relativos à conversão de energia (gerar vapor) e à segurança nuclear (resfriar o núcleo em condição acidental). O papel desempenhado nos cenários acidentais impõe cuidados especiais ao longo de toda a vida da usina. Por exemplo, existem restrições de projeto, tais como projeto dos tubos de acordo com a ASME B & PVC, Seção III, Subseção NB (classe 1), que torna a construção uma ordem de grandeza mais cara. A razão é que a falha dos tubos causa acidentes de perda de refrigerante.

Se o projeto adotar o princípio de segregação funcional de acordo com os níveis de confiabilidade necessários, a solução resultante empregará trocadores diferentes para a geração de energia e resfriamento do núcleo. Assim a geração de energia pode usar trocadores de calor com padrão de qualidade industrial, que são grandes, mas podem ser uma ordem de grandeza mais baratos. A função de remoção de calor residual pode empregar trocadores de calor pequenos (dimensionados para cerca de 3% da potência nominal) de classe 1 que operam normalmente em prontidão, evitando desgaste. Wade afirma que a operação normal de geração de vapor desgasta os trocadores de calor (por exemplo, desgaste devido à vibração, fadiga, corrosão e fluência), causando vazamentos e perdas de tubos, levando a substituições inesperadas e indisponibilidade da usina. Em 1995, problemas nos geradores de vapor ficaram em segundo lugar como causa de indisponibilidade das usinas nucleares, perdendo apenas para o período de recarga de combustível [48].

O projeto deve prevenir falhas da barreira de pressão devido à falha de componentes que não sejam de classe 1. Uma solução para atender essa restrição e adotar o princípio de segregação funcional é colocar o trocador de calor para conversão de energia dentro da barreira de pressão. Assim, o fechamento das válvulas de isolamento de vapor tem a capacidade de parar qualquer vazamento que venha a ocorrer nos trocadores de calor.

Em suma, esta tese defende adotar soluções distintas para funções distintas, sendo um conjunto de trocadores com padrão industrial para converter energia e outro conjunto de pequenos trocadores para remover calor residual em emergência. Essa arquitetura foi nomeada de gerador de vapor híbrido e a Figura 46 apresenta seu diagrama de blocos funcional.

Figura 46 – Diagrama funcional do gerador de vapor híbrido

Como todos os componentes empregados no gerador de vapor são passivos ou tem comportamento trivial (estado aberto ou fechado das válvulas de isolamento), não é necessário estudar diagramas de estado.

5 RESULTADOS

Este capítulo tem o objetivo de apresentar as soluções propostas para alguns sistemas identificados no desenvolvimento, levando em conta todos os requisitos identificados no desenvolvimento.

5.1 Análise de baixo para cima no gerador de vapor

Abordando agora as tecnologias de troca de calor, existem inovações que podem tornar os reatores mais eficientes. Atualmente, a maioria dos geradores de vapor usam trocadores de calor do tipo casco e tubo, usando recirculação e secadores de vapor. Existem alguns geradores de vapor de um passe que fornecem vapor supersaturado (Babcock & Wilcox), que melhoram o ciclo térmico, mas precisam de melhor qualidade da água para evitar erosão da turbina [49]. Um tipo menos usado é o trocador de um passe em espiral, que foi empregado pelos geradores de vapor do NS Otto Hahn, que também fornecem vapor supersaturado [50]. Adicionalmente, existem novos tipos de trocadores baseados em placas e novos métodos de fabricação. Tais trocadores são menores, mais confiáveis e podem ser fabricados em série, sendo uma tecnologia que já é madura na indústria.

Um conceito promissor é o uso de trocadores de calor com micro canais dentro do vaso de pressão do reator [51], que reduz o volume e aumenta a confiabilidade. Outra opção é o emprego de trocadores de calor do tipo casco e placa (por exemplo, da GESMEX), tal como mostrado na Figura 47.

Figura 47 – Trocador de calor do tipo casco e placa

O volume reduzido de uma pilha de placas permite integrar todo o gerador de vapor dentro de um vaso de pressão sem aumentar muito o volume. A Figura 48 apresenta uma comparação de tamanho entre trocadores de calor do tipo casco e tubo (usados nas usinas atuais) e trocadores do tipo casco e placa (propostos nesta tese). Vale ressaltar que os geradores de vapor atuais, além dos trocadores em si, tem volumes para recirculação e para acomodar separadores e secadores de vapor.

Figura 48 – Comparação de tamanho para uma mesma potência

Para reduzir o volume total do gerador de vapor e a potência de bombeamento, uma solução é reduzir o tamanho de cada trocador de calor tanto quanto possível [52]. No caso, o menor modelo é o XPS50 da GESMEX (48 cm de diâmetro), e para maximizar a resistência a pressão usando materiais bem conhecidos, esta tese propõe o aço AISI 316L em placas de 1,25mm de espessura. A Figura 49 mostra como ficariam arranjados 42 conjuntos de pilhas de placas dentro do vaso de pressão.

Figura 49 – Vista superior do arranjo de pilhas de placas no gerador de vapor

Para reduzir o tempo de manutenção, tanto a água de alimentação como a saída de vapor devem conectar no topo de cada pilha de placas. As pilhas de placas ficam na vertical e o fluido secundário tem três passes enquanto o fluido primário tem um único passe para reduzir as perdas de carga, reduzindo a potência de bombeamento e melhorando a circulação natural. O arranjo vertical é normal para esse tipo de trocador de calor. A Figura 50 apresenta como tal trocador de calor poderia ser arranjado dentro do vaso do reator, sendo que o fluido primário é representado por setas azuis e o fluido secundário é representado por setas vermelhas.

Figura 50 – Arranjo proposto para o trocador de calor (não está em escala)

Uma vez que a válvula de isolamento de vapor fecha, vazamentos nas pilhas de placas não afetam a estanqueidade da barreira de pressão. Ao invés de confiar na qualidade dos componentes (tubos trabalhando em tração), essa proposta confia em segurança inerente (pilhas de placas trabalhando em compressão). Uma vez que o fluido secundário (menor pressão) fica na parte interna das pilhas, o modo de falha mais comum será o colapso das pilhas, que reduz a superfície de troca de calor, mas não causa acidentes. Assim, a arquitetura tem o efeito inerente de reduzir a gravidade e frequência dos vazamentos, bem como evita desgaste nos geradores de vapor de segurança.

A parte de segurança dos geradores de vapor não precisa ter o lado do fluido secundário em alta pressão, dispensando o uso de bombas de alimentação. Basta que o tanque contendo o fluido secundário receba o vapor condensado na contenção devido à troca de calor com o meio ambiente. Adicionalmente, a parte de segurança deve também poder injetar água no circuito primário caso este esteja despressurizado, evitando o descobrimento do núcleo.

A Figura 51 apresenta o arranjo geral do gerador de vapor proposto, sendo que a parte de conversão de energia fica dentro do vaso de pressão e a parte de segurança fica fora do vaso.

Figura 51 – Arranjo dos geradores de vapor

A Tabela 32 apresenta a configuração física para cada modo de operação do gerador de vapor, que são homônimos dos respectivos status.

Tabela 32 – Configuração física por modo de operação do circuito primário

Componente		Pronto/ Quente	Operando/ Resfriando	Resf. Alt.	Manutenção	Resf. emerg.	Injetando
Válvula de isolamento de vapor	de	Fechada	Aberta	Fechada	Fechada	Fechada	Fechada
Válvula de desvio de vapor		Fechada	Fechada	Aberta	Aberta, Fechada	Fechada	Fechada
Válvula de isolamento superior	de	Fechada	Fechada	Fechada	Fechada	Aberta	Aberta
Válvula de isolamento inferior	de	Fechada	Fechada	Fechada	Fechada	Aberta	Aberta
Válvula de injeção		Fechada	Fechada	Fechada	Fechada	Fechada	Aberta
Trocador placa	casco	Pronto	Operando	Operando	Pronto, vazio, limpando	Pronto, vazio	Pronto, vazio
Trocador tubo	casco e	Pronto	Pronto	Pronto	Pronto, vazio, limpando	Operando	Vazio

5.2 Análise de baixo para cima no circuito primário

São discutidas as três famílias de soluções já postas à prova de sistema de resfriamento de reatores a água pressurizada para navios. São elas: sistema com circuitos, vasos integrados e tubo dentro de tubo.

O sistema com circuitos é mais fácil de projetar e emprega um vaso de pressão para o reator, dois trocadores de calor para gerar vapor e um vaso de pressão para pressurizar o refrigerante. Foi empregado no NS Savannah e no NS Mutsu. Seu principal problema é a necessidade de duas blindagens: uma primária, para conter a radiação do núcleo e outra secundária, para conter a radiação do fluido refrigerante. Isso aumenta o tamanho e peso da usina nuclear. Além disso, as tubulações de fluido refrigerante são potencial fonte de grandes rupturas. Uma vantagem desse tipo de concepção é a grande potência nominal que a usina pode atingir por usar vasos de pressão distintos para gerar vapor e para fazer a reação nuclear.

O emprego de vasos distintos permite arranjar dentro do casco grandes trocadores de calor e núcleo porque esses vasos não estão na mesma vertical.

Um sistema com vaso integrado reúne os internos do reator, trocadores de calor para gerar vapor, bomba de circulação de refrigerante e o pressurizador em um único vaso de pressão. Essa concepção foi empregada no NS Otto Hahn, que não tinha pressurizador, ficando pressurizado na pressão de vapor da perna quente. Uma variante é o reator integrado francês empregado nas belonaves, que usa um pressurizador separado. A linha de surto do pressurizador se torna então uma fonte potencial de rupturas, o que exige a presença de acumuladores. A concepção integrada necessita de apenas uma blindagem e atinge níveis de dose na tripulação potencialmente mais baixos para um dado peso de blindagem. A concepção integrada também tem menos pontos de falhas que possam causar acidentes de perda de refrigerante. Uma desvantagem é a limitação da potência nominal, já que a localização de todos os componentes no mesmo vaso de pressão impõe limites de tamanho mais reduzidos aos trocadores de calor, dadas as limitações do casco.

A solução com tubos dentro de tubos tem vasos de pressão distintos para geradores de vapor e os internos do núcleo, sendo que a perna quente fica dentro da perna fria. Assim, a quantidade de potenciais falhas fica reduzida ao custo de aumentar um pouco a complexidade interna. Tal solução foi empregada no NS Sevmorput, que usa um sistema com ar comprimido para regular a pressão do fluido refrigerante. Usar tubos dentro de tubos representa uma solução intermediária entre os sistemas com circuitos e vaso integrado. A eliminação das tubulações dos circuitos de água pressurizada reduz o volume em comparação com o sistema com circuitos. Tal redução de volume reduz a blindagem por eliminar a necessidade de uma blindagem secundária, ainda que o tamanho da blindagem primária aumente. A separação em dois ou mais vasos de pressão permite alcançar níveis de potência elevados enquanto a segurança nuclear sofre pouca degradação.

Para este trabalho, adotou-se uma arquitetura com tubos dentro de tubos com pressurizador por meio de bolha de vapor em um vaso de pressão separado. Não foi possível empregar uma arquitetura integral porque o tamanho do vaso ficaria incompatível com o diâmetro do casco. Foi necessário empregar um vaso separado para pressurizar o fluido por que não havia espaço nos outros vasos. Além disso, existe risco tecnológico em tentar

integrar o pressurizador em outro vaso, já que isso seria uma inovação em relação às arquiteturas existentes.

Além disso, foi adotado um sistema de ejetores para mover o fluido refrigerante por uma série de razões. A primeira é facilitar a circulação natural em caso de falha da bomba principal, permitindo atingir um certo nível de potência mesmo sem a bomba. A segunda é permitir a homogeneização da temperatura no circuito primário por meio da vazão do circuito auxiliar. A terceira é empregar a vazão do circuito auxiliar para iniciar e estabilizar a circulação natural no circuito primário com operação em potência.

O tanque de compensação compensa o efeito da contração e expansão do fluido durante o aquecimento e resfriamento do circuito primário, bem como recebe descargas do circuito primário em caso de sobre pressão.

O núcleo do reator assumido foi apresentado em um trabalho anterior [53], cujos detalhes são apresentados na Tabela 33. Um componente muito importante para o circuito primário é o fluido refrigerante. Várias variáveis de processo são necessárias para identificar seu estado, já que as propriedades termodinâmicas da água são complexas. Pressão e temperatura do fluido refrigerante têm relações precisas por estado, tal como apresentado na Figura 54. Tal diagrama inclui limitações (linhas pretas) devido a limites máximos e mínimos de subresfriamento, de margem de pressão, de pressão de projeto (a quente e a frio) e pressão dos acumuladores.

Esse núcleo foi dimensionado usando critérios de projeto usados pela Westinghouse para o AP1000, descrito no *design control document* do reator. A Figura 52 apresenta a arquitetura do circuito primário proposto.

Figura 52 – Arquitetura do Circuito primário proposto

A Figura 53 apresenta um esquema simplificado do arranjo físico do circuito primário proposto.

Figura 53 – Esquema físico do Circuito primário proposto. TC é Tanque de compensação. GV é gerador de vapor. Pz é pressurizador. MAB é mecanismo de acionamento de barras

Um componente muito importante para o circuito primário é o fluido refrigerante. Várias variáveis de processo são necessárias para identificar seu estado, já que as

propriedades termodinâmicas da água são complexas. Pressão e temperatura do fluido refrigerante tem relações precisas por estado, tal como apresentado na Figura 54. Tal diagrama inclui limitações (linhas pretas) devido a limites máximos e mínimos de subresfriamento, de margem de pressão, de pressão de projeto (a quente e a frio) e pressão dos acumuladores.

Tabela 33 – Hipóteses de características do reator

Características do reator	Valor	Unidade
Número de elementos combustíveis	137	
Número de varetas por elemento	289	
Percentual de varetas combustíveis	90,25%	
Diâmetro externo dos tubos	0,0098	m
Comprimento dos elementos combustíveis	2,11	m
Largura do elemento	0,2207	m
Diâmetro do núcleo	3,04	m
Mínima razão de desvio da ebulição nucleada	2,05	
Temperatura de saída	323,7	°C
Variação de temperatura no núcleo	25,7	°C
Potência nominal	240	MWth
Margem de subresfriamento na perna quente	22,1	°C
Vazão mássica de refrigerante	1850	kg/s
Perda de carga no reator	4990	Pa

O limite direito é a temperatura máxima do refrigerante devido a limites mecânicos da contenção em caso de acidentes de perda de refrigerante.

É importante notar que em alguns casos, os status não têm zona contíguas e o fluido vai se deslocar de forma contínua nesse diagrama. Assim, quando o fluido está fora de um estado definido, o sistema de controle reconhece o estado corrente pelos status dos subsistemas, indicando que existe algo que precisa ser mudado (modo de operação degradado).

Figura 54 – Diagrama de pressão versus temperatura do circuito primário

Embora essencial para a descrição dos modos de operação, a pressão e temperatura do fluido refrigerante não são suficientes para identificar o modo de operação. O conteúdo de água líquida também é essencial para saber se o fluido está em condições de remover calor do núcleo do reator. Tal conteúdo é medido pelo nível do pressurizador em operação normal, e, em acidentes de perda de refrigerante, é medido pelo nível no vaso do reator. Apesar de importante e complexa, as variáveis do fluido refrigerante não são as únicas e muitas outras variáveis são empregadas para identificar os modos dos componentes do sistema.

A Tabela 34 apresenta os modos de operação dos componentes do circuito primário para cada status especificado na análise de cima para baixo. Essa tabela faz parte da análise de baixo para cima, onde verifica-se o atendimento aos requisitos com base na descrição dos componentes. Essa tabela inclui implicitamente hipóteses sobre os modos de operação dos componentes. Vale ressaltar que o sistema de controle não precisa ter um painel próprio, com um número de identificação do circuito primário. O sistema de controle, aqui

considerado componente do circuito primário, pode ser uma porção lógica dentro do sistema de controle da usina.

Tabela 34 – Configuração física por modo de operação do circuito primário

Sistema	Vazio	Desligado seguro	Recarga	Desligado a frio	Desligado a quente	Pronto	Em potência
De pressurização	Vazio	Desligado	Vazio	Desligado	Ligado	Ligado	Ligado
De bombas do primário	Desligado	Desligado	Desligado	Desligado	Desligado	Baixa velocidade	Baixa ou alta velocidade
De controle	Desligado	Emergência	Manual	Manual	Manual	Manual	Automático
De alimentação	Desligado	Desligado	Desligado	Desligado	Desligado	Desligado ou ligado	Ligado
De geração de vapor normal	Desligado	Desligado	Desligado	Desligado	Desligado	Desligado ou ligado	Ligado
De geração de vapor de emergência	Desligado	Ligado	Desligado	Desligado	Desligado	Desligado	Desligado
De compensação de volume	Vazio	Nível máximo	Nível mínimo	Nível mínimo	Nível mínimo	Nível máximo	Nível máximo
Barreira de pressão	Intacta	Com falha	Aberta	Intacta	Intacta	Intacta	Intacta
Nível no vaso do reator	Vazio	De vazio a cheio	Cheio	Cheio	Cheio	Cheio	Cheio
Nível no pressurizador	Vazio	Vazio	Vazio	Cheio	Baixo nível	Baixo nível	Baixo nível
Pressão do pressurizador	Atmosférica	Atmosférica	Atmosférica	7 a 22 bar	10 a 24 bar	75 a 166 bar	150 a 164 bar
Pressão do tanque de compensação	Atmosférica	1,2 a 2 bar	Atmosférica	7 a 22 bar	1,2 a 2 bar	1,2 a 2 bar	1,2 a 2 bar
Nível do tanque de compensação	Vazio	Nível máximo	Nível mínimo	Nível mínimo	Nível mínimo	Nível máximo	Nível máximo
Temperatura média refrigerante do	Não aplicável	De ambiente a 325°C	Ambiente	De 20 a 90 °C	De 125 a 180°C	De 230 a 315°C	De 300 a 315°C
Diferença de temperatura no núcleo	Irrelevante	Irrelevante	Irrelevante	Menor do que 10°C	Menor do que 10°C	Menor do que 40°C	Menor do que 40°C

A Tabela 35 apresenta o resultado do cálculo de desempenhos do sistema, que atendem os requisitos definidos previamente.

Tabela 35 – Características não funcionais do Circuito primário

Característica	Valor	Unidade
Massa (vazio)	728,6	ton.
Massa com água	879,3	ton.
Resistência a choque em todas direções	10	g
Potência nominal	240	MWth
Reserva de energia (operando a 75% da potência nominal 280 dias por ano)	20	anos
Tempo de vida	60	anos
Máxima rejeição de carga sem abrir válvula de segurança	90%	Pn
Taxa de falha da barreira de pressão para tubos de instrumentação	1e-5	f/ano
Taxa de falha da barreira de pressão para linhas grandes	1e-6	f/ano

5.3 Análise de baixo para cima na caldeira nuclear

Para efetuar a análise de cima para baixo na caldeira nuclear, foram feitas hipóteses acerca da arquitetura de seus principais sistemas. Assim, a contenção nuclear usa uma divisão horizontal para garantir que o fluido condensado nas paredes volte para o núcleo por ação da gravidade. Evidentemente, tal divisão tem limites de pressão limitados, da ordem de 5 bar de pressão relativa, exigindo o emprego de tanques de supressão de vapor em caso de perda de refrigerante. Para economizar espaço, os tanques de supressão serão parte do tanque de blindagem.

O sistema de resfriamento emergência do núcleo foi também assumido como sendo totalmente passivo, operando por ação da gravidade e circulação natural. Ele tem a mesma função do sistema de alimentação auxiliar em usinas nucleares a água pressurizada que estão em operação. Mas, ao invés injetar água em um gerador de vapor cujo fluido secundário fica na pressão de vapor da água na temperatura do circuito primário, esse sistema emprega um tanque aberto para a atmosfera da contenção para resfriar o gerador de vapor de emergência. No curto prazo, o sistema de resfriamento de emergência conta com a inércia térmica do seu tanque para resfriar o circuito primário por circulação natural. Caso os sistemas normais de remoção de calor residual não estejam disponíveis ou a barreira de pressão esteja comprometida, o sistema de depressurização automática entra em operação. Ele descarrega o vapor do pressurizador nos tanques de supressão, deixando a pressão do circuito primário igual à da atmosfera da contenção. No longo prazo, o sistema de resfriamento emergência depende da contenção para transferir o calor residual do núcleo para o

mar, bem como para retornar água condensada para o núcleo.

mostra a hipótese assumida sobre o arranjo físico da contenção nuclear.

Figura 55 – Esquema físico da contenção após acidente de perda de refrigerante

A Figura 56 apresenta o diagrama de blocos do resfriamento de emergência e da despressurização automática.

Figura 56 – Resfriamento de emergência e despressurização automática

A atuação da despressurização automática ou do sistema de resfriamento em emergência deve ser evitada por meio do uso do sistema de remoção de calor residual quando o sistema de conversão de energia não está disponível. A Figura 57 apresenta a hipótese de sistema de remoção de calor residual.

Figura 57 – Arquitetura do sistema de remoção de calor residual

Além dos sistemas de segurança, existem outras funções feitas em operação normal, tais como purificação da água do circuito primário, amostragem da água, remoção de calor residual quando desligado, desgaseificação, purga e homogeneização da temperatura no circuito. Todas essas funções são exercidas pelo circuito primário auxiliar. A Figura 58 apresenta a hipótese de arquitetura do circuito primário auxiliar.

Figura 58 – Esquema do circuito primário auxiliar

Mesmo sendo passivo, sistema elétrico tem papel fundamental na manutenção da instrumentação e atuação das válvulas que controlam os sistemas passivos. A Figura 59 apresenta o diagrama unifilar do sistema de alimentação elétrica, que conta com quatro baterias independentes.

Figura 59 – Diagrama unifilar do sistema de alimentação elétrica (de segurança)

Cada bateria pode manter o sistema de controle e de proteção até que a caldeira tenha atingido o status seguro mais 4 horas de operação, bem como atuar todas as válvulas de segurança. O sistema de alimentação elétrica e suas baterias atingem o nível de

confiabilidade do fornecimento de energia elétrica sem impor requisitos de qualidade nuclear ao sistema elétrico do navio. A Tabela 36 apresenta as propriedades gerais da caldeira nuclear.

Tabela 36 – Propriedades estimadas da caldeira nuclear

Característica	Valor	Unidade
Massa (vazio)	2390	ton.
Massa com água	2530	ton.
Volume ocupado	1948	m ³
Resistência a choque em todas direções	10	g
Taxa de falha da função de gerar vapor à potência nominal com restabelecimento dentro de 5 horas	0,1	f/ano
Taxa de falha da função de gerar vapor a 25% da potência nominal com restabelecimento dentro de 30 dias	0,01	f/ano
Disponibilidade dentro de 72h ao longo da vida	87%	
Frequência de derretimento do núcleo	1e-6	f/ano
Frequência de vazamento da contenção	1e-7	f/ano

Tabela 37 – Configuração física por modo de operação da caldeira nuclear

Sistema/variável	Em potência	Seguro	Prontidão 6h	Resfriando	Prontidão 72h	Recarga	Manutenção
De proteção	Operando	Operando, desligado	Operando	Operando	Operando	Operando	Desligado
De controle de reatividade	Automático	Desligado	Manual, pronto	Desligado	Desligado	Desmontado	Desligado, desmontado
De auxiliares da contenção	Pronto	Operando, desligado	Pronto	Pronto	Pronto	Desligado	Desligado
De contenção primária	Atmosfera estanque	Estanque total	Atmosfera estanque	Atmosfera estanque	Atmosfera estanque	Aberta	Aberta, atmosfera estanque
De resfriamento de emergência	Pronto	Resfriando, recirculando	Pronto	Pronto	Pronto	Desligado	Desligado
De núcleo e internos	Crítico	Subcrítico	Subcrítico	Subcrítico	Subcrítico	Trocando combustível	Sem combustível
De auxiliares do primário	Operando	Desligado	Operando	Operando	Resfriando	Resfriando	Desligado
De despressurização automática	Pronto	Despressurizando, aberto	Pronto	Pronto	Pronto	Desligado	Desligado
Circuito primário	Em potência	Resfriando em emerg., despressurizando, desligado seguro	Pronto	Resfriando normal, resfriando anormal	Desligado quente ^a	Recarga	Vazio
Remoção de calor residual	Pronto	Desligado	Pronto	Operando, pronto	Pronto	Desligado	Baixo nível
De ar condicionado	Operando	Desligado	Operando	Operando	Operando	Operando	Operando, desligado
De água de resfriamento	Operando	Desligado	Operando	Operando	Operando	Operando	Operando, desligado
De processamento de rejeitos	Pronto, drenando	Desligado	Pronto, drenando	Pronto, drenando	Pronto, drenando, esgotando	Pronto, drenando, esgotando	Pronto, drenando, esgotando
Calor residual (percentual da potência nominal)	De 0 a 7%	De 0 a 7%	De 0 a 1%	De 0 a 7%	De 0 a 1%	De 0 a 0,2%	0 (sem combustível)

5.4 Análise de baixo para cima na usina nuclear móvel

No projeto da usina nuclear móvel, o projeto deve considerar o problema de pesos e centros, haja vista que a usina deve flutuar. Este trabalho empregou técnicas de engenharia naval, usando um navio de referência para estimar pesos e volumes de pequenos itens que são usados em grande quantidade (cabos, tubos, suportes mecânicos, por exemplo). Além da reserva de flutuabilidade, este trabalho previu também uma reserva de lastro fixo de chumbo para permitir equilibrar de forma refinada a usina.

Para itens grandes, tais como a turbina principal, o gerador principal, condensador, diesel geradores e bateria principal, este trabalho assumiu como hipóteses folhas de dados de equipamentos existentes ou extrapolações. Dada a necessidade de manter o fornecimento de energia por um certo tempo após a perda do reator para não deixar o navio sem propulsão, a quantidade de óleo é considerável. Para evitar aumentar muito o tamanho da usina, a blindagem secundária usa óleo combustível, bem como a localização de tanques junto ao reator ajuda a reduzir a dose na tripulação.

A Figura 60 apresenta um esboço do arranjo de uma usina nuclear móvel. Em cinza claro são representados o casco e as estruturas. O sistema de gerenciamento é composto de pequenos gabinetes que ficam dentro das salas dos outros sistemas. A sua única grande estrutura é a sala de controle.

Figura 60 – Arranjo geral da usina nuclear móvel

A Tabela 38 apresenta as propriedades gerais da usina nuclear móvel, obtidas por extrapolação de um submarino nuclear.

Tabela 38 – Propriedades da usina nuclear móvel

Característica	Valor	Unidade
Deslocamento	8294	ton.
Diâmetro	11	m.
Lastro de chumbo	10,6	%
Reserva de flutuabilidade	10	%
Comprimento	94	m
Capacidade de geração nuclear	70	MWe
Capacidade de geração reserva (por meio de diesel geradores)	10	MWe
Autonomia da capacidade reserva	14	dias
Tripulação	21	pessoas
Custo de aquisição (overnight)	596	MUS\$
Custo de ciclo de vida	1317	MUS\$

A Figura 61 compara a usina proposta com um navio mercante da classe post panamax, evidenciando que tal usina seria compatível com o tamanho do navio.

Figura 61 – Comparação de tamanho da usina proposta com um navio

É importante lembrar que dada a complexidade da usina, os modos de operação são bastante flexíveis. Por exemplo, esteja o reator funcionando ou não, a usina precisa manter o fornecimento de energia para o navio, mantendo o modo de operação “Propelindo”, homônimo do status correspondente. A Tabela 39 apresenta a configuração física por modo de operação da usina.

6 ANÁLISE E DISCUSSÃO DOS RESULTADOS

A ideia central do trabalho é a definição formal de status (pacote de informação contendo as atividades relevantes ocorrendo simultaneamente nas interfaces) e que dois sistemas somente serão funcionalmente equivalentes se tiverem os mesmos status e fases. Essa definição é nova e melhor do que as noções existentes de modelo de comportamento porque é completa, é objetiva e sua simplicidade mitiga o problema de explosão de estados. Essa ideia em si é simples, completa e fácil de entender, sendo uma das bases para a construção do método. A simplicidade do conceito de estado fundamenta-se na definição matemática de sistema de Wymore [54]. Não pode ser mais simples por que ignora todos os detalhes internos ao sistema. É completa porque leva em conta todas as interfaces e interações com o ambiente. É fácil de entender porque é objetiva e permite a medida com instrumentos.

Uma fraqueza desta definição é a necessidade de ter todas as funções explicitamente declaradas, o que pode não ser muito fácil na prática. As pessoas tendem a deixar funções implícitas por desconhecimento ou por achar que são óbvias, dispensando declarações explícitas. Por exemplo, atualmente, sistemas integrados de controle tem acesso a todas as variáveis, indistintamente do nível hierárquico da informação. Por exemplo, quando existem funções de regulação no nível de um subsistema, o mesmo precisa receber informações de um componente e enviar comandos a outro. Neste caso, tanto o fornecimento de informações quanto a execução de ordens são funções dos componentes, mas em geral tais funções não são registradas como tal. Tipicamente, somente a especificação do sistema de controle registra estas funções e esquecemos que o sistema de controle apenas distribui a informação. A função de obter e fornecer a informação pertence ao componente, apesar de tipicamente haver um esquecimento deste fato. Isto é evidenciado pelo fato que só quem faz o projeto da instalação tem o poder de adicionar a instrumentação necessária à criação da informação.

Uma decorrência das definições propostas é a mudança no modo de medir o status de um sistema conduzido em malha fechada. Na literatura de controle moderno, tal medida é feita somente nas saídas do sistema. Como mostra a Figura 2, este trabalho defende que a medida deve ser feita em todas as funções relevantes, de acordo com definição de status.

O método é em essência fazer uma simulação mental exaustiva e registrada em uma tabela do comportamento de um sistema antes de partir para a montagem de um protótipo (real ou virtual).

A utilidade dessas definições deve-se à confusão existente em torno do conceito de estado, gerando problemas de pensamento e comunicação. Muitos autores definem estado como conjuntos de objetivos, outros, como configuração física. A maioria nem tem definição formal, valendo-se de noções puramente subjetivas. Dentro de uma equipe de projeto, essa confusão causa muito prejuízo devido aos erros de entendimento, construção de diagramas de estados excessivamente complexos e geração de riscos.

O método proposto é um rascunho, desenvolvido a partir da ideia central da tese e da lei construtal de Adrian Bejan. Não é algo definitivo, mas uma ideia inicial com um valor agregado muito importante para projetos de sistemas sócio técnicos complexos. O valor agregado é a redução de custo e risco no desenvolvimento de projetos.

Os requisitos do método podem ser aprimorados com o tempo e necessidades específicas de aplicações particulares, podendo haver edição, eliminação ou adição de requisitos. O que não deve mudar nunca é a necessidade de redução de energia e tempo para executar um projeto. Também não devem mudar as três funções de um canal de informação: facilitar a comunicação, reduzir o ruído e preservar a integridade da informação.

Outra ferramenta muito discutida atualmente é a linguagem gráfica SysML, que deriva da UML e que serve para criar modelos de sistemas [6] [7]. Alguns diagramas e conceitos presentes nessas linguagens tem paralelo com os conceitos e definições propostos por esta tese. Não por coincidência, existem paralelos entre os conceitos propostos e os conceitos desenvolvidos ao longo do tempo na UML e posteriormente, SysML. Porém, existem diferenças advindas de uma série de fatores, tais como:

- Sistemas de informação podem mudar seu estado (valores de variáveis) com uma simples atribuição, ou seja, em tempo virtualmente nulo;
- Sistemas de informação tem flexibilidade intrínseca, podendo definir máquinas de estado de maneira arbitrária, necessitando apenas respeitar restrições lógicas e funcionais. Outros produtos têm restrições impostas pelas leis naturais. Por exemplo, um motor precisa de combustível, de suportes mecânicos, de interface com o usuário para poder cumprir sua missão;
- O aumento da complexidade funcional de sistemas de informação tem custo muito reduzido, se comparado com outros produtos de engenharia (por exemplo, sistemas mecânicos, sistemas de fluido, sistemas elétricos). A redação de uma classe já é uma solução per si, enquanto que o paralelo de uma classe em relação a uma máquina (no contexto deste trabalho, tal paralelo é um sistema) é só uma especificação. A máquina

precisa ainda de um projeto, que abordará muito mais informação do que a especificação. Além do projeto, a máquina precisa ainda ser construída para que possa ser posta em operação;

- A organização industrial para produção de sistemas de informação é muito mais simples do que daquelas de sistemas sócio-técnicos complexos. Uma empresa produtora de softwares tipicamente desenvolve a especificação de software a partir de diretrizes gerais do cliente, desenvolve o código fonte, testa e entrega o sistema de informação. Uma empresa produtora de sistemas sócio-técnicos complexos começa o projeto de maneira similar a um projeto de sistema de informação: a partir de diretrizes muito genéricas, ela desenvolve uma especificação mais detalhada. Depois ocorrem sucessivos ciclos de especificação e projeto a níveis cada vez mais baixos da decomposição do produto, até o nível que seja possível encontrar um fornecedor externo. A empresa então contrata um conjunto de fornecedores e orquestra o desenvolvimento de cada componente. Depois da entrega dos componentes, existe a necessidade de realizar atividades de integração, verificação e validação a cada nível da decomposição do produto (ciclo V). Somente após a integração no nível do topo a empresa pode entregar o sistema;
- As incertezas do projeto de sistemas sócio-técnicos complexos são muito maiores do que aquelas envolvidas no projeto de sistemas de informação. O conhecimento que programadores tem acerca das possibilidades e limitações das ferramentas de software é mais preciso do que o conhecimento dos engenheiros (encarregados da especificação de sistemas) sobre os produtos disponíveis. As incertezas geram riscos, principalmente se não forem gerenciadas;
- O ciclo de desenvolvimento de software é mais rápido do que ciclos de desenvolvimento de sistemas sócio-técnicos complexos. Durações maiores levam a maiores custos, bem como a maiores riscos;
- No projeto de sistemas de informação, a mesma organização faz a especificação e desenvolve a solução. Em projetos sócio-técnicos complexos, a empresa integradora apenas faz a especificação e os fornecedores projetam, desenvolvem, fabricam e entregam os componentes. Ou seja, ocorre a separação formal (e institucional) entre especificação (identificar o problema) e projeto (desenvolver uma solução para um problema).

Tais fatores fazem com que os conceitos de engenharia de software, apesar de úteis, fiquem insuficientes para o trabalho de engenharia de sistemas, que requer a separação formal entre necessidades e soluções. Tal separação facilita a gerência de risco, a comunicação e cooperação entre organizações, bem como abre espaço para a criatividade e evolução. Assim, este trabalho define conceitos específicos para desenvolver especificações e outros conceitos específicos para fazer projeto de produtos. Para lidar com as incertezas, os conceitos relacionados às especificações são intencionalmente vagos e limitados ao que deve ser feito e aos inconvenientes aceitáveis. Qualquer informação extra aumenta o risco de inviabilidade sem agregar valor ao projeto.

Tabela 40 – Comparação com UML

Conceito proposto	Paralelo da UML/SysML	Diferenças
Sistema	Classe	Um sistema especifica uma família de produtos restringindo um subconjunto de suas características enquanto uma classe define totalmente os atributos e métodos dos objetos a serem instanciados. Um sistema meramente define um problema enquanto uma classe é uma solução. Dada a natureza parcial do sistema em termos de informação, existe a necessidade de descrever os produtos que venham a atender aos requisitos do sistema.
Produto	Objeto	Um produto não tem necessariamente um sistema que o especifica, bem como sua realização depende de muito mais informação do que aquela contida em um sistema. O contrário ocorre com um objeto que é produzido a partir das instruções contidas em uma classe.
Interface	Interface	Interface no contexto deste trabalho é uma especificação flexível da superfície de contato entre dois sistemas, enquanto interface de UML é uma definição exata de atributos e métodos a ser incorporada em uma classe por meio de herança. O paralelo dos dois conceitos é muito grande já que interfaces entre dois sistemas são entidades imateriais que impõem características a um sistema existente, mas nunca especifica um produto per si.
Função	Método	Função de um sistema é um objetivo ou uma ação física desejada que o sistema deve efetuar enquanto método é um algoritmo com entradas e saídas. Ou seja, uma função é uma descrição do que deve ser feito, enquanto que um método é uma definição de como fazer.
Propriedade (de produto)	Atributos	Propriedade de produto é uma grandeza física, mensurável e com unidade de medida (por exemplo, massa, volume, dimensões, potência, pressão de projeto, eficiência) enquanto atributos são dados, tais como texto ou números.

Conceito proposto	Paralelo da UML/SysML	Diferenças
Requisitos não funcionais	Qualificadores de atributos (faixas)	Os requisitos não funcionais de um sistema servem para declarar os limites aceitáveis dos inconvenientes causados por um sistema, impondo limites para certas propriedades do produto (por exemplo, tamanho máximo, massa máxima, custo máximo). Na definição das classes, dependendo da linguagem, é possível estabelecer faixas de valores aceitáveis para um certo dado.
Status	Caso de uso	Um status é uma situação de uso do sistema, definido como uma maneira de interagir com o resto do universo. Um caso de uso é uma situação de uso de um sistema informatizado por um dado usuário. O conceito de status é mais genérico por abranger interações de qualquer tipo de sistema (pessoas, máquinas, sistemas informatizados) e mais completo por levar em conta todas as funções relacionadas ao sistema.
Fase	Requisito de transição	Fase não tem um conceito similar em UML, mas funciona como um requisito de criação de um procedimento de mudança de modo de operação em um produto.
Equivalência	Herança	Equivalência indica que um sistema atende os mesmos status e fases de outro, similar ao conceito de herança, que indica que uma classe tem os mesmos métodos e atributos de outra.
Diagrama funcional	Diagrama de colaboração	O diagrama funcional se assemelha a um diagrama de colaboração. A diferença é o contexto de separação formal entre especificação e projeto (diagrama funcional é exclusivo da especificação), enquanto um diagrama de colaboração representa objetos, que não são definidos tendo em vista a separação formal entre especificação e projeto.
Diagrama de status	Diagrama de máquina de estado	O diagrama de status faz parte da especificação, enquanto que o diagrama de máquina de estado está relacionado à programação do comportamento dos objetos, o que se aproxima de uma atividade de projeto da solução.
Procedimento	Transição (do diagrama de máquina de estado)	Devido às leis naturais, os procedimentos requerem uma série de ações por parte dos componentes do produto ou mudança de status de funções recebidas, e requerem um tempo considerável para ocorrer. Transições, por outro lado, são tipicamente meras atribuições de variável e ocorrem em tempo virtualmente nulo.
Modo de operação	Estado (do diagrama de máquina de estado)	O modo está sempre limitado pela física e pela intenção do usuário. Isso quer dizer que para um produto assumir um modo de operação, ele precisa de uma série de condições físicas (fornecimento de energia, recursos e suporte). Estado é um conceito lógico e pode mudar livremente de acordo com a intenção, bastando fazer uma atribuição de variável para mudar um estado. Somente limitações lógicas restringem mudanças de estado.

Os conceitos deste trabalho teoricamente são mais eficientes do que aqueles empregados na SysML porque são adaptados às relações de poder típicas dos projetos de engenharia de sistemas. A UML e SysML são produtos de relações de poder típicas de desenvolvimento de software, que são mais simples, dada a facilidade relativa do desenvolvimento de software. Por exemplo, ao empregar os conceitos de SysML, os fornecedores tendem a resistir a aprender uma nova linguagem. Mesmo que aprendam, eles tendem a não aceitar que o cliente faça parte do projeto (especificação em caixa branca), impondo arquiteturas, modelos, equações e até dimensionando componentes internos do produto. Isso se deve a dois fatores. O primeiro fator é a dificuldade natural de dois arquitetos concordarem acerca de qual é a melhor solução, principalmente se não houver critérios objetivos para escolha de alternativas. O segundo fator é a força relativa entre as partes, na qual o lado que agregar mais valor ao produto terá maior poder de barganha, podendo reduzir a margem de lucro da outra parte. Sendo o projeto parte do valor agregado do produto, provavelmente os fornecedores não querem perder tal tarefa para o comprador.

Por outro lado, parte dos conceitos de engenharia de software e sua representação gráfica podem ajudar no trabalho de engenharia empregando os conceitos e a metodologia desta tese. Por exemplo, o diagrama de máquina de estados é útil para mostrar os status e fases de um sistema. O diagrama de colaboração pode mostrar os subsistemas e as funções técnicas de um sistema. O diagrama de classes pode mostrar os sistemas e subsistemas, bem como as relações de equivalência, que se usadas inteligentemente podem reduzir o trabalho de especificação por meio de reuso de sistemas. Diagramas de atividade podem descrever os procedimentos de mudança de modo de operação de um produto.

Concluindo, esta tese não descarta os conceitos de engenharia de software, apenas os aperfeiçoa para o uso em engenharia de sistemas, fazendo a distinção formal entre necessidades e soluções. Esta tese propõe um método de especificação que melhora o diálogo entre clientes e fornecedores por formalizar o papel de cada um. Além disso, reduz o tempo para o projeto de um produto por impor que a especificação inclua um modelo comportamental simplificado. Isso evita que o fornecedor tenha que lançar um número de hipóteses e depois retrabalhar a solução na integração, o que costuma dar prejuízo para o cliente.

Existe uma relação harmônica com os conceitos do PMBOK, sendo que as atividades desta metodologia são detalhamentos dos processos do PMBOK. O grupo de processos de planejamento está, grosso modo, relacionado à análise de cima para baixo e o

grupo de processos de controle e monitoração está relacionado à análise de baixo para cima. Essa metodologia fica restrita à definição técnica da solução, deixando de lado aspectos como recursos humanos ou gerenciamento de *stakeholders*. Ou seja, essa metodologia dá um suporte à parte técnica do projeto, implementando processos de maneira otimizada de acordo com a lei construtal (melhorando os fluxos dentro do projeto). A Tabela 41 apresenta a relação de processos do PMBOK com esta metodologia. Vale ressaltar que essa metodologia assume a existência de uma equipe de projeto com vários níveis hierárquicos que executam essa metodologia em paralelo.

Tabela 41 – Relação com alguns processos PMBOK

Processo PMBOK	Implementação por esta metodologia
5.2. Coletar os requisitos	Executado pelo arquiteto durante os estados “Identificando funções”, “identificando transições” e “alocando propriedades”
5.4. Criar a estrutura analítica do projeto	Executado pelo arquiteto durante os estados “Identificando subsistemas”
6.2. Definir as atividades	As atividades para o desenvolvimento da solução técnica são definidas na
	Figura 28
6.3. Sequenciar as atividades	O sequenciamento das atividades de desenvolvimento é também apresentado na
	Figura 28
7.1. Planejar o gerenciamento dos custos	Executado pelo arquiteto durante os estados “Alocando Propriedades” e “Calculando Propriedades”
7.3. Determinar o orçamento	Executado pelo arquiteto durante os estados “Alocando propriedades”
8.1. Planejar o gerenciamento da qualidade	Feito pela definição de sintaxe para requisitos e pela definição de uma lista de requisitos numerados
11.1. Planejar o gerenciamento dos riscos	A metodologia prevê esse gerenciamento em duas etapas: “Alocando propriedades” (de cima para baixo) e “Analisando riscos” (de baixo para cima)
11.4. Realizar a análise quantitativa dos riscos	Executado pelo arquiteto durante o estado “Analisando riscos”
11.5. Planejar as respostas aos riscos	A metodologia prevê retorno ao início da análise de baixo para cima caso existam riscos inaceitáveis
5.5. Validar o escopo	Executado pelo arquiteto durante o estado “Verificando o atendimento”
7.4. Controlar os custos	Executado pelo arquiteto durante o estado “Calculando propriedades”
11.6. Controlar os riscos	Executado pelo arquiteto durante o estado “Verificando atendimento”

Uma pessoa executa parte de cada processo a seu nível, sendo que cada arquiteto executa vários processos, tais como coletar requisitos, criar a estrutura analítica, determinar orçamento, realizar análise de risco e validar o escopo.

Existem também processos do PMBOK que não são abordados diretamente, mas que são facilitados pela metodologia proposta. Um exemplo é a atividade “4.4. Monitorar e controlar o trabalho do projeto”, que é facilitado por meio da definição de estado, que permite monitorar o andamento por meio da observação das interfaces. Ou seja, as atividades desta metodologia foram concebidas para otimizar o controle. Outro exemplo é o processo “8.3. Controlar a qualidade” que pode ser executado por meio da verificação dos requisitos numerados.

O desenvolvimento é incompleto, tratando-se de um exemplo para facilitar a compreensão e ilustrar como a ausência de um método nos deixa escapar o óbvio. O projeto completo de todos os componentes em todos os níveis ocuparia muitas páginas e seria impossível para uma única pessoa realizar ou avaliar dentro do prazo.

Ainda que possa conter erros, acredita-se que a análise apresentada possa servir de base para outros estudos. Por ser uma análise modular, feita a cada nível de maneira independente dos níveis inferiores, as soluções apresentadas podem ser substituídas facilmente por outras tecnologias melhores.

Pode-se questionar o emprego de métodos racionais para questões ligadas à política, que é um assunto humano e não sujeito à razão. Por outro lado, esse é um trabalho científico, cujo valor não é medido pela popularidade de seus conceitos, mas pela aderência à realidade, pelo rigor acadêmico e por sua utilidade prática. Além disso, apesar de envolver a sociedade, este trabalho é estritamente limitado às soluções técnicas.

No desenvolvimento deste trabalho não foram empregadas hipóteses de aceitação social ou crenças de uma dada população. Foram empregados fatos físicos, tais como economia de escala, necessidade de blindagens espessas, riscos de perda de fornecimento de energia e alimentos. Nenhum destes conceitos precisa de aprovação da opinião pública para serem verdadeiros, ainda que sejam, talvez, conceitos desconhecidos da população em geral. É verdade que este trabalho pode ser inútil para uma população que não aceite a ciência, tal como a obra de Galileu não foi útil à Igreja Católica. Mas o fato de ser inútil para uma dada população em certo período histórico não invalida o teor científico de um trabalho.

Um aspecto importante é que, não obstante abordando temas políticos, este trabalho versa exclusivamente sobre possibilidades técnicas em função das leis físicas conhecidas. A aceitação da energia nuclear por parte do público é um aspecto humano e um problema que requer estudos aprofundados. Já existem estudos que demonstram que uma simples palestra de conscientização com estudantes é suficiente para causar mudanças significativas de postura [55]. Assumindo que as pessoas buscam o benefício e evitam malefícios, e que não surja outra fonte de energia melhor, no longo prazo os povos adotarão a energia nuclear devido à segurança, baixo custo ambiental e econômico.

Naturalmente, apesar da inevitável oposição, se o público tiver sido informado corretamente, a maioria da população irá preferir o usufruto da energia nuclear. É fato que os navios nucleares da marinha dos Estados Unidos são aceitos em 150 portos de 50 países [19]. Existem movimentos contra a energia nuclear, mas, formalmente, a aceitação da energia nuclear é ampla nos dias de hoje. Especificamente na Europa, vem ocorrendo um movimento formal de abandono da energia nuclear em vários países. Mas na prática, as usinas na Alemanha têm sido substituídas por usinas na Rússia. No oriente, a quantidade de usinas vem aumentando nos últimos anos, e o sucesso nesses países levará outros países a questionar e abandonar o posicionamento anti-nuclear. Afinal, nenhum povo fica satisfeito de ver outro adquirir um padrão de vida melhor, nem de ficar vulnerável economicamente, o que traz inconvenientes políticos.

Evidentemente, as pessoas naturalmente resistem a mudanças, e se as autoridades não fizerem uma campanha de conscientização, podem haver bloqueios populares, tais como no caso do NS Mutsu [56]. Então, a solução é manter um canal de diálogo com a população para transmitir fatos relevantes, tal como a energia nuclear ter menos mortes por unidades de energia [57] do que outras fontes. Adicionalmente, os impactos ambientais de uma usina nuclear são menores do que a maioria das outras opções [57].

Outro aspecto é a questão da não proliferação nuclear, pois o emprego de uma frota nuclear mercante aumentaria muito a chance de roubo de material radioativo. Isso não se constitui um risco inaceitável porque as usinas são belonaves com resistência a choque, tripulação militar e meios de autodefesa. Relembra-se que a tripulação deve ser militar para impossibilitar a ocorrência de greves gerais nas tripulações das usinas e para assegurar a obediência em caso de guerra. Mesmo que um grupo terrorista fosse capaz de tomar uma usina, por meio da comunicação com a base, a Marinha seria acionada para partir em resgate.

A mesma embarcação destinada a socorrer as usinas após um acidente deve ter meios de coação violenta tais como canhões e metralhadores para submeter possíveis piratas.

Considerando que o reator tem grandes dimensões e que a remoção do urânio é uma operação complexa que leva dias, não haveria tempo para o roubo. Existe sim, o risco de uma potência mais poderosa sequestrar a usina. Para reduzir esse risco, os meios de desacoplar do navio que ela alimenta devem estar na usina, bem como a tripulação deve ter meios de afundar a usina deliberadamente. Além disso, podem ser empregadas tecnologias inerentemente seguras, tais como reatores a sais fundidos de tório. O fato é que não é usual piratas ou terroristas tentarem roubar urânio de navios militares.

Não se pode afirmar que as soluções desenvolvidas neste trabalho estão corretas e sem erros, e que, se construídas, seriam bem-sucedidas. O que se pode afirmar é que esse método facilita a identificação dos erros que porventura tenham sido cometidos. Uma pessoa não se torna imediatamente mais competente pela simples adoção deste método. Apenas seu trabalho se torna mais conciso, completo e fácil de ser analisado e suas deficiências ficam mais expostas.

O método proposto exige que a especificação de um sistema e o projeto de um produto lancem mão de hipóteses realistas, o que é algo subjetivo e que requer conhecimento. Essa fraqueza, porém, é comum a qualquer método de engenharia e é uma dificuldade intrínseca da profissão. Por outro lado, o método proposto registra formalmente as hipóteses tomadas durante o projeto, por exemplo, facilitando a correção por parte de uma auditoria independente.

Acredita-se que a concisão faz com que as pessoas se tornem mais produtivas, pois, a ausência de ruído aumenta a quantidade de trabalho líquido. A completude do trabalho leva à correção ou minimização das deficiências da pessoa que usa esse método após um período longo. A facilidade de análise aumenta a produtividade pela simples redução de tempo e energia gastos para ler, entender e criticar o trabalho. A facilidade de análise também aumenta a quantidade de erros de concepção identificados durante a revisão. Assim, por ter seus erros apontados com mais rapidez, por corrigir deficiências e produzir um trabalho fácil de revisar, uma pessoa desenvolve competência mais rápido se empregar esse método.

Acredita-se também que esse método é inicialmente desagradável para a maioria das pessoas por impor uma série de obrigações durante a concepção. O método exige decisões não habituais, tais como taxa de falha, tempo de reparo, flexibilidade, tempo de

operação e parada. Impede também a livre expressão ou demonstração de conhecimento, exigindo uma exposição simples e direta da solução adotada. Além disso, engessa a construção dos requisitos, evitando estilos pessoais e floreios estéticos.

Por outro lado, acredita-se que esse método torna o trabalho mais motivante a longo prazo por preservar a autonomia de todos. Inversamente à engenharia tradicional que pensa em soluções, esse método pensa somente em problemas, onde cada sistema é um problema a ser definido de maneira completa. Assim, cada projeto é um desafio diferente e cada pessoa tem seu espaço de decisão respeitado pelos níveis hierárquicos superiores.

A formação necessária para aplicar este método não é muito complexa. Bastam conceitos de análise de risco, análise de confiabilidade e balanço de massa e energia. Conceitos sofisticados de física, termodinâmica e mecânica somente são necessários quando os componentes básicos são projetados. Por outro lado, em geral, os componentes básicos são projetados por fornecedores especializados, o que desobriga uma equipe de projeto a ter muitas competências.

Assim pode ser afirmado que esse método é eficiente em termos de custos de treinamento de pessoal por exigir poucos conhecimentos além da graduação. Esse é um aspecto muito importante, pois o custo e o tempo de aprendizagem representam um dos maiores problemas ao crescimento e manutenção da equipe. De acordo com a lei construtal, a redução de custo representa facilitar o fluxo.

O fundamento dessa tese é matemático, ou seja, é puramente um estado de mente sem qualquer hipótese na realidade, é algo abstrato. Na prática isso significa que o campo de aplicação do método proposto é vasto, abrangendo qualquer entidade que possa ser identificada, individualizada e com interfaces definidas. Como exemplos, podem ser incluídos: gestão de negócios, projetos de sistemas sócio-técnicos complexos, automação de sistemas e até direito constitucional.

Em gestão de negócios, o papel de uma pessoa pode ser visto como um sistema, e as diversas formas de interação com outras pessoas são os estados. Uma empresa de serviços é um sistema, e as formas de interação da empresa com clientes e fornecedores ao longo de um contrato são seus estados.

Em automação, a noção de estado é muito usada, mas existe muita confusão sobre a definição de estado, bem como decisões infelizes no sentido de identificar os estados do um sistema. Em Three Miles Island, o projetista decidiu exibir para o operador o último comando como o estado de uma válvula, ao invés de usar chaves de fim de curso para

monitorá-la. Durante o acidente, a válvula estava travada devido a um erro de manutenção, mas quando os operadores comandaram o fechamento, ela foi mostrada erroneamente como fechada. Esse erro foi uma das causas do derretimento do reator.

Vale ressaltar que a EDF começou a partir dos anos 1995, uma nova abordagem para condução das usinas nucleares, chamada abordagem por estados. Foi identificada a necessidade de monitorar o estado do fluido refrigerante dentro do reator para permitir a correta tomada de decisão por parte dos operadores. Autoridades francesas consideram que tal abordagem aumentou a segurança e simplificou os procedimentos, exigindo menos dos operadores. Esse projeto da EDF faz parte de uma tendência mundial, que busca de maneira ad hoc simplificar e melhorar projetos existentes de automação e controle. Tal fato se alinha com a ideia central deste trabalho que preconiza a identificação dos estados por meio da monitoração das interfaces. Esse exemplo mostra também que a ideia central da tese tem valor já comprovado na indústria nuclear. Uma vez que não existe uma teoria formal dando base à abordagem por estados da EDF [35], este trabalho agrega valor por formalizar de maneira matemática um conceito útil para projeto e não somente aperfeiçoamento.

Quanto à viabilidade econômica, o trabalho de O'Rourke [19] traz uma série de considerações sobre os aspectos econômicos do emprego de energia nuclear para diversos tipos de navios. Como já falado anteriormente, grandes reatores são muito mais baratos do que pequenos em termos de custo de ciclo de vida por unidade de energia produzida. Para cada tipo de navio (navios aeródromos, navios anfíbios e grandes escoltas) O'Rourke traz preços do petróleo bruto que tornariam mais barata a energia nuclear [19]. A Figura 62 apresenta o custo do barril em função da potência média consumida assumindo que uma belonave opera a 15% de sua capacidade nominal, em média [58].

Assumindo que a usina nuclear móvel atinja a disponibilidade desejada de 87% e que durante este período ela seja empregada 75% do tempo na potência nominal, a potência média fornecida seria de 41,8MWe.

O preço do petróleo foi calculado por meio da média do petróleo cru de Illinois, nos últimos 20 anos, corrigida pela inflação [59]. Com base nas informações expostas na Figura 62, é possível concluir que tal usina móvel é economicamente viável por ser um pouco mais barata do que o petróleo, desde que as hipóteses assumidas se provem verdadeiras. Da Figura 62 também pode levar a considerar questionável a decisão de construir uma usina que forneça uma potência elétrica média inferior a 25 MWe. Do ponto de vista econômico, a

mínima potência térmica, mantidas as hipóteses adotadas para essa usina proposta, seria por volta de 145MWth térmicos.

A redução de custo devido à produção em massa (curva de aprendizado) pode ser nula ou até negativa, pois a base de comparação leva em conta custos de reatores que são produzidos em quantidades da ordem de dezenas. De acordo com O'Rourke [19], a marinha americana declarou que os custos poderiam abaixar cerca de 7% ao aumentar a produção de reatores nucleares em uma unidade a cada dois anos. Evidentemente, tais ordens de grandeza estão balizadas por uma realidade específica que pode não ser observável em outro contexto, porém evidenciam que os ganhos potenciais com a curva de aprendizado são pequenos.

Vale ressaltar que o petróleo tem um preço muito volátil, sendo que sua média anual variou de 17,9 a 103,7 dólares, corrigida pela inflação nestes últimos 20 anos. Do ponto de vista de planejamento e gestão de risco, a volatilidade tem que ser compensada com margens financeiras que oneram a taxa de retorno sobre o capital investido. Assim, a solução nuclear fica ainda mais barata pela menor volatilidade no preço do combustível e da menor sensibilidade do custo em relação ao minério de urânio. Tais considerações são feitas à luz da experiência da marinha dos Estados Unidos, que empregam reatores militares com alto grau de enriquecimento [60] e resistência a choque de 50 g [58].

Consistente com O'Rourke são os estudos do JAERI [61] que propõem um reator integrado a água pressurizada para navios mercantes (MRX). Estes estudos indicam que para navios com potência no eixo na faixa de 50 a 60 MW, a energia nuclear seria economicamente comparável a motores diesel. Para navios ainda maiores, a energia nuclear seria ainda mais competitiva. Dois fatores podem explicar a diferença nas ordens de grandeza da potência competitiva mínima entre os dois estudos (cerca de 25MWe na Figura 62 contra 50MW do JAERI). Em primeiro lugar, a análise da figura usa potência média efetiva ao longo da vida da usina enquanto o JAERI adota a potência instalada na linha de eixo, que é maior. Em segundo lugar, O'Rourke leva em conta custos logísticos do combustível militar, o que adiciona cerca de 15% de custo em cima do preço de mercado do óleo cru [19]. A solução proposta pode ser construída com tecnologias já postas à prova na indústria, o que reduz o risco tecnológico e provavelmente são mais baratas do que as tecnologias militares usadas como referência na Figura 62.

Figura 62 – Efeito da potência sobre o custo da energia

Outro conjunto de evidências acerca da potência necessária para atingir preços competitivos são as potências nominais das barcas flutuantes russa (KLT-40S [15]) e chinesa (ACPRS-50). Não é possível determinar com certeza se a energia nuclear é seguramente competitiva, pois cada país parece ter experiências distintas quanto ao custo e sua evolução no tempo [62]. Por exemplo, nos Estados Unidos houve um crescimento do custo ao longo do tempo, enquanto que na Coreia do Sul o custo foi reduzindo à medida que a experiência em construção amadurecia. Além disso, o custo global na Coreia sempre foi mais baixo do que nos Estados Unidos [62]. O que é certo é que países com sistemas de fornecimento de energia e de transporte menos eficientes ficarão para trás em um mundo globalizado, o que torna arriscado desconsiderar a opção nuclear.

Vale ressaltar ainda que os estudos mencionados adotam como base soluções nucleares vinculadas aos navios, enquanto a proposta desta tese propõe um módulo destacável. Considerando que a vida útil de um navio é de cerca de 25 anos e que a vida da usina nuclear móvel pode atingir 60 anos, pode-se afirmar que esta proposta torna a energia nuclear mais atrativa. Tal atratividade vem do maior fator de uso (o ciclo de manutenção do reator fica desacoplado do ciclo de manutenção do navio) e do menor impacto do custo de aquisição (uma vida mais longa dilui o custo) no preço da energia fornecida. Assim, existem evidências sólidas da viabilidade econômica de usinas nucleares móveis com potências

nominais elétricas acima de 60 MWe para navios, ilhas, plataformas de petróleo e regiões remotas.

Com as hipóteses e dados da Tabela 42, este trabalho levantou os custos por contêiner para várias capacidades em termos de TEU, para três opções distintas: navios convencionais a diesel, navios nucleares e navios modulares recebendo energia elétrica de um módulo nuclear.

Tabela 42 – Hipóteses adotadas na estimativa de custo

Parâmetros de hipótese	Valor / fórmula	Unidades
Preço do óleo combustível	415 [59]	US\$/ton
Despesa com tripulação por pessoa	0,12	MUS\$/ano
Tripulação de um navio a diesel	14 [61]	Pessoas
Vida útil de um navio a diesel	25 [37]	Anos
Custo operacional	$375,83 \times TEU^{0,396}$ [63]	US\$/dia
Consumo de diesel	$3,8548 \times (P_{\text{eixo (hp)}}/1000)^{0,9412}$ [63]	Ton/dia
Custo de aquisição de um navio a diesel	$0,1727 \times TEU^{0,7022}$ [63]	MUS\$
Preço do combustível nuclear	3 [61]	MUS\$/ton
Despesa com tripulação nuclear por pessoa	0,144	MUS\$/ano
Tripulação da usina nuclear móvel	21	Pessoas
Vida útil de uma barca	25	Anos
Vida útil de uma usina nuclear móvel	60	Anos
Deslocamento de usina nuclear móvel	9000	Ton
Lucro líquido da empresa nuclear	10%	
Fator de uso da usina	75 [37]	%
Taxa de queima média do combustível	28,89 [61]	MW*dia/kg
Eficiência do ciclo térmico	25%	
Custo do casco da usina nuclear móvel	$0,0035 \times \text{Deslocamento}_{(\text{ton})}$ [61]	MUS\$
Custo da turbina e gerador	$3,55 \times (\text{Pot. no eixo (hp)}/1000)^{0,6}$ [61]	MUS\$
Custo do reator da usina nuclear móvel	$43,205 \times \text{Pot. Térmica (MW)}^{0,4524}$ [19]	MUS\$
Custo de aquisição da barca	$0,1727 \times TEU^{0,7022} - 210 \times P_{\text{eixo (hp)}/1000}$	MUS\$
Custo do reator de um navio nuclear	$43,205 \times P_{\text{thermal_MW}}^{0,4524}$ [19]	MUS\$
Custo do casco e propulsão do navio	$0,1727 \times TEU^{0,7022}$ [63]	MUS\$
Velocidade	23 [63]	Nós
Número de viagens	20 [61]	/ano
Taxa de ocupação dos contêineres	75 [61]	%
Dias em operação	280 [37]	/ano
Potência no eixo (Peixo)	$0,3799 \times TEU^{0,5298}$ [37]	MW
Custos de capital	$1,05 \times 1,08 \times \text{Custo de aquisição}$ [59]	MUS\$

É importante lembrar que os estudos do JAERI (de 2000) [61] estão desatualizados em termos do custo do petróleo, cujo preço médio em 20 anos quase triplicou desde então, bem como o custo de construção de navios diminuiu [63]. Para fazer a estimativa de custos, foram adotadas curvas de custos de aquisição e de operação de navios porta contêineres

mostradas por [63]. O custo dos reatores foi retirado do estudo do departamento de reatores navais da marinha dos EUA [19], subtraídos os custos com combustível. O custo do combustível nuclear foi retirado da estimativa de custo do JAERI [61]. Este trabalho adotou, como hipótese, uma tripulação de 21 pessoas e um lucro bruto de 10% para a empresa nuclear. A velocidade adotada para todos os casos foi de 23 nós, pois, tal como relatado por [63], os navios vêm adotando essa velocidade nos últimos anos porque o combustível encareceu.

Os resultados são apresentados na Figura 63, que mostra que a energia nuclear precisa de escala para ficar competitiva. Fica também evidente que a vida relativamente curta de um navio não permite que um reator integrado à estrutura seja competitivo para as classes mais numerosas. Ou seja, a estratégia de uma arquitetura modular beneficia a energia nuclear dada a longevidade elevada dos reatores.

Figura 63 – Comparação do custo de transporte das opções

Para fornecer uma ideia de comparação em termos percentuais da economia gerada pela adoção do módulo nuclear, a Figura 64 apresenta os ganhos percentuais da adoção de um módulo nuclear. Os ganhos em relação ao navio nuclear variam em torno de 15 a 20%, aumentando com o tamanho do navio e da potência instalada. A partir de 8000 TEU, o módulo fica competitivo com navios diesel, atingindo 10% de economia para navios de 13000 TEU, que se enquadra na classe New Panamax, que vem crescendo nos últimos anos. Vale ressaltar que atualmente, navios nucleares com reatores integrados na sua estrutura

parecem não ser capazes de bater seus concorrentes convencionais. Tal fato pode ser questionado pois o modelo de custo baseia-se em reatores navais militares, que tem requisitos de choque militar. Por outro lado, tais reatores são simplificados e produzidos em série, que torna questionável se realmente seria possível reduzir muito o custo de sua fabricação. O que é certo é que tais custos são baseados em fatos reais, bem como a equação da Tabela 42 de estimativa de custo de reatores aproxima os custos de construção dos reatores AP1000 (assumindo que 28% do custo total está relacionado à ilha nuclear e que o custo de aquisição é 5500 US\$/kW).

Figura 64 – Comparação do diesel e de um navio nuclear com módulo nuclear

Em relação ao direito constitucional, o conceito de estado é muito importante para definir as ações a serem tomadas em cada situação, bem como realizar a mudança de um estado a outro. Existe uma definição parcial nas constituições dos países, mas costuma ser incompleta e não leva em conta instituições estatais entre o poder executivo e os indivíduos. Ou seja, a noção de hierarquia não é respeitada na abordagem do direito constitucional, deixando em aberto as atribuições ou limitações de municípios, províncias, empresas, banco central e outras pessoas jurídicas.

Essa falta de definição, por si mesma, deixa a sociedade sujeita a muitas incertezas e riscos, pois não existem diretrizes formais para que o poder executivo siga nessas circunstâncias. Guerras e cataclismos naturais são eventos que não ocorrem tipicamente várias vezes no governo de um único indivíduo, logo não existe possibilidade de aprendizado. Assim, a pessoa no papel de chefe executivo fica potencialmente perdida e precisa agir na base do improviso.

Existem ainda riscos decorrentes, pois se o texto base não se preocupa com os estados e transições, as leis subsequentes também não levam em conta tais aspectos. Assim, o executivo pode acabar em uma situação de ilegalidade compulsória por ter que prover direitos que sejam impossíveis em condição de guerra. Um exemplo é o controle de inflação em tempos de guerra, que não pode ser controlado como em tempo de paz.

Outro risco é que a falta de definição leva à incapacidade de estimar os custos, tal como ocorre em projetos de sistemas. Assim, antes da guerra, as pessoas tendem a subestimar o custo da guerra, que inclui o custo da mobilização, a inflação decorrente dos gastos do governo e da desmobilização. Existem ainda as perdas humanas e materiais na guerra, a desorganização das estruturas produtivas, o risco de agressão e problemas na pirâmide etária que podem afetar a previdência. Enfim, este trabalho defende que parte dos erros cometidos em gestão de projetos, operação de usinas e políticas públicas deve-se à falta de um método de análise que leve à percepção realista dos problemas.

7 CONCLUSÃO

O objetivo geral deste trabalho foi o desenvolvimento de um método, orientado pela lei construtal, para desenvolver sistemas cibernéticos complexos com funções conhecidas. A partir da lei construtal, foram identificadas as funções presentes em um canal por onde deve passar um fluxo necessário a um sistema. Fazendo a analogia para o canal de comunicações, foram derivados e justificados requisitos para o trabalho de desenvolvimento de sistemas. Em suma, esses requisitos visam reduzir a energia total e o tempo gastos para realizar a concepção de um sistema complexo. Constatou-se que para minimizar essa energia, é necessário reduzir a energia dispendida na comunicação, evitar a introdução de dados falsos ou irrelevantes e assegurar que todos os dados necessários estejam presentes.

Os métodos baseados em documentos têm o problema da fragmentação da informação, havendo dificuldade em manter a consistência dos dados. Além disso, existe o problema da falta de distinção formal entre necessidades (especificação) e soluções (projeto), bem como os requisitos são alocados a diversos níveis da decomposição do produto. Os métodos baseados em engenharia aeronáutica contêm muitos passos para definir o conceito de operações, já que muitas vezes um novo projeto não tem seus objetivos claros logo de início. Tal quantidade de passos requer um tempo e esforço que pode ser considerado excessivo para a maior parte dos projetos de engenharia cujos objetivos são bem conhecidos. Os métodos baseados em engenharia de software têm o problema de não separar formalmente necessidades (especificação) e soluções (projeto). Tal fato ocorre porque projetos de software desenvolvem parte das especificações de maneira alternada com o desenvolvimento porque tipicamente o cliente não sabe com exatidão quais são as necessidades. Além disso, a mesma organização desenvolve os requisitos e a solução, o que leva a uma certa mistura entre especificação e solução.

Em um projeto de engenharia de sistemas, a organização líder precisa comprar sistemas complexos e produtos simples de uma vasta gama de fornecedores. Assim, existe uma distinção formal (organizacional) entre especificação e projeto, onde a organização líder faz a especificação e os fornecedores fazem o projeto. Considerando que o projeto faz parte do valor adicionado, os fornecedores tipicamente resistem a especificações que invadam o seu perímetro de responsabilidade. Além da questão comercial, muitas vezes a especificação fica inviável por entrar em detalhes excessivos. Assim o método deve estabelecer a distinção

formal entre necessidades e solução para atingir os seguintes objetivos. O primeiro é evitar que a especificação entre em domínios desconhecidos pela organização líder. O segundo é manter o caminho aberto para a evolução tecnológica e a criatividade. O terceiro é evitar conflitos inadvertidos entre cliente e fornecedores acerca do valor agregado.

Para demonstrar o poder do método desenvolvido, este trabalho buscou um objetivo específico, que implicou no emprego do método a casos particulares. A energia nuclear é uma peça fundamental na matriz energética devido a suas características intrínsecas. A primeira característica é a alta concentração de energia por área ou volume de instalação. A segunda é a independência do clima, que dadas as inevitáveis mudanças climáticas, a torna relativamente segura. A terceira é a alta densidade do combustível, que permite a formação de grandes estoques a baixo custo, o que permite obter robustez a bloqueios comerciais mais barato. A quarta é a estabilidade e insignificância do preço do combustível nuclear, que torna a geração de energia estável e pouco volátil. A quinta é a distribuição geográfica no mundo dos fornecedores de minério de urânio, que evitam o problema de falha comum que ocorre com o petróleo. A sexta é a segurança, especialmente em se tratando de usinas com reatores a água pressurizada. Mesmo que haja um relaxamento completo por parte das autoridades nucleares, pela simples necessidade de proteção do capital, as usinas nucleares seriam as mais seguras. Por fim, a sétima característica é o pequeno impacto ambiental, sendo que o combustível usado pode ser reaproveitado e o volume final de rejeitos radioativos será pequeno. Além de ser pequeno, ele é facilmente controlável, diferentemente de outras formas de energia que jogam grandes quantidade de rejeitos na atmosfera sem qualquer controle.

Dadas as implicações de maiores dificuldades nos estados de exceção, a falta de energia nuclear leva qualquer país a maiores perdas no longo prazo, reduzindo a eficiência e a competitividade. Um país sem competitividade em um mundo globalizado está fadado ao colapso, já que a população urbana não achará atividades econômicas para seu sustento.

O objetivo específico foi verificar se uma usina nuclear móvel pode ser comercialmente viável para um mercado amplo. Essa usina não pode existir sem uma estrutura organizacional adequada, pois as competências técnicas e infraestrutura possuem custos elevados. Adicionalmente, não pode operar sem um suporte que resolva problemas em caso de acidentes. Assim, foi concebida também a empresa provedora de usinas nucleares usando sempre o método prescrito no primeiro objetivo.

A usina concebida foi dimensionada em regime permanente, verificando se os requisitos poderiam ser satisfeitos, o que teve resultado positivo do ponto de vista técnico. Duas fontes diferentes apontaram para a viabilidade econômica de usinas nucleares móveis se o consumo médio for superior a um valor aproximado de 30MWe elétricos.

Concluindo, esses exemplos demonstraram que o método representa um ganho considerável sobre a prática atual de engenharia. O método permite identificar requisitos que não são óbvios a priori, elucidando uma série de problemas graves que ficam de fora das discussões sobre matriz energética. Comparado também com os requisitos da EPRI, que misturam vários níveis de concepção e repetem requisitos, existe um ganho sensível de eficiência. Além disso, mantém a flexibilidade do projeto, pois não mistura necessidade com solução, ficando fácil mudar qualquer componente porque as especificações estão explícitas.

Evidentemente, não é possível afirmar que os requisitos do método enunciado sejam definitivos e, juntos, definam um método insuperável para todos os casos. O que se pode afirmar é que esse método representa um ganho sobre o pensamento corrente e que pode ser facilmente revisto e aperfeiçoado dada a maneira modular e atômica de cada requisito enunciado. Ou seja, o método defendido representa uma base sobre a qual podem ser desenvolvidos métodos superiores à prática atual, o que merece o título de tese por agregar valor ao cabedal de conhecimentos da humanidade.

Sendo o método proposto uma ferramenta para ajudar na decisão e evitar riscos, acredita-se que sua implementação no âmbito da engenharia contribuirá para a redução de mortes em acidentes e melhoria da prosperidade. Como trabalhos futuros, vislumbra-se aplicar os conceitos propostos em modelagem de negócios e até na política estatal, visto que os conceitos são genéricos. No âmbito da gestão empresarial, acredita-se que reduzirá o número de falências e melhorar a capacidade empresarial de um país. No âmbito do direito e da política, talvez contribuirá para a consolidação de um mundo mais pacífico e seguro por evidenciar de maneira transparente os custos das opções políticas.

8 REFERÊNCIAS BIBLIOGRÁFICAS

- [1] WYMORE, A. W. **Model-Based Systems Engineering**. 1. ed. Boca Raton: CRC Press, 1993.
- [2] OGATA, K. **Modern Control Engineering**. 5th. ed. [S.l.]: Pearson, 2010.
- [3] WASSON, C. S. **System Analysis, Design, and Development: Concepts, Principles, and Practices**. 1. ed. Hoboken: John Wiley & Sons, Inc., 2006. 832 p.
- [4] IEEE. **IEEE Standard Glossary of Software Engineering Terminology**. Institute of Electrical and Electronics Engineers - C/S2ESC - Software & Systems Engineering Standards Committee. [S.l.]. 1990. (IEEE Std 610.12-1990).
- [5] INGHAM, M. D. et al. Generating requirements for complex embedded systems using State Analysis. **Acta Astronautica**, v. 58, p. 648 – 661, 2006.
- [6] WEILKIENS, T. **Systems Engineering with SysML/UML - Modeling, Analysis, Design**. 1^a. ed. Heidelberg: Morgan Kaufmann OMG Press, 2006. ISBN 978-0-12-374274-2.
- [7] LYKINS, H.; FRIEDENTHAL, S.; MEILICH, A. Adapting UML for an Object-Oriented Systems Engineering Method. **Proceedings of the INCOSE International Symposium**, 15-20 July 2000. 490–497.
- [8] KEMMENY, J. G. **The Need for Change: The Legacy of TMI**. The President's Commission on the Accident at TMI. Washington DC, p. 179. 1979.
- [9] TARRIDE, B. **Physique, fonctionnement et sûreté des REP**. 1. ed. France: EDP Sciences, 2013. ISBN 978-2-7598-0738-3.
- [10] BATAILLE, M. C.; SIDO, M. B.; BIRRAUX, M. C. **Rapport de la mission parlementaire sur la sécurité nucléaire, la place de la filière et son avenir**. ASSEMBLÉE NATIONALE. Paris, p. 565. 2011. (N° 3614).
- [11] EYRING, V. E. A. Transport Impacts on Atmosphere and Climate: Shipping, Atmospheric Environment. **Journal of Atmosphere and Environment**, v. 44, n. 37, p. Pages 4735-4771, 2009. ISSN 1352-2310. Disponível em: <<http://www.sciencedirect.com/science/article/pii/S1352231009003379>>.
- [12] ROYAL ACADEMY OF ENGINEERING. **Future Ship Powering Options Exploring alternative methods of ship propulsion**. Royal Academy of Engineering. United Kingdom. 2013.

- [13] GRAVINA, J. . E. A. **Concepts for a Modular Nuclear Powered Containership.** 17th International Conference on Ships and Shipping Research (Nav2012). Napoli: [s.n.]. 2012.
- [14] CARLTON, J. . J. V. & S. B. The nuclear propulsion of merchant ships: Aspects of Engineering, Science and Technology. **Proceedings of IMarEST - Part A - Journal of Marine Engineering and Technology**, 2011. 10 (2).
- [15] ONDIR FREIRE, L.; DE ANDRADE, D. A. Historic survey on nuclear merchant ships. **Nuclear Engineering and Design**, n. 293, p. 176–186, 2015. ISSN 0029-5493.
- [16] MAGWOOD, W. D. **Report to Congress on Small Modular Nuclear Reactors.** United States of America. 2001.
- [17] HIRDARIS, S. E. E. A. Considerations on the potential use of Nuclear Small Modular Reactor (SMR) technology for merchant marine propulsion. **Ocean Engineering**, v. 79, p. 101-130, 15 March 2014. ISSN 0029-8018.
- [18] HIRDARIS, S. E. . E. A. Concept Design of a Suezmax Tanker Propelled by a 70 MW SMR. **Trans. of the Royal Institution of Naval Architects International Journal of Maritime Engineering**, v. 156(A1), p. 37-59, 2014. ISSN 14798751.
- [19] O'ROURKE, R. **Navy Nuclear-Powered Surface Ships: Background, Issues, and Options for Congress.** Congressional Research Service. United States of America. 2010.
- [20] RAND. **Sustaining US Nuclear Submarine Design capabilities.** RAND. United States of America. 2007.
- [21] BEJAN, A. . L. S. Constructal law of design and evolution: Physics, biology, technology, and society. **Journal of Applied Physics**, 113, n. 151301, 2013. 15. Disponivel em: <<http://dx.doi.org/10.1063/1.4798429>>.
- [22] NASA. **NASA Systems Engineering Handbook.** 1. ed. [S.l.]: [s.n.], 2007.
- [23] SCHLAGER, J. Systems engineering: key to modern development. **IRE Transactions EM-3**, v. 3, p. 64–66, 1956.
- [24] HALL, A. D. **A Methodology for Systems Engineering.** 1^a. ed. Princeton: Van Nostrand Reinhold, 1962. 478 p.

- [25] BLANCHARD, B. S. . F. W. J. **System Engineering and Analysis**. 4. ed. New Jersey: Prentice Hall, 2006. 804 p.
- [26] PROJECT MANAGEMENT INSTITUTE. **Um Guia do Conhecimento Em Gerenciamento de Projetos - Guia Pmbok®**. 5ª. ed. Pennsylvania: Project Management Institute, 2014.
- [27] US DEPARTMENT OF DEFENSE. **System engineering fundamentals**. Fort Belvoir: Defense Acquisition University Press, 2001. 222 p.
- [28] ESTEFAN, J. A. **Survey of Model-Based Systems Engineering (MBSE) Methodologies**. [S.l.]. 2008.
- [29] DOUGLASS, B. P. **The Harmony Process**. [S.l.]. 2005.
- [30] CANTOR, M. **Rational Unified Process® for Systems Engineering, RUP SE® Version 2.0**. [S.l.]. 2003.
- [31] CHILDERS, S. R.; LONG, J. E. A Concurrent Methodology for the System Engineering Design Process. **INCOSE International Symposium**, August 1994. 226-231. Disponivel em: <<http://onlinelibrary.wiley.com/doi/10.1002/j.2334-5837.1994.tb01709.x/abstract>>.
- [32] LANGE, R. S. **Theme Study – Large Vessel NS Savannah**. U.S. Department of the Interior, History Division. Washington, DC, p. 32. 1990.
- [33] ONDIR FREIRE, L.; DE ANDRADE, D. A. Constructal Law of Institutions within Social Organizations. **Open Journal of Applied Sciences**, v. Vol.8, n. No.3, p. 103-125, March 2018 2018. ISSN 2165-3925.
- [34] FELLOWS, R. . L. D. N. R. &. U. S. **Construction Management in Practice**. Oxford: John Wiley & Sons, 2009. ISBN 1444314300.
- [35] SENADO DA FRANÇA. **Relatório da missão parlamentar sobre a segurança nuclear, o papel do setor e seu futuro**. Paris. 2011.
- [36] E. LONG, J. **COTS: What You Get (In Addition to the Potential Development Savings)**. Vitech Corp. Vienna, Virgínia, USA, p. 5. 2000.
- [37] MAM DIESEL A/S. **Propulsion Trends in Container Vessels**. Denmark. 2009.
- [38] BUREAU VERITAS. **Merchant Ships Structural Hull**, 2005.

- [39] PAPANIKOLAOU, A. et al. Statistical analysis of ship accidents that occurred in the period 1990–2012 and assessment of safety level of ship types. **2nd International Conference on Maritime Technology and Engineering - MARTECH 2014**, Lisbon, 15-17 October 2014. 7.
- [40] APOSTOLIDIS, A.; KOKARAKIS, J.; MERIKAS, A. Modeling the Dry-Docking Cost – The Case of Tankers. **Journal of Ship Production and Design** **28** (3), 2012. 134-143.
- [41] MAM DIESEL A/S. **Propulsion Trends in Tankers**. Denmark. 2009.
- [42] MAM DIESEL A/S. **Propulsion Trends in Bulk Carriers**. Denmark. 2007.
- [43] UWATOKO, K.; WATANABE, M.; SUZUKI, N. Considerations for the Global Environment in the Latest Large Container Vessels. **Technical Review**, v. 44, n. 3, 2007. Disponivel em: <<https://www.mhi.co.jp/technology/review/pdf/e443/e443024.pdf>>.
- [44] MAM DIESEL A/S. **Propulsion of 8,000-10,000 teu Container Vessel**. Copenhagen. 2012.
- [45] OFFICE OF SHIP DISPOSAL - MARITIME ADMINISTRATION. N.S. **Savannah Updated Final Safety Analysis Report – (STS-004-002)**. [S.l.]. 2011.
- [46] ELECTRIC POWER RESEARCH INSTITUTE. **Advanced Light Water Reactor Utility Requirements Document Volume III - ALWR Passive Plant**. EPRI. Palo Alto, Califórnia, p. 3265. 1999.
- [47] AMERICAN NUCLEAR SOCIETY. **Nuclear Safety Criteria for the Design of Stationary Pressurized Water Reactor Plants**. R1988. ed. Illinois: American National Standards Institute, Inc., 1988. 101 p.
- [48] WADE, K. C. **Steam Generator Degradation and Its Impact on Continued Operation of Pressurized Water Reactors in the United States**. [S.l.]. 1995.
- [49] ELECTRIC POWER RESEARCH INSTITUTE. **PWR Secondary Water Chemistry Guidelines - Revision 5**. EPRI. Palo Alto. 2000.
- [50] BRUENS, N. W. S. **PWR Plant and Steam Generator Dynamics (Doctoral Thesis)**. Rotterdam: Delft University of Technology, 1981.

- [51] FRIBOURG, C. **Nuclear Reactor Having Plate or Micro-Channel Heat Exchangers integrated in the Vessel**. WO 2013/153076 A1, 2012.
- [52] BEJAN, A. et al. Entrance-length dendritic plate heat exchangers. **International Journal of Heat and Mass Transfer**, n. 114, p. 1350–1356, 2017.
- [53] ONDIR FREIRE, L.; DE ANDRADE, D. A. On applicability of plate and shell heat exchangers for steam generation in naval PWR. **Nuclear Engineering and Design**, n. 280, p. 619–627, 2014. ISSN 0029-5493. Disponivel em: <<http://dx.doi.org/10.1016/j.nucengdes.2014.09.039>>.
- [54] WYMORE, A. W. **A Mathematical Theory of Systems Engineering: The Elements**. 1. ed. New York: John Wiley & Sons, 1967.
- [55] HAN, E. O. . K. J. R. . C. Y. S. Korean Students` Behavioral Change Toward Nuclear Power Generation Through Education. **Nuclear Engineering and technology** , October 2014. 12.
- [56] NAKAO, M. Radiation Leaks from Nuclear Power Ship "Mutsu". **Failure Knowledge Database**, 1992. Disponivel em: <<http://www.sozogaku.com/fkd/en/cfen/CA1000615.html>>. Acesso em: 21 Maio 2017.
- [57] STRUPCZEWSKI, A. Accident risks in nuclear-power plants. **Applied Energy**, v. 75, n. Issues 1–2, p. 79–86, 2003. ISSN 0306-2619.
- [58] MINISTRY OF FOREIGN AFFAIRS. **Fact Sheet on U.S. Nuclear Powered Warship (NPW) Safety**. Okinawa, p. 10. 2004.
- [59] MCMAHON, T. Historical Crude Oil Prices (Table). **inflationdata.com**, 2017. Disponivel em: <https://inflationdata.com/Inflation/Inflation_Rate/Historical_Oil_Prices_Table.asp> . Acesso em: 10 Setembro 2017.
- [60] JR., T. D. I. **Effects of variation of uranium enrichment on nuclear submarine reactor design**. Lowell: Massachusetts Institute of Technology, 1990.
- [61] KUSUNOKI, T. et al. Design of advanced integral-type marine reactor, MRX. **Nuclear Engineering and Design**, v. 201(2), p. 155-175, 2000.
- [62] LOVERING, J. R.; YIP, A.; NORDHAUS, T. Historical construction costs of global nuclear power reactors. **Energy Policy**, n. 91, p. 371–382, 2016. ISSN 0301-4215.

- [63] MURRAY, W. **Economies of Scale in Container Ship Costs**. US Merchant Marine Academy. New York, p. 25. 2016.

ANEXO 1 – Lista de requisitos e suas justificativas

Status	Requisito	Justificativa	Flex.
Identificando subsistemas	As especificações de subsistemas serão em forma de caixa preta	Especificações em forma de caixa preta ignoram detalhes internos dos subsistemas, concentrando a atenção na interação nas interfaces. Consequentemente, ocorre o respeito à hierarquia, já que requisitos são enviados apenas para o nível imediatamente inferior e nunca para dois ou mais níveis hierárquicos abaixo. A hierarquia permite a quebra de um problema complexo em problemas menores, permitindo que uma pessoa consiga resolver o problema em um tempo razoável. É uma decorrência do princípio de separação formal entre necessidades e soluções. Também melhora a qualidade da tomada de decisão por preservar a autonomia de cada projetista e reduzir a quantidade de requisitos desnecessariamente conflitantes. Assim, o ruído é reduzido e a qualidade do trabalho é melhorada sem que haja um aumento de trabalho, requerendo apenas disciplina das pessoas.	Mandatório
	A especificação deve identificar todos os subsistemas	Se este requisito for atendido, a possibilidade de retrabalho na arquitetura fica reduzida, pois a falta de um subsistema implicaria em uma modificação substancial. Para que este requisito seja atendido, os subsistemas têm que ser definidos com hipóteses realistas sobre suas interfaces e funções. Para isso, pode ser adotado o reuso de subsistemas conhecidos ou um desenvolvimento iterativo até todas as funções e interfaces estejam coerentes. Esse requisito é mandatório porque é certamente viável para um especialista saber quais são os componentes necessários para executar uma tarefa e ignorar esse requisito causa grandes prejuízos. Esse requisito tem o objetivo de preservar a integridade das informações necessárias ao projeto de um sistema.	Mandatório
	A análise de cima para baixo deverá escolher a opção com o menor custo	Este requisito impõe que os recursos a serem empregados devem ser sempre mínimos, mantendo o desperdício tão baixo quanto possível. O custo deve ser encarado em seu sentido mais amplo, significando trabalho humano, dinheiro, materiais, energia, volume, peso e risco. Outro aspecto é que o elo mais fraco de uma corrente determina a capacidade da corrente, o que leva a concluir que a corrente ótima é aquela que tem todos os elos iguais. Manter em mente a necessidade de redução de custo evita a introdução de subsistemas desnecessários, de qualidade desnecessária ou segurança desnecessária, que seriam um ruído no processo.	Desejável

Status	Requisito	Justificativa	Flex.
Identificando funções	A especificação deve identificar todas as funções de cada subsistema	As funções precisam ser completamente identificadas porque são a base do trabalho. As funções de um subsistema serão posteriormente especificadas por meio de requisitos funcionais. Começar a refinar a especificação antes de identificar todas as funções leva necessariamente a retrabalho e ineficiência. A identificação completa das funções de um sistema confere autonomia para o projeto, permitindo a escolha da melhor solução técnica disponível. Esse requisito é mandatório porque é barato identificar as funções internas para executar uma função de serviço e ignorar esse requisito causa grandes prejuízos. Esse requisito preserva a integridade das informações necessárias ao trabalho.	Mandat ório
	Toda função deve ser composta por verbo e talvez por objetos direto ou indiretos, com a seguinte forma: [verbo] {objeto direto} {objeto indireto}	O cérebro humano é um sistema de fluxo de informação que se torna mais eficiente se os dados forem escritos em uma única forma padrão (mínima surpresa). Função é uma ação quantificável, como entregar um certo fluxo, uma certa potência ou transportar uma certa carga, por exemplo. Por exemplo: “bombear água”, “remover calor”, “fornecer energia”. Tal requisito facilita o fluxo de informação.	Mandat ório
	As funções recebidas pelo sistema devem ser desmembradas em funções técnicas	Uma dada função de serviço do sistema em estudo é decomposta em funções técnicas. O mesmo vale para as funções recebidas, que serão decompostas em funções técnicas dos outros sistemas. Tal formalismo serve para não confundir as funções de níveis de decomposição diferente. É uma comunicação entre sistemas de mesmo nível de decomposição, onde um sistema solicita que outro integre uma ou mais funções técnicas. Tal requisito serve para facilitar o fluxo de informação, evitando que seja necessário mudar a especificação de nível superior.	Desejáv el

Status	Requisito	Justificativa	Flex.
	Para cada função, a especificação deve identificar um único sistema responsável	Essa regra representa unicidade de comando e de responsabilidade. A alocação de tarefas a vários subsistemas como um conjunto deixaria cada um sem definição específica de tarefas. Uma deliberação entre os encarregados de subsistema seria necessária para resolver esse problema, causando atrasos e riscos. Existe risco porque a solução dada por esse grupo, sem ter total acesso às necessidades do sistema, pode ser inadequada. Outro risco é os encarregados de subsistema não serem capazes de entrar em acordo devido a conflitos de interesse. Assim, a alocação de funções a dois ou mais subsistemas em conjunto aumenta os riscos. Adicionalmente, a unicidade da responsabilidade facilita a verificação do trabalho por evitar o compartilhamento de responsabilidades. Assim, caso ocorram erros, será possível identificar um único autor com facilidade, coibindo atitudes irresponsáveis e facilitando a correção. A unicidade de comando e responsabilidade facilita o fluxo de informação entre os níveis hierárquicos.	Mandat ório
	Para cada função, a especificação deve identificar os sistemas alvos	Uma função técnica pode prestar serviços para vários subsistemas, cujos status dependem das funções fornecidas e recebidas. Assim, o trabalho de especificação precisa registrar quais subsistemas recebem cada função para posteriormente identificar os status de subsistema. Esta regra serve para manter a integridade das informações relevantes.	Mandat ório
	Um dado subsistema deve realizar funções técnicas com propriedades similares	Em suma, esta regra significa separar subsistemas executando funções críticas (de segurança, por exemplo) do resto dos subsistemas menos críticos. Outro aspecto é que funções críticas costumam não evoluir tanto quanto funções normais durante um projeto. Se os dois tipos de função forem mesclados, uma maior quantidade de revisões em subsistemas críticos será necessária para assegurar que não haja erros sistemáticos. Considerando que subsistemas críticos requerem severo controle de qualidade, a redução do número de revisões tem um impacto significativo na redução do custo de um projeto. Se tais revisões são evitáveis, pode ser afirmado que elas são um ruído de processo que deve ser minimizado para facilitar o fluxo de produção de informação.	Negoci ável
	Funções técnicas com confiabilidade elevada devem permanecer em prontidão nos status normais	Funções de alta confiabilidade requerem alta qualidade, que implica em alto custo e grande esforço de projeto. Mesmo com tamanho gasto, se tais subsistemas forem empregados durante o uso normal, eles podem sofrer desgaste e falhar quando necessários em uma emergência. Tal regra minimiza a quantidade de trabalho e recursos para obter uma solução, facilitando o fluxo de informação.	Desejáv el

Status	Requisito	Justificativa	Flex.
Definindo nexos causais	A especificação deve identificar o nexo causal entre funções de serviço e funções técnicas	Tal nexo causal é a chave para fazer a tradução dos requisitos de desempenho das funções de serviço em requisitos de desempenho das funções técnicas. Quando uma função técnica é usada para realizar duas funções de serviço diferentes (tem nexo causal com as duas), podem haver diferentes requisitos para uma mesma propriedade. Neste caso, o requisito mais restritivo domina a especificação do subsistema. Além disso, essa regra estabelece a rastreabilidade de requisitos. Esta regra serve para manter a integridade das informações relevantes.	Mandatório
	A especificação deve identificar o nexo causal entre as propriedades do sistema e suas funções técnicas	Uma propriedade pode requerer funções técnicas para ser atingida, por exemplo a frequência de incêndio pode ser reduzida pelo emprego de uma função de combate a incêndio. Além disso, essa regra estabelece a rastreabilidade de requisitos. Assim, identificar tais nexos causais permite traduzir os requisitos não funcionais do sistema em requisitos de desempenho, mantendo a integridade das informações relevantes.	Mandatório
Classificando funções técnicas	Para cada subsistema, a especificação deve definir quais funções técnicas são relevantes	A classificação em relevante ou irrelevante permite simplificar o modelo comportamental de um sistema mantendo os riscos sob controle. O trabalho de fazer essa classificação é muito pequeno comparado com o esforço de levar em conta um número potencialmente elevado de funções, incorrendo em risco de explosão de status. Ou seja, essa classificação reduz o ruído na comunicação.	Desejável
Identificando status	A especificação deve definir os possíveis status de cada função técnica	Os status de função são a base para definir os status de sistema, bem como a base para determinar a instrumentação para observar o modo de operação de um produto. Funções podem estar ativas, em prontidão, inativas ou até inibidas. Funções irrelevantes não precisam ter uma definição de status. Tal informação é fundamental para escolher alternativas de solução, mantendo a integridade das informações relevantes.	Mandatório
	Para cada status do sistema, a especificação deve definir os status de cada função técnica	Tal tabela permite entender as dependências funcionais em cada status do sistema e identificar combinações de funções internas ativas simultaneamente. Essa tabela facilita o trabalho de identificação dos estados de cada subsistema. Entretanto, essa tabela não é um dado de saída nas especificações, mas um elemento de justificativa para facilitar a avaliação do trabalho. Essa tabela reduz o esforço de projeto por guiar o raciocínio e facilitar a avaliação e verificação do trabalho, facilitando a comunicação com revisores.	Mandatório

Status	Requisito	Justificativa	Flex.
	A especificação deve identificar todas as combinações de status das funções relevantes de cada subsistema	Identificar corretamente os status dos subsistemas é crítico, pois erros nesta etapa levará a problemas de integração. Subsistemas especificados sem uma parte de seus status podem não ser capazes de realizar todas as funções simultaneamente. Ou podem ser superdimensionados se forem concebidos com uma flexibilidade desnecessária. Subsistemas concebidos com mais status do que os necessários irão demandar uma série de estudos desnecessários, implicando em desperdício de trabalho e ineficiência. Em suma, falta de status leva a retrabalho na fase de concepção e perda de material na fase de testes e integração. Excesso de status, seja na especificação ou na forma de hipóteses não declaradas de concepção, leva a soluções mais complexas e custosas. De qualquer jeito, falhar na identificação de status dificulta o trabalho de engenharia em geral. Esta regra preserva a integridade da informação relevante.	Mandat ório
	Todo status de subsistema deve ser único	As pessoas tendem a criar mais status do que os necessários, geralmente devido à confusão de status com as configurações físicas. O problema é que cada status requer requisitos funcionais, dimensionamento e verificações. Quanto maior o número de status, maior o número de fases, que também requerem demonstrações e verificações. Tudo isso adiciona uma carga de trabalho considerável que deve ser evitada sempre que possível pela redução do número de status definidos. Para assegurar que os status sejam únicos, basta verificar se existem maneiras de interação idênticas usando a tabela de atividade das funções internas. Maneiras de interagir idênticas devem ser eliminadas antes de começar a identificação de transições para evitar retrabalho. Esta regra adiciona um pequeno trabalho e acarreta grandes reduções de trabalho inútil a posteriori, reduzindo ruído e esforço global durante a atividade de projeto.	Desejá vel
Identificando fases	Para cada fase ativa do sistema, a especificação deve identificar as fases necessárias dos subsistemas	A falha em identificar as fases de um subsistema pode levar à falta de atuadores na solução, causando problemas de integração. A falta de fases pode levar à especulação e hipóteses excessivamente conservadoras, o que leva também a soluções desnecessárias. Tais problemas podem inutilizar parcialmente ou totalmente um sistema. No melhor caso, tais erros geram retrabalho na documentação, se detectados na fase de projeto. No pior caso, a falta de requisitos funcionais de transição pode levar ao fracasso do projeto ou pelo menos grandes e custosas modificações após a construção. Em todo caso, o trabalho de identificação e especificação de transições preserva a integridade das informações relevantes ao projeto.	Mandat ório

Status	Requisito	Justificativa	Flex.
	A especificação deve classificar as fases em ativas ou passivas	Quando um subsistema tem uma fase ativa, isso impõe um estudo durante a especificação de seus componentes. Por outro lado, se durante a especificação do subsistema é evidente que uma fase é passiva, tal estudo é desnecessário e tal informação deve ser passada adiante. Esta regra adiciona um pequeno trabalho e reduz ruído e esforço global durante a atividade de especificação de subsistemas.	Desejável
Declinando requisitos	Para cada propriedade do sistema, a especificação deve definir se existe relação com cada propriedade dos subsistemas	Essa relação permite a rastreabilidade de requisitos e facilita o trabalho de tradução dos requisitos não funcionais do sistema para os requisitos não funcionais de cada subsistema. Essa regra contribui para preservar a integridade de informações essenciais ao projeto dos subsistemas.	Mandatário
	A especificação deve traduzir os requisitos não funcionais do sistema em requisitos não funcionais dos subsistemas	Essa atividade é essencial para o cumprimento dos requisitos não funcionais do sistema. Essa regra contribui para preservar a integridade de informações essenciais ao projeto dos subsistemas.	Mandatário
	Requisitos não-funcionais serão uma relação de uma propriedade do com uma condição	Exemplo: “Em plena potência, o poder de processamento do computador será maior do que 300 Mips”. Tipicamente as pessoas tendem a escrever lista de desejos e não requisitos concretos. Adjetivos devem ser evitados para estabelecer as propriedades de um sistema por criar mensagens vagas e subjetivas, tais como seguro, confiável, bonito, barato e bom. Substantivos e números devem ser usados para caracterizar as propriedades, tais como frequência de acidentes, taxas de falha, custo e padrões da indústria. Essa restrição ao formato de requisitos funcionais evita a introdução de ruído no processo, que é a redação de requisitos subjetivos, sob pena de introduzir entraves na escrita. O efeito principal é facilitar a comunicação após as pessoas terem se habituado, pois as pessoas têm mais facilidade de ler textos padronizados.	Mandatário

Status	Requisito	Justificativa	Flex.
	Requisitos não-funcionais devem definir as condições ambientais que os subsistemas devem suportar	As condições ambientais a serem suportadas são frequentemente ignoradas durante um projeto, com resultados catastróficos em alguns casos. É fundamental informar as condições ambientais nas quais o sistema deve trabalhar. A faixa de temperatura, de pressão atmosférica e de humidade do ambiente são fundamentais para o projeto. Pode ser necessário também incluir informações sobre vibração, choque, inclinação, movimentos, presença de pó e presença de água. Ignorar tais aspectos pode causar prejuízos. Logo, esta regra assegura que uma parte importante das informações necessárias ao projeto não seja perdida. Esse aspecto é crucial para a escolha de tecnologias e deve ser conhecido antes de começar o trabalho. As tecnologias adequadas a um sistema determinam todas as propriedades não funcionais de um sistema, como custo, peso e volume. Assim, se as condições ambientais não forem levadas em conta desde o início, assume-se um risco de retrabalhar tudo, pois os requisitos não funcionais provavelmente não serão atendidos. Por outro lado, hipóteses podem ser feitas pela equipe de projeto caso o cliente não faça essa definição, sendo um requisito negociável por não precisar parar um projeto. Essa regra tem o objetivo de preservar a integridade das informações necessárias ao projeto de um sistema.	Negociável
	Requisitos não-funcionais devem definir as resistências aos riscos externos	Sistemas podem ser expostos a diversos tipos de riscos externos, tais como alagamento, terremoto, furacão, impacto e incêndio. Neste caso, a especificação deve prover requisitos não funcionais de resistência a tais riscos. Como soluções dispendiosas podem ser necessárias para atender a tais requisitos, tais definições têm que ser feitas durante a análise de cima para baixo. Por outro lado, hipóteses podem ser feitas pela equipe de projeto caso o cliente não faça essa definição, sendo um requisito negociável por não precisar parar um projeto. Esse requisito tem o objetivo de preservar a integridade das informações necessárias ao projeto de um sistema.	Desejável
	A especificação deve criar requisitos não funcionais limitando o tempo de operação em cada estado	A duração de operação em cada estado é um parâmetro fundamental para calcular a confiabilidade e definir as rotinas de reparo e manutenção. Um subsistema que passa a maior parte de sua vida parado, entrando em operação por um período curto é bem diferente de um sistema que opera continuamente. A duração dos estados parados ou não operacionais é também importante para escolher arquiteturas devido aos impactos nas restrições à manutenção. Essa regra é fundamental para assegurar que os cálculos de confiabilidade sejam realistas, contribuindo para manter a integridade de informações relevantes.	Desejável

Status	Requisito	Justificativa	Flex.
	Requisitos não funcionais serão relacionados aos status do subsistema	Muitas vezes determinados status têm requisitos não funcionais mais restritivos do que outros. Por exemplo, componentes eletrônicos suportam temperaturas mais altas para armazenamento do que em operação. Tal distinção permite fazer um projeto sem superdimensionamento, contribuindo para manter a integridade de informações relevantes.	Desejável
	Pelo menos um requisito de verificação deve refinar todo requisito não funcional	O método de verificação ser incluído porque pode ter efeitos sobre a arquitetura e seguramente tem efeitos sobre o custo de até duas ordens de grandeza acima do custo de aquisição do sistema em si. Essa regra contribui para manter a integridade de informações relevantes.	Desejável
Caracterizando status	A especificação deve traduzir os requisitos das funções de serviço em requisitos das funções técnicas	Essa tradução é essencial para que o sistema atenda aos requisitos. Trata-se de preservar a integridade das informações relevantes ao projeto.	Mandatário
	A especificação deve traduzir os requisitos não funcionais do sistema em requisitos das funções técnicas	Essa tradução é essencial para que o sistema atenda aos requisitos. Trata-se de preservar a integridade das informações relevantes ao projeto.	Mandatário
	Requisitos devem ser compreensíveis pelo receptor	As mentes humanas são sistemas de fluxo de informação que precisam de treinamento custoso para se tornarem eficientes. A maioria das pessoas não pode ou não quer aprender um método diferente de processamento de informação dentro de prazos apertados. Internamente à equipe de projeto, é possível estabelecer programas de treinamento para uniformizar o protocolo de comunicação entre os membros da equipe. Entretanto, ao se comunicar com representantes de fornecedores que não tem a mesma cultura, linguagens ou vocabulários estranhos ao fornecedor devem ser evitadas. Ao entrar em contato com pessoas de diferente cultura, algumas pessoas tendem a entrar em conflito ou cometer enganos. Este requisito advém da necessidade de facilitar a comunicação.	Mandatário

Status	Requisito	Justificativa	Flex.
	Para cada par função técnica e status no qual a função técnica está ativa, a especificação deve vincular pelo menos um requisito de desempenho	A falta de informação de desempenho por status do sistema pode causar problemas de atendimento aos requisitos ou superdimensionamento. O desempenho tem que estar presente porque é um aspecto com efeito determinante sobre o dimensionamento da solução. A definição de requisitos de desempenho por status leva a soluções mais eficientes porque variam de status para status. Por exemplo, um sistema pode precisar executar uma função de serviço com alto desempenho e alta confiabilidade em um status e, em outro status, fazer a mesma função com baixo desempenho e baixa confiabilidade. A redução da confiabilidade permite a realização de operações de manutenção, reduzindo a quantidade de redundâncias. Neste caso, um requisito funcional por status leva a soluções eficientes em termos de custo benefício. Existe um custo, em termos de tempo, para que a pessoa calcule e justifique toda a informação intrínseca a um requisito funcional tal como o proposto. Entretanto, tal esforço é muito menor do que aquele necessário para conceber uma solução, reduzindo o trabalho médio dentro de uma equipe de projeto. Em todo caso, essa regra preserva a integridade das informações relevantes ao projeto.	Desejável
	A especificação deve vincular pelo menos um requisito de desempenho a cada função irrelevante	Funções irrelevantes podem ser ignoradas na definição de status, mas elas continuam a existir e seus desempenhos podem ser necessários para evitar superdimensionamento. Ainda que o componente tenha custo muito inferior ao do produto, seu superdimensionamento pode ser mais caro do que o trabalho de especificação. Neste caso, essa regra preserva a integridade das informações relevantes ao projeto.	Desejável
	Para cada par função técnica e status no qual a função técnica está em prontidão, a especificação deve vincular pelo menos um requisito de resposta temporal	A resposta temporal de acionamento de uma função é um aspecto dimensionante para alguns componentes, tais como motores de partida. Pode inclusive restringir as soluções possíveis, levando a impor arquiteturas específicas. Essa regra preserva a integridade das informações relevantes ao projeto.	Desejável

Status	Requisito	Justificativa	Flex.
	Para cada par função técnica e status no qual a função técnica está inibida, a especificação deve vincular pelo menos um requisito de máxima frequência de atuação inadvertida	Em alguns casos, se um sistema mudar seu estado em um momento errado, acidentes podem ocorrer. Por exemplo, um disjuntor que protege uma rede elétrica pode causar corrupção da memória de um computador. Sempre que isso ocorrer, a especificação deve definir a taxa máxima de atuação inadvertida. Em consequência, soluções para evitar tais eventos devem ser concebidas, o que ocorrerá somente se houver requisitos para tanto. Requisitos funcionais definem como o sistema deve operar e como não deve operar, definindo também limites para a operação. A falta de requisitos limitando a operação levará à falta de funções de segurança e de intertravamentos, o que gerará retrabalho durante o projeto ou acidentes durante a vida útil do sistema. Assim, um trabalho de análise de segurança é adicionado, mas contribui para preservar a integridade de informações essenciais ao projeto dos subsistemas.	Mandat ório
	Pelo menos um requisito de taxa de falha deve refinar todo requisito de desempenho	Taxa de falhas indica um objetivo de confiabilidade, que precisa ser incluído por ser dimensionante em termos de nível qualidade ou de redundância. A taxa de falhas pode ser em termos de falha por tempo de operação ou falhas sob demanda. Essa regra contribui para preservar a integridade de informações essenciais ao projeto dos subsistemas.	Negoci ável
	Pelo menos um requisito de taxa de reparo deve refinar todo requisito de taxa de falha	O tempo médio de restauração (<i>Mean Time To Restore</i> - MTTR) é um objetivo de manutenibilidade a ser fixado. A manutenção também é determinante em termos de escolhas tecnológicas e arquiteturais, sendo complementar à confiabilidade, pois não basta saber a frequência de falhas para obter a disponibilidade do produto. Essa regra contribui para preservar a integridade de informações essenciais ao projeto dos subsistemas.	Negoci ável
	Um requisito de probabilidade de falha sob demanda deve refinar todo requisito de resposta temporal	A fase será realizada por uma solução que terá uma confiabilidade imperfeita. Essa informação requer pouco esforço para ser produzida, mas evita superdimensionamento ou confiabilidades inaceitáveis. Essa regra contribui para preservar a integridade de informações essenciais ao projeto dos subsistemas.	Desejáv el

Status	Requisito	Justificativa	Flex.
	Especificações devem ser listas de requisitos atômicos numerados	Muitas pessoas estão acostumadas a processar requisitos em uma sequência linear de informação. Computadores também processam as informações de maneira linear sob a forma de tabelas em bancos de dados. Uma lista pode ser usada para entregar requisitos, e para checar o atendimento de uma solução a todos os requisitos. Especialmente para este último caso, o uso de listas é considerado muito cômodo por muitas pessoas. O uso de números para identificar requisitos torna mais fácil referenciar, localizar e rastrear requisitos durante um projeto. Requisitos devem ser atômicos no sentido que eles devem ter uma única ideia (relaciona uma propriedade com uma condição) com todos seus qualificadores necessários, tais como a flexibilidade. Se mais de uma ideia for incluída, durante a verificação poderão haver problemas, pois poderá haver atendimento parcial. Por outro lado, se os requisitos forem atômicos, a informação sobre o atendimento é binária. Logo, listas de requisitos atômicos numerados facilita a comunicação durante todo o projeto.	Desejável
	Propriedades podem ser grandezas com unidade de medida	Exemplos de propriedades: massa, preço, volume. É necessário estabelecer uma regra de transição da linguagem humana para a linguagem de projeto. Para facilitar esta transição, este trabalho usa a gramática da língua para enquadrar a definição de conceitos, dado que a gramática é amplamente conhecida. A falta de uma definição objetiva do que é uma propriedade pode acarretar incompreensão dos requisitos baseados nas mesmas. Quantificável significa que existe uma unidade de medida da característica, como quilograma é uma unidade de medida de massa. Tal regra custa pouco para ser imposta e elimina muito erro de comunicação ao longo de todo o projeto.	Opcional
	Propriedades podem ser uma opção dentro de uma lista pré-definida	Exemplos são cores definidas em termos de bytes vermelho, verde e azul (RGB) ou em termos de padrões. Opções definidas são uma lista de possíveis variantes que a característica pode assumir, como método de fabricação pode ser por usinagem, estampagem, forja. Tal regra custa pouco para ser imposta e elimina muito erro de comunicação ao longo de todo o projeto.	Opcional
	Propriedades podem ter complementos nominais ou adjetivos	Exemplos de propriedades com complementos nominais: taxa de falha, frequência de uso, método de fabricação. Tal regra custa pouco para ser imposta e elimina muito erro de comunicação ao longo de todo o projeto.	Opcional

Status	Requisito	Justificativa	Flex.
	Pelo menos um requisito de verificação deve refinar todo requisito de desempenho	O método de verificação ser incluído porque pode ter efeitos sobre a arquitetura e seguramente tem efeitos sobre o custo de até duas ordens de grandeza acima do custo de aquisição do sistema em si. Tal regra minimiza os seguintes riscos: 1 – perder tempo com um fornecedor sem a capacidade necessária; 2 – perder tempo com uma solução fora do orçamento; 3 – estourar o orçamento do projeto; 4 – estourar o prazo do projeto; 5 – degradar a solução final em termos de desempenho ou segurança. Essa regra contribui para preservar a integridade de informações essenciais ao projeto dos subsistemas.	Desejável
	Todo requisito de verificação deve definir o método de verificação	Existem quatro famílias de métodos de verificação, de acordo com a NASA (2007). São elas, em ordem crescente de custo, qualidade e confiabilidade: inspeção, análise, demonstração e teste. Além do método de verificação, é desejável que o requisito de refino estabeleça a norma para fazer a verificação. Essa regra contribui para preservar a integridade de informações essenciais ao projeto dos subsistemas.	Desejável
	Todos os requisitos devem ser refinados por um requisito de flexibilidade	A importância da flexibilidade vem do fato de que ninguém tem conhecimento total sobre o que é possível ou não na prática. Do lado do fornecedor, por outro lado, é fundamental saber quais clientes ele pode realmente satisfazer para evitar perder tempo e dinheiro com concorrências nas quais ele não tem chance. Assim, a declaração de flexibilidade leva a instituição contratante a receber menos ofertas inadequadas e mais ofertas adequadas, reduzindo o ruído no processo.	Mandatário

Status	Requisito	Justificativa	Flex.
	Em um requisito, a flexibilidade será proporcional ao risco de inviabilidade	No contexto de uma equipe de projeto, a produção de especificações demanda tempo, bem como os fornecedores precisam de tempo para produzir propostas. A rigor, poucos sabem exatamente o que é viável ou não, exceto em caso de reuso. Do lado do fornecedor, a redação de propostas comerciais pode ser cara e tem pouca probabilidade de resultar em um contrato. Ao identificar requisitos mandatórios inviáveis, um fornecedor provavelmente não perderá tempo em redigir uma proposta. Mesmo que haja uma resposta, a existência de um requisito mandatório impossível implicará em retrabalho das especificações e atraso do projeto. Isso ocorre porque mandatório significa que o projeto não pode avançar sem que o requisito seja atendido. Por outro lado, o emprego exclusivo de requisitos seguramente viáveis entrava a inovação e a otimização. Uma solução é assegurar que apenas requisitos mandatórios sejam viáveis. Requisitos negociáveis devem ser provavelmente viáveis. Requisitos desejáveis ou opcionais podem ter alto risco de serem inviáveis. Assim, a chave para minimizar os riscos de estagnação e de tecnologia é acoplar o nível de exigência de desempenho com a razão inversa da flexibilidade. Ou seja, para aspectos centrais do projeto, fazer requisitos mandatórios que sejam seguramente atingíveis, e para aspectos secundários, requisitos desejáveis que estejam além da última geração. Concluindo, em um projeto bem gerenciado, quase nunca todos os requisitos serão viáveis. Do lado do fornecedor, por outro lado, é fundamental saber quais clientes ele pode realmente satisfazer para evitar perder tempo e dinheiro com concorrências nas quais ele não tem chance. Quando uma empresa fornecedora recebe uma especificação onde está definido o que é essencial e o que é acessório, ela terá maior probabilidade de fazer uma oferta adequada. Do contrário, ela pode adotar uma perspectiva arrojada e fazer uma proposta ignorando os requisitos não atendidos, ou adotar uma postura conservadora e não fazer oferta caso algum requisito não seja atendido. Essa gradação permite que o projeto avance rapidamente com abertura à inovação, facilitando a comunicação enquanto o ruído gerado por requisitos inviáveis é reduzido.	Mandat ório

Status	Requisito	Justificativa	Flex.
	Os requisitos classificados como mandatórios devem ser viáveis tanto individualmente como coletivamente	No contexto de um projeto, requisitos inviáveis são causa de perda de tempo, energia e dinheiro, o que significa ineficiência. Na interação com fornecedores, o efeito de requisitos inviáveis é particularmente nefasto, pois fornecedores podem passar a evitar a ler toda e qualquer pedido de informação posterior. Cuidado especial deve ser tomado para averiguar se o conjunto de requisitos mandatórios é simultaneamente viável mesmo que cada requisito seja individualmente viável. Por exemplo, um motor pode ter uma dada potência nominal. Um motor pode também uma restrição de peso máximo. Mas pode ser que nenhum motor possa ter uma certa potência e um peso muito pequeno. O responsável por um sistema deve demonstrar que o conjunto de requisitos mandatórios é viável para reduzir ruído na comunicação dentro da equipe de projeto e com fornecedores. Uma vez que requisitos mandatórios inviáveis são inúteis e danosos, devem ser considerados como ruído a ser eliminado.	Mandatório
Escolhendo método	Para cada subsistema, a especificação deve escolher o método de obtenção (projeto interno, projeto externo, prateleira)	O método de obtenção de um subsistema afeta a maneira de especificar não somente o subsistema em si como os subsistemas adjacentes. Assim, tal decisão facilita o fluxo de informação.	Mandatório
Caracterizando interfaces	Se um subsistema for reusado, a especificação deve incluir requisitos das interfaces aplicados aos subsistemas adjacentes	O reuso permite ter acesso a uma grande gama de informação. Em paralelo, reuso implica em ausência de alterações para evitar custos. Assim, os subsistemas adjacentes que forem obtidos por outros métodos precisam se adequar às interfaces que já estão definidas. Tal regra facilita o fluxo de informação por reduzir os custos.	Desejável

Status	Requisito	Justificativa	Flex.
	A especificação deve declarar a autoridade de projeto das interfaces	No início do projeto, naturalmente as especificações não contém requisitos não funcionais impondo características das interfaces, pois o mais importante são as funções. Outra razão é a falta de conhecimento da pessoa que escreve a especificação sobre as tecnologias envolvidas nas interfaces. As interfaces podem ser definidas pelo projeto e integradas na especificação somente no momento de formalizar o contrato. Embora detalhes das interfaces não sejam importantes no início, é fundamental gerenciar as interfaces durante a redação do contrato e posterior obtenção. Se houver um erro no detalhamento das interfaces, problemas de integração certamente ocorrerão e criarão gastos e atrasos que podem implicar em prejuízos muito maiores do que o valor dos subsistemas em questão. A definição de uma autoridade de projeto de interfaces reduz os riscos de atraso uma vez que as responsabilidades ficam claras. Assim, essa regra preserva a integridade de dados, evitando prejuízos.	Negociável
Compatibilizam do interfaces	Sempre que necessário, o projeto deverá revisar a arquitetura do sistema	Cada uma dessas atividades pode requerer mudanças arquiteturais para manter a consistência do sistema. É melhor mudar incrementalmente a arquitetura do que esperar até o fim da atividade de análise de cima para baixo para fazer todas as mudanças. A razão é a dependência de cada passo da análise em relação à arquitetura, sendo que cada passo também pode mostrar a necessidade mudar a arquitetura. Assim, a convergência para uma solução será mais lenta se a arquitetura não for mudada prontamente, entretanto o fluxo de informação. Essa regra facilita o fluxo de informação no projeto.	Desejável

Status	Requisito	Justificativa	Flex.
	O projeto deve empregar subsistemas sob a forma de caixa preta	Em termos de arquitetura de controle, os produtos devem enviar aos componentes apenas ordens de procedimentos e valores de referência para variáveis de processo. Os componentes devem informar apenas seu modo de operação e os valores efetivos das variáveis de processo relacionadas aos valores de referência recebidos. Em geral, um produto não deve usar informações de subcomponentes de seus componentes nem comandar tais subcomponentes. Produtos devem apenas enviar comandos a seus componentes para possibilitar a operação em malha fechada de cada componente. O fluxo de informação (ordens ou dados para tomada de decisão) fora de relações de subordinação direta podem tornar o produto inteiro instável a uma frequência inaceitável. Por exemplo, um computador de coordenação não deve dar ordens a atuadores de campo. Ao invés disso, deve enviar ordens a controladores que levem o modo de operação corrente (calculado em função de variáveis de processo) em consideração antes de decidir as ações a serem tomadas. Essa regra implicitamente força o respeito à hierarquia, reduzindo o risco por concentrar a tomada de decisão em um dado nível hierárquico antes de começar o próximo nível. Essa regra também reduz o tempo gasto pelos arquitetos para conceber uma solução porque inibe a tentação de imaginar o que existe dentro de cada caixa preta. Adicionalmente, essa regra permite melhores decisões, seja de projeto ou de operação, por preservar a autonomia e evitar requisitos ou ordens conflitantes. O respeito à via hierárquica reduz o ruído.	Desejável
	O projeto deve compatibilizar os requisitos de interface dos componentes	O primeiro passo do projeto é checar a compatibilidade de interface entre os componentes. Se as interfaces não forem compatíveis, o uso de adaptadores é uma opção. Outra opção é impor novos requisitos de interface aos componentes. A incompatibilidade de interfaces pode até impor mudanças na arquitetura do produto. Essa regra é importante para prevenir problemas de integração nas fases subsequentes do projeto. O projeto deve também verificar as interfaces com o usuário e as funções de controle para certificar que os componentes sejam capazes de atender às necessidades operacionais. Essa regra impõe que os problemas de compatibilização de interface sejam resolvidos no nível mais baixo e mais fácil, sintetizando a informação para os níveis superiores. Assim o fluxo de informação fica simplificado, facilitando o fluxo de informação durante o projeto.	Mandatário

Status	Requisito	Justificativa	Flex.
Definindo modos de operação	Variáveis e modos de operação de componentes devem permitir o reconhecimento imediato do modo de operação do produto	Os modos de operação de um produto são soluções para atender aos status do sistema, o que permite identificar o modo de operação por meio de informações que indiquem o status das funções. A chave é identificar, diretamente a partir das variáveis medidas previstas em projeto, o modo de operação corrente do produto sem recorrer ao histórico de operação. Uma vez que o produto obedeça a essa regra, é possível mudar ou reiniciar o sistema de controle sem incorrer em riscos de decisões erradas. Essa regra reduz a complexidade do sistema de controle e melhora a segurança a um preço baixo por tornar a operação robusta a perturbações. Essa regra facilita o fluxo de informação através do produto, o que atende ao enunciado da lei construtal.	Desejável
	O projeto deverá definir as configurações físicas permitidas para cada modo	Configurações físicas são faixas de variáveis de processo e combinações de modos de componentes. É interessante ter a definição de mais de uma configuração física para cada modo de operação para conferir flexibilidade à operação e aumentar a confiabilidade. A identificação de configurações físicas é essencial para identificar dependências funcionais para calcular desempenhos e confiabilidade. Pular esse passo pode levar a cálculos baseados em hipóteses que podem ser falsas e provavelmente não registradas. Assim, esse passo reduz a entrada de informação falsa no projeto, melhorando o fluxo de informação.	Desejável
	O projeto deverá identificar as configurações físicas proibidas, se houver	Dependendo da natureza dos produtos, podem haver configurações físicas que causem acidentes ou eventos indesejáveis. Tais configurações devem ser declaradas e soluções para evitá-las devem ser incluídas no produto. A definição de configurações físicas é fundamental para checar se as sequências de atuação dos componentes são adequadas e para fazer a análise de risco. Esta regra assegura que informações relevantes sejam preservadas durante um projeto, melhorando o fluxo de informações.	Mandatário
	Os modos de operação devem atender a todos os status	O diagrama de modos de operação é a base para o resto da análise e esse passo é importante para identificar novos modos de operação o mais cedo possível. Descumprir essa regra pode levar a problemas de integração e manutenção porque necessidades sistêmicas não foram atendidas. Na melhor das hipóteses, o descumprimento desta regra causa problemas de confiabilidade e disponibilidade e, na pior das hipóteses, a integração pode vir a ser impossível. Em outras palavras, esta regra gera um trabalho adicional na fase de concepção, mas elimina muitos riscos e contratempos na fase de integração por manter a integridade das informações relevantes.	Mandatário

Status	Requisito	Justificativa	Flex.
	Mais de um modo pode atender um dado status	Após obter novos dados sobre os componentes, novos modos de operação podem ser requeridos devido a razões tecnológicas. O diagrama de modos de operação deve levar em conta restrições tecnológicas e incluir mais modos de operação não funcionais, como manutenção, parada longa, parada curta e prontidão. Modos de operação não funcionais podem diferir uns dos outros pelo tempo para entrar em operação, já que estar pronto para partir imediatamente (prontidão) é bem diferente de manutenção de longa duração. Por exemplo, um modo de operação de parada curta pode vir a ser necessário para realizar manutenção em componentes, necessidade que só será identificada depois de escolher as soluções tecnológicas. Em outras palavras, esta regra gera um trabalho adicional na fase de concepção, mas elimina muitos riscos e contratempos na fase de integração por manter a integridade das informações relevantes.	Opcional
	Um modo pode atender vários status	Às vezes um mesmo ato físico (modo de operação) pode servir a diferentes propósitos (funções), dependendo da situação. Um exemplo é um gerador de vapor que tem duas funções distintas: resfriar o circuito primário e fornecer vapor para a conversão de energia. O modo de operação para atender ambos casos pode ser o mesmo. Tal permissão reduz o número de modos de operação e procedimentos, evitando ruído.	Opcional
Definindo configurações	O projeto deve definir as configurações físicas de referência	Os modos de operação são flexíveis, não sendo adequados para o cálculo das propriedades do produto. Vale ressaltar que as propriedades muitas vezes são antagônicas e, se forem consideradas no pior caso, irão requerer desempenhos impossíveis. Assim, o projeto deve definir configurações físicas (definições exatas de modo de operação dos componentes e valores de variáveis de processo) para o cálculo de propriedades do produto. Tal regra reduz o ruído no projeto por uniformizar as hipóteses de cálculo.	Mandatário
	A justificativa de inclusão de uma configuração física de referência deve ser verificação de dimensionamento de componentes	Cada configuração física de referência demanda tempo para ser definida e mais tempo para efetuar o cálculo das propriedades do produto. Assim, reduzir as configurações físicas ao mínimo necessário contribui para reduzir o ruído.	Desejável

Status	Requisito	Justificativa	Flex.
Calculando desempenhos	O projeto deve estimar o desempenho das funções para cada configuração física de referência	Usando as configurações físicas de referência, os requisitos de desempenho podem ser verificados. Calcular desempenhos é fundamental para saber se a solução proposta é aceitável e os resultados servem como dados para tomada de decisões. Essa regra contribui para preservar a integridade de informação relevante ao longo do projeto.	Mandat ório
	O projeto deve estimar a confiabilidade das funções para cada configuração física de referência	Calcular a confiabilidade (taxa de falhas) é fundamental para saber se a solução proposta é aceitável e os resultados servem como dados para tomada de decisões. Essa regra contribui para preservar a integridade de informação relevante ao longo do projeto.	Desejáv el
	O projeto deve estimar a taxa de reparo das funções para cada configuração física de referência	Junto com a confiabilidade, a reparabilidade é fundamental para determinar a disponibilidade do produto, que será útil para determinar o custo total de ciclo de vida, que é uma informação fundamental à tomada de decisão. Essa regra contribui para preservar a integridade de informação relevante ao longo do projeto.	Desejáv el
Definindo transições	O modo de operação medido deverá guiar o comportamento do produto	Pegando o exemplo de uma válvula de isolamento e duas chaves de fim de curso para detectar as posições aberto ou fechado. Quando a posição medida for aberta, o controlador deve apenas comandar o fechamento, e quando a posição medida for fechada, devem haver somente comandos para abrir. Essa regra é importante porque vários atores podem controlar um mesmo produto, que pode sofrer também muitas perturbações do ambiente. Um computador, um operador remoto ou um operador podem controlar um produto em momentos diferentes. Com essa regra sendo obedecida, o controlador saberá sempre o que fazer independentemente do histórico de operação. A um produto concebido de acordo com essa regra é um verdadeiro sistema cibernético, pois opera em malha fechada. Sistemas cibernéticos cometem menos erros e sofrem menos acidentes, o que reduz custos globais durante a vida do produto devido à maior disponibilidade e prejuízos menores e mais raros. Os grandes benefícios da operação em malha fechada podem ser obtidos com um pequeno aumento do esforço de projeto e investimento em instrumentação. De acordo com a lei construtal, essa regra facilita o fluxo de informação durante a vida do produto por reduzir ao ruído de processo na forma de ordens e comandos incoerentes com a realidade.	Negoci ável

Status	Requisito	Justificativa	Flex.
	O projeto deve prever pelo menos um procedimento por fase ativa	Toda fase representa uma necessidade de implementação de um procedimento para efetuar a mudança de modo de operação correspondente à mudança de status. Quando o sistema muda de status exclusivamente sob a ação dos sistemas externos, tal fase é passiva e não requer procedimentos relativos ao produto. Mas se o status do sistema requer alguma mudança interna, então a fase é ativa e requer um procedimento. Esta regra gera um trabalho adicional na fase de concepção, mas elimina muitos riscos e contratempos na fase de integração por manter a integridade das informações relevantes.	Mandat ório
	Se o mesmo modo realiza os status de início e fim de uma fase, tal fase não precisa de um procedimento	Quando um único modo realiza dois status, quaisquer fases entre tais status dispensam a implementação de um procedimento. Essa regra simplifica o projeto, reduzindo ruído.	Opcion al
	A definição de procedimentos pode requerer a definição de novos status	Os procedimentos de um produto podem impor novos modos de operação ao produto, como o uso de uma fonte de energia para dar a partida. Um exemplo é o uso de ar comprimido para dar partida em um motor diesel. Procedimentos podem até impor a adição de novos componentes, tais como motores de arranque. Tal fato advém da incapacidade do especificador de prever todas as necessidades do produto que venha a atender o sistema. Assim, permitir que o projeto adicione funções recebidas, novos status e novas fases melhora a rapidez com que o projeto avança, facilitando o fluxo de informações.	Opcion al
	Um procedimento pode realizar várias fases	Isso pode ocorrer quando existem várias fases levando ao mesmo status, tal como desligamento em emergência. A definição de um único procedimento simplifica o projeto, reduzindo ruído.	Opcion al

Status	Requisito	Justificativa	Flex.
	O projeto deve definir cada procedimento como sequência de procedimentos dos componentes ou sistemas externos	Os procedimentos de mudança de modo de operação são uma fonte de riscos de projeto, já que eles podem requerer novos atuadores ou serviços de outros sistemas externos. Um procedimento pode ser impossível devido a limitações físicas ou tecnológicas. Assim sendo, é importante declarar os procedimentos operacionais desejados para que haja confirmação por parte dos fornecedores, especialistas ou pessoas com experiência. Tal definição operacional pode revelar a necessidade de mudança na arquitetura, incluindo adição de novos componentes ou interfaces e modos de operação para receber apoio de sistemas externos. Se o projeto contar com procedimentos que os componentes não têm, haverá problemas de integração. Assim, esta regra contribui para reduzir o ruído.	Mandatório
	O projeto deve demonstrar que todo procedimento respeita as configurações físicas permitidas	As transições de modo de operação de um produto precisam ser descritas em detalhe e verificações (por meio de análise) de sua efetividade precisam ser realizadas. Não apenas a efetividade, mas a segurança deve ser levada em conta verificando se, em todos os passos, as configurações físicas não causam riscos. Tais verificações podem ser feitas por meio de simulações, que reduzem os riscos de integração durante a fase de construção a um custo relativamente baixo. Esta regra demanda esforço no início do projeto e reduz esforços muito maiores na fase de construção, integração e teste. Esta regra reduz a propagação de ruído na forma de comportamentos (operação) ou arquitetura inadequados dos produtos.	Mandatório
Projetando interfaces	O projeto deverá definir requisitos de interface	Interfaces incluem flanges, conexões elétricas, calços e interfaces com o ser humano. Interfaces com o ser humano requerem atenção especial porque sua descrição é complexa, tendo muitos requisitos funcionais definindo funções de controle. Além de ter custo considerável, as interfaces são fonte de risco industrial (acidentes) e gerencial (atraso no projeto). Esta regra mantém a integridade das informações relevantes.	Desejável

Status	Requisito	Justificativa	Flex.
	A observabilidade deve ser compatível com os riscos de operação	Podem existir informações cuja perda pode levar o produto a um risco inaceitável. Por exemplo, quando entidades (computadores ou pessoas) decidem com base em informações falsas ou incompletas, acidentes podem ocorrer, causando danos ao material ou ao pessoal. Neste caso, são necessárias medidas para reduzir a frequência da perda da informação, o que tornaria o risco aceitável. Tais medidas podem ser redundância, segregação, independência e diversidade dos canais de informação, que devem ser proporcionais à gravidade da consequência da perda do dado. Do outro lado, a observabilidade tem o seu custo e excessos devem ser evitados, reduzindo o ruído.	Negociável
Analisando riscos	O projeto deverá gerenciar riscos criados pelos componentes	Vale lembrar que os acidentes são sempre movidos pela presença de energia acumulada (velocidades elevadas, combustíveis, pressão) e a análise de risco deve priorizar componentes onde haja grandes quantidades de energia. O nível mais baixo da hierarquia deve gerenciar a segurança e limitações operacionais porque níveis hierárquicos inferiores têm melhor acesso à informação sobre os riscos causados pelos componentes e os melhores meios de mitigá-los. Esta regra é uma aplicação da hierarquia para atingir objetivos de segurança, facilitando o fluxo de informação.	Negociável
	O projeto deverá declarar os riscos internos do produto em termos de natureza, gravidade, efeitos nas interfaces e frequência	Sempre que existir energia armazenada ou transformada, existe risco de liberações de energia descontrolas que podem matar pessoas ou causar danos financeiros. Tal informação é necessária para gerenciar a segurança no produto de nível superior, que poderá incluir meios para mitigar as consequências das fontes de risco internas. Somente quando não for possível tornar todos os riscos aceitáveis, uma síntese dos riscos inaceitáveis deve ser transmitida para o nível superior. Isso significa que o arquiteto do nível imediatamente acima precisa conhecer os riscos causados pelos componentes para fazer o balanço de segurança. Assim sendo, esta regra contribui para preservação de informações relevantes.	Mandatário
	O projeto deve analisar os riscos para cada passo dos procedimentos	Durante a execução dos procedimentos, os riscos ocasionados pela falha de componentes devem ser analisados. Ninguém pode prevê tudo de uma vez, sendo necessário realizar um estudo iterativo, identificando as consequências de cada passo. Tais consequências podem ser riscos, danos a componentes ou efeitos indesejados, que podem impor mudanças no projeto. Assim sendo, esta regra contribui para preservação de informações relevantes.	Negociável

Status	Requisito	Justificativa	Flex.
Calculando propriedades	Caso o projeto tenha mudado a arquitetura do produto, o projeto deve recomeçar desde o começo	Para facilitar a atividade de projeto, não é necessário recomeçar o projeto toda vez que a arquitetura do produto sofre uma mudança. Entretanto, antes de calcular as propriedades, e preencher a matriz de atendimento, é fundamental fazer todas as atividades do projeto com a arquitetura definitiva. A razão desta regra é evitar inconsistências, reduzindo o ruído do processo na forma de dados errados como resultado do projeto.	Mandat ório
	Balancos devem calcular intervalos de confiança das estimativas	Uma vez que a informação é sempre imprecisa e incompleta, o processo de projeto precisa gerenciar riscos em termos de probabilidade de sucesso para cada desempenho ou propriedade. Cada vez que um desempenho (por exemplo, potência) ou uma propriedade (como peso) é calculada, o resultado é uma estimativa, que tem um intervalo de erro. Para evitar excesso de conservadorismo, toda solução proposta precisa incluir o intervalo de confiança, permitindo o gerenciamento de risco do produto de nível superior. Excesso de conservadorismo significa ineficiência do ponto de vista da lei construtal e pode ser evitado com a preservação da informação de intervalos de confiança.	Desejáv el
	O projeto deverá definir rotinas de manutenção e reparo em termos de natureza e duração	Rotinas de reparo e manutenção são informações relevantes para calcular a disponibilidade do produto de nível superior. As naturezas de algumas rotinas podem impor tempos significativos de parada devido à desmontagem. A duração de cada manutenção ou reparo será usada para estimar o tempo para restabelecer funções, que é usado para calcular a disponibilidade do produto. Esta regra contribui para manter a integridade de uma informação relevante que são os dados de entrada para calcular a disponibilidade do produto.	Negoci ável
Verificando atendimento	O projeto deve preencher a matriz de atendimento	Para facilitar a verificação de conformidade e melhorar a qualidade do projeto, a descrição de produto deve apresentar a matriz de atendimento. A matriz de atendimento é uma tabela que deve integrar os requisitos em um conjunto de colunas e o atendimento a cada requisito em outra coluna. Adicionalmente, deve haver uma coluna com referência à prova ou demonstração de atendimento do requisito na descrição de produto ou memorial de cálculo. A matriz de atendimento é uma ferramenta que reduz enormemente o tempo para verificar o trabalho, sendo uma grande solução para facilitar o fluxo de informação.	Mandat ório

Status	Requisito	Justificativa	Flex.
	O projeto deverá verificar o cumprimento dos requisitos não funcionais	Requisitos não funcionais também são fundamentais por se relacionar com propriedades do produto, como peso, custo e segurança. O cumprimento dos requisitos não funcionais é uma informação relevante a ser sempre preservada durante um projeto, pois afeta diretamente a tomada de decisões.	Mandatário
	A matriz de atendimento deverá incluir a probabilidade de atendimento dos requisitos mandatórios	Durante os estágios iniciais do projeto, quando várias opções competem entre si, é necessário saber o risco de não atender requisitos mandatórios. Durante o desenvolvimento de produtos complexos, pode não ser possível assegurar o atendimento de todos requisitos mandatórios, funcionais e não funcionais. Em alguns casos, pode ser necessário demandar o desenvolvimento simultâneo de duas alternativas para reduzir riscos de projeto. Por exemplo, uma solução cara com baixo risco e outra solução com alto risco e performance, mas com baixo custo devido ao uso de novas tecnologias. Porém, o arquiteto do produto de nível superior pode tomar conhecimento da necessidade de buscar caminhos alternativos somente após receber informação sobre os riscos de projeto. Vale ressaltar que a probabilidade de atender os requisitos é sempre inferior ao valor unitário, pois mesmo em caso de reuso, podem ocorrer externalidades que impeçam a aquisição. A questão é saber o risco e quem o assumirá ou tomará medidas para reduzi-lo. O risco deve ser informado sempre, pois é uma informação relevante para a tomada de decisão no gerenciamento do projeto.	Negociável