RENAN AGUZZOLI TRAVI

Avaliação do Sistema Diverso de Atuação em Plantas Nucleares de Potência

São Paulo
2023

RENAN AGUZZOLI TRAVI

Avaliação do Sistema Diverso de Atuação em Plantas Nucleares de Potência

Versão Corrigida

Dissertação apresentada à Escola Politécnica da Universidade de São Paulo para a obtenção do título de Mestre em Ciências.

Área de Concentração:
Engenharia de Sistemas.

Orientador:
Prof. Dr. Claudio Garcia.

São Paulo
2023

Este exemplar foi revisado e corrigido em relação à versão original, sob responsabilidade única do autor e com a anuência de seu orientador.

São Paulo, _____ de _____ de _____

Assinatura do autor: _____

Assinatura do orientador: _____

Catalogação-na-publicação

Travi, Renan Aguzzoli
Avaliação do sistema diverso de atuação em plantas nucleares de potência / R. A. Travi -- versão corr. -- São Paulo, 2023.
78 p.

Dissertação (Mestrado) - Escola Politécnica da Universidade de São Paulo. Departamento de Engenharia de Telecomunicações e Controle.

1.USINAS NUCLEARES 2.PREVENÇÃO DE ACIDENTES (SEGURANÇA) I.Universidade de São Paulo. Escola Politécnica. Departamento de Engenharia de Telecomunicações e Controle II.t.

Às minhas meninas, Soraia e Bianca.

Agradecimentos

Agradeço primeiramente ao meu orientador, Prof. Dr. Claudio Garcia, por todo apoio, ensinamentos e paciência. Tenho certeza que como fruto dessa orientação me tornei um profissional mais qualificado e uma pessoa melhor.

Gostaria de expressar meu profundo agradecimento à minha amada esposa, Soraia. Sua paciência, compreensão e apoio incondicional foram essenciais para que eu pudesse me dedicar plenamente à realização deste mestrado. Além de todo apoio emocional na realização deste trabalho, sua contribuição técnica foi de extrema importância.

Aos meus estimados professores que me guiaram e compartilharam conhecimento valioso, deixo meu sincero agradecimento. Em especial ao amigo Dr. Fellipe Garcia Marques e Dr. Marcos Santana Farias que contribuíram de forma enriquecedora ao desenvolvimento desta dissertação.

À Marinha do Brasil e aos amigos que a Marinha me deu, eu agradeço pela colaboração, troca de ideias e apoio mútuo ao longo desses anos. As discussões enriquecedoras, os momentos compartilhados e o trabalho em equipe contribuíram significativamente para minha formação. Seja nos momentos de estresse, dúvidas ou comemorações, vocês foram uma fonte de apoio inestimável.

"*A vida é igual a andar de bicicleta. Para manter o equilíbrio é preciso se manter em movimento.*"

Albert Einstein

Resumo

A crescente importância da energia nuclear e a geração de eletricidade a partir de usinas nucleares tornam necessário aprimorar a segurança e confiabilidade destas usinas. Para atender a estes requisitos, sistemas digitais redundantes são utilizados e, com isso, surge a possibilidade de Falha de Causa Comum. Para mitigar esta ocorrência, uma alternativa é a implementação do Sistema Diverso de Atuação (SDA), que tem se mostrado muito eficaz na consecução desse objetivo. Não há muitas publicações sobre o SDA, uma vez que o assunto é relativamente novo na indústria nuclear e não há consenso sobre suas bases de projeto. Ainda, os órgãos reguladores internacionais não possuem uma diretriz unificada sobre o tema. O presente trabalho apresenta um levantamento do estado da arte do SDA, assim como de seus motivadores, a falha de causa comum e os conceitos de diversidade e defesa em profundidade. Com base no levantamento bibliográfico, é realizada uma análise comparativa dos preceitos da literatura, assim como uma avaliação destes. O trabalho apresenta também a possibilidade do uso do *Field Programmable Gate Arrays* (FPGA) no desenvolvimento de SDA e a discussão de alguns projetos que implementaram o SDA.

Palavras-chaves: Sistema Diverso de Atuação; Planta Nuclear de Potência; Falha de Causa Comum; FPGA.

Abstract

The growing significance of nuclear energy and electricity generation from nuclear power plants make it necessary to enhance the safety and reliability of these plants. To meet these requirements, redundant digital systems are employed, giving rise to the potential for Common Cause Failure. To mitigate such occurrences, an alternative approach is the implementation of the Diverse Actuation System (DAS), which has proven highly effective in achieving this goal. There are limited publications on the DAS, as the topic is relatively novel in the nuclear industry, and there is no consensus regarding its design basis. Furthermore, international regulatory agencies lack a unified guideline on the subject. The present work provides a survey of the state of the art in DAS, along with its driver, common cause failure, and the concepts of diversity and defense in depth. Based on a literature review, a comparative analysis of the literature's precepts is conducted, as well as an evaluation of these. The paper also explores the potential use of Field Programmable Gate Arrays (FPGA) in DAS development and discusses some projects that have implemented DAS.

Keywords: Diverse Actuation System; Nuclear Power Plant; Common Cause Failure; FPGA.

Lista de Figuras

Lista de Tabelas

Lista de Abreviaturas e Siglas

AOO	Ocorrência Operacional Esperada, do inglês, *Anticipated Operational Occurrence*
ATWS	Transitório Esperado sem Desligamento Rápido, do inglês, *Anticipated Transient Without Scram*
CCF	Falha de Causa Comum, do Inglês, *Common Cause Failure*
CNEN	Comissão Nacional de Energia Nuclear
D3	Diversidade e Defesa em Profundidade, do inglês, *Diversity and Defense-in-Depth*
DBA	Acidente de Base de Projeto, do inglês, *Design Basis Accident*
DEC	Condições de Extensão do Projeto, do inglês, *Design Extension Conditions*
EPRI	*Electric Power Research Institute*
ESFAS	Sistemas de Atuação de Dispositivos Técnicos de Segurança, do inglês, *Engineered Safety Features Actuation Systems*
FPGA	*Field-Programmable Gate Array*
HDL	*Hardware Description Languages*
IAEA	Agência Internacional de Energia Atômica, do inglês *International Atomic Energy Agency*
IEC	*International Electrotechnical Commission*
IEEE	*Institute of Electrical and Electronic Engineers*
I&C	Instrumentação e Controle
INSAG	*International Nuclear Safety Advisory Group*
LOCA	Acidente de Perda de Refrigerante, do inglês, *Loss of Coolant Accident*
NPP	Plantas Nucleares de Potência, do inglês, *Nuclear Power Plant*
NRC	*United States Nuclear Regulatory Commission*
ONU	Organização das Nações Unidas
PIE	Evento Iniciador Postulado, do inglês, *Postulated Initiating Event*

PLC	Controlador Lógico Programável
RAS	Relatório de Análise de Segurança
SDA	Sistema Diverso de Atuação
SCRAM	Desligamento de emergência do reator
V&V	Verificação e Validação
WNA	World Nuclear Association

Sumário

1 Introdução

No ano de 2020, a produção de energia elétrica no mundo a partir da matriz nuclear foi de aproximadamente 391 GW, produzidos em 443 reatores nucleares. Isso corresponde a 10% da energia elétrica produzida mundialmente (EMPRESA BRASILEIRA DE ENERGIA, 2020). Ressalta-se ainda que no Brasil, as duas usinas nucleares existentes (Angra 1 e Angra 2) produziram 14,6 GW no ano de 2022, o que corresponde a 2,1% da energia elétrica produzida no país (EMPRESA BRASILEIRA DE ENERGIA, 2023).

A energia nuclear pode ter um papel de destaque nos próximos anos, por alguns motivos. O primeiro é a baixa emissão de CO_2, que vai ao encontro dos objetivos de desenvolvimento sustentável da Organização das Nações Unidas (ONU), para a geração de energia limpa e acessível. Outro motivo é a possibilidade de aumento da robustez e resiliência dos sistemas elétricos na transição energética, com uma maior participação de fontes renováveis, como a energia solar e eólica, tendo em conta a sua alta variabilidade de fornecimento (EMPRESA BRASILEIRA DE ENERGIA, 2020).

Com o desenvolvimento dos sistemas digitais nos mais diversos setores da indústria, o setor nuclear também passou a utilizar esses recursos, aproveitando assim os seus benefícios, como o aumento da confiabilidade e disponibilidade, a automatização de alarmes, facilidade de desenvolvimento e implementação, entre outros. A indústria nuclear passou a utilizar sistemas digitais também em sistemas de segurança de plantas nucleares de potência - *Nuclear Power Plants* (NPP).

A elevada confiabilidade nos sistemas de segurança deve-se em parte à utilização de *hardwares* independentes e redundantes, o que assegura a execução de suas funções críticas, mesmo na ocorrência de falhas. Entretanto, a utilização de sistemas digitais induz a um potencial risco de *Common Cause Failures* (CCF), devido aos erros realizados durante o seu desenvolvimento, que podem tornar ineficiente a redundância e desabilitar múltiplos equipamentos ou sistemas, que utilizam recursos compartilhados ou elementos idênticos de software (NGUYEN, 2010).

A falha de causa comum, do inglês *Common Cause Failures* (CCF), pode ser definida como a falha simultânea de duas ou mais funções, sistemas, subsistemas ou componentes como consequência da mesma causa. Esta falha simultânea é considerada quando o intervalo de tempo entre as falhas é muito curto, para permitir o reparo completo do primeiro item a falhar antes que um ou mais itens também falhem. Destaca-se ainda que a CCF pode ocorrer devido a diversos fatores iniciadores, com origem no projeto, operação, aspectos ambientais e fatores humanos (NGUYEN, 2010).

Para suprir a deficiência da CCF nos sistemas de segurança das plantas nucleares,

uma estratégia possível é a implementação do Sistema Diverso de Atuação (SDA). O SDA é considerado um dos métodos mais eficazes para combater a CCF de sistemas digitais de segurança. Ele atua como um *backup* do sistema de segurança do reator (WANG et al., 2021).

Devido à importância do tema, a Agência Internacional de Energia Atômica - *International Atomic Energy Agency* (IAEA) publicou um documento técnico em 2018 com o objetivo de identificar critérios comuns para o projeto e implementação de um SDA, o *Criteria for Diverse Actuation Systems for Nuclear Power Plants* (INTERNATIONAL ATOMIC ENERGY AGENCY, 2018b).

O presente trabalho propõe-se a explorar, com detalhes, o Sistema Diverso de Atuação, incluindo a sua concepção, uma análise detalhada da *Common Cause Failure*, exemplos de como o SDA tem sido projetado em diversas plantas nucleares, seus benefícios e desafios.

1.1 Objetivos

A presente dissertação tem como objetivo fazer um levantamento do estado da arte do Sistema Diverso de Atuação (SDA) na indústria nuclear, com foco em plantas nucleares de potência - *Nuclear Power Plants* (NPP). O tema é relativamente novo e não possui referências extensivas, logo este trabalho se propõe também a enriquecer a bibliografia disponível e difundir o assunto.

O propósito do estudo inclui ainda detalhar a *Common Cause Failure* (CCF), que é a origem da necessidade de implantação do SDA e também levantar alguns projetos nucleares que já utilizam o sistema, assim como as características particulares de cada um deles. Como não existe uma norma orientativa única para o SDA, existem muitas possibilidades de implementá-lo, mas sempre reduzindo consideravelmente a possibilidade de CCF e atingindo condições de maior confiabilidade para os sistemas.

O trabalho propõe-se também a avaliar o uso da tecnologia *Field-Programmable Gate Array* (FPGA) para o desenvolvimento do SDA. O uso do FPGA traz diversas vantagens, entre elas a diversidade de seu funcionamento em comparação aos sistemas digitais normalmente utilizados, o que é interessante para reduzir a ocorrência da CCF.

Por fim, o objetivo também engloba a realização de uma avaliação abrangente das vantagens e desvantagens inerentes à implementação do SDA, incluindo não somente seus benefícios imediatos, mas também sua influência substancial na configuração geral da arquitetura de controle da planta.

1.2 Motivação

Com a crescente importância da energia nuclear e a geração de eletricidade a partir de usinas nucleares, faz-se necessário o aumento da segurança e confiabilidade dessas plantas. Para atender a esse requisito, sistemas digitais redundantes são utilizados e com isso surge a possibilidade de ocorrência da *Common Cause Failure* (CCF). A fim de mitigar essa ocorrência, uma alternativa é a implementação do Sistema Diverso de Atuação (SDA), que tem se mostrado muito eficaz para atingir este objetivo. O estudo do SDA é a motivação do presente trabalho, que inclui a sua origem, implementação, vantagens e desvantagens e exemplos de aplicação.

Outra motivação para o trabalho é o fato de não haver muitas publicações sobre o SDA, pois o assunto é relativamente novo na indústria nuclear e não há um consenso sobre as suas bases de projeto e as agências reguladoras internacionais não têm uma orientação unificada.

2 Revisão da Literatura

Neste capítulo é apresentada uma revisão bibliográfica dos principais trabalhos de pesquisa, normas e publicações relacionadas ao tema desta dissertação. São utilizadas principalmente as definições da Agência Internacional de Energia Atômica, do inglês *International Atomic Energy Agency* (IAEA) para unificar o entendimento, visto que as definições da IAEA servem como uma referência global para a proteção das pessoas e do meio ambiente e contribuem para um alto nível de segurança harmonizado em todo o mundo (INTERNATIONAL ATOMIC ENERGY AGENCY, 2019). Quando necessário, são incluídas as definições de outras organizações, como por exemplo *International Electrotechnical Commission* (IEC), *Institute of Electrical and Electronic Engineers* (IEEE), *United States Nuclear Regulatory Commission* (NRC), Comissão Nacional de Energia Nuclear (CNEN), entre outros. Quando possível, a tradução para o português dos termos chaves utilizados na área nuclear seguirá as traduções adotadas pela CNEN.

Entre as principais publicações da IAEA, estão seus padrões de segurança, que fornecem os princípios fundamentais, requisitos e guias de segurança para garantir a segurança nuclear. A IAEA define uma hierarquia para os padrões de segurança emitidos por ela, que é dividida conforme a Figura 2.1.

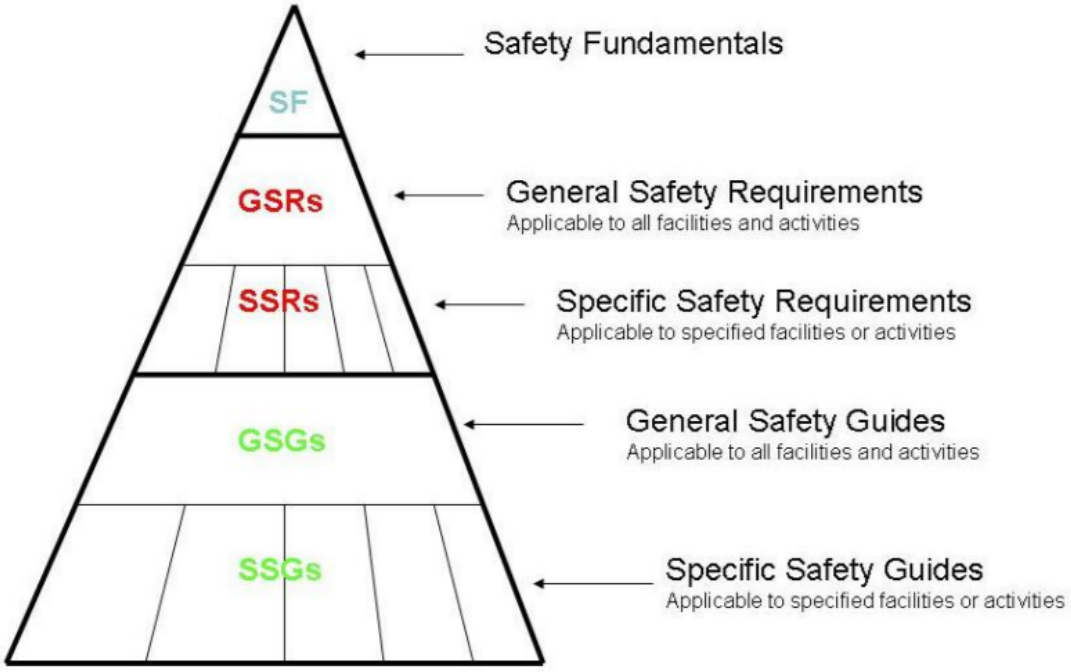

Figura 2.1 – Hierarquia da série de padrões de segurança da IAEA.
Fonte: (LONG. . . , 2021)

Assim, temos diversas categorias para os padrões de segurança. No topo estão

os fundamentos de segurança, que são documentos mais abrangentes. Eles contêm os princípios de proteção e segurança e servem de base para os requisitos de segurança que estão no meio da pirâmide. Na base da pirâmide, têm-se os documentos técnicos e guias detalhados e específicos, aplicados a determinada atividade e/ou categoria.

2.1 Os Estados da Planta

A IAEA usa uma definição dos estados da planta bastante comum na indústria nuclear. Segundo o glossário de segurança da IAEA, têm-se os estados da planta descritos a seguir (INTERNATIONAL ATOMIC ENERGY AGENCY, 2019).

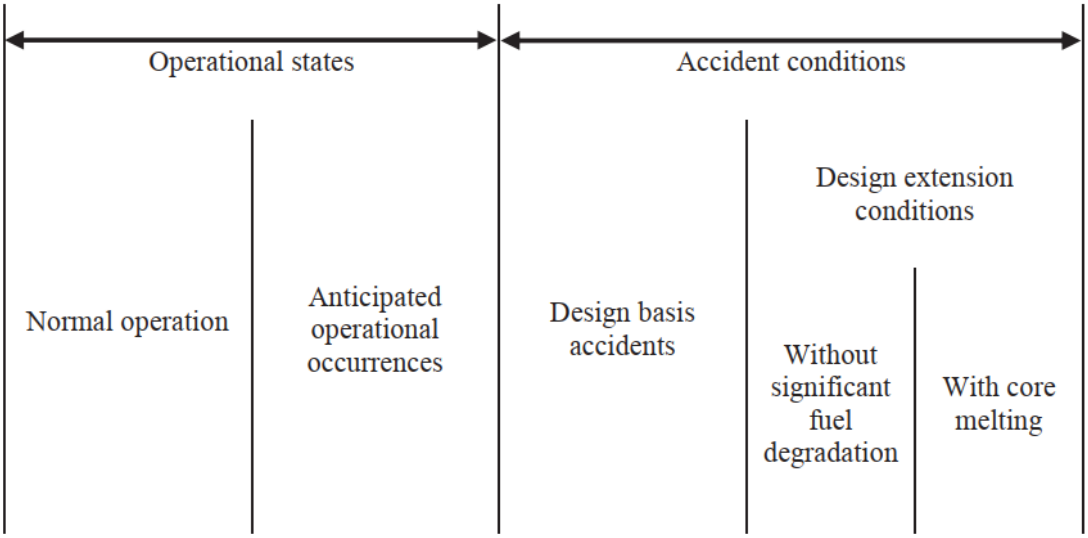

Figura 2.2 – Os estados da planta.
Fonte: (INTERNATIONAL ATOMIC ENERGY AGENCY, 2019)

Os estados operacionais são divididos em operação normal e ocorrência operacional esperada, do inglês, *Anticipated Operational Occurrence* (AOO). Operação normal é a operação dentro dos limites e condições operacionais especificados. Neste caso, cita-se como exemplo de eventos de operação normal a partida da planta, o desligamento da planta, testes, rotinas de manutenção, etc. A AOO é um desvio da operação normal, para a qual é esperada a sua ocorrência pelo menos uma vez durante a vida operacional da planta. Este estágio não deve causar nenhum dano significativo para os itens importantes para a segurança ou levar à condição de acidente. Exemplos de AOO são a perda da energia elétrica na planta, a perda de energia na bomba principal de resfriamento do núcleo, a parada do conjunto gerador da turbina, o isolamento do condensador principal, entre outros (US NUCLEAR REGULATORY COMMISSION, 2021).

Condições de Acidente são desvios da operação normal, que são menos frequentes e mais graves do que as AOOs. As condições de acidente são divididas em acidentes de

base de projeto, do inglês, *Design Basis Accidents* (DBA) e condições de extensão do projeto, do inglês *Design Extension Conditions* (DEC). Um exemplo de DEC ocorreu no acidente nuclear de Fukushima, que foi desencadeado por um terremoto e tsunami em 2011, resultando em múltiplos reatores sofrendo fusões parciais, gerando vazamentos radioativos significativos. As DECs podem ser divididas em duas classes: eventos sem degradação significativa do combustível e eventos com derretimento do núcleo do reator.

Complementando as definições de estados de operação da planta, é interessante definir os conceitos de evento iniciador, que é um evento identificado que conduz a uma AOO ou a um DBA e evento iniciador postulado, do inglês, *Postulated Initiating Event* (PIE), que é um evento hipotético identificado/previsto na fase de projeto.

A seguir são definidos dois estados da planta, conforme referência (INTERNATIONAL ATOMIC ENERGY AGENCY, 2019):

Estado controlado: estado da planta após a ocorrência de uma AOO ou de uma condição de acidente, no qual as funções fundamentais de segurança (detalhadas na Seção 2.2) são mantidas por um tempo suficiente para atingir o estado seguro; e

Estado seguro: estado da planta após a ocorrência de uma AOO ou de uma condição de acidente, no qual o reator está subcrítico e as funções fundamentais de segurança (detalhadas na Seção 2.2) podem ser garantidas e mantidas estáveis por um longo período.

2.2 Funções de Segurança Fundamentais

As funções de segurança fundamentais para plantas nucleares de potência, do inglês, *Nuclear Power Plant* (NPP) estão indicadas no primeiro requerimento técnico da publicação da IAEA *Safety of Nuclear Power Plants: Design (SSR-2/1)* (INTERNATIONAL ATOMIC ENERGY AGENCY, 2012) que traz uma série de requisitos de segurança para projetos de NPP. Trata-se do requisito número 4, funções fundamentais de segurança. Em outras publicações da própria IAEA também são utilizadas as seguintes denominações: funções básicas de segurança e funções principais de segurança.

A seguir são listadas e explicadas as funções de segurança fundamentais, conforme a referência *Safety of Nuclear Power Plants: Design (SSR-2/1)* (INTERNATIONAL ATOMIC ENERGY AGENCY, 2012) e o glossário de segurança publicado pela IAEA (INTERNATIONAL ATOMIC ENERGY AGENCY, 2019).

(a) Controle de reatividade: Trata-se da capacidade de desligar o reator com segurança e mantê-lo em estado seguro durante e após os estados operacionais e nas condições de acidente;

(b) Resfriamento de material radioativo: Trata-se da capacidade de remover o calor residual do reator e do combustível armazenado durante e após os estados operacionais e nas condições de acidente; e

(c) Confinamento de material radioativo: Trata-se da capacidade de reduzir o potencial de liberação de material radioativo e garantir que quaisquer liberações estejam dentro dos limites prescritos durante e após os estados operacionais e dentro dos limites aceitáveis, durante e após os acidentes de base do projeto (DBA).

2.3 Classificação de Segurança

O documento da IAEA *"Safety of Nuclear Power Plants: Design (SSR-2/1)"* identifica os principais requisitos de segurança de NPPs (INTERNATIONAL ATOMIC ENERGY AGENCY, 2012). Nele são identificados dois requisitos fundamentais para a classificação de segurança. O requisito 18 da SSR-2/1 afirma que as diretrizes de projeto de engenharia para itens importantes para a segurança em NPPs devem ser especificados e estar em conformidade com os padrões nacionais ou internacionais relevantes e com práticas provadas de engenharia. No requisito 22 do mesmo documento, a IAEA afirma que todos os itens importantes para a segurança devem ser identificados e classificados com base em sua função e importância para a segurança. A metodologia para classificar os itens importantes para a segurança deve ser baseada principalmente em métodos determinísticos e complementados (quando apropriado) por métodos probabilísticos, atendendo aos seguintes fatores:

a) A(s) função(ões) de segurança a serem desempenhadas pelo item;

b) As consequências da falha ao desempenhar a função de segurança do item;

c) A frequência com que o(s) item(ns) será(ão) exigido(s) para executar uma função de segurança; e

d) O tempo após um evento inicial postulado (PIE) em que o item será demandado para desempenhar uma função de segurança.

O documento da IAEA que detalha como é feita a classificação de segurança é o *Safety Classification of Structures, Systems and Components in Nuclear Power Plants (SSG-30)* (INTERNATIONAL ATOMIC ENERGY AGENCY, 2014). Neste documento são definidos os níveis de severidade das funções de segurança como sendo alta, média ou baixa. Em seguida, com base nesses níveis de severidade, são definidas as classificações de segurança.

- Severidade alta
  - Levar a uma liberação de material radioativo que exceda os limites aceitos pelo órgão regulador para acidentes de base de projeto (DBAs); ou

  - Fazer com que os valores dos parâmetros físicos principais excedam os critérios de aceitação para acidentes de base de projeto (DBAs).

- Severidade média
  - Levar a uma liberação de material radioativo que exceda os limites estabelecidos para ocorrências operacionais esperadas (AOOs); e
  - Fazer com que os valores dos parâmetros físicos principais excedam os limites projetados para ocorrências operacionais esperadas (AOOs).

- Severidade baixa
  - Levar a doses de radiação para os trabalhadores acima dos limites autorizados.

Ainda na referência (INTERNATIONAL ATOMIC ENERGY AGENCY, 2014), é feita a seguinte categorização:

- Categoria de Segurança 1
  - Qualquer função que seja necessária para atingir o estado controlado (detalhes na Seção 2.1) após uma ocorrência operacional esperada (AOO) ou um acidente de base do projeto (DBA), cuja falha resultaria em consequências de severidade alta.

- Categoria de Segurança 2
  - Qualquer função que seja necessária para atingir o estado controlado (detalhes na Seção 2.1) após uma ocorrência operacional esperada (AOO) ou um acidente de base do projeto (DBA), cuja falha resultaria em consequências de severidade média.
  - Qualquer função que seja necessária para atingir e manter a planta por um longo tempo no estado seguro e cuja falha resultaria em consequência de severidade alta.
  - Qualquer função que seja projetada para ser *backup* de uma função classificada como Categoria de Segurança 1 e que seja obrigatória para controlar as condições de extensão do projeto (DEC), sem derretimento do núcleo do reator.

- Categoria de Segurança 3
  - Qualquer função que seja atuada em uma ocorrência operacional esperada (AOO) ou um acidente de base do projeto (DBA), cuja falha resultaria em consequências de severidade baixa;

- Qualquer função que seja necessária para atingir e manter a planta por um longo tempo no estado seguro e cuja falha resultaria em consequência de severidade média;
- Qualquer função que seja necessária para mitigar as consequências das condições de extensão do projeto (DEC), a menos que já seja necessária para ser classificada como Categoria de Segurança 2, e cuja falha, quando solicitada, resultaria em consequências de severidade "alta";
- Qualquer função que seja projetada para reduzir a frequência de atuação do desligamento do reator (SCRAM) ou Sistemas de Atuação de Dispositivos Técnicos de Segurança, do inglês, *Engineered Safety Features Actuation Systems* (ESFAS) em um evento de desvio da operação normal, incluindo aquelas funções projetados para manter os principais parâmetros da planta dentro da faixa normal de operação da planta;
- Qualquer função relacionada ao monitoramento necessário para fornecer aos operadores da planta e ao grupo de emergência fora do local (*off-site*) um conjunto suficiente de informações confiáveis em caso de acidente (acidente básico do projeto ou condições de extensão do projeto), incluindo monitoramento e meios de comunicação como parte do plano de resposta a emergências (defesa em profundidade nível 5, ver Seção 2.5), a menos que já atribuído a uma categoria superior.

Tabela 2.1 – Categorias de segurança. Adaptado de: (INTERNATIONAL ATOMIC ENERGY AGENCY, 2014)

Funções creditadas na avaliação de segurança	Severidade das consequências se a função não for desempenhada		
	Alta	Média	Baixa
Funções para atingir o estado controlado após AOO	Categoria de Segurança 1	Categoria de Segurança 2	Categoria de Segurança 3
Funções para atingir o estado controlado após DBA	Categoria de Segurança 1	Categoria de Segurança 2	Categoria de Segurança 3
Funções para atingir e manter a planta no estado seguro	Categoria de Segurança 2	Categoria de Segurança 3	Categoria de Segurança 3
Funções para mitigar as consequências de uma DEC	Categoria de Segurança 2 ou Categoria de Segurança 3	Sem classificação	Sem classificação

A Tabela 2.1 foi adaptada da referência (INTERNATIONAL ATOMIC ENERGY AGENCY, 2014) e resume as categorias de segurança das diversas funções.

É importante ressaltar que existe uma pequena diferença na classificação de segurança das principais normas e organizações. Por exemplo, a classificação de segurança da IAEA é muito parecida com a classificação da IEC (IEC-61226) e essa mesma classificação se assemelha às normas utilizadas como referência para os órgãos reguladores europeus, como por exemplo da França e da Alemanha. Entretanto, a classificação é diferente da utilizada pela IEEE (IEEE-323), que é usada como referência pela NRC. A Tabela 2.2 mostra um comparativo das diferenças supracitadas (WORLD NUCLEAR ASSOCIATION, 2020).

Tabela 2.2 – Classificação de Sistemas de Segurança. Adaptado de: (WORLD NUCLEAR ASSOCIATION, 2020)

Organizações e países	Classificação de segurança para funções e sistemas de I&C			
IAEA SSG-30	Categoria de Segurança 1	Categoria de Segurança 2	Categoria de Segurança 3	Sistemas não importantes para a segurança
IEC 61226	Categoria A	Categoria B	Categoria C	Não classificado
França	F1A	F1B	F2	Não classificado
Alemanha	Categoria 1	Categoria 2	Categoria 3	Não classificado
IEEE e NRC	Sistemas importantes para a segurança			Não classificado
	Relativo à segurança (*Safety-related*)	-		

2.4 Transitório Esperado sem Desligamento Rápido, do inglês, *Anticipated Transient Without Scram* (ATWS)

Segundo o (INTERNATIONAL ATOMIC ENERGY AGENCY, 2019), o ATWS é um dos mais severos acidentes que podem ocorrer em uma NPP. Trata-se de um acidente em que o evento iniciador é a ocorrência de uma AOO e o sistema de desligamento rápido do reator (SCRAM) não funciona. Em termos práticos, significa que as barras de controle e segurança do reator (que objetivam reduzir rapidamente a criticidade do núcleo do reator) não são inseridas no núcleo do reator ao ocorrer uma AOO, o que pode levar a planta a uma situação insegura.

2.5 O conceito de Defesa em Profundidade

Outro conceito importante para a área nuclear e também para o desenvolvimento desta dissertação é a defesa em profundidade. Ele aparece como um princípio fundamental de segurança, no topo da pirâmide da Figura 2.1, justamente por sua definição abrangente e aplicabilidade em diversas funções e sistemas. A publicação "Princípios Fundamentais de Segurança" (INTERNATIONAL ATOMIC ENERGY AGENCY, 2006), afirma que a defesa em profundidade é o principal meio de prevenção e mitigação das consequências dos acidentes. A defesa em profundidade é implementada principalmente por meio da combinação de uma série de níveis consecutivos e independentes de proteção, que teriam que falhar antes que efeitos prejudiciais pudessem ser causados às pessoas ou ao meio ambiente. A publicação deixa evidente a importância da independência dos diversos níveis.

Conforme a (INTERNATIONAL ATOMIC ENERGY AGENCY, 2019), defesa em profundidade é o uso de diferentes níveis de equipamentos e procedimentos diversos, para prevenir a escalada de ocorrências operacionais esperadas, do inglês, *Anticipated Operational Occurrence* (AOO) e para manter a efetividade das barreiras físicas colocadas entre a fonte de radiação (ou material radioativo) e os trabalhadores, público em geral e meio ambiente.

Segundo o *International Nuclear Safety Advisory Group* (INSAG), em sua publicação sobre a defesa em profundidade em segurança nuclear (INTERNATIONAL ATOMIC ENERGY AGENCY, 1996), os objetivos da defesa em profundidade são:

- Compensar as possíveis falhas humanas e de componentes;
- Manter a efetividade das barreiras, evitando o dano à NPP e às próprias barreiras; e
- Proteger o público e o meio ambiente dos danos, no caso dessas barreiras não serem totalmente eficazes.

A IAEA define 5 níveis de defesa em profundidade (INTERNATIONAL ATOMIC ENERGY AGENCY, 2012; INTERNATIONAL ATOMIC ENERGY AGENCY, 1999; INTERNATIONAL ATOMIC ENERGY AGENCY, 2011), são eles:

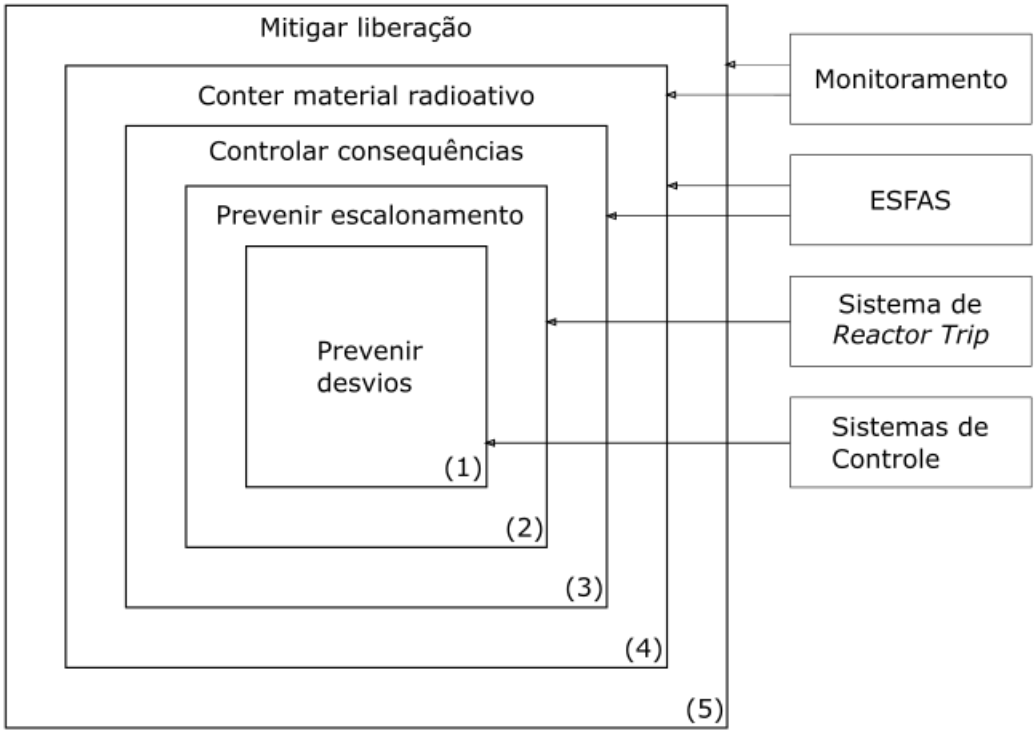

Figura 2.3 – Níveis da Defesa em profundidade. Adaptado de: (INTERNATIONAL ATOMIC ENERGY AGENCY, 2011)

(1) Prevenção de operação anormal e falha

A ideia do primeiro nível de proteção ("prevenir desvios" na Figura 2.3) é evitar que ocorram desvios da operação normal e falhas nos itens de segurança. Para isso, é necessário o uso de requisitos conservadores no projeto e construção da planta, alta qualidade de gestão e práticas de engenharia comprovadas. O objetivo de prevenir desvios pode então ser alcançado com o uso e seleção de normas e códigos de projeto apropriados, assim como com o controle de qualidade da fabricação dos componentes da planta. Por fim, pode-se citar ainda a boa execução do comissionamento e partida da planta.

(2) Controle de operação anormal e detecção de falhas

O segundo nível de proteção ("prevenir escalonamento" na Figura 2.3) tem como objetivo detectar e controlar desvios da operação normal para prevenir o escalonamento das AOOs. Este nível de proteção existe também devido ao fato que durante a vida útil da planta irão ocorrer eventos iniciadores postulados, do inglês, *Postulated Initiating Events* (PIE), independentemente do cuidado tomado para evitar a sua ocorrência.

Neste nível, faz-se necessária a inclusão de procedimentos operacionais para prevenir os possíveis eventos iniciadores ou minimizar as suas consequências, trazendo a planta para um estado seguro, isso é, onde todas as funções fundamentais estejam garantidas,

conforme já explicado na Seção 2.2.

(3) Controle das consequências de um acidente

O terceiro nível ("controlar consequências" na Figura 2.3) considera que não foi possível o completo controle da escalada de certos AOOs ou PIEs no segundo nível e que um acidente, mesmo que muito improvável, poderia ocorrer. Neste nível, é postulada a possível ocorrência de acidentes, o que implica na necessidade da inclusão de Sistemas de Atuação de Dispositivos Técnicos de Segurança, do inglês, *Engineered Safety Features Actuation Systems* (ESFAS). Estes sistemas têm como objetivo garantir as funções fundamentais de retirar calor do núcleo e prevenir a liberação de material radioativo, retornando a planta para um estado seguro.

(4) Contenção do material radioativo

O quarto nível de proteção ("conter material radioativo" na Figura 2.3) tem como intuito mitigar as consequências de acidentes, que derivaram da falha do terceiro nível de proteção. A intenção é prevenir o progresso de tal acidente e mitigar a consequência de um acidente severo.

(5) Mitigação das consequências

O quinto e último nível de proteção ("mitigar liberação" na Figura 2.3) atua de forma a mitigar as consequências radiológicas de uma liberação de materiais radioativos, que poderiam ser originados de acidentes. Este nível exige a previsão de planos/procedimentos emergenciais para resposta dentro e fora da instalação.

Os sistemas de Instrumentação e Controle (I&C) das NPPs têm a função de dar suporte aos diversos níveis de defesa em profundidade descritos anteriormente. Uma arquitetura tradicional está representada na Figura 2.3, na qual diferentes sistemas de I&C garantem a independência dos diversos níveis (INTERNATIONAL ATOMIC ENERGY AGENCY, 2011). Para o completo entendimento da Figura 2.3, faz-se necessária uma explicação dos itens de Instrumentação e Controle (I&C) presentes nela. Conforme a referência (PRECKSHOT, 1994), tem-se:

Sistema de Controle Este sistema, geralmente sem classificação nuclear, atua de forma manual ou automática, prevenindo regimes de operação inseguros. Ele é usado para manter a operação do reator em um estado seguro.

Sistema de Desligamento do Reator / *Reactor Trip* / SCRAM Este sistema tem como objetivo reduzir rapidamente a reatividade do reator, em resposta a uma excursão descontrolada. Consiste em instrumentos para detectar excursões potenciais ou reais e meios para inserir rápida e completamente as barras de controle e segurança do reator. Este sistema também pode incluir outros sistemas de moderação química de nêutrons (por exemplo, injeção de boro).

ESFAS O Sistema de Atuação de Dispositivos Técnicos de Segurança, do inglês, *Engineered Safety Features Actuation Systems* (ESFAS) é composto por equipamentos de segurança, que removem calor do reator e apoiam na manutenção das barreiras físicas, que impedem a liberação de material radioativo. O sistema detecta a necessidade e executa funções como o resfriamento de emergência, isolamento da contenção, acionamento dos geradores de emergência, entre outros sistemas e dispositivos (válvulas, motores, bombas).

Sistema de Monitoramento O sistema de monitoramento é o mais lento e mais flexível dos níveis de defesa. Sua importância deve-se ao fato de que os operadores dependem de informações precisas dos sensores para entender a situação da planta e executar suas tarefas.

A Tabela 2.3, adaptada da referência (INTERNATIONAL ATOMIC ENERGY AGENCY, 1999), traz um resumo dos diferentes níveis de defesa em profundidade.

Tabela 2.3 – Níveis da defesa em profundidade em plantas nucleares existentes. Adaptado de: (INTERNATIONAL ATOMIC ENERGY AGENCY, 1999)

Níveis	Objetivos	Meios essenciais
Nível 1	Prevenção de falhas e operações anormais	Projeto conservativo e alta qualidade na construção e operação
Nível 2	Controle da operação anormal e detecção de falhas	Sistemas de controle, limitação, proteção e outras características de vigilância
Nível 3	Controle de acidentes de base de projeto (DBA)	ESFAS e outros procedimentos de acidente
Nível 4	Controle de condições severas da planta, incluindo prevenção da escalada de acidentes e mitigação das consequências de acidentes severos	Ações complementares e gestão de acidentes
Nível 5	Mitigação das consequências radiológicas de liberações significativas de materiais radioativos	Resposta de emergência externa à planta

2.6 Diversidade

O conceito de diversidade é importante para o desenvolvimento deste trabalho e é tratado em diversos pontos no decorrer desta dissertação. O glossário da IAEA define a diversidade como a presença de dois ou mais sistemas ou componentes independentes, que possuem atributos distintos e são usados para desempenhar uma função identificada. Tais atributos distintos reduzem a possibilidade de falha de causa comum, do inglês *Common Cause Failure* (CCF) (INTERNATIONAL ATOMIC ENERGY AGENCY, 2019).

Segundo (PRECKSHOT, 1994), diversidade é um princípio dos sistemas de I&C, que utiliza diferentes tecnologias, diferentes parâmetros, lógicas distintas ou modos de atuação distintos para fornecer várias maneiras de detectar e responder a um evento significativo.

Para os exemplos de tipos de diversidade, são utilizadas a definição da IAEA

(INTERNATIONAL ATOMIC ENERGY AGENCY, 2016b) e os documentos da NRC (NUREG/CR-6303 (PRECKSHOT, 1994) e NUREG/CR-7007 (WOOD et al., 2010)), que trazem exemplos de como tais tipos podem ser aplicados na prática em NPPs. A Figura 2.4 representa os tipos de diversidade que são detalhados nas próximas seções desta dissertação.

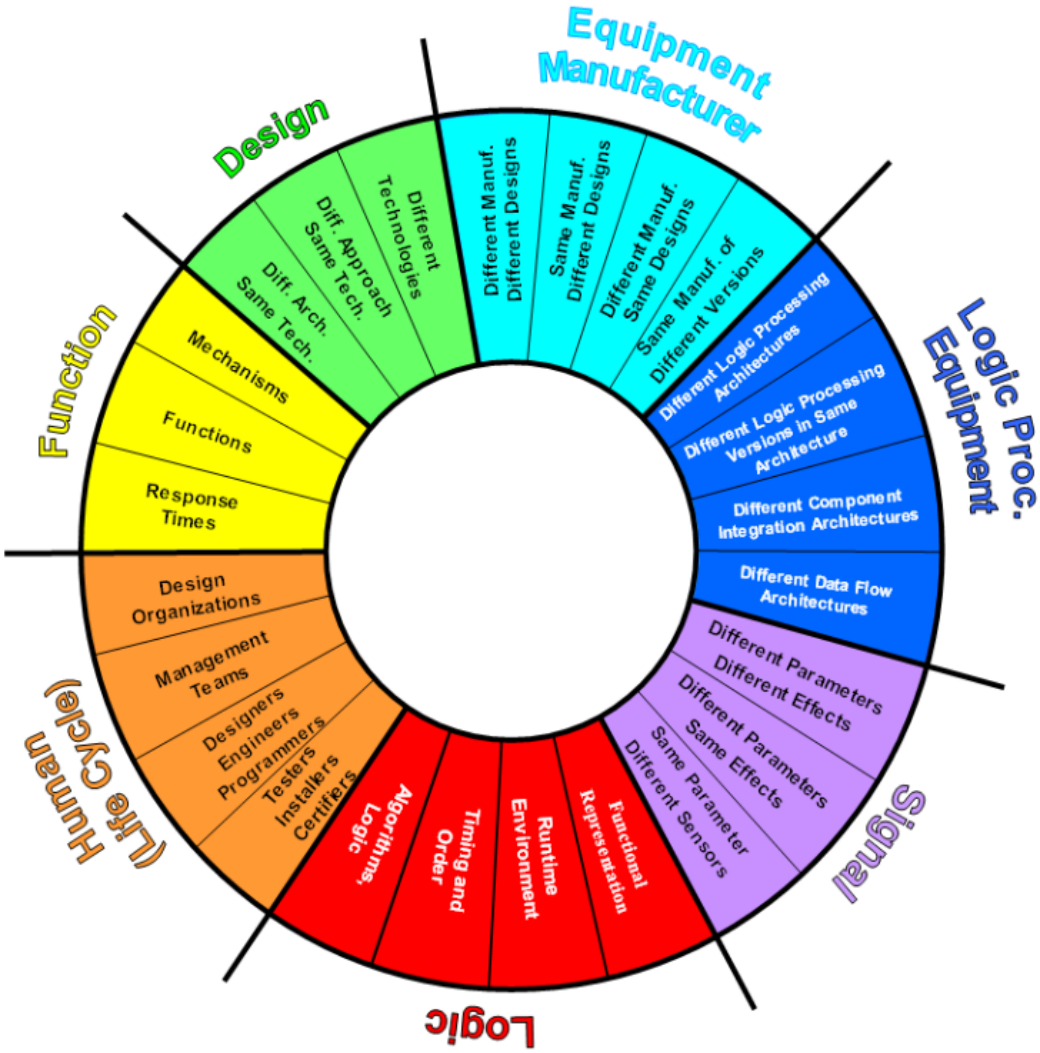

Figura 2.4 – Tipos de diversidade.
Fonte:(WOOD et al., 2010)

2.6.1 Diversidade de Projeto

Segundo a IAEA (INTERNATIONAL ATOMIC ENERGY AGENCY, 2016b), a diversidade de projeto é alcançada com o uso de diferentes abordagens, para resolver um problema idêntico ou similar.

Segundo a NUREG/CR-6303 (PRECKSHOT, 1994), o uso de diferentes abordagens inclui o uso de *software* e *hardware* para a solução de problemas parecidos ou idênticos. O foco deste tipo de diversidade está na tecnologia, na abordagem e na arquitetura diferen-

tes. A NUREG/CR-6303 (PRECKSHOT, 1994) identifica três critérios de atributos de diversidade (listados em ordem decrescente de eficácia), que contribuem para a diversidade de projeto:

- Diferentes tecnologias (exemplo: analógica e digital);
- Diferentes abordagens com a mesma tecnologia; e
- Diferentes arquiteturas.

2.6.2 Diversidade de Equipamentos

Segundo a IAEA (INTERNATIONAL ATOMIC ENERGY AGENCY, 2016b), este tipo de diversidade é obtido via *hardware*, com o emprego de diferentes tecnologias, por exemplo, com o uso de um equipamento analógico e um equipamento digital. Outro exemplo é o uso de um PLC *computer-based* e um controlador baseado em *Field Programmable Gate Arrays* (FPGA).

A NUREG/CR-7007 (WOOD et al., 2010) subdivide este tipo de diversidade em dois subitens, que são descritos a seguir. São eles: diversidade de equipamento de lógica de processamento e diversidade de fabricantes de equipamentos.

2.6.2.1 Diversidade de Equipamento de Lógica de Processamento

A NUREG/CR-6303 (PRECKSHOT, 1994) identifica que o foco desse tipo de diversidade está na espécie de lógica de processamento empregado. A publicação é de 1994 e por isso não é citado o uso do FPGA (tecnologia ainda incipiente na época), mas ela certamente entraria neste quesito de diversidade. Ainda segundo (PRECKSHOT, 1994), são listadas quatro formas de diversidade (listadas em ordem decrescente de eficácia):

- Diferentes arquiteturas da lógica de processamento (exemplo: arquitetura Intel e arquitetura Motorola);
- Diferentes versões da mesma arquitetura;
- Diferentes componentes de integração da arquitetura (exemplo: projeto das placas de circuitos impressos diferentes); e
- Diferentes arquiteturas de fluxo de dados.

2.6.2.2 Diversidade de Fabricantes de Equipamentos

Segundo a NUREG/CR-6303 (PRECKSHOT, 1994), o foco para este tipo de diversidade está no equipamento, isto é, está nos componentes de *hardware* utilizados

e/ou no sistema agregado. A NUREG/CR-6303 (PRECKSHOT, 1994) identifica quatro atributos (listados em ordem decrescente de eficácia), que contribuem para este tipo de diversidade:

- Diferentes fabricantes com projetos fundamentalmente diferentes;
- Mesmo fabricante com projetos fundamentalmente diferentes;
- Diferentes fabricantes com o mesmo projeto; e
- Diferentes versões de um mesmo projeto.

2.6.3 Diversidade Funcional

Segundo a IAEA (INTERNATIONAL ATOMIC ENERGY AGENCY, 2016b), a diversidade funcional é alcançada pelos sistemas que tomam ações diferentes para obter o mesmo resultado. A NUREG/CR-6303 (PRECKSHOT, 1994) cita os seguintes critérios (listados em ordem decrescente de eficácia), que contribuem para a diversidade funcional:

- Diferentes mecanismos (exemplo: inserção de barras e injeção de boro para desligar o reator);
- Diferentes propósitos, funcionalidades, lógicas de controle ou meios de atuação (exemplo: controle normal das barras e inserção de emergência das barras); e
- Diferentes tempos de resposta (exemplo: um sistema diverso atua se as condições de um acidente persistirem por muito tempo).

2.6.4 Diversidade Humana

Este tipo de diversidade tem nomenclaturas distintas, de acordo com as diferentes organizações. A IAEA (INTERNATIONAL ATOMIC ENERGY AGENCY, 2016b) chama esse tipo de diversidade de diversidade no processo de desenvolvimento. A NUREG/CR-6303 (PRECKSHOT, 1994) identifica esse tipo de diversidade como humana, devido à influência dos seres humanos no projeto, desenvolvimento, instalação, operação e manutenção de sistemas de segurança. O foco é a influência humana no ciclo de vida dos recursos, que constituem fontes potenciais de falhas sistemáticas. Abaixo estão listados, em ordem decrescente de eficácia, os atributos que contribuem para adicionar à diversidade humana:

- Diferentes empresas/organizações de projeto;
- Diferentes equipes de gestão de engenharia na mesma empresa;

- Diferentes equipes de projeto e desenvolvimento (engenheiros, projetistas e programadores); e
- Diferentes equipes de implementação e testes.

2.6.5 Diversidade Lógica

A IAEA (INTERNATIONAL ATOMIC ENERGY AGENCY, 2016b) e a NUREG/CR-6303 (PRECKSHOT, 1994) definem este item como diversidade de *software*. Nesse tipo de diversidade, são identificados quatro atributos (listados em ordem decrescente de eficácia), que contribuem para a diversidade lógica:

- Diferentes algoritmos, lógicas e arquitetura de programação;
- Diferentes tempos e/ou ordens de execução;
- Diferentes sistemas operacionais; e
- Diferentes linguagens de programação.

2.6.6 Diversidade de Sinal

A IAEA (INTERNATIONAL ATOMIC ENERGY AGENCY, 2016b) define a diversidade de sinal como sendo alcançada pelos sistemas nos quais uma ação de segurança pode ser iniciada com base no valor de diferentes parâmetros (variáveis de processo) da planta.

A NUREG/CR-6303 (PRECKSHOT, 1994) identifica a diversidade de sinal como o uso de diferente variáveis de processo da planta, que devem ser detectadas para dar início a uma ação de proteção. A diversidade de sinal possui uma relação com a diversidade funcional, sendo que a primeira fornece diversidade na detecção do problema enquanto a segunda fornece diversidade na atuação. A NUREG/CR-6303 (PRECKSHOT, 1994) lista (em ordem decrescente de eficácia) algumas formas de diversidade de sinal existentes:

- Diferentes parâmetros do processo (ou do reator) detectados por diferentes efeitos físicos (exemplo: pressão do reator ou fluxo de nêutrons);
- Diferentes parâmetros do processo (ou do reator) detectados pelo mesmo efeito físico (exemplo: pressão e vazão medidas por diferença de pressão); e
- Mesmos parâmetros do processo (ou do reator) detectados por um conjunto redundante diferente de sensores semelhantes (por exemplo, um conjunto de quatro sensores de temperatura redundantes e um conjunto de *backup* composto por quatro sensores de temperatura redundantes, resultando no projeto de um equipamento de proteção diverso).

2.7 Falha de Causa Comum, do Inglês, *Common Cause Failure*

O texto principal do documento da IAEA que traz requisitos de segurança para o projeto de NPPs, tem um requisito específico para a CCF (Requisito 24 em (INTERNATIONAL ATOMIC ENERGY AGENCY, 2012)). O requisito 24 exige que o projeto de equipamentos leve em consideração o risco potencial de CCF em itens importantes para a segurança e determine como os conceitos de diversidade, redundância, separação física e independência funcional devem ser aplicados para obter a confiabilidade necessária. Ainda nesse documento, é expressa a preocupação quanto à CCF em equipamentos digitais (*computer based*), que sejam categorizados como importantes para a segurança. Nesses equipamentos é exigido que seja levada em consideração a CCF de *software*.

Devido à importância do assunto, a CCF é abordada por diversas organizações e agências reguladoras. Por exemplo, a IAEA já abordou o assunto no Relatório Técnico "*Protecting Against Common Cause Failures in Digital I&C Systems of Nuclear Power Plants*" (INTERNATIONAL ATOMIC ENERGY AGENCY, 2009) e a *Electric Power Research Institute* (EPRI) publicou o trabalho "*Protecting Against Digital Common-Cause Failure: Combining Defensive Measures and Diversity Attributes*" (NGUYEN, 2010).

O glossário de segurança da IAEA (INTERNATIONAL ATOMIC ENERGY AGENCY, 2019) define falha como a perda da capacidade de uma estrutura, sistema ou componente de funcionar dentro dos critérios de aceitação. A CCF é definida como a falha de duas ou mais estruturas, sistemas ou componentes devido a um único evento ou causa específica. Observa-se que esse único evento específico ou causa da falha (a qual pode ser de diferentes tipos) pode ser devida a uma deficiência de projeto, a uma deficiência de fabricação, a erros de operação e manutenção, a um fenômeno natural, a um evento induzido por humanos, à saturação de sinais ou a um efeito em cascata não intencional de qualquer outra operação ou falha dentro da planta ou de uma mudança nas condições ambientais. A CCF pode ser interna ou externa a um sistema.

É importante não confundir as noções de falta (*fault*) e falha (*failure*) digitais. A falta digital em um sistema pode ser definida como um defeito que pode causar a redução ou perda de capacidade do sistema em executar uma função, quando sujeito a determinadas condições (normais ou anormais). A falta pode também fazer com que o sistema execute uma função em um momento incorreto (atuação espúria) (NGUYEN, 2010). São exemplos de faltas digitais:

- Defeitos no *hardware* devido ao envelhecimento;
- Erros ou inadequações na especificação dos requisitos do sistema;
- Erros no projeto, fabricação, instalação, operação ou manutenção do *hardware* do sistema; e

- Erros no projeto e/ou implementação da lógica do sistema (por exemplo, no *software* de um Controlador Lógico Programável (PLC) ou na programação de um Field Programmable Gate Array (FPGA)).

Quanto à falha digital (*digital failure*), trata-se de um desvio de um comportamento esperado de uma função, sistema, subsistema ou componente (*hardware* ou *software*). Tal desvio impede que o serviço seja executado. Para sistemas importantes para a segurança, por exemplo, um objetivo essencial dos projetistas é garantir que as falhas de componentes não resultem em falhas do sistema completo ou de funções essenciais. Essas falhas de componente são frequentemente chamadas de falhas parciais (NGUYEN, 2010).

As falhas digitais são muito preocupantes, em especial para os sistemas importantes para a segurança, devido à sua natureza determinística. Isso é, os sistemas digitais tendem a apresentar exatamente o mesmo comportamento, sempre que são colocados nas mesmas condições de funcionamento. Em sistemas de segurança, geralmente é utilizada uma configuração com sistemas redundantes, nos quais as redundâncias são idênticas (ou quase idênticas) e, portanto, contêm as mesmas especificações e/ou falhas de projeto. Isso pode levar à falha de causa comum simultânea de redundâncias múltiplas. Assim, ao contrário de outros tipos de falhas, como aquelas originadas em falhas aleatórias, a redundância não fornece necessariamente uma defesa adequada contra falhas digitais. A CCF também pode afetar vários sistemas em diferentes níveis da defesa em profundidade, se estes sistemas contiverem componentes com falhas idênticas ou semelhantes (NGUYEN, 2010).

As falhas comentadas anteriormente podem causar duas condições: a saída do sistema muda de estado (ou valor); ou a saída continua sem alteração. As CCFs nas quais as saídas causam mudanças espúrias de estados evidenciam a falha e não precisam ser consideradas na análise de acidente. Entretanto, uma falha de causa comum (CCF) que não altera de estado (ou valor) é mais preocupante, pois a falha não é revelada até que o sistema seja demandado (seja em resposta a um acidente ou a um teste). Em um sistema de segurança do reator de uma NPP não seria realizado o desligamento rápido do reator, nem o acionamento de uma ESFAS e nem o acionamento de algum alarme (INTERNATIONAL ATOMIC ENERGY AGENCY, 2009). Portanto esse tipo de falha deve ser avaliado pelos projetistas, conforme é abordado na Seção 2.8.

2.7.1 Condições Necessárias Para a Ocorrência de uma CCF

De forma mais detalhada, para ocorrer uma CCF potencialmente insegura para a planta, algumas condições precisam ocorrer, conforme elencado abaixo e representado pela Figura 2.5 (INTERNATIONAL ATOMIC ENERGY AGENCY, 2009).

- O sistema deve conter uma ou mais faltas (*faults*) que possam causar incapacidade funcional;

- Um evento desencadeador (*triggering event*) ocorre para ativar a falha, geralmente uma condição operacional imprevista ou não testada;
- Múltiplos canais são afetados ao mesmo tempo;
- As falhas causam uma condição insegura para a planta, normalmente na forma de degradação ou perda de uma função necessária para mitigar um acidente de base do projeto (DBA) ou uma ocorrência operacional esperada (AOO). Uma CCF pode desabilitar uma função de mitigação e simultaneamente iniciar um evento que requeira a função de mitigação; e
- Para afetar adversamente vários sistemas, esses sistemas devem compartilhar a(s) mesma(s) falha(s) e serem suscetíveis simultaneamente ao mesmo evento desencadeador (*triggering event*).

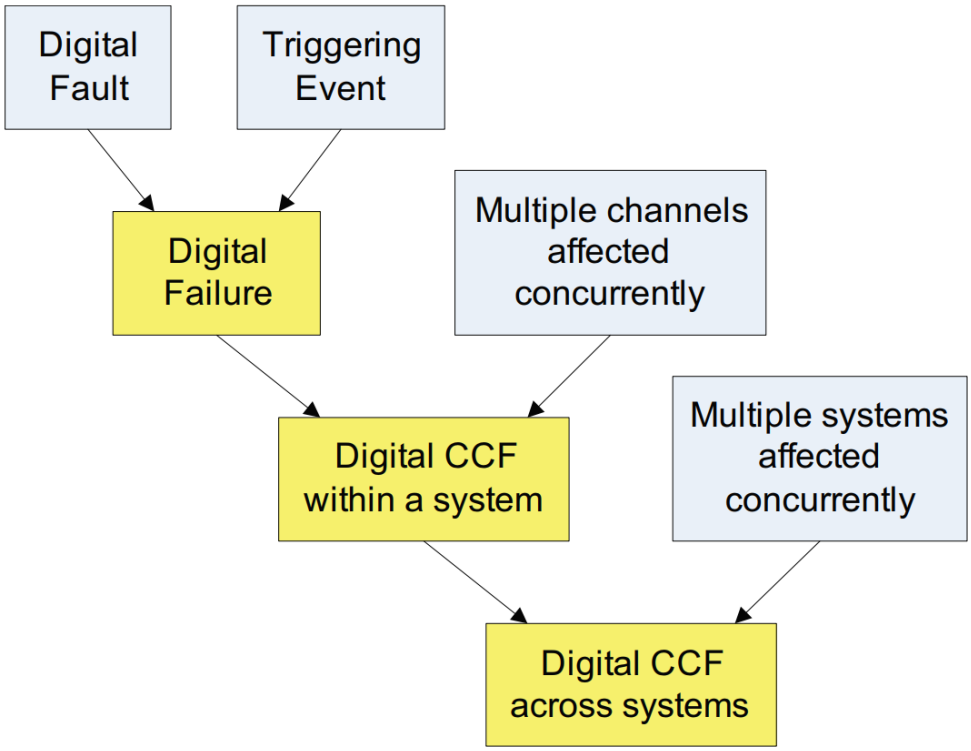

Figura 2.5 – Condições para a ocorrência de uma CCF digital. Fonte: (INTERNATIONAL ATOMIC ENERGY AGENCY, 2009)

2.7.2 Fonte das faltas que Causam CCF

O objetivo desta subseção é descrever possíveis fontes das faltas ocultas que podem gerar CCFs. Desta forma, tais fontes devem ser evitadas pelo projetista. A seguir, estão listados exemplos de faltas que podem ser encontradas em quaisquer sistemas de I&C, sejam eles analógicos ou digitais (INTERNATIONAL ATOMIC ENERGY AGENCY, 2009):

- Erro em função padrão, como por exemplo função trigonométrica, que pode resultar em cálculo incorreto;
- Operar fora dos limites de parâmetros válidos de um algoritmo ou função padrão, que podem resultar em cálculos incorretos ou resultados fora do intervalo;
- Algoritmo mal elaborados;
- Falha devido a uma relação sinal/ruído baixa;
- Incompatibilidade das tensões de alimentação dos diversos equipamentos;
- Uso de unidades de engenharia inconsistentes; e
- Projeto de sistema mal elaborado.

Ainda segundo a referência (INTERNATIONAL ATOMIC ENERGY AGENCY, 2009), outras faltas ocultas são mais comuns em sistemas de I&C digitais, como por exemplo:

- A integração inadequada de um sistema computacional distribuído, que pode resultar na operação incorreta do sistema de I&C. O fluxo de dados por meio de um sistema de computação distribuído, normalmente emprega operação assíncrona. O projeto precisa garantir um desempenho funcional determinístico. Onde barramentos de dados são usados, as prioridades funcionais precisam ser garantidas.
- Erros na quantização e frequência de amostragem, que podem afetar a resposta transiente, resultando na operação incorreta do sistema de controle. A interface para os dados detectados e os atuadores pode ser afetada. Amostragens assíncronas ou diferentes frequências de amostragem em sistemas distribuídos podem aumentar a complexidade desse problema, se os dados forem avaliados nos domínios do tempo e da frequência.
- Inconsistências nos protocolos de comunicação de dados podem causar operação incorreta. Os protocolos de dados devem ser estabelecidos para garantir uma comunicação consistente. As comunicações não podem ser tratadas como uma "caixa preta"; o comportamento das funções em cada dispositivo deve ser compreendido.
- Erros em bibliotecas de *software* podem resultar em uma variedade de operações impróprias. As bibliotecas são usadas não apenas para funções matemáticas, mas também para funções como geração de ícones de exibição e protocolos de transferência de dados. Erros em bibliotecas podem afetar todas as funções do aplicativo que usam essa função de biblioteca.
- O equipamento digital é mais suscetível a variações na tensão e frequência de entrada do que o equipamento analógico;

- Os efeitos da filtragem dos dados e dos sinais precisam ser compreendidos. Os sensores, bem como os módulos de comunicação, podem atuar como filtros passa-baixa, passa-banda ou passa-alta e têm tempos de resposta que precisam ser considerados ao determinar o desempenho do sistema.

A identificação de potenciais faltas ocultas deve começar na fase conceitual do projeto. Entretanto, as faltas podem ser introduzidas em qualquer fase do ciclo de vida do sistema de I&C e portanto a sua verificação deve ocorrer em todas as fases (INTERNATIONAL ATOMIC ENERGY AGENCY, 2009).

2.7.2.1 Projeto Conceitual

O projeto conceitual estabelece a arquitetura fundamental do sistema de I&C, alocando as funções básicas para cada elemento dentro da arquitetura e deve estabelecer a abordagem conceitual a ser empregada. Esta fase do projeto define o escopo do projeto de I&C, incluindo a identificação dos sistemas da planta a serem controlados. Geralmente, um diagrama de blocos é desenvolvido para identificar as principais classes de equipamentos, interfaces de alto nível e um número inicial estimado de itens em cada classe. Durante esta fase de desenvolvimento, as fontes potenciais de faltas a serem consideradas são (INTERNATIONAL ATOMIC ENERGY AGENCY, 2009):

- Um entendimento incompleto dos processos da planta e da instrumentação necessária;
- Incertezas significativas na especificação do projeto conceitual;
- Excessiva complexidade do projeto conceitual. Às vezes, isso se deve ao desejo de se ter a capacidade de executar funcionalidades adicionais, além daquelas exigidas para as funções de segurança adequadas do sistema.

2.7.2.2 Especificação de Requisitos

Durante a especificação de requisitos, são estabelecidas as interfaces entre os sensores, condicionamento de sinais, comunicação, sistemas de I&C e atuadores. A fase de especificação de requisitos tem o potencial de introduzir falhas ocultas, que podem ser causas potenciais de CCF. Os exemplos a seguir abordam fontes essenciais de erros, nas quais os requisitos especificados podem ser incompletos ou inadequados, causando faltas ocultas no sistema de I&C resultante (INTERNATIONAL ATOMIC ENERGY AGENCY, 2009):

- Os projetistas responsáveis pela especificação dos requisitos possuem um entendimento incompleto dos processos da planta e da instrumentação necessária;

- A especificação de requisitos não é formulada de forma clara, causando interpretações errôneas em uma fase posterior do ciclo de vida;
- Complexidade excessiva é introduzida na especificação do projeto. O desejo de introduzir funcionalidades adicionais deve ser cuidadosamente considerado durante todas as fases do projeto.

2.7.2.3 Desenvolvimento

No processo de desenvolvimento, a tecnologia selecionada é utilizada para implementar os requisitos de um sistema. Os efeitos da especificação inadequada de um projeto podem se propagar por todas as fases do ciclo de vida do sistema, e alguns passos são necessários para assegurar que a especificação de projeto foi transferida adequadamente para o projeto final. Com base nos requisitos do sistema, diferentes abordagens para o projeto podem ser utilizadas. Algumas abordagens focam na simplicidade do projeto, enquanto outras empregam níveis mais altos de complexidade e funcionalidade. Nos sistemas digitais, as funções e a comunicação são mais integradas. Nesse tipo de sistema, as informações são compartilhadas em diferentes partes do sistema. Isso permite que vários canais sejam usados e vários esquemas de votação sejam implementados. Nessa abordagem, com sistemas integrados, devem ser tomadas precauções para garantir o isolamento dos canais principais e para fornecer proteção contra os diversos tipos de interferência eletromagnética. Em todos os casos, os benefícios da complexidade adicional devem ser avaliados em relação aos erros potenciais que podem ser introduzidos pelas funções adicionais (INTERNATIONAL ATOMIC ENERGY AGENCY, 2009).

2.7.2.4 Fabricação

A fabricação abrange uma série de processos e, portanto, pode ser a causa raiz de várias fontes de faltas. Essas faltas podem estar em equipamentos instalados em várias partes do sistema. Algumas fontes de faltas são (INTERNATIONAL ATOMIC ENERGY AGENCY, 2009):

- Controle de qualidade insuficiente, incluindo testes em componentes elementares, controle intermediário em subconjuntos e controle final;
- Mudanças no projeto do componente ou processo de fabricação;
- Processo de fabricação defeituoso. Isso pode incluir erros de montagem, devido ao gerenciamento inadequado de configuração.

2.7.2.5 Instalação e Comissionamento

As fases de instalação e comissionamento podem introduzir faltas ocultas no sistema de I&C. Isso pode ocorrer com sistemas analógicos e digitais, mas os sistemas digitais

apresentam um risco maior devido à comunicação mais complexa dentro do sistema. Alguns exemplos de problemas de instalação e comissionamento incluem (INTERNATIONAL ATOMIC ENERGY AGENCY, 2009):

- Identificação inadequada de equipamentos;
- Falha ao remover o equipamento de teste e fiação;
- Fiação instalada incorretamente;
- Configurações incorretas de parâmetros; e
- Teste de comissionamento inadequado.

2.7.2.6 Modificações Pós-instalação

As modificação feitas após a instalação estão suscetíveis aos mesmos erros que foram discutidos nas etapas anteriores. Como a modificação é focada na parte do sistema que está sendo alterada, existe um risco adicional de que possa ocorrer um impacto em uma parte diferente do sistema e isso deve ser considerado durante a preparação desta modificação. Algumas causas de erro durante o estágio de modificação são (INTERNATIONAL ATOMIC ENERGY AGENCY, 2009):

- Impactos desconhecidos da modificação em outras partes do sistema;
- Teste incompleto (que pode resultar em interferência não detectada, problemas ou alterações funcionais indesejadas);
- Documentação que não reflete o estado real da planta.

2.7.2.7 Manutenção e Operação

A manutenção do sistema de I&C introduz riscos que são similares aos dos estágios iniciais do projeto, de fabricação e instalação. Exemplos que podem ocorrer dentro do processo de manutenção e operação são (INTERNATIONAL ATOMIC ENERGY AGENCY, 2009):

- Manutenção incorreta de equipamento;
- Procedimento elaborado ou executado de forma incorreta;
- Danos aos sistemas e/ou aos equipamentos;
- Instalação incorreta de peças sobressalentes;
- Treinamento inadequado da equipe de manutenção; e
- Utilização de ferramentas que podem introduzir erros.

2.7.3 Mecanismos de Acionamento da CCF

Os mecanismos de acionamento são um fator necessário para ativar uma falta oculta, que causa a CCF de alguns ou de todos os componentes envolvidos. Portanto, evitar os mecanismos de acionamento comuns é tão importante quanto evitar as faltas ocultas para minimizar o potencial de CCF (INTERNATIONAL ATOMIC ENERGY AGENCY, 2009).

2.7.3.1 Ações Humanas

A experiência com CCF em uma variedade de indústrias mostrou que as ações humanas são um dos gatilhos mais importantes para iniciar faltas ocultas. As ações humanas podem colocar dois ou mais canais ou elementos do sistema em um estado não analisado/testado, no qual as CCFs ocultas serão iniciadas. A seguir, estão os motivos mais comuns para falhas humanas que irão desencadear faltas ocultas (INTERNATIONAL ATOMIC ENERGY AGENCY, 2009):

- Procedimentos insuficientes para a execução de atividades de manutenção específicas;
- Treinamento insuficiente ou falta de experiência do pessoal de manutenção;
- Projeto ambíguo na interface homem-máquina para os sistemas envolvidos.

Um projeto de programa de interface homem-máquina bem concebido pode reduzir o potencial para desencadear eventos iniciados por ação humana.

2.7.3.2 Trajetória do Sinal

As trajetórias do sinal descrevem a combinação de todos os fatores que podem influenciar o comportamento do sistema. Tais trajetórias são as principais fontes estressoras, que causam CCFs. Uma falha digital de um sistema de I&C operacional que passou nos testes de sistema estabelecidos (incluindo Teste de Aceitação de Fábrica, Teste de Aceitação de Campo) e foi comissionado, provavelmente será desencadeada apenas por uma trajetória de sinal não verificada em teste ou durante a operação antes da falha. Essas trajetórias de sinal não testadas anteriormente podem ser causadas por uma condição rara da planta ou por dados de entrada inconsistentes. Por exemplo, dados de uma falha de sensor ou transdutor ou transmissão de dados defeituosa entre unidades redundantes podem representar condições de planta “fisicamente impossíveis”. O acionamento de CCFs pode, adicionalmente, depender de estados internos específicos do sistema de I&C (INTERNATIONAL ATOMIC ENERGY AGENCY, 2009).

A introdução de diversidade na trajetória de sinal entre canais ou outros elementos do sistema de I&C pode minimizar o potencial para CCFs devido a trajetórias de sinal

específicas. Por exemplo, essa diversidade pode ser fornecida por meio de procedimentos que proíbem a modificação de parâmetros em vários canais ou elementos funcionais ao mesmo tempo (INTERNATIONAL ATOMIC ENERGY AGENCY, 2009).

2.7.3.3 Eventos Externos

Existem possíveis mecanismos de acionamento causados por eventos externos ao sistema de I&C, que podem influenciar diretamente apenas o *hardware* dos sistemas de I&C. Os eventos mais relevantes nesta categoria a serem considerados durante o projeto dos sistemas de I&C são (INTERNATIONAL ATOMIC ENERGY AGENCY, 2009):

- Eventos sísmicos ou fortes vibrações de eventos fora do normal;
- Condições ambientais extremas (alta temperatura, alta umidade, congelamento, etc.);
- Atividades de manutenção, como soldagem, partida de bombas ou motores;
- Interferência eletromagnética e interferência por rádio-frequência;
- Inundação ou incêndio nas salas, gabinetes e/ou bandejas de cabos contendo equipamentos de I&C;
- Picos no fornecimento de energia nos equipamentos de I&C.

2.7.3.4 Efeitos Temporais

A data do calendário ou as condições de tempo específicas podem ser mecanismos de acionamento. Exemplos relevantes são (INTERNATIONAL ATOMIC ENERGY AGENCY, 2009):

- Datas de calendário específicas, que não foram tratadas adequadamente no projeto do *software* (exemplos: 29 de fevereiro e mudança entre o horário de verão e o horário normal); e
- *Overflow* do tempo de execução do ciclo de processamento programado.

Erros ocultos não precisam ser permanentes para afetar os sistemas digitais; condições transitórias também podem afetar o comportamento destes sistemas. Os efeitos de condições ou erros transitórios fora do normal devem ser evitados. Esse tópico se torna ainda mais importante com o crescente interesse no aumento da vida útil do projeto de NPPs (atualmente 60 anos) e extensão da vida útil dos projetos existentes (entre 30 e 60 anos). Então, uma adequada consideração deve ser dada ao gerenciamento do ciclo de vida dos sistemas de I&C, incluindo sensores, atuadores, cabos, módulos de comunicação e processamento e exibição de dados. Para novas plantas, os planos de ciclo de vida para

substituição e atualização de computadores e *softwares* devem ser tratados na especificação do projeto.

2.8 Análise da Diversidade e Defesa em Profundidade, do inglês, *Diversity and Defense-in-Depth*

Faz-se necessário citar a avaliação da Diversidade e Defesa em Profundidade, do inglês, *Diversity and Defense-in-Depth* (D3), conhecida como análise D3. O tema é de tal importância, que a NRC publicou um *Branch Technical Position* (BTP) apenas sobre esse item. Trata-se do "*Guidance for Evaluation of Diversity and Defense-in-Depth in Digital Computer-Based Instrumentation and Control Systems*", no qual é discutida a forma de fazer a avaliação D3. Segundo o BTP 7-19, uma avaliação D3 é uma abordagem sistemática usada para analisar um sistema digital de I&C para as falhas de causa comum (CCFs), que podem ocorrer simultaneamente em um projeto redundante, por exemplo, em duas ou mais divisões independentes. Afinal, as CCFs podem fazer com que o sistema digital de I&C deixe de executar a sua função de segurança pretendida ou podem levar a operações espúrias.

Na referência NUREG-6303 (PRECKSHOT, 1994), um método para análise da Diversidade e Defesa em Profundidade é proposto, sugerindo ainda um modelo de relatório a ser apresentado ao órgão regulador. Tal método deve ser aplicado quando existe um grande potencial para a ocorrência de uma CCF, que é caso dos sistemas de proteção do reator *computer-based*. O método pode ser usado na etapa de projeto, como uma técnica para adicionar proteção diversa, ou ainda para demonstrar que a NPP possui adequada diversidade e defesa em profundidade. Outra referência importante para o tema é a NUREG-7007 (WOOD et al., 2010), que se propõe a avaliar a necessidade de diversidade em um projeto de NPP.

A análise D3 também é mencionada pela IAEA, como uma forma de investigar as vulnerabilidades de CCF nos sistemas de segurança (INTERNATIONAL ATOMIC ENERGY AGENCY, 2016b). Em especial para sistemas digitais de I&C, essa análise D3 deve ser feita para demonstrar que as vulnerabilidades que poderiam ocasionar CCFs estão adequadamente endereçadas (INTERNATIONAL ATOMIC ENERGY AGENCY, 2011). Ressalta-se ainda que tal análise D3 é requerida pelos órgãos reguladores, como por exemplo a NRC e CNEN.

2.9 *Field Programmable Gate Array* (FPGA)

Os FPGAs são circuitos integrados pertencentes à família dos dispositivos lógicos programáveis, que são programáveis através de uma linguagem de programação conhecida

como *Hardware Description Language* (HDL) após a sua fabricação.

Conforme será comentado no Item 4.2.2.1, o FPGA possui a capacidade de programar suas interconexões e funções lógicas através da HDL (INTERNATIONAL ATOMIC ENERGY AGENCY, 2018b). O FPGA é um tipo de circuito integrado, em que sua arquitetura interna de *hardware* é configurada para uma aplicação específica pelo projetista após a produção do chip. Os circuitos são fabricados sem qualquer tipo de funcionalidade e totalmente configuráveis através da HDL. Desta forma, o circuito integrado se comporta de maneira análoga à tecnologia *hardwired*. A HDL é uma forma de representar a arquitetura interna e o comportamento dos componentes lógicos elementares dos dispositivos, bem como os *links* entre esses componentes. Os dois tipos de padrão de linguagens HDL são a Verilog e a *Very high speed integrated circuit Hardware Description Language*, conhecida pela sigla VHDL (INTERNATIONAL ATOMIC ENERGY AGENCY, 2016a).

Os FPGAs dos diferentes fornecedores diferem em seu *design*, entretanto, eles compartilham a mesma arquitetura básica, que está ilustrada na Figura 2.6.

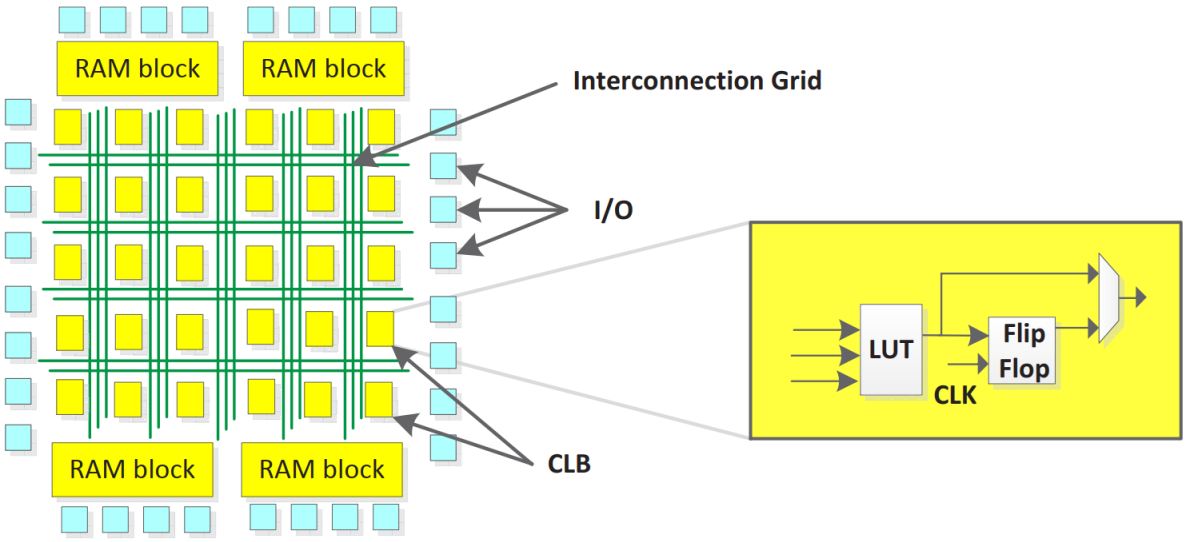

Figura 2.6 – Arquitetura típica de um FPGA.
Fonte: (INTERNATIONAL ATOMIC ENERGY AGENCY, 2016a)

A seguir está a explicação dos itens mostrados na arquitetura da Figura 2.6, extraída da referência (INTERNATIONAL ATOMIC ENERGY AGENCY, 2016a):

CLB (*Configurable Logic Blocks*): O CLB pode ser configurado para implementar qualquer função lógica (AND, OR, NOT, etc.). Cada CLB utiliza uma **LUT** (*Look-Up Table*) para implementar as funções lógicas. Vários CLBs podem ser interconectados para realizar funções lógicas mais complexas. A saída de cada CLB tem um **Flip-Flop** para sincronizar o fluxo de dados do FPGA.

I/O (*Input/Output*): Os FPGAs têm inúmeras entradas e saídas digitais. Cada I/O pode ser configurada como uma entrada ou uma saída de um ou mais CLBs.

***Interconnection Grid*:** A rede de interconexão interna é um conjunto de fios a serem interconectados em pontos de interseção através da programação HDL do FPGA. Essas interconexões ligam diferentes entradas/saídas das CLBs, assim como os blocos de I/O do FPGA, de acordo com o objetivo do projetista.

***RAM Block*:** Alguns FPGAs possuem memória do tipo SRAM e outros FPGAs, quando necessitam de uma reinicialização rápida de energia, são equipados com memórias não voláteis do tipo Flash.

3 Metodologia

Primeiramente faz-se necessário retomar a definição dos principais termos utilizados no presente trabalho. O Sistema Diverso de Atuação (SDA) é um *backup* do sistema de proteção principal de uma planta nuclear de potência. Ele é de suma importância para reduzir a possibilidade de ocorrência de falhas de causa comum em conjunto com acidentes de base de projeto ou ocorrências operacionais esperadas, além de reduzir a Probabilidade de Falha sob Demanda de certos eventos iniciadores. O uso do SDA é um requisito normativo de diversos órgãos reguladores (nacional e internacionais), implicando em um aumento da complexidade da arquitetura de I&C da planta.

A falha de causa comum (CCF) pode ser definida como a falha de duas ou mais estruturas, sistemas ou componentes, devida a um único evento ou causa específica. Os sistemas de segurança têm como requisito reduzir as chances de sua ocorrência. As NPPs utilizam o SDA para cumprir com esse objetivo.

Os conceitos de diversidade e defesa em profundidade são distintos, porém complementares. A diversidade é a presença de dois ou mais sistemas ou componentes diferentes funcionalmente usados para executar uma dada função. O uso deste conceito reduz a possibilidade de falha de causa comum. A defesa em profundidade é o uso de níveis distintos de equipamentos e procedimentos diversos para prevenir a escalada de ocorrências operacionais esperadas e para manter a efetividade das barreiras físicas colocadas entre a fonte de radiação (ou material radioativo) e os trabalhadores, público em geral e meio ambiente em uma NPP.

O *Field Programmable Gate Array* (FPGA) é um circuito integrado pertencente à família dos dispositivos lógicos programáveis, que é programável através de uma linguagem de programação conhecida como *Hardware Description Language* (HDL). O uso do FPGA é uma opção de projeto interessante para o desenvolvimento de um SDA.

O presente trabalho utilizou como metodologia os seguintes passos:

- Avaliação do estado da arte do Sistema Diverso de Atuação, assim como, de seus motivadores, a falha de causa comum e os conceitos de diversidade e defesa em profundidade e FPGA;
- Avaliação dos guias de segurança gerais e específicos da Agência Internacional de Energia Atômica (IAEA);
- Levantamento e estudo das normas, guias e documentos técnicos da *United States Nuclear Regulatory Commission* (NRC);

- Levantamento e estudo das normas técnicas da *International Electrotechnical Commission* (IEC) e *Institute of Electrical and Electronic Engineers* (IEEE);
- Comparação e avaliação dos preceitos encontrados na literatura;
- Análise do uso do FPGA no SDA;
- Apresentação, comparação e análise de projetos que utilizam o SDA; e
- Conclusão das análises sobre o SDA.

4 O Sistema Diverso de Atuação

Com o desenvolvimento dos sistemas digitais nas mais diversas áreas do conhecimento, a indústria nuclear também tem se beneficiado do seu progresso. Eles têm sido usados inclusive no desenvolvimento de sistemas de segurança em plantas nucleares de potência.

Conforme pode ser observado na Figura 4.1, adaptada da (INTERNATIONAL ATOMIC ENERGY AGENCY, 2011), em algumas plantas nucleares o sistema de proteção digital acumula funções de segurança. No caso de uma NPP hipotética, em que a defesa em profundidade está representada na Figura 4.1, é possível observar que o sistema de proteção digital acumula a função de SCRAM (*Reactor Trip*) e também outras funções de segurança (ESFAS). Uma falha de causa comum (CCF) desse sistema pode comprometer o isolamento dos níveis de proteção, implicando na possível perda do conceito de defesa em profundida da NPP. Desta forma, mesmo que seja muito improvável a ocorrência de uma CCF no sistema de proteção, devido à sua alta confiabilidade, a ocorrência de uma CCF levaria a planta a uma situação insegura.

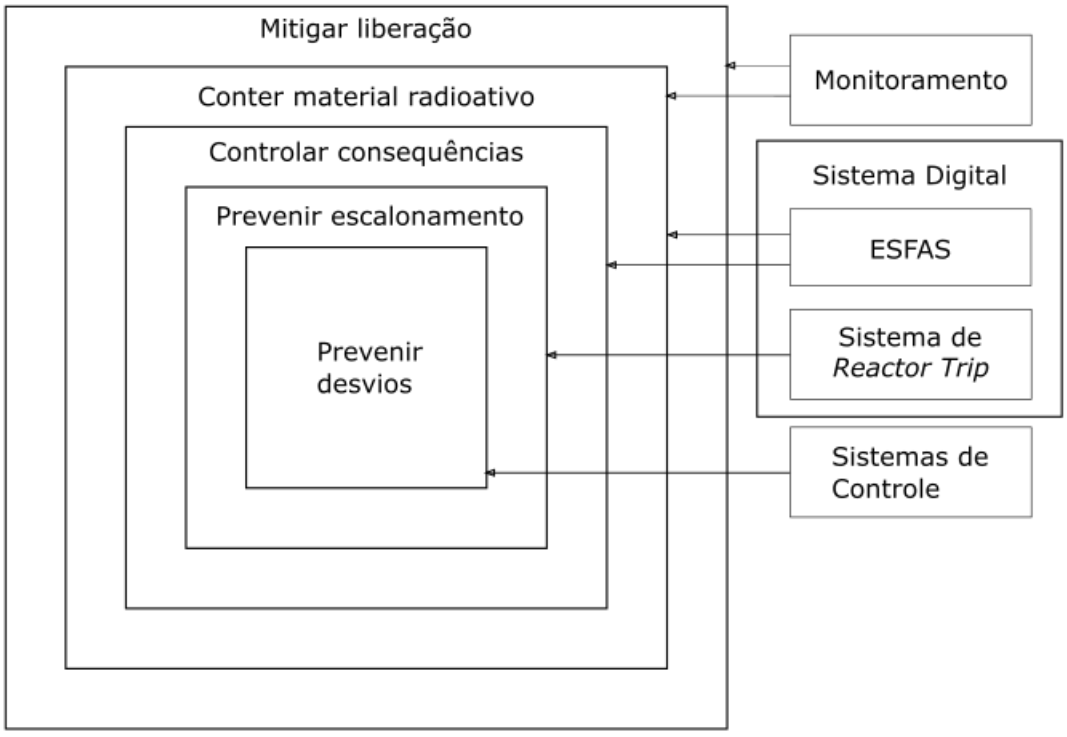

Figura 4.1 – Níveis da Defesa em profundidade. Adaptado de: (INTERNATIONAL ATOMIC ENERGY AGENCY, 2011)

O desenvolvimento do SDA é de extrema importância para reforçar o conceito da defesa em profundidade. Conforme mencionado na referência (WORLD NUCLEAR ASSOCIATION, 2018), o conceito de defesa em profundidade é diferente do conceito de diversidade, mas os dois devem trabalhar juntos em prol da segurança. A adição do SDA na arquitetura de uma NPP tem exatamente este objetivo, isto é, adicionar diversidade para reforçar o conceito de defesa em profundidade.

O desenvolvimento do SDA é considerado no presente trabalho, assim como em outras publicações da literatura, como um sistema de *backup* do sistema de proteção principal do reator. O termo Sistema Diverso de Atuação é utilizado na maioria das referências sobre o assunto, mas dependendo do órgão regulador outras nomenclaturas podem ser utilizadas, como por exemplo, Sistema Secundário de Proteção, Sistema Adicional de Proteção e Sistema de Segurança Não Computadorizado. Entretanto, todos eles têm em comum a característica principal de terem um *design* distinto ao do sistema principal de segurança (INTERNATIONAL ATOMIC ENERGY AGENCY, 2018b).

Quanto ao projeto do sistema de I&C da NPP, um conceito básico é a simplicidade, conforme pode ser visto na Seção 6.2 do guia de segurança específico para o projeto de I&C de uma NPP da IAEA (INTERNATIONAL ATOMIC ENERGY AGENCY, 2016b). O documento explicita que complexidades desnecessárias devem ser evitadas no projeto dos sistemas de segurança. Este conceito de simplicidade é reforçado no documento que trata das arquiteturas de I&C da IAEA (INTERNATIONAL ATOMIC ENERGY AGENCY, 2018a). Neste documento é indicada a importância da simplicidade, posto que ela promove um maior senso de entendimento e validação dos conceitos, reduzindo ainda o potencial de eventos inesperados. Na referência (INTERNATIONAL ATOMIC ENERGY AGENCY, 2018b) é feita a consideração que o projeto do SDA deve considerar a simplicidade em conjunto com os outros princípios fundamentais de projeto, como por exemplo: redundância, independência, defesa em profundidade, diversidade e determinismo (previsibilidade e repetibilidade).

Conforme comentado no Capítulo 2, o projeto da NPP deve levar em consideração o potencial de CCF em itens importantes para a segurança. No guia específico para projeto de sistemas de I&C (INTERNATIONAL ATOMIC ENERGY AGENCY, 2016b), a IAEA deixa explícita a sua preocupação em relação às CCFs do sistema de proteção. O documento declara que deve ser feita uma análise das consequências de cada evento iniciador postulado (PIE), combinada com uma CCF que impeça o sistema de proteção de executar suas funções de segurança. Nesse sentido, é importante que o projeto da planta tenha uma arquitetura, que leve em consideração a CCF do sistema de proteção principal. O SDA pode ser inserido com o claro objetivo de proporcionar um reforço à defesa em profundidade e ser independente do sistema de proteção principal da NPP, garantindo os requisitos supracitados.

Na referência (BURZYNSKI, 2017a) são apresentados seis diferentes tipos de arquiteturas de I&C, nos quais são adicionados sistemas diversos, com o objetivo de reduzir a possibilidade de CCF. O texto evidencia que isto torna a arquitetura indesejavelmente mais complexa, o que vai contra a premissa da IAEA de manter o conceito de simplicidade nos sistemas de I&C.

4.1 Classificação de Segurança do SDA

Conforme visto no Capítulo 2, a classificação de segurança varia de acordo com as normas de referência utilizadas. Para a IAEA, as classificações de segurança são divididas em Categorias de Segurança 1, 2 e 3, enquanto a IEC divide em Categorias A, B e C. Apesar das nomenclaturas distintas, as classificações são similares. Já a IEEE e a NRC subdividem as classes de segurança em *safety* e *non-safety*, não havendo similaridades com as classificações anteriores.

Quanto à classificação de segurança do SDA, conforme visto na Seção 2.3 do presente trabalho, os sistemas que tenham a atribuição de ser *backup* de uma função classificada como Categoria de Segurança 1 e que sejam obrigatórios para controlar as condições de extensão do projeto (DEC), sem derretimento do núcleo do reator, devem estar na Categoria de Segurança 2. Entretanto, para o projeto do SDA é necessário considerar os requisitos dos órgãos reguladores a respeito do assunto. Nesse ponto, a classificação de segurança do SDA não é um consenso entre os órgãos reguladores. Alguns deles exigem que o sistema tenha classificação de segurança, enquanto que outros permitem que esse sistema tenha uma classificação inferior (WORLD NUCLEAR ASSOCIATION, 2020). Alguns órgãos reguladores baseiam a classe de segurança esperada nas demandas de confiabilidade feitas para o sistema diverso de atuação.

4.2 Tecnologias Utilizadas no Desenvolvimento do SDA

O objetivo dessa seção é descrever as possíveis tecnologias em que o SDA pode ser desenvolvido. Nela serão discutidas as vantagens e desvantagens do uso dessas tecnologias para o desenvolvimento do SDA, conforme pode ser observado na Figura 4.2.

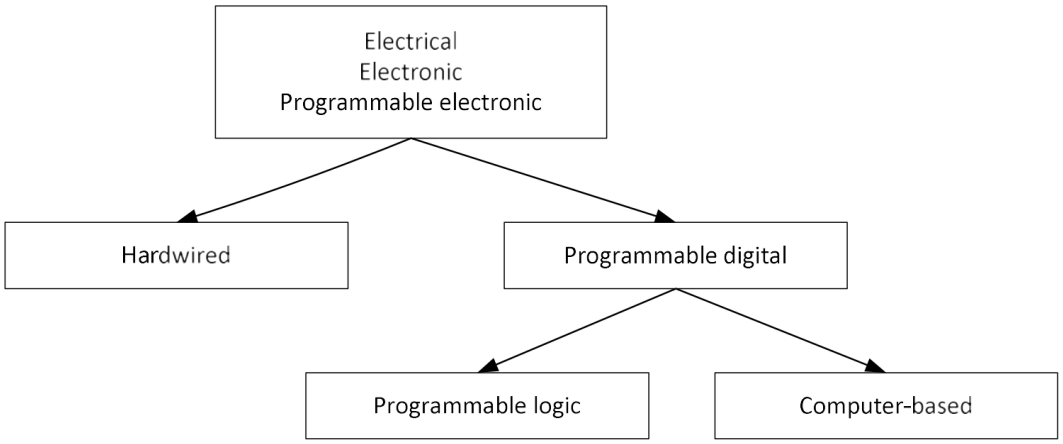

Figura 4.2 – Tecnologias utilizadas no SDA.
Fonte: (INTERNATIONAL ATOMIC ENERGY AGENCY, 2018b)

Em linhas gerais, as tecnologias que podem ser usadas no desenvolvimento do SDA têm origem eletro-eletrônica. Elas podem ser subdivididas em tecnologia *hardwired* e tecnologia digital programável. A tecnologia digital programável pode se subdividir ainda em tecnologia de lógica programável e tecnologia baseada em computador (*computer-based*).

4.2.1 Tecnologia *Hardwired*

A tecnologia *hardwired* está associada ao uso de relés, de circuitos de eletrônica analógica e de lógicas digitais discretas. Nesta tecnologia estão presentes os relés, que são itens simples, baratos e imunes a muitas das interferências eletromagnéticas. Entretanto, esta tecnologia é suscetível a vibrações e efeitos sísmicos. Outro exemplo da tecnologia *hardwired* são os dispositivos de estado sólido. Neste grupo encontram-se os transistores, capacitores, resistores e ainda os circuitos integrados, que são mais compactos e podem possuir várias portas AND/OR ou circuitos de amplificadores operacionais.

No uso da tecnologia *hardwired* é possível o uso de memórias e temporizadores e ainda a realização de lógicas booleanas. Funções analógicas também podem ser implementadas, entretanto não é possível realizar cálculos com ponto fixo, nem com ponto flutuante (INTERNATIONAL ATOMIC ENERGY AGENCY, 2018b).

A tecnologia *hardwired* é geralmente menos suscetível a CCF, devido a relativamente baixa complexidade das funcionalidades que podem ser implementadas com esta tecnologia. Entretanto a CCF não deve ser desconsiderada no projeto (INTERNATIONAL ATOMIC ENERGY AGENCY, 2018b).

4.2.2 Tecnologia Digital Programável

A tecnologia digital programável pode ser subdividida em duas, a tecnologia lógica programável, que pode ser configurada para executar uma função lógica pelo projetista (por exemplo, FPGA) e a tecnologia baseada em computador (*computer-based*), que executa instruções de *software* para realizar suas funções.

4.2.2.1 Tecnologia Lógica Programável

Trata-se de uma tecnologia que possui blocos lógicos básicos e que tem a capacidade de programar suas interconexões, como por exemplo *Programmable Logic Device* (PLD), *Complex Programmable Logic Device* (CPLD) e *Field Programmable Gate Array* (FPGA). O presente trabalho foca no uso de FPGA, que tem a capacidade de ser programado pelo projetista após a sua fabricação, através de uma linguagem de programação conhecida como *Hardware Description Language* (HDL) (INTERNATIONAL ATOMIC ENERGY AGENCY, 2018b). Maiores detalhes sobre o FPGA podem ser vistos no Capítulo 5.

Na tecnologia lógica programável é possível realizar funções booleanas e funções analógicas. Cálculos também podem ser feitos utilizando essa tecnologia, porém de forma mais difícil do que na tecnologia *computer-based*. É importante mencionar que um microprocessador pode ser implementado em um FPGA. Neste caso, ele apresenta os benefícios e malefícios da tecnologia *computer-based* e não da tecnologia lógica programável (INTERNATIONAL ATOMIC ENERGY AGENCY, 2018b).

A suscetibilidade a CCF não depende da tecnologia lógica programável em si, ela depende de como são desenvolvidas e implementadas as funções de I&C no equipamento. Se forem implementadas funções simples, facilmente verificáveis e testadas, então o equipamento terá uma baixa suscetibilidade a CCF. Entretanto, se forem implementadas funções complexas, ou até mesmo um microprocessador, então teremos um dispositivo suscetível a CCF (INTERNATIONAL ATOMIC ENERGY AGENCY, 2018b).

4.2.3 Tecnologia Baseada em Computador (*computer-based*)

A tecnologia baseada em computador (*computer-based*) depende de instruções de *software*, que são executadas em microprocessadores ou microcontroladores. As funções são descritas em um programa (exemplo: linguagem de programação C), que é traduzido por um compilador em um código para ser executado em um microprocessador ou microcontrolador (INTERNATIONAL ATOMIC ENERGY AGENCY, 2018b).

A suscetibilidade à CCF para a tecnologia baseada em computador (*computer-based*) é considerada significativa, devido à alta complexidade das funcionalidades implementadas no sistema. Mesmo quando utilizando funções de lógica simples, o programa resultante dificilmente consegue ser testado exaustivamente na prática, o que impede o descarte da

consideração da CCF (INTERNATIONAL ATOMIC ENERGY AGENCY, 2018b).

4.2.4 Comparação Entre as Tecnologias Utilizadas Para o Desenvolvimento do SDA

A Tabela 4.1 apresenta uma descrição das principais características das tecnologias que podem ser utilizadas no desenvolvimento do SDA. A tabela foi adaptada da referência (INTERNATIONAL ATOMIC ENERGY AGENCY, 2018b).

Tabela 4.1 – Comparação entre as tecnologias utilizadas para o desenvolvimento do SDA. Adaptado de: (INTERNATIONAL ATOMIC ENERGY AGENCY, 2018b)

	Tecnologia *hardwired*	Tecnologia lógica programável	Tecnologia *computer-based*
Lógica booleana	Sim	Sim	Sim
Funções analógicas	Sim	Sim	Sim
Cálculos complexos	Não	Sim*	Sim
Modificabilidade	Baixa	Alta	Alta
Capacidade de auto-diagnóstico	Baixa	Alta	Alta
Suscetibilidade à CCF	Baixa	Alta**	Alta

* : É possível a inclusão de cálculos, porém com uma maior dificuldade.
** : A suscetibilidade depende da complexidade das funções inseridas.

4.2.5 Outros Pontos Sobre as Tecnologias

É importante mencionar que a tecnologia utilizada no desenvolvimento do SDA é outro ponto que não é consenso entre os órgãos reguladores. Alguns órgãos reguladores exigem que o SDA seja desenvolvido com tecnologia *hardwired*. Outros órgãos reguladores desencorajam o uso de tecnologia *computer-based*, mas não o proíbem. Por fim, outros órgãos reguladores permitem o uso de sistemas digitais no desenvolvimento do SDA, desde que seja demonstrada uma diversidade adequada (INTERNATIONAL ATOMIC ENERGY AGENCY, 2016b).

Outro ponto a ser levado em consideração é que os sistemas diversos de atuação baseados em tecnologia *hardwired* oferecem menor vulnerabilidade ao risco cibernético que os sistemas que utilizam tecnologia programável digital (INTERNATIONAL ATOMIC

ENERGY AGENCY, 2016b). No capítulo 5 será demonstrado como a tecnologia FPGA também pode contribuir para a diminuição do risco cibernético.

4.3 Ações Manuais no SDA

Segundo o guia de segurança específico para projetos de sistemas de I&C para NPPs (INTERNATIONAL ATOMIC ENERGY AGENCY, 2016b), em geral a maioria das funções do sistema de proteção terá sua iniciação de forma automática. Para que o uso de ações manuais seja aceitável, o operador deve ter tempo suficiente para avaliar o *status* da planta e as ações que serão necessárias. A análise do tempo determina a margem de segurança e a sua diminuição leva à redução desta margem, portanto a incerteza na estimativa da diferença entre esses tempos deve ser considerada. Ainda segundo o mesmo guia (INTERNATIONAL ATOMIC ENERGY AGENCY, 2016b), para novos projetos de NPPs, é aconselhável que durante os primeiros 30 minutos de um acidente de base de projeto (DBA), não seja necessária nenhuma ação do operador para manter os parâmetros da planta dentro de limites estabelecidos. Tanto o guia de segurança (INTERNATIONAL ATOMIC ENERGY AGENCY, 2016b), quanto a *World Nuclear Association* (WNA) (WORLD NUCLEAR ASSOCIATION, 2020) consideram este ponto como divergente entre os órgãos reguladores para o projeto do SDA. Normalmente, a atuação manual pode ser aceita no SDA, mas as condições para que essas ações sejam aceitas variam. As seguintes práticas são observadas nos diferentes órgãos reguladores:

- A ação manual pode ser aceita se ela não for necessária em pelo menos 30 minutos após o acidente e a análise de fatores humanos confirmar que uma decisão adequada pode ser tomada e implementada dentro desses 30 minutos;
- A ação manual pode ser aceita se ela não for necessária em pelo menos 20 minutos após o acidente;
- A ação manual pode ser aceita para os ESFAS, mas não para o SCRAM; e
- A ação manual pode ser aceita sem restrições.

A questão da atuação manual deve ser levada em consideração no projeto do SDA e embora estejam citadas acima algumas práticas adotadas pelos órgãos reguladores, um órgão regulador específico pode adotar uma abordagem diferente com base na situação particular proposta (WORLD NUCLEAR ASSOCIATION, 2020).

4.4 A Comissão Reguladora Nuclear Norte Americana

O uso do SDA em NPPs está baseado principalmente em um requisito da Comissão Reguladora Nuclear Norte Americana - *U.S. Nuclear Regulatory Commission* (NRC). Trata-se do requisito para mitigação do ATWS, item 62, da parte 50 do título 10 da *Code of Federal Regulations* (CFR), representado como "10 CFR 50.62". Tal requisito está descrito a seguir:

> *Each pressurized water reactor must have equipment from sensor output to final actuation device, that is diverse from the reactor trip system, to automatically initiate the auxiliary (or emergency) feedwater system and initiate a turbine trip under conditions indicative of an ATWS. This equipment must be designed to perform its function in a reliable manner and be independent (from sensor output to the final actuation device) from the existing reactor trip system.*

No trecho percebe-se que a NRC exige expressamente o uso de equipamentos diversos para iniciar automaticamente a alimentação de emergência e desligar as turbinas em caso de ATWS. O equipamento deve ter confiabilidade e ser independente do sistema de *Reactor Trip*.

A NRC tem uma extensa lista de documentos de referência sobre os mais diversos assuntos. Dentre eles, tem-se o sistema de I&C, as CCFs e também o SDA. Uma classe de documentos muito importante é a dos Planos de Revisão Padrão (*Standard Review Plan* - SRP) que têm como um dos objetivos tornar as informações sobre questões regulatórias amplamente disponíveis e melhorar a comunicação entre a NRC, os membros interessados do público e a indústria de energia nuclear, entre outros objetivos.

Para os sistemas de I&C tem-se o Capítulo 7 da NUREG-0800, que é o SRP para a revisão do Relatório de Análise de Segurança (RAS) (US NUCLEAR REGULATORY COMMISSION, 2007). Este capítulo fornece orientação para a revisão dos sistemas de I&C para pedidos de licenças de NPPs. A Seção 7.8 trata dos sistemas diversos de I&C para adicionar proteção ao risco potencial de CCF. Nela é explicitada a importância da Análise da Diversidade e Defesa em Profundidade (D3), conforme comentado na revisão da literatura na Seção 2.8. Outro ponto importante deste documento, Seção 7.8 da NUREG-0800, é a definição pela NRC que o SDA pode acumular duas funções normativas. A primeira de cumprir com o requisito de diversidade apontado pelo relatório D3, servindo como um sistema de *backup* para o sistema de proteção. E a segunda de mitigar o ATWS, requisito 10 CFR 50.62 mencionado anteriormente.

Por fim, outro documento importante publicado pela NRC é o *Branch Technical Position* (BTP 7-19: "*Guidance for Evaluation of Defense in Depth and Diversity to*

address Common-Cause Failure due to Latent Design Defects in Digital Safety Systems" que traz diretrizes de como resolver a questão de falhas de causa comum ocultas e deve ser consultado como referência para o desenvolvimento do SDA. Nele são citados quatro pontos relacionados à CCF, diversidade e defesa em profundidade. Tais itens são citados em diversas referências e devem ser levados em consideração no desenvolvimento do projeto do SDA.

Ponto 1: O projeto da NPP deverá verificar a avaliação D3 dos sistemas de I&C propostos, a fim de demonstrar que as possíveis vulnerabilidades às CCFs foram adequadamente tratadas;

Ponto 2: Ao realizar a avaliação D3 indicada no Ponto 1, o projeto da NPP deverá verificar todas as CCFs de cada evento avaliado nos RAS, usando o método de melhor estimativa ou qualquer método citado no capítulo referente à analise de acidentes e transientes (Capítulo 15 da referência NUREG-0800) (US NUCLEAR REGULATORY COMMISSION, 2007). O projeto deverá demonstrar adequada diversidade em todos os eventos avaliados;

Ponto 3: Para os casos nos quais uma CCF postulada tiver a capacidade de desabilitar uma função de segurança, é exigido que um meio diverso realize a mesma função do sistema vulnerável ou uma função diferente, que proporcione uma proteção adequada para o sistema. O sistema diverso ou equipamento distinto poderá não ter classificação de segurança, se o sistema/equipamento tiver qualidade suficiente para executar a ação necessária nas condições associadas ao evento; e

Ponto 4: O projeto da NPP deverá prever um conjunto de controles e *displays* localizados na sala de controle principal, a fim de garantir a atuação das funções críticas de segurança manuais e para monitorar os parâmetros que dão suporte às funções de segurança. Estes controles e *displays* devem ser independentes e distintos dos sistemas de segurança *computer-based* indicados nos pontos 1 e 3.

5 O Uso do FPGA em SDA

O uso do *Field Programmable Gate Array* (FPGA) tem ganhado uma atenção mundial em sistemas de I&C das NPPs, particularmente nos sistemas de segurança (NASER, 2009). Este assunto tem sido muito pesquisado nos últimos anos por diversas instituições e organizações (WANG et al., 2021).

O emprego do FPGA é uma opção de projeto interessante para o desenvolvimento de um sistema de *backup* do sistema de proteção, quando este sistema de proteção é implementado usando a tecnologia *computer-based*. O uso do FPGA pode proporcionar uma solução mais prática e com um melhor custo-benefício do que a utilização de um outro sistema baseado em microprocessador diverso, ou ainda quando os requisitos de diversidade exigirem uma solução que não seja *computer-based* (NASER, 2009). O uso do FPGA pode adicionar uma boa diversidade à arquitetura de I&C, quando utilizado em um sistema que já possua uma filosofia *computer-based* ou quando o uso do FPGA é feito por diferentes fornecedores e/ou tecnologias e/ou técnicas de desenvolvimento dos sistemas principal e diverso (FARIAS; CARVALHO; SANTOS, 2015).

5.1 Vantagens do FPGA

Além da facilidade em projetar, é importante considerar outras vantagens do uso do FPGA, conforme descrição a seguir (INTERNATIONAL ATOMIC ENERGY AGENCY, 2016a):

- Baixa complexidade

Os microprocessadores possuem um sistema operacional, que por si próprios já trazem complexidade ao sistema, tornando mais difícil o projeto, o processo de Verificação e Validação (V&V) e o processo de licenciamento. Por não ter um sistema operacional, os sistemas baseados em FPGA podem ser mais simples e fáceis para testar e qualificar as aplicações de segurança. Algumas das vantagens do uso de FPGA podem ser perdidas ou significantemente reduzidas ao introduzir microprocessadores nos FPGAs, aumentando a complexidade do sistema (INTERNATIONAL ATOMIC ENERGY AGENCY, 2016a).

- Grande portabilidade das aplicações

A rápida obsolescência dos componentes eletrônicos resulta na necessidade de renovação de componentes dos sistema de I&C durante o ciclo de vida de uma NPP. Ainda, os próprios fornecedores de tais itens não conseguem garantir a compatibilidade completa entre componentes adquiridos em períodos distintos durante essas renovações. O uso de FPGA garante um grau significativo de portabilidade e compatibilidade de

projeto (portabilidade da HDL entre versões de diferentes chips FPGA produzidos pelo mesmo fabricante ou mesmo por fabricantes diferentes), o que mitiga a vulnerabilidade à obsolescência (INTERNATIONAL ATOMIC ENERGY AGENCY, 2016a).

- Suporte técnico com maior durabilidade

A portabilidade do código HDL ajuda a obter aplicativos independentes de *hardware*. É esperado que isso resulte em suporte técnico disponível durante toda a vida útil da NPP. Tal portabilidade também ajuda a reduzir substancialmente o custo de renovar um aplicativo existente para uma plataforma FPGA diferente, que estará disponível no futuro (INTERNATIONAL ATOMIC ENERGY AGENCY, 2016a).

- Tempos de resposta mais rápidos

Os FPGAs podem fazer processamentos paralelos e em altas velocidades de *clock*. Portanto, o uso de FPGA é ideal para as aplicações que necessitem de tempos de resposta muito curtos (INTERNATIONAL ATOMIC ENERGY AGENCY, 2016a).

- Processo de verificação e validação mais simples

O projeto que utiliza o FPGA pode incluir apenas as funcionalidades desejadas, não havendo funções ocultas, que podem permanecer sem serem testadas ou aparecerem de forma imprevisível em determinados estados. Isso resulta em uma menor complexidade e menor esforço na verificação e validação (INTERNATIONAL ATOMIC ENERGY AGENCY, 2016a).

- Redução da vulnerabilidade a ataques cibernéticos

A segurança cibernética em sistemas programáveis é sempre uma preocupação, independentemente da tecnologia adotada. O uso do FPGA tende a aumentar a segurança a ataques cibernéticos, por mais que não remova integralmente este risco. Uma característica que melhorara a segurança cibernética de alguns FPGAs é a impossibilidade de serem configurados *online*. Ainda, é possível que o FPGA seja baseado em chips do tipo antifusível (os quais são programáveis apenas uma vez). Alternativamente, o FPGA pode ser programado de tal maneira que o acesso físico seja necessário para modificar a sua programação (INTERNATIONAL ATOMIC ENERGY AGENCY, 2016a). É de suma importância destacar que essas estratégias desempenham um papel significativo na redução do potencial de exposição a ameaças cibernéticas, no entanto, não podem ser consideradas como uma eliminação completa delas. É imperativo reconhecer que a adoção de medidas de avaliação e mitigação desses riscos é essencial. Contudo, é relevante ressaltar que a abordagem abrangente deste tema ultrapassa os limites delineados pelo escopo desta dissertação.

- Melhor escolha tecnológica, quando se é necessário cumprir requisitos de diversidade

O uso do FPGA pode constituir uma opção viável para a diversidade entre as funções de segurança primárias e redundantes. O microprocessador redundante e os sistemas baseados em FPGA devem, no mínimo, atender aos critérios de diversidade em NUREG-6303 (PRECKSHOT, 1994), como segue (INTERNATIONAL ATOMIC ENERGY AGENCY, 2016a):

- Diversidade de *design* (diferentes tecnologias e arquitetura);
- Diversidade de equipamentos;
- Diversidade funcional (diferentes formas de alcançar o mesmo resultado);
- Diversidade de *software* (diferentes linguagens de programação, metodologias de *design* e arquitetura de *software*).

- Boa relação custo-benefício

A redução de custo advém de justificativas de segurança e/ou avaliações de confiabilidade mais simples e eficazes. Além disso, o desenvolvimento de soluções baseadas em FPGA pode ser feito usando métodos, linguagens e ferramentas já existentes. Alguns exemplos de fatores adicionais que podem ter um impacto ainda mais importante na relação custo-benefício são: o reduzido número de componentes e o baixo consumo; e a portabilidade de aplicativos de I&C, devido à linguagem HDL (NASER, 2009).

- Alta Confiabilidade e longa vida útil

Existem fornecedores de FPGA que possuem linhas de produtos para indústrias que exigem alta confiabilidade e longa vida útil, como por exemplo, as indústrias aeroespacial, aeronáutica e militar. Estes fornecedores tendem a oferecer um suporte de longo prazo maior às linhas de produtos do que os fornecedores de microprocessadores (INTERNATIONAL ATOMIC ENERGY AGENCY, 2016a).

- Outras vantagens

O uso do FPGA ainda pode ter outras vantagens menores, como por exemplo a flexibilidade de acomodar mudanças de projeto; a possibilidade da separação entre funções de segurança e funções não relacionadas com a segurança dentro de um mesmo FPGA; e a possibilidade de simulação e otimização das funcionalidades do FPGA (INTERNATIONAL ATOMIC ENERGY AGENCY, 2016a).

5.2 Desvantagens e Desafios do FPGA

Por outro lado, o FPGA possui algumas desvantagens e desafios, que são abordados a seguir.

- Poucas aplicações atuais na indústria de energia nuclear

Embora os FPGAs tenham sido amplamente utilizados em várias indústrias, eles ainda são relativamente novos em NPPs. Não há grande experiência operacional no setor nuclear para construir um banco de dados confiável e significativo para obter lições aprendidas e boas práticas. O FPGA ainda não tem um papel de destaque em aplicações de segurança, sendo um risco para as análises de segurança e licenciamento. Atualmente, existe apenas um padrão, publicado pela IEC, que fornece orientações e requisitos para soluções baseadas em FPGA para a indústria de energia nuclear ((INTERNATIONAL ELECTROTECHNICAL COMMISSION, 2020)); até o momento, essa norma ainda não foi adotada pela maioria dos órgãos reguladores (INTERNATIONAL ATOMIC ENERGY AGENCY, 2016a).

- Disponibilidade limitada de produtos e ferramentas

Atualmente, há apenas um pequeno número de plataformas de I&C baseadas em FPGA e produtos disponíveis e prontos para uso em NPPs. Embora métodos de desenvolvimento, linguagens e ferramentas sólidas estejam disponíveis no mercado, eles não alcançaram o nível de facilidade de uso e aceitação pelos desenvolvedores alcançado por suas contrapartes baseadas em microprocessador, como CLPs. Também há dúvidas sobre a transparência dessas ferramentas (INTERNATIONAL ATOMIC ENERGY AGENCY, 2016a).

- Devido à propriedade intelectual dos blocos de lógica funcional (*IP core*) proprietários , os objetos são menos transparentes

Os fornecedores oferecem bibliotecas de blocos de lógica funcional (*IP core*) para os usuários finais, como um meio de desenvolvimento mais rápido, dado que o circuito está pronto para o uso. Um *IP core*, que é uma unidade reutilizável, pode complicar o processo de aceitação quando é usado em um projeto. Como o *IP core* é propriedade intelectual do fornecedor, sua programação geralmente não está disponível para que o cliente demonstre para o órgão regulador. Além disso, o cliente não tem controle sobre a alteração do *IP core* (INTERNATIONAL ATOMIC ENERGY AGENCY, 2016a).

O uso de *IP core* deve ser evitado em projetos que envolvam sistemas críticos, funções de segurança e até mesmo no desenvolvimento de um projeto de SDA, pois além dos motivos supracitados, não é possível testar os pontos internos do seu circuito, o que dificultaria o licenciamento desse sistema, além de trazer mais complexidade ao projeto.

- Acesso reduzido a sinais internos para monitoramento, teste e solução de problemas

Em comparação com a eletrônica convencional ou soluções baseadas em microprocessador, uma solução baseada em FPGA pode resultar em menos observabilidade e menos acesso aos sinais internos da lógica funcional. Portanto, a análise deve ser realizada durante a fase de projeto, para poder fornecer acesso a sinais importantes para atividades como

monitoramento, teste e solução de problemas (INTERNATIONAL ATOMIC ENERGY AGENCY, 2016a).

- Dificuldade ao lidar com funções gráficas e interfaces homem-máquina complexas

Os FPGAs são muito eficientes para o processamento de dados envolvendo cálculos matemáticos. No entanto, eles não são a melhor solução para o processamento de interfaces gráficas, sistemas de menu e interfaces baseadas em janelas, que permitem a seleção de diferentes formas de exibição de informações, controles virtuais e filtragem e gerenciamento de alarmes (INTERNATIONAL ATOMIC ENERGY AGENCY, 2016a). Desta forma o FPGA não é recomendado pare este fim.

5.3 Arquiteturas de SDA com FPGA

O artigo (BURZYNSKI, 2017b), demonstra uma arquitetura típica baseada em FPGA como *backup* de um sistema de proteção, que utiliza uma tecnologia *computer-based*. Nessa solução é adicionado um SDA com um pequeno escopo, sem qualificação de segurança, que pode ser visualizado na Figura 5.1.

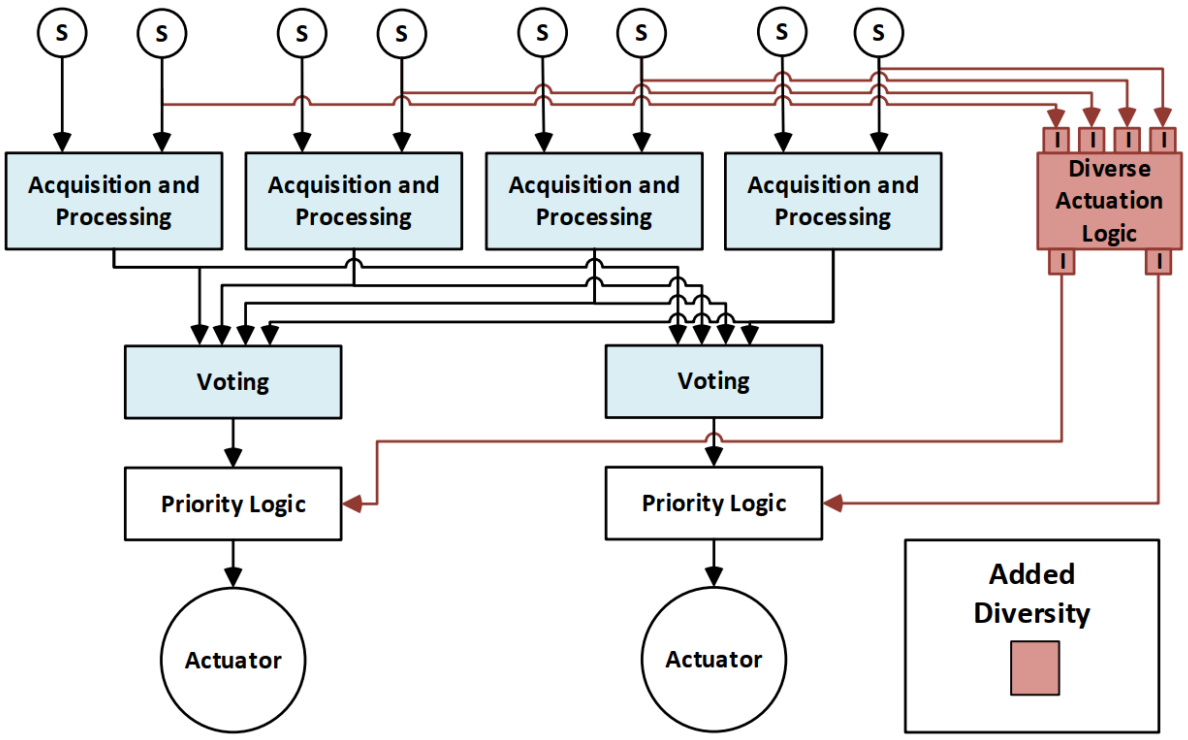

Figura 5.1 – Arquitetura típica de um SDA utilizando FPGA.
Fonte: (BURZYNSKI, 2017b)

Esse SDA adiciona complexidade à arquitetura de I&C da NPP. O sistema também torna mais complicadas as tarefas a serem realizadas pelos operadores, afinal em condições normais, sem a ocorrência de uma CCF, dois sistemas terão que ser gerenciados pelos

operadores (BURZYNSKI, 2017b). Para solucionar esse problema, o autor sugere algumas arquiteturas utilizando o FPGA, para adicionar diversidade à arquitetura de I&C, de forma a combater as possíveis CCFs do sistema.

5.4 Discussões Adicionais e Licenciamento

A escolha da tecnologia a ser utilizada no desenvolvimento do SDA é um ponto essencial do projeto. O uso da tecnologia *hardwired* é indicada, visando proporcionar uma importante diversificação do sistema de proteção principal. Isso se justifica, pois atualmente é comum que o Sistema de Proteção seja desenvolvido com equipamentos *computer-based* e a utilização da tecnologia *hardwired* evita a falha de modo comum de *software*. O uso da tecnologia FPGA mostrou-se capaz de atender esta diversificação. O principal motivo é que o FPGA se comporta como um circuito *hardwired* depois de programado. Entretanto, o processo de compilação dos circuitos FPGA utiliza um *software* para criação do circuito, que não é aberto pelo fabricante, e por isso, a resistência de alguns órgãos reguladores. Este software realiza um "processo de compilação" que é, na realidade, uma série de etapas que incluem síntese e *place-and-route* do circuito definido em HDL, culminando na criação do arquivo de configuração (*bitstream*).

Para contornar a resistência dos órgãos reguladores, é possível testar as entradas, saídas e pontos internos do circuito FPGA, como se fosse um circuito *hardwired*, tornando o sistema mais transparente e facilitando o processo de V&V.

O licenciamento de sistemas digitais baseados em FPGA é uma parte importante do projeto, desenvolvimento, implementação e operação. Embora o uso do FPGA em aplicações não relacionadas à segurança tenha ocorrido sem problemas, o esforço de licenciamento associado ao uso de FPGAs em sistemas de segurança tem sido mais trabalhoso (INTERNATIONAL ATOMIC ENERGY AGENCY, 2016a), conforme explicado anteriormente.

6 Exemplos da aplicação do SDA em Plantas Nucleares de Potência

O objetivo deste capítulo é apresentar exemplos de algumas plantas nucleares que utilizam o SDA em sua arquitetura de controle. Conforme mencionado no Capítulo 4 do presente trabalho, outras nomenclaturas podem ser utilizadas para representar este sistema, que atua como *backup* do sistema principal de proteção.

Foram selecionados exemplos com o intuito de abordar uma diversidade de projetos que foram submetidos para avaliação de diferentes órgãos reguladores. Foi analisado um projeto americano, um europeu (França), um sul coreano e um chinês. Estes projetos adotam abordagens distintas e compartilham algumas semelhanças, como é explorado adiante e discutido na conclusão deste capítulo.

6.1 Projeto da US-APWR

A planta US-APWR foi projetada pela Mitsubishi Heavy Industries Ltd. Os principais sistemas que compõem a arquitetura de controle desta planta estão descritos a seguir (MITSUBISHI HEAVY INDUSTRIES, 2013) (MITSUBISHI HEAVY INDUSTRIES, 2011) (INTERNATIONAL ATOMIC ENERGY AGENCY, 2018b).

- O *Protection and Safety Monitoring System* (PSMS), sistema digital que engloba todos os sistemas I&C relacionados à segurança na planta;
- O *Plant Control and Monitoring System* (PCMS), sistema que contém diversos subsistemas com controladores digitais, utilizados para regular a planta em operação normal e podem ser usados para mitigar as consequências em transientes;
- Através do *Human-System Interface System* (HSIS), todas as funções necessárias para atingir e manter o desligamento normal e seguro podem ser monitoradas e iniciadas manualmente. O HSIS é separado em duas partes, uma delas é classificada como sistema relacionado à segurança e fornece todos os controles e informações da planta relacionados à segurança (incluindo parâmetros críticos necessários para condições pós-acidente), enquanto a outra parte não é relacionada com a segurança.
- O SDA deste projeto fornece monitoramento, controle e atuação de sistemas de segurança e sistemas não considerados de segurança, necessários para lidar com condições anormais da planta, concomitante com um CCF que desativa todas as funções digitais do sistema de segurança digital (PSMS) e do sistema de controle digital (PCMS).

Vale ressaltar que tanto o PSMS quanto o PCMS são sistemas digitais baseados em microprocessadores (*computer-based*), que alcançam alta confiabilidade, conforme descrito no Relatório Tópico do Sistema I&C de Segurança (MITSUBISHI HEAVY INDUSTRIES, 2009). Estes sistemas são completamente digitais e utilizam a tecnologia *Mitsubishi Electric Total Advanced Controller* (MELTAC) (MITSUBISHI HEAVY INDUSTRIES, 2009).

Além disso, os sistemas de segurança (PSMS e parte de segurança do HSIS) são completamente isolados, segregados e independentes dos sistemas não relacionados à segurança (PCMS, SDA, e parte não relacionada à segurança do HSIS). Então, uma falha nos sistemas que não tem classificação de segurança não afeta o sistema de segurança (PSMS).

A Figura 6.1 mostra a arquitetura completa da US-APWR (MITSUBISHI HEAVY INDUSTRIES, 2009).

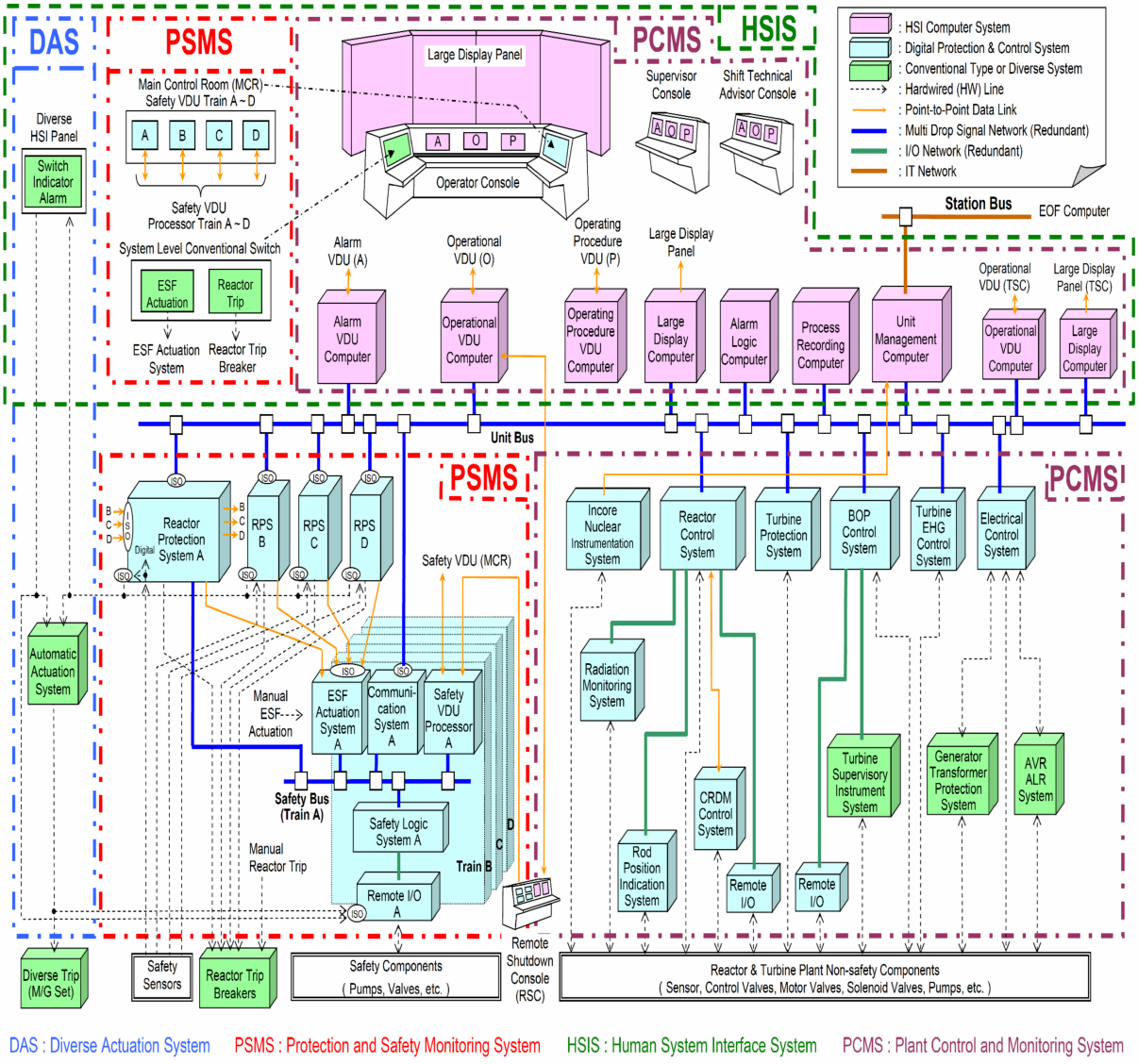

Figura 6.1 – Arquitetura de I&C US-APWR.
Fonte: (MITSUBISHI HEAVY INDUSTRIES, 2009)

O Sistema Diverso de Atuação deste projeto possui atuação automática, interface humano-máquina em um painel diverso e interface com os sistemas PSMS e PCMS.

No que concerne à qualificação de segurança do SDA da US-APWR, ele não foi projetado com classificação de segurança (*non-safety*), porém como o SDA é um sistema importante para a segurança da planta, ele deve atender aos requisitos de um programa de garantia de qualidade aumentada.

Em relação à tecnologia utilizada neste projeto, este SDA possui tecnologia *hardwired* (circuitos analógicos, dispositivos de processamento lógico de estado sólido, circuitos de relé), que são diversos e independentes dos sistemas *computer-based*. Além disso, o projeto contempla dispositivos que são instalados em quatro diferentes gabinetes de atuação automática. Estes gabinetes estão localizados em salas elétricas Classe 1E fisicamente separadas. Os gabinetes são qualificados como Categoria Sísmica II para lidar com eventos sísmicos (INTERNATIONAL ATOMIC ENERGY AGENCY, 2018b).

A Tabela 6.1 foi adaptada da referência (MITSUBISHI HEAVY INDUSTRIES, 2013), nela está apresentado o tempo de resposta necessário para o operador tomar a ação necessária no SDA para cada sistema da planta em cada evento iniciador. A partir dela é possível definir o requisito para o projeto do SDA, como por exemplo as ações que devem ser automatizadas.

Tabela 6.1 – Tempo de Atuação para Cada Evento Iniciador no SDA. Adaptado de: (MITSUBISHI HEAVY INDUSTRIES, 2013)

Função	AOO	Ruptura dos Tubos do GV	LOCA	Requisito SDA
Trip do Reator (SCRAM)	A	A	A	A
Sistema de Água de Alimentação de Emergência	A	C	C	A
Sistema de Resfriamento do Núcleo de Emergência		C	A	A
Isolamento do Sistema Secundário		B		B

Nota:
* A: Ação necessária em até 10 minutos, portanto o SDA atua de forma automática.
* B: Ação necessária em até 30 minutos, portanto indicações e controles manuais estarão no painel de controle do SDA (Trata-se do *Diverse HSI Panel* da Figura 6.1).
* C: Ação necessária após 30 minutos, portanto indicações e controles manuais serão fornecidos fora da sala de controle principal.

As operações que necessitem atuação do operador em até dez minutos são realizadas de forma automática pelo SDA. O relatório de análise de defesa em profundidade e de diversidade (MITSUBISHI HEAVY INDUSTRIES, 2011) fornece justificativas para ações

manuais do operador, creditadas após 10 minutos.

6.2 Projeto da EPR Flamanville 3

O projeto da EPR Flamanville 3 está em construção na França, próximo à cidade que leva o mesmo nome da NPP, Flamanville. A arquitetura de I&C da EPR Flamanville 3 é formada pelos seguintes subsistemas.

- Sistema de proteção *Protection System* (PS na Figura 6.2). Ele fornece a proteção automática para as funções de proteção do reator necessárias para atingir um estado controlado após um evento iniciador da base de projeto;
- Sistema de automação de segurança *Safety Automation System* (SAS na Figura 6.2); e
- Sistema de Controle e Informação de Segurança *Safety Information and Control System* (SICS na Figura 6.2).

Tanto o SAS quanto o SICS fornecem comandos manuais e *displays* necessários para a operação pós-acidente após a ocorrência de um evento iniciador da base de projeto. Eles possibilitam a transição da planta de um estado controlado para um estado seguro. No projeto dessa NPP, estes sistemas fornecem atuação automática, de forma que nenhuma ação dos operadores é necessária nos primeiros 30 minutos após um evento iniciador (INTERNATIONAL ATOMIC ENERGY AGENCY, 2018b).

A Figura 6.2 mostra a arquitetura completa da EPR Flamanville 3.

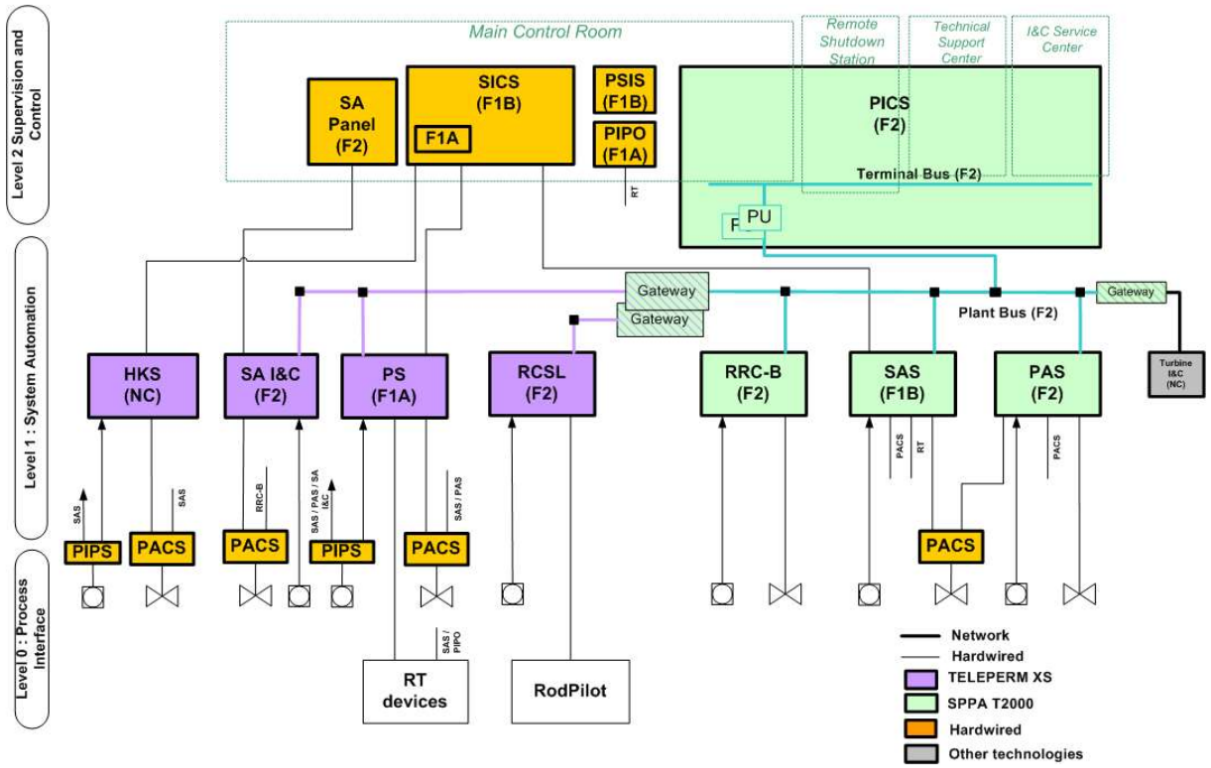

Figura 6.2 – Arquitetura de I&C EPR Flamanville 3.
Fonte: (INTERNATIONAL ATOMIC ENERGY AGENCY, 2018b)

Em relação à classificação de segurança, tanto o PS quanto o SAS possuem mais de uma classificação de segurança, dependendo das funções realizadas. As funções diversas de segurança do PS têm qualificação F2, que é equivalente à Classificação de Segurança 3 da IAEA apresentada nesse trabalho no Capítulo 2. Já as funções diversas de segurança do SAS possuem classificação F1B, que equivale à Classificação de Segurança 2 (INTERNATIONAL ATOMIC ENERGY AGENCY, 2018b).

O projeto da EPR Flamanville 3 não possui um sistema intitulado Sistema Diverso de Atuação. Entretanto, o projeto demonstra que as possíveis CCFs são mitigadas através dos dois sistemas de segurança, o PS e o SAS. O PS é implementado utilizando a plataforma Teleperm XS, enquanto o SAS utiliza a plataforma da Siemens SPPA T2000. Ambos utilizam uma tecnologia *computer-based*. Uma CCF do sistema PS é mitigada pelo sistema SAS, enquanto uma CCF no sistema SAS é mitigada pelo sistema PS, em conjunto com o sistema *Hard kernel system* (HKS), também implementado pela plataforma Teleperm XS. Embora os sistemas tenham sido implementados utilizando uma tecnologia *computer-based*, uma justificativa detalhada foi produzida para estabelecer que as duas plataforma são diversas e que, por isso, uma CCF das duas plataformas não é possível (INTERNATIONAL ATOMIC ENERGY AGENCY, 2018b).

6.3 Projeto da APR1400

Para o projeto da APR1400, desenvolvido pela *Korea Electric Power Corporation & Korea Hydro & Nuclear Power Co.*, existem duas plantas em operação na Coreia do Sul e outras duas em construção no mesmo local, entre outras plantas pelo mundo. Na APR1400, o SDA foi projetado com foco na mitigação de possíveis CCFs dos sistemas de segurança de I&C, incluindo o sistema principal de proteção da planta *Plant Protection System* (PPS na Figura 6.3) e o ESFAS *Engineered Safety Features-Component Control System* (ESF-CCS na Figura 6.3). O SDA desta NPP consiste na combinação de três subsistemas, são eles:

- O sistema de proteção diverso *Diverse Protection System* (DPS na Figura 6.3). Tal sistema possui as funções de desligamento rápido do reator (SCRAM), desligamento da turbina, acionamento do sistema de alimentação de água auxiliar e acionamento da injeção de segurança;

- As chaves manuais para atuação diversa das ESFs (DMA na Figura 6.3). Estas chaves permitem a operação manual dos EFAS a partir da sala de controle principal, no caso da ocorrência de uma CCF. Estas chaves enviam sinais para acionamento dos seguintes sistemas: sistema de injeção de segurança; sistema de isolamento de vapor principal; sistema de isolamento da contenção; sistema de atuação do *spray* da contenção; e sistema auxiliar de alimentação de água. Essas chaves usam tecnologia *hardwired* e são independentes do sistema de segurança da planta; e

- O sistema de indicação diversa *Diverse Indication System* (DIS na Figura 6.3). Este sistema fornece monitoramento das variáveis críticas, no caso da ocorrência de uma CCF de *software*.

O SDA implementado possui diversidade e defesa em profundidade suficientes para atender a um ATWS e a um dado AOO ou acidente postulado concorrente com uma CCF de *software*, que impossibilitaria o sistema principal de proteção de executar as suas funções.

A Figura 6.3 apresenta a arquitetura completa de I&C da APR1400.

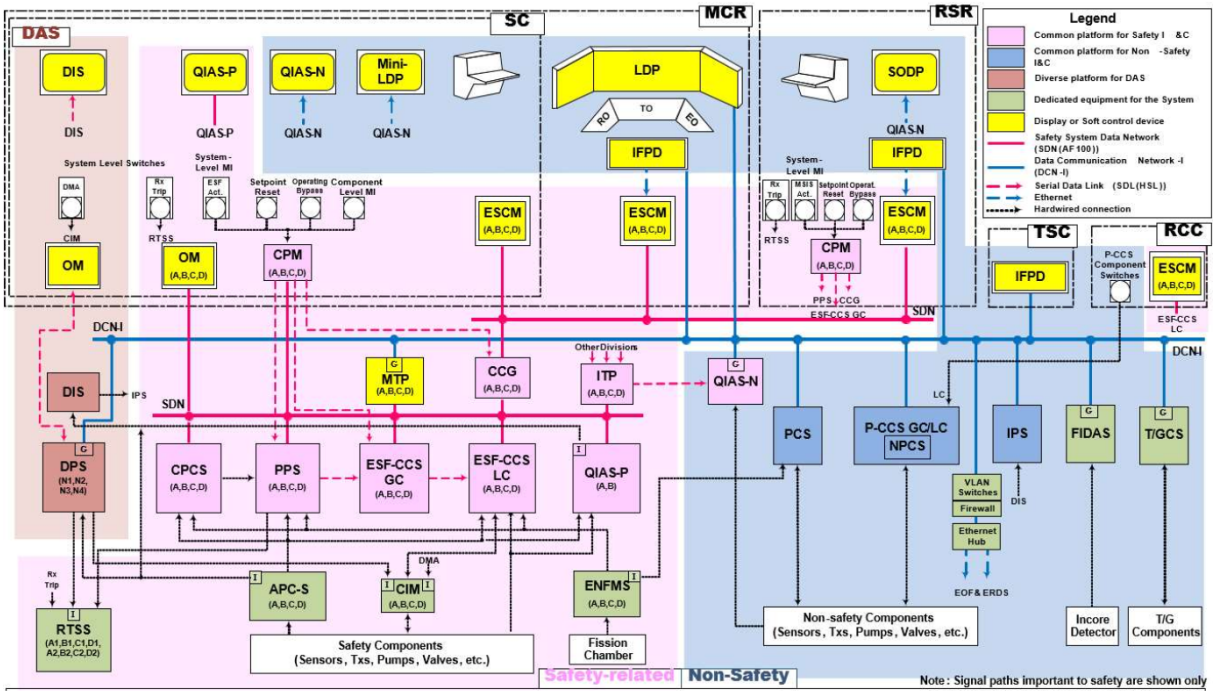

Figura 6.3 – Arquitetura de I&C da APR1400.
Fonte: (KEPCO&KHN, 2018)

Com relação à qualificação de segurança dos subsistemas do SDA desta NPP, eles não foram projetados com classificação de segurança. Isto é, eles possuem equipamentos *non-safety*, porém em seu projeto é considerado o uso de uma qualidade aumentada.

No SDA da APR1400, tanto o sistema de proteção diverso (DPS) quanto o sistema de indicação diversa (DIS) foram implementados utilizando um controlador baseado em tecnologia FPGA, diferente do sistema comum de segurança da NPP (INTERNATIONAL ATOMIC ENERGY AGENCY, 2018b). O uso da tecnologia FPGA forneceu dois tipos de diversidade distintas ao projeto de I&C, conforme visto no Capítulo 2: a diversidade de equipamento (isto se deve ao fato do sistema principal de proteção ser baseado em tecnologia PLC *computer-based*) e a diversidade de *software*, justificada pelo uso da linguagem HDL para o desenvolvimento do programa no FPGA.

6.4 Projeto da ACPR1000

O projeto da ACPR1000 foi desenvolvido pela *China General Nuclear Power Group*. Uma de suas unidades, está localizada na Província de Guangdong, China. Na ACPR1000, um sistema diverso de atuação (*Diverse Actuation System* - DAS) foi introduzido na arquitetura de I&C para combater uma possível CCF de software do sistema de proteção e monitoramento do reator (*Reactor Protection and Monitoring System* - RPMS). A Figura 6.4 mostra em detalhes a composição do SDA desta NPP.

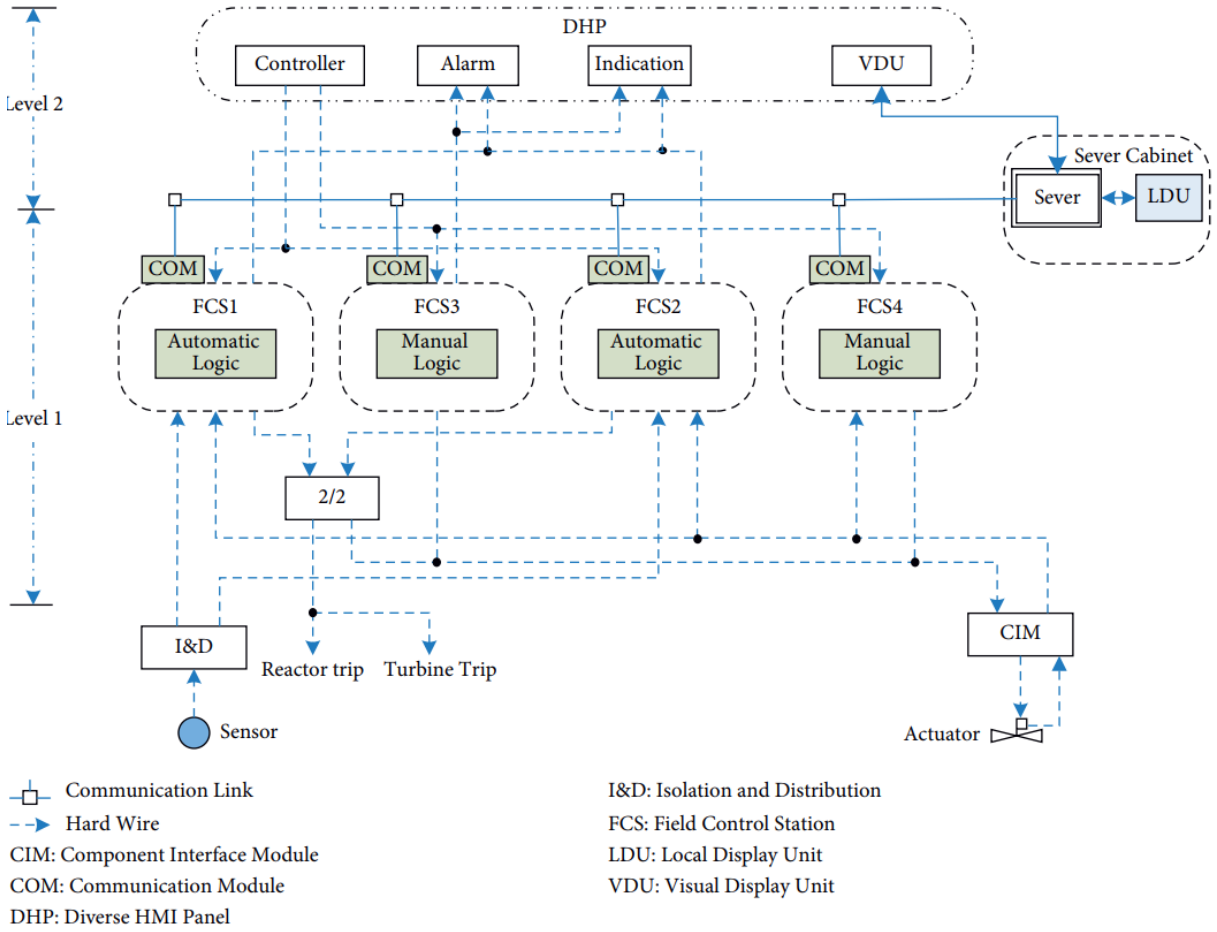

Figura 6.4 – Arquitetura do SDA da ACPR1000.
Fonte: (WANG et al., 2021)

O projeto do SDA desta planta foi realizado com o objetivo claro de lidar com a CCF de *software* do RPMS. Desta forma, o projeto considerou que uma CCF de *software* do RPMS não levaria à indisponibilidade dos instrumentos e atuadores utilizados pelo RPMS, se precauções especiais fossem tomadas. Com isso, é aceitável que o projeto do SDA compartilhe esses instrumentos e atuadores com o RPMS. O SDA projetado possui uma diversidade entre a entrada do sensor (excluindo o sensor, o sinal do sensor é compartilhado por meio de circuitos analógicos convencionais antes de entrar no RPMS) até a saída do atuador (excluindo o atuador). As exceções são os atuadores que promovem o desligamento rápido do reator (SCRAM). Neste caso, o *Reactor Trip* (RT) do SDA é diferente do RT do RPMS. O RT do RPMS abre os disjuntores de alimentação, enquanto o RT do SDA emite um sinal para as cabines de alimentação do sistema de controle de barras, cortando assim a alimentação de energia deste mecanismo (WANG et al., 2021).

Outra característica deste SDA é a prevenção contra sinais espúrios. Uma medida tomada para isso é uma atuação somente quando há energização do sinal, o que permite que não haja acionamento espúrio em caso de perda de energia elétrica. Outra medida é a votação 2 de 2 para o acionamento do *Reactor Trip* e desligamento das turbinas, conforme

pode ser observado na Figura 6.4.

Conforme comentado no Capítulo 4, um ponto divergente entre os órgãos reguladores é a questão da atuação manual. No projeto do SDA desta NPP, foi considerado que o operador tem 20 minutos para avaliar a situação e poder atuar em caso de um evento iniciador (WANG et al., 2021).

O FPGA foi utilizado para o desenvolvimento do SDA, por ser diverso do RPMS que foi implementado na tecnologia *computer-based*. Os testes de comissionamento verificaram que o SDA proposto é capaz de executar as funções que foram projetadas (WANG et al., 2021).

6.5 Avaliação dos Projetos de SDA

O trabalho buscou exemplos significativos para demonstrar como o SDA pode ser abordado de maneiras distintas nos diversos projetos. Conforme comentado, existe uma forte influência do órgão licenciador e as principais diferenças nos projetos de SDA são relacionadas aos seguintes itens:

- Classificação de Segurança do SDA;
- Tecnologia utilizada no desenvolvimento do SDA;
- Tipos de Diversidade; e
- Interface Homem-Máquina.

Em função disso foi elaborada a Tabela 6.2, que compara os projetos de SDA supracitados.

Tabela 6.2 – Comparativo dos Projetos de SDA

Comparação	US-APWR	EPR Flamanville *
Classificação de Segurança	SDA é classificado como *non-safety*. Entretanto o sistema é considerado importante para a segurança e, por isso, deve atender requisitos de um programa de garantia de qualidade aumentada.	A classificação de segurança dos sistemas (PS e SAS) depende das funções realizadas.
Tecnologia utilizada	SDA é de tecnologia *hardwired*.	Ambos os sistemas utilizados no projeto (PS e SAS) são tecnologia *computer-based*.
Tipos de Diversidade do projeto	Diversidade de projeto, equipamento (com tecnologia diferente), funcional, lógica.	Diversidade de sinal, equipamento (com a mesma tecnologia), funcional, de projeto e lógica.
Interface Homem-Maquina	O tempo de resposta depende da função realizada. Ações que necessitem de uma resposta em menos de 10 minutos após o acidente são automáticas, ações que necessitem até 30 minutos após o acidente foram aprovadas pela NRC após estudo e existem funções que não necessitam resposta em menos de 30 minutos.	Nenhuma ação dos operadores é necessária nos primeiros 30 minutos após um evento iniciador.

*: O projeto da EPR Flamanville não possui um sistema intitulado Sistema Diverso de Atuação. Entretanto, o projeto demonstra que as possíveis CCFs são mitigadas através dos dois sistemas de segurança, o Protection System (PS) e o Safety Automation System (SAS).

Tabela 6.2 – Comparativo dos Projetos de SDA (continuação)

Comparação	APR1400	ACPR1000
Classificação de Segurança	SDA é classificado como *non-safety*. Entretanto o sistema é considerado importante para a segurança e, por isso, deve atender requisitos de um programa de garantia de qualidade aumentada.	SDA é classificado como *non-safety*. Entretanto o sistema utiliza sensores e atuadores com classificação de segurança.
Tecnologia utilizada	Utiliza a tecnologia FPGA.	Utiliza a tecnologia FPGA.
Tipos de Diversidade do projeto	Diversidade de sinal, equipamento (com tecnologia diferente), funcional, software, humana e de projeto.	Diversidade de projeto, equipamento (com tecnologia diferente), funcional, lógica.
Interface Homem-Maquina	Utiliza o DIS e DMA (ambos diversos dos sistemas principais). O tempo para ação do operador não foi mencionado.	O operador tem 20 minutos para avaliar a situação e atuar no caso de um evento iniciador.

Na Tabela 6.2 ficam evidentes as diferenças entre os projetos apresentados. Em relação à Classificação de Segurança, os projetos da US-APWR e APR1400 foram classificados como *non-safety*. Entretanto o SDA é considerado importante para a segurança e, por isso, deve atender aos requisitos de um programa de garantia de qualidade aumentada. O projeto da ACPR1000, também foi classificado como como *non-safety*, mas utiliza sensores e atuadores com classificação de segurança. O projeto da EPR Flamanville não possui um sistema intitulado Sistema Diverso de Atuação, a classificação de segurança dos sistemas responsáveis pela segurança depende das funções realizadas.

Em relação à tecnologia utilizada, observa-se que o projeto francês (EPR Flamanville) possui os sistemas utilizados para a segurança com tecnologia *computer-based*. O

projeto americano (US-APWR) possui tecnologia *hardwired* e os projetos APR1400 e ACPR1000 possuem tecnologia FPGA. Novamente, é possível ver a influência do órgão regulador na escolha da tecnologia.

No âmbito dos tipos de diversidade, é evidente que todos os projetos incorporam uma grande variedade de diversidade, tanto em aspectos quantitativos quanto qualitativos. Essa diversificação revela-se de extrema importância para mitigar a ocorrência de falhas de modo comum e aprimorar a abordagem da defesa em profundidade.

Por fim, no que diz respeito à Interface Homem-Máquina, observa-se um projeto francês bastante conservador, no qual nenhuma ação dos operadores é necessária nos primeiros 30 minutos após um evento iniciador. No projeto americano (US-APWR) o tempo de resposta do operador depende da função realizada. No projeto chinês, o operador tem 20 minutos para avaliar a situação e atuar em caso de um evento iniciador. No projeto sul coreano (APR1400), o tempo para ação do operador não foi mencionado.

7 Conclusão

Após análise exaustiva sobre o tema, conclui-se que o uso do sistema diverso de atuação tem um impacto positivo no combate às CCFs dos sistemas de segurança de uma NPP.

O posicionamento do órgão regulador tem um papel decisivo no projeto do SDA e até mesmo da sua existência. Ele terá uma grande influência em vários aspectos do projeto, mas em especial na classificação de segurança que será empregada, na tecnologia que será utilizada (*hardwired*, FPGA, *computer-based*) e na forma que serão projetadas as ações manuais.

O ponto principal do projeto do SDA é combater as possíveis CCFs do sistema principal de segurança. Logo, dependendo do projeto da NPP, existem formas de ajustar a arquitetura do sistema de I&C, de tal maneira que não haja necessidade de um SDA. Deve-se ter em mente, entretanto, que o projeto será avaliado por um órgão regulador, que via de regra exige a implementação de um SDA. Portanto, tal assunto deve ser cuidadosamente avaliado.

Outro ponto que deve ser levado em consideração no projeto do SDA é a sua complexidade. A adição de um SDA irá trazer maior complexidade à arquitetura de I&C, indo de encontro a um dos princípios básicos de projeto de sistemas de I&C, que é a simplicidade do sistema. Então, o projeto do SDA deve ser o mais simples possível.

O emprego do FPGA se destaca como uma alternativa atrativa para o desenvolvimento de um SDA. Fornecendo uma solução prática e de bom custo-benefício, o FPGA pode superar sistemas baseados em microprocessadores, especialmente quando requisitos de diversificação exigem abordagens não *computer-based*. Embora a tecnologia FPGA satisfaça essas necessidades de diversidade ao imitar um circuito *hardwired* após a programação, a relutância de órgãos reguladores é notável devido à falta de acesso ao software usado na compilação do FPGA. Para contornar essa resistência, é possível testar as entradas, saídas e pontos internos do circuito FPGA, como se fosse um circuito *hardwired*, tornando o sistema mais transparente e facilitando o processo de verificação e validação (V&V).

Por fim, o projeto do SDA deve contemplar mais de um tipo de diversidade para melhor combater as CCFs. Devem ser avaliados os aspectos de custo e requisitos normativos do local da instalação da NPP.

Referências Bibliográficas

BURZYNSKI, M. Impacts of common cause failure regulatory requirements on protection system architectures. *NPIC&HMIT*, 2017.

BURZYNSKI, M. J. Case for the adoption of fpga technology in the implementation and replacement of equipment and systems in nuclear power plants. In: *ISOFIC 2017*. [S.l.: s.n.], 2017. p. 1–10.

EMPRESA BRASILEIRA DE ENERGIA. *Plano Nacional de Energia 2050*. Empresa Brasileira de Energia, 2020.

EMPRESA BRASILEIRA DE ENERGIA. *Balanço Energético Nacional 2023: Ano Base 2022*. Empresa Brasileira de Energia, 2023.

FARIAS, M. S.; CARVALHO, P. V. R.; SANTOS, A. L. dos. Design issues on using fpga-based i&c systems. *Instituto de Engenharia Nuclear: Progress Report*, n. 2, p. 38–38, 2015.

INTERNATIONAL ATOMIC ENERGY AGENCY. *Defence in Depth in Nuclear Safety*. Vienna: INTERNATIONAL ATOMIC ENERGY AGENCY, 1996. (INSAG Series, 10). ISBN 92-0-102596-3. Disponível em: <https://www.iaea.org/publications/4716/defence-in-depth-in-nuclear-safety>.

INTERNATIONAL ATOMIC ENERGY AGENCY. *Basic Safety Principles for Nuclear Power Plants 75-INSAG-3 Rev. 1*. Vienna: INTERNATIONAL ATOMIC ENERGY AGENCY, 1999. (INSAG Series, 12). ISBN 92-0-102699-4. Disponível em: <https://www.iaea.org/publications/5811/basic-safety-principles-for-nuclear-power-plants-75-insag-3-rev-1>.

INTERNATIONAL ATOMIC ENERGY AGENCY. *Fundamental Safety Principles*. Vienna: INTERNATIONAL ATOMIC ENERGY AGENCY, 2006. (Safety Fundamentals, SF-1). ISBN 92-0-110706-4. Disponível em: <https://www.iaea.org/publications/7592/fundamental-safety-principles>.

INTERNATIONAL ATOMIC ENERGY AGENCY. *Protecting Against Common Cause Failures in Digital IC Systems of Nuclear Power Plants*. Vienna: INTERNATIONAL ATOMIC ENERGY AGENCY, 2009. (Nuclear Energy Series, NP-T-1.5). ISBN 978-92-0-106309-0. Disponível em: <https://www.iaea.org/publications/8151/protecting-against-common-cause-failures-in-digital-ic-systems-of-nuclear-power-plants>.

INTERNATIONAL ATOMIC ENERGY AGENCY. *Core Knowledge on Instrumentation and Control Systems in Nuclear Power Plants*. Vienna: INTERNATIONAL ATOMIC ENERGY AGENCY, 2011. (Nuclear Energy Series, NP-T-3.12). ISBN 978-92-0-113710-4. Disponível em: <https://www.iaea.org/publications/8490/core-knowledge-on-instrumentation-and-control-systems-in-nuclear-power-plants>.

INTERNATIONAL ATOMIC ENERGY AGENCY. *Safety of Nuclear Power Plants: Design*. Vienna: INTERNATIONAL ATOMIC ENERGY AGENCY, 2012. (Specific Safety Requirements, SSR-2/1). ISBN 978-92-0-121510-9. Disponível em: <https://www.iaea.org/publications/8771/safety-of-nuclear-power-plants-design>.

INTERNATIONAL ATOMIC ENERGY AGENCY. *Safety Classification of Structures, Systems and Components in Nuclear Power Plants*. Vienna: INTERNATIONAL ATOMIC ENERGY AGENCY, 2014. (Specific Safety Guides, SSG-30). ISBN 978-92-0-115413-2. Disponível em: <https://www.iaea.org/publications/10555/safety-classification-of-structures-systems-and-components-in-nuclear-power-plants>.

INTERNATIONAL ATOMIC ENERGY AGENCY. *Application of Field Programmable Gate Arrays in Instrumentation and Control Systems of Nuclear Power Plants*. Vienna: INTERNATIONAL ATOMIC ENERGY AGENCY, 2016. (Nuclear Energy Series, NP-T-3.17). ISBN 978-92-0-103515-8.

INTERNATIONAL ATOMIC ENERGY AGENCY. *Design of Instrumentation and Control Systems for Nuclear Power Plants*. Vienna: INTERNATIONAL ATOMIC ENERGY AGENCY, 2016. (Specific Safety Guides, SSG-39). ISBN 978-92-0-102815-0. Disponível em: <https://www.iaea.org/publications/10838/design-of-instrumentation-and-control-systems-for-nuclear-power-plants>.

INTERNATIONAL ATOMIC ENERGY AGENCY. *Approaches for Overall Instrumentation and Control Architectures of Nuclear Power Plants*. Vienna: INTERNATIONAL ATOMIC ENERGY AGENCY, 2018. (Nuclear Energy Series, NP-T-2.11). ISBN 978-92-0-102718-4. Disponível em: <https://www.iaea.org/publications/12292/approaches-for-overall-instrumentation-and-control-architectures-of-nuclear-power-plants>.

INTERNATIONAL ATOMIC ENERGY AGENCY. *Criteria for Diverse Actuation Systems for Nuclear Power Plants*. Vienna: INTERNATIONAL ATOMIC ENERGY AGENCY, 2018. (TECDOC Series, 1848). ISBN 978-92-0-103518-9. Disponível em: <https://www.iaea.org/publications/12367/criteria-for-diverse-actuation-systems-for-nuclear-power-plants>.

INTERNATIONAL ATOMIC ENERGY AGENCY. *IAEA Safety Glossary: 2018 Edition*. Vienna: INTERNATIONAL ATOMIC ENERGY AGENCY, 2019. (Non-serial Publications). ISBN 978-92-0-104718-2. Disponível em: <https://www.iaea.org/publications/11098/iaea-safety-glossary-2018-edition>.

INTERNATIONAL ELECTROTECHNICAL COMMISSION. *IEC 62566 - Nuclear power plants - Instrumentation and control systems important to safety - Development of HDL-programmed integrated circuits*. [S.l.], 2020.

KEPCO&KHN. *Technical Report - Advanced Power Reactor 1400 (APR1400)*. Korea Electric Power Corporation & Korea Hydro & Nuclear Power Co., Ltd, 2018.

LONG term structure of the IAEA safety standards and current status 2021. INTERNATIONAL ATOMIC ENERGY AGENCY, 2021. Disponível em: <http://www-ns.iaea.org/committees/fileS/CSS/205/status.pdf>.

MITSUBISHI HEAVY INDUSTRIES. *Defence-in-Depth and Diversity, MUAP-07006-NP-A*. Tokyo: MITSUBISHI HEAVY INDUSTRIES, Ltd, 2009. Disponível em: <https://www.nrc.gov/docs/ML0928/ML092820330.pdf>.

MITSUBISHI HEAVY INDUSTRIES. *Defence-in-Depth and Diversity Coping Analysis, MUAP-07014-NP*. Tokyo: MITSUBISHI HEAVY INDUSTRIES, Ltd, 2011. Disponível em: <https://www.nrc.gov/docs/ML1122/ML11229A124.pdf>.

MITSUBISHI HEAVY INDUSTRIES. *US-APWR Design Control Document (DCD)*. Tokyo: MITSUBISHI HEAVY INDUSTRIES, Ltd, 2013. Disponível em: <https://www.nrc.gov/reactors/new-reactors/large-lwr/design-cert/apwr/dcd.html#dcd>.

NASER, J. *Guidelines on the Use of Field Programmable Gate Arrays in Nuclear Power Plant I&C Systems*. [S.l.], 2009.

NGUYEN, T. *Protecting Against Digital Common-Cause Failure: Combining Defensive Measures andDiversity Attributes*. EPRI - Electric Power Research Institute, 2010.

PRECKSHOT, G. G. *NUREG–6303, "Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems"*. [S.l.]: Division of Reactor Controls and Human Factors, Office of Nuclear Reactor Regulation, U.S. Nuclear Regulatory Commission (NRC), 1994.

US NUCLEAR REGULATORY COMMISSION. *NUREG-0800, "Standard Review Plan for the Review of Safety Analysis Reports for NuclearPower Plants, LWR Edition."*. U.S. Nuclear Regulatory Commission (NRC), 2007. Disponível em: <https://www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr0800/index.html>.

US NUCLEAR REGULATORY COMMISSION. *Appendix A to Part 50—General Design Criteria for Nuclear Power Plants*. 2021. Disponível em: <https://www.nrc.gov/reading-rm/doc-collections/cfr/part050/part050-appa.html>.

WANG, Z.-Y. et al. The implementation of diverse actuation system in ACPR1000 nuclear power plants. *Science and Technology of Nuclear Installations*, v. 2021, 2021.

WOOD, R. et al. *NUREG-7007, "Diversity Strategies for Nuclear Power Plant Instrumentation and Control Systems"*. [S.l.]: Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission (NRC), 2010.

WORLD NUCLEAR ASSOCIATION. *Defence-in-Depth and Diversity: Challenges Related to IeC Architecture*. World Nuclear Association, 2018.

WORLD NUCLEAR ASSOCIATION. *Safety Classification for I&C Systems inNuclear Power Plants – Current Status and Difficulties*. World Nuclear Association, 2020. Disponível em: <https://world-nuclear.org/our-association/publications/online-reports/cordel-safety-classification-for-i-c-systems-in-nu.aspx>.