UNIVERSIDADE DE SÃO PAULO
ESCOLA DE ENGENHARIA DE SÃO CARLOS

LUIZ FERREIRA ALVES

**Laboratório remoto para controle e supervisão de processos industriais em
planta didática multitarefa**

São Carlos
2018

LUIZ FERREIRA ALVES

**Laboratório remoto para controle e supervisão de processos industriais em
planta didática multitarefa**

Versão Original

Dissertação apresentada para obtenção do título de mestre em
Ciências, Programa de Engenharia Elétrica, Área de
Concentração: Sistemas Dinâmicos.

Orientador: Prof. Dr. Dennis Brandão

São Carlos

2018

Trata-se da versão original.

AUTORIZO A REPRODUÇÃO TOTAL OU PARCIAL DESTE TRABALHO,
POR QUALQUER MEIO CONVENCIONAL OU ELETRÔNICO, PARA FINS
DE ESTUDO E PESQUISA, DESDE QUE CITADA A FONTE.

Ficha catalográfica elaborada pela Biblioteca Prof. Dr. Sérgio Rodrigues Fontes da
EESC/USP com os dados inseridos pelo(a) autor(a).

F9521 Ferreira Alves, Luiz
Laboratório remoto para controle e supervisão de
processos industriais em planta didática multitarefa /
Luiz Ferreira Alves; orientador Dennis Brandão. São
Carlos, 2018.

Dissertação (Mestrado) - Programa de Pós-Graduação
em Engenharia Elétrica e Área de Concentração em
Sistemas Dinâmicos -- Escola de Engenharia de São
Carlos da Universidade de São Paulo, 2018.

1. Laboratório remoto. 2. Protocolo de acesso
remoto. 3. Controle e supervisão de processos
industriais. 4. Experimentos à distância. 5. Educação
na engenharia. I. Título.

FOLHA DE JULGAMENTO

Candidato: Engenheiro **LUIZ FERREIRA ALVES**.

Título da dissertação: "Remoto para controle e supervisão de processos industriais em planta didática multitarefa".

Data da defesa: 04/12/2018.

Comissão Julgadora:

Resultado:

Prof. Associado **Dennis Brandão**
(Orientador)
(Escola de Engenharia de São Carlos/EESC)

Aprovado

Prof. Associado **Júlio Cezar Estrella**
(Instituto de Ciências Matemáticas e de Computação/ICMC)

Aprovado

Prof. Dr. **André Carmona Hernandes**
(Universidade Federal de São Carlos/UFSCar)

Aprovado

Decano do Coordenador do Programa de Pós-Graduação em
Engenharia Elétrica:
Prof. Associado **Luís Fernando Costa Alberto**

Presidente da Comissão de Pós-Graduação:
Prof. Associado **Luís Fernando Costa Alberto**

Dedico este trabalho à minha família e aos meus amigos, pelo apoio incondicional durante esta caminhada, e aos meus professores, que sempre agregaram conhecimento técnico ou pessoal.

AGRADECIMENTOS

Aos meus pais, Valéria e Siderval, minha irmã, Beatriz, minha avó, Generosa, e aos familiares pela compreensão e carinho durante a jornada do Mestrado.

Aos meus amigos em Marília, São Carlos e São Paulo pelos momentos de descontração e memórias construídas ao longo dos anos como aluno da Escola de Engenharia de São Carlos.

Aos companheiros do Laboratório de Automação Industrial, Marcelo, Fabrício, Murilo e Guilherme, pelo apoio e trabalho em conjunto.

Ao Professor Dennis, pela orientação e parceria durante o Mestrado, e ao Departamento de Engenharia Elétrica e de Computação, pela oportunidade de contribuir para o crescimento da Universidade.

À Universidade de São Paulo, pelo investimento e infraestrutura que permitiram o desenvolvimento deste trabalho.

Finalmente, à Coordenação de Aperfeiçoamento de Pessoal de Nível Superior, pelo suporte financeiro.

RESUMO

ALVES, Luiz Ferreira. **Laboratório remoto para controle e supervisão de processos industriais em planta didática multitarefa**. 2018. 96 f. Dissertação (Mestrado em Sistemas Dinâmicos) – Universidade de São Paulo, São Carlos, 2018.

Esta dissertação aborda o desenvolvimento e a implementação de um laboratório remoto para a disciplina “SEL0431 - Laboratório de Controle de Processos Industriais”, a qual visa proporcionar aos alunos o contato direto com sistemas de controle e supervisão de processos industriais através de projetos desenvolvidos em uma planta didática industrial. O laboratório foi implementado em 2017 e é constituído por uma planta de escala reduzida, que contém instrumentos de campo, controladores lógicos programáveis, redes de comunicação digitais e um servidor, que conecta a rede local do laboratório à rede da Universidade. Os estudantes acessam este servidor através de aplicações de protocolo remoto RDP sobre VPN com portais online e ferramentas adicionais de suporte para que realizem seus experimentos à distância com a planta. Além de atuar como gateway entre a planta e as máquinas dos alunos, o servidor autentica seus usuários, gerencia acessos simultâneos e permite que os alunos visualizem e obtenham os dados da planta mais facilmente. Ao final de cada projeto, o autor deste trabalho conduziu um questionário para registrar a impressão dos estudantes sobre o uso do laboratório remoto e comparou os resultados apresentados pelos alunos da turma de 2016 e os da turma de 2017 desta disciplina. Esta análise indicou que a adição de um laboratório remoto apresentou um impacto positivo no desempenho acadêmico dos estudantes nesta disciplina: eles atingiram resultados mais completos, exploraram mais a fundo os recursos da planta e avaliaram positivamente o uso da ferramenta. Ademais, esta solução técnica adotada para desenvolver o laboratório remoto é replicável a outras disciplinas e possui a vantagem de permitir o controle total da planta pelos alunos sem abdicar da segurança durante os experimentos.

Palavras-chave: Laboratório remoto. Protocolo de acesso remoto. Controle e supervisão de processos industriais. Experimentos à distância. Educação na Engenharia.

ABSTRACT

ALVES, Luiz Ferreira. **Remote laboratory for control and supervision of industrial processes in multitask didactic plant.** 2018. 96 f. Thesis (Master Degree in Dynamic Systems Area) – University of São Paulo, São Carlos, 2018.

This thesis addresses the development and implementation of a remote laboratory for the discipline “SEL0431 – Industrial Processes Control Laboratory”, which aims to provide students with direct contact with control and supervision systems of industrial processes through projects developed in a didactic plant. The laboratory was first implemented in 2017 and consists of a reduced scale plant, which contains field instruments, programmable logic controllers, digital communication networks and a server that connects the laboratory’s local network to the University Wide Area Network (WAN). Students access the server through RDP applications over VPN and they are supported by online portals and additional tools to perform their remote experiments with the plant. In addition to serving as a gateway between the plant and the students’ machines, the server authenticates its users, manages simultaneous access and enables students to view and obtain plant data more easily. At the end of each project, the author of this paper conducted a survey to record the students’ impression of the use of the remote laboratory and compared the results presented by the students of 2016 classes and those of 2017 classes of this discipline. The analysis revealed the remote laboratory positively impacted on the academic performance of students in this discipline: they achieved more complete results, explored more deeply the plant resources and positively evaluated the use of such tool as a support for teaching industrial processes control and supervision. Furthermore, the technical solution is replicable to other practical courses and presents the advantage of enabling students to totally control the plant without forgoing the security during their experiments.

Keywords: Remote laboratory. Remote access protocol. Industrial processes control and supervision. Distance experiments. Engineering education.

LISTA DE ILUSTRAÇÕES

Figura 1 – Quantidade de equipamentos com conexão à Internet, em milhares, de 2004 a 2018.	16
Figura 2 - Equipamentos acessados por dispositivos mobile através de gateways 4G-LTE.....	26
Figura 3 – Conexão entre máquinas de redes diferentes através de uma VPN.....	29
Figura 4 – Interface web para controle de posição de uma plataforma.	33
Figura 5 – Exemplo de redes locais acessadas de acordo com as boas práticas de segurança.....	38
Figura 6 – Equipamentos de campo conectados por uma rede DeviceNet.....	40
Figura 7 – WebLab Deusto: exemplo de sistema de gerenciamento de laboratórios remotos.	43
Figura 8 – Cronograma com a metodologia do desenvolvimento do laboratório remoto.	46
Figura 9 – Planta didática multitarefa.	52
Figura 10 – Da esquerda à direita, o instrumento de medição de nível por diferencial de pressão, o sensor ultrassônico e o Coupler DP/PA da Siemens.....	54
Figura 11 – Bomba d'água centrífuga do fabricante Ferrari, à esquerda, e inversor de frequência CFW-08, à direita.....	54
Figura 12 – Interface do aplicativo Cisco AnyConnect para Windows.	58
Figura 13 – Aplicativo e extensão web do protocolo RDP.....	59
Figura 14 – Arquitetura de implementação do laboratório remoto.....	62
Figura 15 – Diferentes ângulos da planta vistos pela webcam.....	62
Figura 16 – Dashboard online para supervisão das variáveis do CLP de controle de temperatura.....	63
Figura 17 – Ambiente Moodle com instruções sobre a disciplina e os equipamentos....	64
Figura 18 – Desktop do servidor virtualizado em uma máquina com Windows 10.....	65
Figura 19 – Comparação do desempenho dos grupos quanto à entrega das tarefas nos projetos em 2016 e 2017.....	70
Figura 20 – Desempenho dos grupos em cada um dos projetos em 2016 e 2017	71

Figura 21 – Quantidade de acessos remotos à planta por semana.	73
Figura 22 – Tempo médio de conclusão das práticas em 2016 e 2017.	75

LISTA DE TABELAS

Tabela 1 – Principais aspectos das tecnologias de acesso remoto.	28
Tabela 2 – Aplicações para acesso remoto a desktop.	31
Tabela 3 – Algumas soluções para acesso remoto de equipamentos industriais.	35
Tabela 4 – Sequência de projetos para cada grupo.	48
Tabela 5 – Variáveis da malha de controle de temperatura.	53
Tabela 6 – Variáveis da malha de controle de nível.	55
Tabela 7 – Variáveis da malha de controle de vazão.	55
Tabela 8 – Valores médios dos tempos mínimo, máximo e médio, em milissegundos, da conexão com o servidor por uma rede privada de 10MB.	60
Tabela 9 – Resumo das medidas de segurança implementadas no laboratório remoto.	66
Tabela 10 – Etapas de cada projeto, segundo os critérios adotados neste trabalho.	67
Tabela 11 – Questionário de avaliação do uso do laboratório remoto com o resumo das respostas.	76
Tabela 12 – Lista de acessos, com duração, a cada usuário padrão.	95

LISTA DE ABREVIATURAS E SIGLAS

AC	Alternating Current
AES	Advanced Encryption Standard
AVA	Ambiente Virtual de Aprendizagem
CLP	Controlador Lógico Programável
CPU	Central Processing Unit
CSS	Cascading Style Sheets
DoS	Denial of Service
HTML	Hyper Text Markup Language
HTTPS	Hyper Text Transfer Protocol Secure
IIoT	Industrial Internet of Things
IoT	Internet of Things
IP	Internet Protocol
L2TP	Layer To Tunneling Protocol
LaaS	Laboratory as a Service
LAN	Local Area Network
LED	Light Emitting Diode
PBL	Project-Based Learning
PID	Proporcional Integral Derivativo
PPTP	Peer-to-Peer Tunneling Protocol
PWM	Pulse Width Modulation
RDP	Remote Desktop Protocol
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TIC	Tecnologias de Informação e Comunicação
TLS	Transport Layer Security
VDI	Virtual Desktop Infrastructure
VNC	Virtual Network Computing
VPN	Virtual Private Network
WAN	Wide Area Network

SUMÁRIO

1	INTRODUÇÃO	15
1.1	OBJETIVO GERAL.....	18
1.2	OBJETIVOS ESPECÍFICOS E JUSTIFICATIVA DESTA DISSERTAÇÃO.....	18
1.3	ORGANIZAÇÃO DO TRABALHO.....	19
1.4	ARTIGOS RELACIONADOS A ESTA DISSERTAÇÃO.....	21
2	REVISÃO BIBLIOGRÁFICA	22
2.1	TÉCNICAS DE ACESSO REMOTO A EQUIPAMENTOS INDUSTRIAIS	22
2.1.1	Redes Privadas Virtuais.....	28
2.1.2	Protocolos de acesso remoto a desktop.....	30
2.1.3	Portais de aplicação.....	32
2.1.4	Segurança em acesso remoto de equipamentos.....	35
2.2	CONTROLE E SUPERVISÃO DE PROCESSOS INDUSTRIAIS	38
2.3	LABORATÓRIOS REMOTOS PARA ENGENHARIA	41
2.4	METODOLOGIA PBL PARA DISCIPLINAS PRÁTICAS	44
3	DESCRIÇÃO DOS MÉTODOS E FERRAMENTAS.....	46
3.1	CONTEXTO DO TRABALHO	46
3.2	A DISCIPLINA DE LABORATÓRIO DE CONTROLE DE PROCESSOS INDUSTRIAIS.....	48
3.2.1	Organização da disciplina	48
3.2.2	Planta didática multitarefa	51
3.3	DESENVOLVIMENTO DO LABORATÓRIO REMOTO	56
3.3.1	Requisitos de projeto e implementação do laboratório remoto	57
3.3.2	Arquitetura do laboratório remoto	61
3.3.3	Ferramentas adicionais.....	61
3.3.4	Segurança a nível físico e de aplicação	65
3.4	MÉTODO PARA AVALIAÇÃO DO DESEMPENHO TÉCNICO DOS ALUNOS.....	66
3.5	MÉTODO PARA AVALIAÇÃO DO USO DO LABORATÓRIO REMOTO	68
4	RESULTADOS E DISCUSSÕES	69
4.1	EFEITOS DA IMPLEMENTAÇÃO DO LABORATÓRIO REMOTO.....	69
4.1.1	Comparação do desempenho acadêmico dos estudantes	69

4.1.2	Quantidade de acessos realizados durante o semestre	73
4.1.3	Comparação dos tempos de conclusão dos projetos.....	74
4.2	RESULTADOS DA AVALIAÇÃO DOS ALUNOS SOBRE O LABORATÓRIO REMOTO.....	75
5	CONCLUSÕES	79
5.1	SUGESTÕES DE TRABALHOS FUTUROS	80
	REFERÊNCIAS BIBLIOGRÁFICAS	82
	APÊNDICE A – SCRIPT PARA GERENCIAMENTO DE ACESSOS REMOTOS AO SERVIDOR.....	86
	APÊNDICE B – LISTA DE ACESSOS AO SERVIDOR.....	95

1 INTRODUÇÃO

Os diversos campos da Engenharia necessitam cada vez mais de profissionais com habilidades técnicas e interpessoais, capazes de enfrentar situações e problemas reais no cotidiano, trabalhar em grupo e gerir equipes no ambiente de trabalho. Segundo Efstratia (2014, p.1256), para satisfazer a demanda por engenheiros com tais competências, a maioria dos cursos de Engenharia adotam em suas grades curriculares disciplinas que envolvem práticas experimentais, individuais ou em grupo, com dispositivos reais.

No contexto deste trabalho, a disciplina SEL0431- Laboratório de Controle de Processos Industriais tem como objetivo proporcionar a alunos de graduação em Engenharia Elétrica da Escola de Engenharia de São Carlos (EESC) o contato direto com equipamentos de campo, como sensores e Controladores Lógicos Programáveis (CLPs), malhas de controle, redes de comunicação digital e sistemas de supervisão através de projetos feitos em grupo em uma planta industrial de escala reduzida (ALVES; BRANDÃO; OLIVEIRA, 2018).

Durante a execução desses projetos, os alunos lidam com situações reais no cotidiano de um profissional que trabalha com controle de processos em ambiente industrial: configuração de dispositivos de campo, desenvolvimento de aplicações em software industrial, paradas de emergência e falhas em equipamentos são alguns exemplos (ALVES; BRANDÃO; OLIVEIRA, 2018). Portanto, os alunos adquirem conhecimento através da experiência própria com situações e problemas reais e complementam o aprendizado do conteúdo teórico ministrado em sala de aula.

Esta abordagem onde os discentes aprendem através da experimentação em projetos com objetivos específicos é denominada Aprendizagem Baseada em Projetos, ou Project Based Learning (PBL), e é uma das abordagens mais utilizadas em disciplinas práticas desenvolvidas em laboratório (FERNANDES, 2016). Contudo, a implementação de cursos práticos baseados em laboratórios tradicionais nas grades curriculares de Engenharia apresenta algumas restrições (CHEVALIER et al., 2017):

- a) Custo de equipamentos e licenças de software para construir laboratórios;

- b) Capacidade limitada dos laboratórios frente ao crescimento do número de alunos e de disciplinas experimentais nas turmas de Engenharia;
- c) Restrição de tempo e local para realizar as práticas;
- d) Restrição de recursos humanos, em alguns cursos, para atender aos alunos em cursos experimentais.

Em contrapartida, os avanços nas tecnologias de informação e comunicação e o acesso crescente à Internet e dispositivos eletrônicos, como computadores e smartphones, motivam as Universidades a investirem na modalidade de educação à distância. A Figura 1 mostra o crescimento da quantidade de equipamentos com conexão à rede mundial de computadores de 2004 até agora.

Figura 1 – Quantidade de equipamentos com conexão à Internet, em milhares, de 2004 a 2018.

Fonte: Buyya e Dastjerdi (2016).

De acordo com Caminero et al. (2016, p.134), devido também ao crescente acesso à Internet, cursos on-line sob demanda, laboratórios virtuais e laboratórios remotos são alguns exemplos de aplicações de ensino à distância que vêm se popularizando e ajudando instituições de ensino a superar restrições de tempo, orçamento e espaço quando planejam suas grades curriculares.

Este trabalho destaca os laboratórios remotos, os quais são laboratórios constituídos de equipamentos reais com os quais os alunos interagem à distância. Há

cursos cujos laboratórios tradicionais de Engenharia não possuem equipamentos que atendam a toda a classe, o que torna as práticas limitadas a turmas menores ou meramente demonstrativas. Uma das ideias centrais dos laboratórios remotos é permitir com que os alunos interajam com sistemas físicos, como em laboratórios tradicionais, porém sem se restringir ao horário e local da aula ou à quantidade de equipamentos disponíveis por pessoa ou grupo (FERRATER-SIMON, 2009). O processo de aprendizagem por meio da experimentação ocorre da mesma maneira como em um laboratório presencial que adota a metodologia PBL.

Outro fator importante na difusão dos laboratórios remotos está relacionado à Quarta Revolução Industrial, ou Indústria 4.0. A integração das TIC às tecnologias no campo da automação permite com que sensores, máquinas e fábricas inteiras se comuniquem, processem informações e tomem decisões de forma autônoma e descentralizada. Portanto, conforme Encalada e Sequera (2017, p. 117), os profissionais do futuro deverão estar preparados para lidar com fábricas inteligentes, e conceitos como Internet das Coisas Industrial (IIoT), virtualização de sistemas físicos e acesso remoto a equipamentos industriais, estarão cada vez mais presentes no currículo dos futuros engenheiros.

Esta modalidade de laboratório operado e monitorado remotamente é uma introdução às indústrias do futuro, onde os profissionais identificarão problemas, coletarão dados e tomarão decisões de unidades fabris inteiras via qualquer dispositivo com acesso à Internet.

Há uma gama extensa de trabalhos e exemplos de aplicação de laboratórios e experimentos remotos em cursos superiores; grande parte deles estão relacionados às áreas de engenharia, com destaque para cursos de eletrônica (LUTHON; LARROQUE, 2015, MENDES et al, 2016), sistemas embarcados (FERNANDES, 2016; ANGULO; RODRIGUEZ-GIL; GARCIA-ZUBIA, 2018), computação (IANNUCCI et al., 2018; KIST et al., 2014), automação (IONESCU et al., 2013, JAGADEESH; SIDDARAJU; RANGANATHA, 2018) e robótica (JIMENEZ; SANCHEZ; MAULEDOUX, 2018, SHYR; SU; LIN, 2013). Contudo, a ampla quantidade de hardware e software disponíveis permite criar soluções e arquiteturas diferentes para laboratórios remotos. Ademais, a quantidade de trabalhos diferentes relacionados a laboratórios remotos para controle e automação

de processos industriais que surge todo ano mostra que esse tema pode ser melhor explorado por instituições de ensino superior.

Neste caso, é desenvolvido e implementado um laboratório remoto para a disciplina SEL0431 que permite com que os alunos desenvolvam projetos com malhas de controle e sistemas supervisórios envolvendo hardware industrial. Os alunos são responsáveis por todas as etapas de cada projeto: desde mapear as entradas e saídas de cada CLP e configurar os softwares para programá-los a desenvolver aplicações que controlem e supervisionem processos industriais à distância.

Este estudo apresenta uma solução para a operação e monitoramento remotos de um equipamento industrial de escala reduzida, compara a arquitetura da solução com outras soluções existentes na área de controle de processos industriais e discute quais os efeitos que a adição de um laboratório remoto trouxe para o ensino de temas de controle e automação nesta disciplina ao comparar o desempenho dos alunos matriculados em 2016 e 2017, ano da implementação da ferramenta. Além das contribuições a nível técnico e pedagógico, este trabalho discute quais os ajustes necessários no laboratório remoto para melhorar a experiência dos alunos envolvidos na disciplina e adotá-la em outros cursos na área de controle e automação industrial.

1.1 OBJETIVO GERAL

O objetivo principal deste trabalho é desenvolver e implementar um laboratório remoto para que os alunos envolvidos na disciplina SEL0431 realizem experimentos à distância com equipamentos e software industriais e aprendam na prática diversos conceitos teóricos na área de controle e automação de processos, como instrumentação e sensoriamento, controladores industriais, sistemas de aquisição de dados e redes de comunicação digital.

1.2 OBJETIVOS ESPECÍFICOS E JUSTIFICATIVA DESTA DISSERTAÇÃO

Os objetivos específicos deste trabalho incluem:

- a) Estudar e comparar soluções já existentes de laboratórios físicos acessados remotamente para implementar uma solução para a disciplina SEL0431 que seja replicável a outras disciplinas;
- b) Definir a arquitetura e os materiais utilizados para criar a solução, de tal forma a gerenciar múltiplos acessos simultâneos ao equipamento físico, tornar a planta didática disponível para experimentação didática de qualquer lugar, a qualquer momento dentro do horário permitido pelo laboratório, de forma segura e com latência aceitável na comunicação entre as máquinas dos alunos e a planta;
- c) Analisar do ponto de vista dos tutores da disciplina quais os efeitos no processo de aprendizagem dos alunos quando eles se engajam com a ferramenta de acesso remoto, em comparação com o laboratório tradicional;
- d) Analisar do ponto de vista dos alunos da disciplina quais os pontos de melhoria e vantagens que a ferramenta de acesso remoto trouxe.

A contribuição científica deste trabalho é apresentar uma ferramenta baseada em hardware acessível e software gratuito que permite com que os alunos aprendam conceitos de controle de processos industriais a partir de experimentos remotos com uma planta industrial de escala reduzida.

A partir da experiência dos alunos com este laboratório remoto e da comparação com outros laboratórios remotos, este trabalho discute a viabilidade de utilizá-lo em turmas de engenharia de outras universidades e replicar esta solução para outras disciplinas práticas de engenharia.

1.3 ORGANIZAÇÃO DO TRABALHO

O primeiro capítulo deste trabalho descreve o contexto do uso de laboratórios remotos em disciplinas práticas, quais os objetivos principais e específicos deste trabalho e quais os trabalhos acadêmicos gerados durante o período do mestrado.

O capítulo 2 aborda a revisão bibliográfica sobre os temas relacionados a laboratórios remotos focados em disciplinas de controle e automação, fornecendo a base teórica para que este trabalho fosse desenvolvido. O subcapítulo 2.1 trata das técnicas de acesso remoto de equipamentos industriais, enquanto o subcapítulo 2.2 apresenta o

hardware e software mais comumente utilizados para controle de processos em ambientes industriais. O subcapítulo 2.3 demonstra como as técnicas expostas em 2.1 são aplicadas a equipamentos mostrados no subcapítulo 2.2 para produzir laboratórios controlados remotamente. Este subcapítulo não trata somente do aspecto técnico da implementação dos laboratórios, mas também do efeito sobre o aprendizado dos alunos. O subcapítulo 2.4 explica qual a abordagem pedagógica utilizada na disciplina SEL0431 e por que ela foi adotada neste caso.

O terceiro capítulo, então, demonstra quais foram as ferramentas utilizadas para criar a ferramenta de acesso remoto, a arquitetura escolhida para este laboratório e como a disciplina foi planejada. O subcapítulo 3.1 expõe o contexto que motivou o desenvolvimento deste trabalho, o subcapítulo 3.2 detalha a disciplina SEL0431 e a planta didática que é utilizada neste curso, o subcapítulo 3.3 explica como o laboratório remoto foi implementado e quais foram os materiais utilizados e os subcapítulos 3.4 e 3.5 demonstram como os tutores da disciplina avaliaram os alunos matriculados na disciplina e como os alunos avaliaram suas experiências com o laboratório remoto, respectivamente.

O quarto capítulo mostra os resultados obtidos com o uso do laboratório: o subcapítulo 4.1 compara os desempenhos dos alunos quando eles cursaram a disciplina SEL0431 de forma exclusivamente presencial e quando eles foram suportados pelo laboratório remoto, enquanto o subcapítulo 4.2 mostra a avaliação do laboratório do ponto de vista dos alunos.

A partir dos resultados, o quinto capítulo discute as vantagens e desvantagens da abordagem escolhida para este laboratório remoto. Neste capítulo, tanto a abordagem pedagógica quanto a arquitetura da solução são avaliadas pelo autor do trabalho. Sugestões de mudanças para os próximos anos são discutidas no subcapítulo 5.1 e visam melhorar a experiência dos alunos envolvidos no laboratório remoto e tornar a solução escalável para outras disciplinas na área de controle e automação e para turmas de engenharia outras universidades.

1.4 ARTIGOS RELACIONADOS A ESTA DISSERTAÇÃO

Trabalhos aprovados em congressos:

ALVES, L. F.; BRANDÃO D.; TIETZ, F. Desenvolvimento de Laboratório Remoto para Suporte ao Ensino de Controle de Processos Industriais para Estudantes de Engenharia Elétrica. In: CONGRESSO INTERNACIONAL DE EDUCAÇÃO E TECNOLOGIAS, 4., Julho 2018, São Carlos. **Anais...** São Carlos: UFSCar, 2018.

TIETZ, F.; BRANDÃO D.; ALVES, L. F. Development of an Internet of Things Gateway Applied to a Multitask Industrial Plant. In: IEEE/IAS INTERNATIONAL CONFERENCE ON INDUSTRY APPLICATIONS, 13., Novembro 2018, São Paulo.

Trabalhos aprovados ou em processo de revisão em revistas:

ALVES, L. F.; BRANDÃO D.; OLIVEIRA, M. A. A Multi-Process Pilot Plant as a Didactic Tool for the Teaching of Industrial Processes Control in Electrical Engineering Course. **International Journal of Electrical Engineering Education**, Londres, v.55, n.3, 9 Jul. 2018. Disponível em: <<https://doi.org/10.1177/0020720918787455>>.

ALVES, L. F.; BRANDÃO D. A Remote Laboratory as a Support for an Industrial Processes Control Discipline. **IEEE Transactions on Education**, Columbus. (Em processo de revisão).

Capítulo de livro eletrônico:

ALVES, L. F.; BRANDÃO D.; TIETZ, F. Desenvolvimento de Laboratório Remoto para Suporte ao Ensino de Controle de Processos Industriais para Estudantes de Engenharia Elétrica. *Educação e Tecnologias: Experiências, Desafios e Perspectivas*, 1. ed., Atena Editora: São Paulo.

2 REVISÃO BIBLIOGRÁFICA

Neste capítulo, três eixos principais serão abordados: o primeiro, exposto no subcapítulo 2.1, demonstra e explica as principais técnicas utilizadas para controle e supervisão remotos de unidades industriais e quais são as práticas adotadas para tornar estas conexões mais seguras. Este subcapítulo fornece o embasamento técnico para escolher qual a solução implementada neste trabalho. Os equipamentos envolvidos na transmissão de dados e controle dentro das unidades industriais são apresentados no subcapítulo 2.2. Contudo, o ambiente industrial não foi o único beneficiado com o surgimento de novas tecnologias para controle e supervisão de processos.

Com o crescimento da modalidade de educação à distância, muitos conceitos apresentados em 2.1 e 2.2 foram adotados em instituições de ensino para a criação de laboratórios físicos manipulados remotamente. O subcapítulo 2.3 discute como são implementados alguns laboratórios remotos que serviram de base para este caso. Finalmente, o capítulo 2.4 discute qual a abordagem pedagógica utilizada em disciplinas práticas e por que ela foi adotada para este laboratório.

2.1 TÉCNICAS DE ACESSO REMOTO A EQUIPAMENTOS INDUSTRIAIS

A constante evolução das TIC permitiu que conceitos como computação em nuvem, virtualização de equipamentos físicos e protocolos machine-to-machine (M2M) ajudassem a ampliar a conexão entre pessoas e equipamentos físicos – estes podem, inclusive, trocar informações entre si e tomar decisões de forma autônoma, um paradigma denominado por Kevin Ashton de Internet das Coisas (BUYYA; DASTJERDI, 2016), que se estendeu ao ambiente industrial a toda a cadeia produtiva.

A integração das TIC às tecnologias de automação industrial possibilita que sensores, máquinas e máquinas fabris inteiras sejam monitoradas e controladas à distância, uma das características da atual revolução industrial. O acesso remoto a equipamentos industriais é definido por Souppaya e Scarfone (2016, p.8) como

“A capacidade de usuários e operadores de uma organização de acessar seus recursos físicos, dados e sistemas particulares que residem em uma

rede protegida fisicamente ou logicamente a partir de redes externas que devem ser consideradas de fora da organização”.

A possibilidade de trocar informações entre dispositivos, redes industriais e sistemas diferentes sem a necessidade de conexões físicas trouxe vantagens para diferentes áreas do conhecimento além da automação industrial: saúde, urbanismo, agroindústria e educação (BUYA; DASTJERDI, 2016), por exemplo:

- a) Aumento da produtividade e redução de custos ao integrar as redes dos sistemas de controle das unidades fabris, corporativas e externas;
- b) Agilidade na tomada de decisões e na manutenção de máquinas;
- c) Virtualização de sistemas físicos, permitindo o monitoramento e controle remotos de unidades inteiras;
- d) Reposta mais rápida às mudanças nos processos produtivos e às demandas de mercado;
- e) Interoperabilidade entre unidades que possuem dispositivos e protocolos de comunicação diferentes.

Essas vantagens motivam centros de pesquisa, instituições privadas e governamentais a investirem em assuntos relacionados ao controle e comunicação remotos com equipamentos físicos. Uma vasta gama de hardware, como sensores e atuadores inteligentes e gateways para Internet das coisas, software e protocolos de comunicação surgiram e continuam surgindo nesta década como resultado desses investimentos. Contudo, o acesso remoto a dados de redes internas traz alguns desafios para a implementação de laboratórios acessados remotamente (XU; JIANG; WANG, 2014).

Informações relevantes que antes eram restritas a redes internas e protegidas agora são transmitidas por redes externas, e garantir a confidencialidade desses dados é um dos maiores desafios no cenário industrial atual. Conforme Souppaya e Scarfone (2016, p.13), além do vazamento intencional ou não de dados confidenciais, outra ameaça à segurança da informação é a não integridade das informações, ou seja, dispositivos corrompidos nas redes internas ou ataques externos intencionais podem mudar os dados de processos em unidades industriais e acarretar acidentes e prejuízos incalculáveis. Técnicas modernas de acesso remoto empregam ferramentas e algoritmos

que visam proteger as informações que transitam para fora e para dentro das redes internas. Esse assunto é abordado no subcapítulo 2.1.5.

Assim como prevenir pessoas não-autorizadas a acessar ou corromper informações confidenciais, garantir que usuários autorizados tenham acesso aos dados que precisarem e quando precisarem é um requisito importante em projetos de implementação de acesso remoto a plantas industriais. Redes de telecomunicações são um dos principais meios pelos quais ocorre a conexão remota entre dispositivos físicos, e elas estão sujeitas a oscilações e interrupções na transmissão de dados (TANENBAUM; WHETERALL, 2011). Nesses casos, deve-se evitar a perda de informações de processos e impedir que a conexão esteja indisponível por tempo indeterminado.

Além dos desafios quanto a segurança da informação, grande parte das unidades fabris possuem equipamentos que não são compatíveis com os novos protocolos de comunicação e sequer possuem infraestrutura para conexão à rede de dados ou Internet. O custo de integração com as novas tecnologias de hardware e software industriais nesses casos pode ser elevado.

Apesar dos inúmeros métodos para controle e acesso remotos a equipamentos industriais, eles possuem características comuns (SOUPPAYA; SCARFONE, 2016; XU; JIANG; WANG, 2014):

- a) Devem garantir confidencialidade e integridade dos dados. Para tal, podem utilizar diversos métodos de autenticação, senha e criptografia combinados ou não, conforme está detalhado em 2.1.5;
- b) Os usuários autorizados podem armazenar informações em suas máquinas particulares, portanto, a organização pode e deve rastrear e limitar as informações transmitidas de dentro para fora da rede interna;
- c) Informações críticas devem sempre estar disponíveis aos requisitantes autorizados. Taxa de latência aceitável na comunicação entre o cliente e o servidor é um requisito fundamental quando há a necessidade de acompanhar em tempo real alguma operação ou extrair rapidamente alguma informação. É o caso dos laboratórios remotos.

Há maneiras distintas de acessar remotamente recursos físicos e em muitos casos mais de um método é aplicado na mesma solução para torná-la mais segura. Alguns autores classificam a técnica de acesso remoto de acordo com a tecnologia utilizada, a arquitetura da implementação ou a finalidade do acesso, contudo, com a crescente integração entre diferentes tecnologias de informação e comunicação, a separação em categorias se tornou mais difícil.

Este subcapítulo introduz as tecnologias mais utilizadas para conexão remota a equipamentos físicos em unidades fabris, enquanto os próximos subcapítulos detalham as tecnologias estudadas para desenvolver este trabalho.

Uma das técnicas mais antigas de conexão remota é o acesso via modem. As primeiras organizações a utilizarem esta tecnologia empregavam conexão discada na década de 1980, seja através de linhas de telecomunicação próprias ou de um provedor de serviços (TANENBAUM; WHTEREALL, 2011). Com a evolução das tecnologias de telecomunicação, a cobertura de serviço e a velocidade de transmissão de dados aumentaram substancialmente e unidades fabris que operam em áreas isoladas, por exemplo, transmitem e recebem dados por meio de modems 3G, 4G e, mais recentemente, 5G. Esse tipo de transmissão de dados, entretanto, são suscetíveis a ataques externos, como man-in-the-middle, na qual uma agente intercepta mensagens que trafegam entre dois dispositivos, roubando informações ou mesmo alterando-as.

Outras tecnologias wireless para comunicação remota de dados surgiram como alternativa aos dados móveis e ao Wireless LAN e são muito aplicados em projetos IoT e IIoT: LoRaWAN, 6LowPAN, Bluetooth Low Energy, ZigBee são alguns exemplos (BUYYYA; DASTJERDI, 2016). Estas tecnologias se popularizaram também devido ao baixo consumo de energia dos dispositivos que as implementam.

Tanto os modems baseados em linhas telefônicas quanto modems celulares para criar conexões WAN atuam como gateways conectando a rede local à rede externa. A Figura 2 mostra um exemplo de arquitetura de conexão remota onde o gateway é um modem 4G. Apesar de populares, as redes baseadas em protocolos wireless são suscetíveis a ataques externos e devem aplicar alguma camada de segurança, como criptografia de mensagens ou firewall (TANENBAUM; WHETERALL, 2011; MORIMOTO, 2011).

Figura 2 - Equipamentos acessados por dispositivos mobile através de gateways 4G-LTE.

Fonte: Anyi e Jingjing (2018).

Segurança é um dos fatores que tornam o tunelamento uma das técnicas mais adotadas para acesso remoto de máquinas e unidades industriais. Essa técnica consiste em encapsular um protocolo dentro de outro para que os dados sejam transmitidos de uma rede a outra. Este método permite com que dados de uma rede privada sejam transmitidos por uma rede pública, como a Internet, de forma transparente (TANENBAUM; WHETERALL, 2011). As redes privadas virtuais (Virtual Private Networks, ou VPN) são o principal exemplo de técnica que utiliza tunelamento para transportar dados encriptados por uma rede pública, e esta camada de segurança é essencial para manter a integridade e confidencialidade das mensagens transportadas (XU; JIANG; WANG, 2014; SOUPPAYA; SCARFONE, 2014).

A VPN estabelece conexões seguras entre dispositivos de redes diferentes que geralmente usam a Internet como meio de comunicação. Em alguns casos, esta técnica tem a função de apenas estabelecer a comunicação entre um cliente em uma rede e uma máquina em outra rede local, mas é através de outra técnica que a troca de dados entre

estes agentes ocorre. Um dos métodos mais utilizados são os programas de acesso remoto a computadores.

Esta técnica permite com que o usuário controle remotamente e acesse os recursos da máquina à qual ele está conectado, portanto, é um método recomendado em casos onde é necessário algum tipo de manutenção, aquisição de dados ou operação remota (MORIMOTO, 2011). Há aplicações que utilizam diferentes protocolos e geralmente aplicam técnicas de segurança, como autenticação e criptografia de ponta a ponta, contudo, como essa técnica envolve transporte de dados encriptados para fora e para dentro da rede local, o que representa um risco à confidencialidade dos dados. Assim, algumas organizações que adotam esse tipo de solução proíbem o uso de acesso remoto direto a uma máquina da rede interna e implementam VPN, firewalls ou servidores internos para gerenciar as conexões a máquinas em suas redes locais (SOUPPAYA; SACRPHONE, 2014).

O risco de transmitir informações relevantes pela Internet é inerente a outro método de acesso remoto: os portais de aplicação. Eles consistem em servidores que oferecem acesso a uma aplicação ou serviço, na maioria das vezes, via web. Muitos ambientes de e-learning, com destaque para laboratórios remotos e virtuais, são implementados a partir de websites, os quais possuem a vantagem de ser altamente escaláveis (LOPES et al., 2017).

Algumas organizações mantêm servidores próprios para controle de acesso aos dados das aplicações. Contudo, esta solução é custosa e em casos de baixo risco algumas organizações optam por terceirizar o serviço de armazenamento dos seus dados (PANDEY, 2017; PORTNOY, 2012). Virtualização de servidores e aplicações em nuvem são exemplos de uso de portais de aplicação pelos quais os usuários acessam plataformas de monitoramento e controle online de unidades industriais, por exemplo. Amazon, Microsoft e IBM são alguns dos provedores mais populares de software, plataformas e infraestrutura como serviços para criação de portais de aplicação.

Assim como em VPN, os portais podem aplicar técnicas de segurança, como controle de acesso e autenticação. A Tabela 1 traz um resumo das categorias de tecnologias de acesso remoto.

Tabela 1 – Principais aspectos das tecnologias de acesso remoto.

Tipo de tecnologia	Exemplos	Vantagens	Desvantagens
Modem	DSL Cabeado 3G, 4G, 5G WiFi	*Alcance *Largura de banda *Custo	*Vulnerável a ataques
Tunelamento	VPN Microsoft Direct Access IPsec SSH SSL-VPN	*Segurança na transmissão dos dados *Custo	*Dificuldade em configurar conexões *Sessões limitadas por tempo
Protocolos e aplicações de acesso remoto a desktops	RDP VNC TeamViewer Chrome Remote Desktop	*Controle total do ambiente *Transferência de arquivos de/para máquina do cliente	*Pode representar um furo na camada de segurança *Sessões simultâneas prejudicam performance do servidor
Portais de aplicação	Portais web Desktops virtualizados na nuvem (VDI)	*Escalabilidade *Disponibilidade das aplicações	*Custo para manter datacenter próprio *Segurança em caso de opção por provedores

Fonte: Adaptado de National Institute of Standards and Technology (2018).

2.1.1 Redes Privadas Virtuais

Uma rede privada é constituída por máquinas que utilizam o espaço privado de IPs e seu acesso pode ser restrito pelas políticas de segurança da respectiva organização. Há casos onde as unidades de uma mesma corporação estão espalhadas geograficamente apesar de suas máquinas pertencerem à mesma rede privada, portanto, algumas empresas possuem linhas dedicadas para ligação entre essas unidades.

Apesar desta estratégia mitigar riscos de invasão de rede, o custo é elevado e o acesso remoto feito por membros autorizados que não estão conectados à rede privada é limitado. Uma solução é utilizar a Internet para a transmissão de dados entre máquinas

de fora da rede e máquinas pertencentes à rede, porém sem abdicar da segurança das redes privadas, através das redes privadas virtuais (SOUPPAYA; SACRFONE, 2014).

As VPN utilizam o processo de tunelamento, o qual garante que as mensagens trafeguem sobre a rede pública, mas se comportando como mensagens de uma rede privada. Elas são encriptadas, ou seja, ficam ilegíveis caso interceptadas, e somente as máquinas pertencentes à mesma VPN possuem a chave para decifrá-las (TANENBAUM; WHETERALL, 2011). A Figura 3 mostra a arquitetura da conexão de uma máquina em uma rede qualquer a uma rede local através de uma VPN.

Figura 3 – Conexão entre máquinas de redes diferentes através de uma VPN.

Fonte: technet.microsoft.com (2018).

Para acesso a equipamentos industriais, a máquina do usuário deve primeiramente se conectar à VPN. Essa conexão pode ser feita através de um aplicativo como, por exemplo, o Cisco AnyConnect Secure Mobility Client ou o ExpressVPN, pelo qual o usuário realiza sua autenticação para se conectar a uma rede privada, ou através de um navegador web.

No primeiro caso, o encapsulamento da mensagem é feito na camada de rede, pelo protocolo IPsec, e pode ser feito na camada de enlace, pelos protocolos L2TP ou PPTP. Além do encapsulamento, os pacotes são criptografados e as chaves para deciptação são distribuídas entre os dispositivos que farão a comunicação. Além da autenticação e da proteção das mensagens que trafegam pela rede pública, as organizações que adotam soluções baseadas em VPN configuram firewalls para filtrar

pacotes indesejados vindo da rede externa, gerenciar as chaves de criptografia e implementar o gateway para conexão com a rede privada (GEANEY; O'MAHONY, 2015).

No segundo caso, a rede utiliza o protocolo TLS para estabelecer uma conexão remota segura. Este método utiliza criptografia ponta-a-ponta para transmitir os pacotes pela rede pública e autenticação do usuário para que este possa acessar o gateway VPN. Este método é independente da plataforma da máquina do cliente e não requer configurações específicas de software nem do firewall, apenas um navegador. Apesar das vantagens em relação ao IPsec-VPN, o SSL-VPN apresenta alguns riscos à segurança. A conexão é estabelecida entre a máquina do cliente e o gateway, que está conectado à rede local, logo, o usuário pode injetar malware na rede da organização. Conforme Souppaya e Scarfone (2016, p. 18), outro risco à segurança da rede é o não término das sessões pelo usuário, ou seja, a conexão é encerrada pelo cliente, o que pode expor a rede interna a ataques caso ele esqueça de se desconectar da VPN.

O uso de redes privadas virtuais é uma das formas mais populares de conexão remota a equipamentos e unidades industriais e diversos fabricantes possuem soluções de hardware e software para implementar gateways VPN em grandes corporações. Ainda que estes produtos implementem medidas de segurança da informação, as equipes internas de TI das corporações podem acrescentar medidas extras, como configuração de firewalls e políticas de acesso a equipamentos na rede.

2.1.2 Protocolos de acesso remoto a desktop

Os protocolos e aplicações de acesso remoto a desktop permitem com que a máquina de um cliente tenha controle sobre a máquina servidora. O cliente pode manipular o servidor como se fosse sua máquina, portanto, ele acessa aplicações, dados e os recursos que forem necessários (MELKONYAN; AKOPYAN; CHEN, 2009). A imagem da máquina servidora é exportada para a máquina do cliente, e este trabalha remotamente no ambiente do servidor. Esta técnica de disponibilizar a tela de uma máquina física para que esta possa ser manipulada por outra máquina é denominada virtualização de desktop.

O principal uso desta tecnologia é manutenção e operação de máquinas que estejam na mesma rede interna, porém, é possível associar uma aplicação de conexão remota a desktop a uma VPN para permitir o acesso a máquinas de outras redes internas (SOUPPAYA; SCARFONE, 2014). Ao estabelecer a comunicação, o protocolo disponibiliza somente a tela da máquina e todo o processamento e alocação de memória é compartilhado pelo servidor. Portanto, múltiplos acessos a um mesmo servidor podem sobrecarregá-lo e prejudicar operações que necessitam de alto uso de CPU e memória.

Técnicas mais modernas alocam toda a CPU, memória e sistema operacional do desktop para serem acessadas na nuvem, assim cada cliente acessa uma instância de uma única máquina virtual (PANDEY et al. 2017). Esse conceito é denominado infraestrutura de desktop virtual, ou VDI, e será melhor detalhado no subcapítulo 2.1.3.

Utilizar uma aplicação de acesso remoto de desktop para conectar uma máquina em uma rede externa requer algumas configurações no firewall, como liberação de porta TCP e no servidor, como gerenciamento de listas de acesso (MORIMOTO, 2011). Este servidor pode ser a própria máquina que será controlada pelo cliente, ou uma máquina intermediária que, juntamente com o firewall, gerencia a conexão a outras máquinas da rede interna.

Após estabelecida a política de segurança e arquitetura da solução, a organização opta pela aplicação a ser utilizada. Cada aplicação disponibiliza recursos e utiliza protocolos de criptografia distintos. A Tabela 2 traz a comparação entre os aplicativos mais utilizados para acesso e controle de desktop de máquinas.

Tabela 2 – Aplicações para acesso remoto a desktop.

Programa (Protocolo)	Sistemas Operacionais Compatíveis		Segurança	Latência	Recursos extras
	Cliente	Servidor			
TightVNC (VNC)	Windows Mac OS Linux Android	Windows Linux	Apenas para estabelecer a conexão (AES- 64 na senha de autenticação)	baixa/média	*Transferência de arquivo *Múltiplas sessões

RealVNC (VNC)	Windows Mac OS Linux Android iOS	Windows Linux Mac OS	AES-128	baixa/média	*Transferência de arquivo *Múltiplas sessões *Suporte a IPv6
Remote Desktop Client (RDP)	Windows Mac OS Linux Android iOS	Windows	TLS/SSL e criptografia RC4 128-bit	baixa/média	*Transferência de arquivo *Múltiplas sessões *Suporte a IPv6 *Suporte a áudio *Suporte a vídeo
TeamViewer (proprietário)	Windows Mac OS Linux Android iOS	Windows Mac OS Linux Android	AES-128	baixa/média	*Transferência de arquivo *Múltiplas sessões (limitado) *Suporte a IPv6 *Suporte a áudio *Suporte a vídeo
Chrome Remote Desktop (Chromoting)	Windows Mac OS Linux Android iOS	Windows Mac OS Linux Android iOS	TLS/SSL	média	*Múltiplas sessões *Suporte a IPv6 *Suporte a áudio *Suporte a vídeo
OpenSSH (X11)	Windows Mac OS Linux Android iOS	Linux	SSH-2	baixa/média	*Transferência de arquivo *Múltiplas sessões
GoToMyPC (proprietário)	Windows Mac OS Linux Android iOS	Windows Mac OS	AES	alta	*Transferência de arquivo *Suporte a áudio
LogMeIn (proprietário)	Windows Mac OS Android	Windows Mac OS	SSL	alta	*Suporte a áudio

Fonte: Adaptado de Morimoto (2011) e Melkonyan, Akopian e Chen (2009).

2.1.3 Portais de aplicação

De acordo com Souppaya e Scarfone (2014, p.21), um portal é um servidor que oferece acesso a uma ou mais aplicações por meio de uma interface centralizada. Esse portal pode ser uma página web ou alguma aplicação implementada em servidores alugados de empresas que prestam serviços de computação em nuvem, como a Amazon.

Muitos laboratórios de experimentação remota utilizam sistemas web de gerenciamento de aprendizado, no qual o usuário se autentica, realiza seus testes pela página e o servidor web se comunica com os equipamentos industriais, transformando os comandos do usuário em comandos para os controladores e atuadores no laboratório (IONESCU et al., 2013; CHEVALIER et al., 2017). A Figura 4 mostra um exemplo de portal web onde os alunos de uma disciplina de controle trabalham com uma plataforma de controle de posição e a arquitetura da solução que gera essa interface web.

Figura 4 – Interface web para controle de posição de uma plataforma.

Fonte: Adaptado de Ionescu et al. (2013) e Chevalier et al. (2017).

Em outros casos, uma organização pode alugar serviços de plataforma na nuvem, escrever sua aplicação e hospedá-la para que os usuários com permissão tenham acesso a essas aplicações (VICENTE et al., 2010). Em situações onde a corporação opta por alocar bancos de dados e aplicações na nuvem, o custo é menor que manter servidores físicos próprios, contudo, em casos onde trafegam dados confidenciais manter os dados fora do domínio da empresa representa um alto risco.

É possível inclusive hospedar máquinas virtuais inteiras em tais plataformas, com CPU e memória dedicadas no lado do servidor: são as VDI. De maneira análoga aos protocolos de acesso remoto de desktop, o usuário possui total controle sobre a máquina, porém, em uma VDI ele tem recursos dedicados de hardware virtualizados no servidor na nuvem (JANA et al., 2017). O acesso a esse desktop pode ser via algum protocolo descrito no subcapítulo 2.1.2 ou via thin client.

Conforme Pandey (2017, p. 746), as tecnologias de virtualização são muito úteis para a criação de sistemas ciber-físicos, ou seja, cópias virtuais de máquinas ou unidades industriais inteiras são criadas e são capazes de monitorar processos através da resposta da comunicação com sensores e atuadores na planta.

O acesso à informação varia de acordo com o portal utilizado. Enquanto a VDI fornece uma máquina com hardware e software virtualizados, portais web fornecem aplicações através de páginas web. Apesar da diferença técnica entre as soluções, os portais podem apresentar uma característica comum: eles podem ser configurados para restringir os dados dentro da máquina virtual ou servidor web durante uma sessão remota. Ao final da sessão, os dados são excluídos ou resetados para que o usuário se conecte a uma máquina virtual limpa no início de uma nova sessão (SOUPPAYA; SCARFONE, 2016, p. 20).

Por exemplo, em laboratórios remotos acessados via web o usuário altera parâmetros e envia comandos que alteram o estado do equipamento físico. Ao final da conexão remota, essas alterações são descartadas e o equipamento retorna ao seu estado original. O cliente pode obter esses dados via download, porém, toda a aplicação está protegida do lado do servidor. Essa característica torna alguns portais de aplicação mais seguros que as soluções baseadas em VPN e softwares de acesso remoto a desktop, onde os clientes têm maior controle sobre os dados (SOUPPAYA; SCARFONE, p. 21). A desvantagem no caso dos portais é a restrição para fazer modificações permanentes nos dados. Em operações que requerem alteração em um processo ou manutenções permanentes em equipamentos industriais, o acesso via portal não é a melhor opção porque o usuário pode não ter acesso às configurações do servidor.

Além dessa característica, os portais de aplicação aplicam técnicas de segurança assim como VPN: proteção de mensagens via SSL, autenticação e controle de acesso. As diferenças entre técnicas de acesso remoto residem nas arquiteturas das aplicações, finalidade, protocolos e políticas de segurança utilizadas. Contudo, essas diferenças não impedem duas ou mais soluções de serem aplicadas juntas. A Tabela 3 mostra algumas soluções fornecidas pelos principais fabricantes de equipamentos industriais.

Tabela 3 – Algumas soluções para acesso remoto de equipamentos industriais.

Fabricante	Solução Técnica	Nome
Weidmuller	Túnel VPN + portal online	U-link
	Gateway industrial WiFi + 3G + WAN	IE-SR-2GT-UMTS-3G
eWON	Gateway SSL-VPN	COSY (hardware) + TALK2M (portal)
Phoenix Contact	Gateway VPN + portal web	mGuard
Siemens	Servidor VPN	SINEMA RC
	Gateway industrial Ethernet, 3G e 4G	SCALANCE Series
	Gateway industrial Ethernet	SIMATIC IoT2040
GE	Modem rádio	MDS LEDR Series
Secomea	Gateway WiFi, Ethernet, 3G e 4G-LTE	SiteManager Hardware
	Software de acesso remoto	SiteManager Software

Fonte: Próprio autor (2018).

2.1.4 Segurança em acesso remoto de equipamentos

A segurança da transmissão de dados em ambientes industriais é garantida pela equipe de tecnologia da informação e pela equipe de operação da unidade industrial. Apesar da discussão sobre segurança em protocolos de transmissão de dados pela rede de computadores, medidas de prevenção de acidentes a nível físico também são cruciais. Portanto, plantas industriais possuem controladores dedicados exclusivamente a garantir a segurança de equipamentos, alarmes e chaves de emergência. Esses elementos geralmente ficam inacessíveis inclusive pela rede interna e são manipulados somente em casos de extrema necessidade.

Quanto aos equipamentos acessíveis remotamente, há diversos níveis e práticas de segurança implementadas em conjunto para evitar ataques externos a redes privadas. Uma das práticas mais comuns quando uma rede privada é exposta a redes externas é

a criação de uma zona desmilitarizada ou rede de perímetro. Essa rede é responsável por garantir o acesso entre rede local e Internet implementando políticas de proteção à rede local (TANENBAUM; WHETERALL, 2011).

Um dos principais componentes de criação de uma DMZ é o firewall, um dispositivo da rede responsável por filtrar pacotes que entram na rede e que saem dela. O critério para criar este filtro é definido pelo administrador do sistema, que define uma política de acesso às mensagens que chegam e saem da rede local e quais portas TCP estão liberadas para acesso ou restringidas, por exemplo (MORIMOTO, 2011).

Contudo, o firewall não consegue evitar todo tipo de ataque à rede local. Ataques como DoS não visam roubar informações confidenciais mas tornar um website, por exemplo, indisponível. Em conexões feitas com aplicativos de acesso remoto pode haver vazamento de informações relevantes que também não são detectadas pelo firewall. Ademais, a atuação do firewall se restringe à rede perimetral, portanto, quando dados trafegam pela Internet, eles podem ser interceptados ou modificados por ataques do tipo man-in-the-middle sem que o dispositivo possa atuar (SOUPPAYA; SCARFONE, 2016).

Logo, outras técnicas de segurança são adotadas junto ao firewall. Uma das mais implementadas e presente na maioria das tecnologias de acesso remoto é a autenticação, feita através de um nome de usuário e uma senha. Na rede local, políticas de acesso são implementadas para restringir o acesso a equipamentos para determinados funcionários autorizados.

Ainda assim, quando os dados trafegam por redes externas, eles são legíveis por qualquer pessoa que os intercepte. Para torná-los ilegíveis, os próprios protocolos e técnicas de acesso remoto aplicam algoritmos de criptografia. Esta técnica é aplicada em diferentes camadas: SSL para a camada de transporte, HTTPS para a de aplicação, IPsec para a rede e PPTP e L2TP para a camada de enlace. Basicamente, a criptografia modifica o formato original das mensagens de acordo com algum padrão matemático de forma a torna-las ilegíveis por terceiros. Somente usuários ou aplicações com uma chave de decipação consegue decifrar os dados alterados (XU; JIANG; WANG, 2014).

Em teoria, aplicar a maior quantidade possível de algoritmos e técnicas de segurança é a melhor escolha para soluções de acesso remoto. Contudo, algumas técnicas consomem largura de banda e podem aumentar a latência na comunicação

entre cliente e servidor. Portanto, ao escolher quais métodos de segurança utilizados, a organização deve considerar quais os recursos podem ser acessados por quais pessoas autorizadas, qual o balanço entre os benefícios de se acessar remotamente os seus recursos físicos e os malefícios caso eles sejam comprometidos por invasores, e que as redes externas por onde os usuários vão se conectar às redes privadas são naturalmente inseguras.

Alguns autores recomendam uma lista de boas práticas para garantir a segurança de unidades industriais acessadas remotamente (XU; JIANG; WANG, 2014; SOUPPAYA; SCARFONE, 2016):

- a) Levantar todas as possíveis ameaças e quais os riscos que elas representam aos recursos físicos da corporação;
- b) Eliminar todos os pontos de acesso sem proteção aos recursos físicos da organização;
- c) Separar redes de diferentes domínios por zonas desmilitarizadas;
- d) Utilizar políticas de autenticação e autorização nas técnicas de acesso remoto;
- e) Implementar hardware e software específicos e dedicados para suportar o acesso remoto aos recursos físicos da rede privada;
- f) Em técnicas de tunelamento, utilizar protocolos criptografados;
- g) Considerar técnicas de segurança ao iniciar e ao finalizar uma sessão remota, como por exemplo, desconectar um usuário após certo tempo inativo.

A Figura 5 traz um exemplo de conexão remota segura por VPN a uma rede corporativa e a uma rede local industrial por dois usuários distintos, de acordo com as boas práticas expostas anteriormente.

Figura 5 – Exemplo de redes locais acessadas de acordo com as boas práticas de segurança.

Fonte: Centre for the Protection of National Infrastructure (2010).

2.2 CONTROLE E SUPERVISÃO DE PROCESSOS INDUSTRIAIS

Sistemas de controle são responsáveis por manter variáveis de processos físicos em torno de valores predeterminados. Para atingir esse objetivo, o sistema conta com dispositivos que medem em tempo real o valor das variáveis de processo e, a partir de algoritmos de controle, calcula uma saída para o(s) atuador(es) deste sistema, a fim de mantê-la próxima ao valor desejado (MORAES; CASTRUCCI, 2013).

Esse valor próximo do qual a variável de processo deve se manter é chamado setpoint. Ele é comparado com a saída produzida pelo atuador de forma a gerar um erro, que é transmitido ao controlador do sistema. Sobre o controlador atuam algoritmos, como PID, ON-OFF e PWM, cujos parâmetros são ajustados para produzir uma resposta rápida às mudanças na saída do processo. A comparação entre setpoint e variável de saída medida por um equipamento de campo para ajustar a saída do processo é o que define controle por realimentação.

Os sistemas de supervisão são integrados, porém independentes dos sistemas de controle. Eles são o elo entre os usuários, os sistemas de controle e outros sistemas e sua função é registrar e mostrar através de uma interface intuitiva o estado das variáveis de processo a partir da comunicação com os equipamentos de campo e, por essa razão, também são chamados de sistemas SCADA, ou sistemas de aquisição de dados e controle supervisão (MORAES; CASTRUCCI, 2013). Através deles também é possível enviar comandos a equipamentos físicos. Um dos principais componentes de um sistema supervisão é a interface homem-máquina, uma tela interativa que recebe os dados de processo e permite a navegação, visualização e inserção de dados.

Os elementos principais que compõem os sistemas de controle e supervisão de processos industriais a nível de campo são os sensores, responsáveis pela medição das variáveis de processo; atuadores, responsáveis por modificar os estados das variáveis de processo; controladores, responsáveis por ler os sinais provenientes dos sensores, aplicar operações matemáticas de controle e traduzi-las em sinais para os atuadores; as interfaces de monitoramento de variáveis, as quais também gerenciam alarmes, e as redes de comunicação de dados, que transmitem os sinais entre todos os componentes anteriores. A Figura 6 resume a arquitetura dos sistemas de controle e supervisão industriais.

Os dispositivos abordados neste subcapítulo contemplam a base da pirâmide da automação. Os sistemas de controle e supervisão de uma unidade industrial se comunicam também com redes de outras unidades industriais, redes de supervisão da estação de trabalho inteira, redes do alto nível corporativo e, no contexto de Indústria 4.0, redes externas à instalação (BUYA; DASTJERDI, 2016).

Centros de pesquisa, empresas e iniciativas governamentais vêm desenvolvendo trabalhos a respeito deste assunto e a abordagem tradicional de sistemas de controle e aquisição de dados com protocolos proprietários e restritos a redes locais vem sendo substituído por um novo paradigma, onde o time de operações da fábrica pode atuar mesmo remotamente. Como discutido no subcapítulo 2.1, as instalações mais modernas permitem conexão remota a unidades fabris por meio de técnicas que envolvem as equipes de segurança de informação e tecnologia da informação.

Figura 6 – Equipamentos de campo conectados por uma rede DeviceNet.

Fonte: www.smar.com.br (2011).

Conforme Encalada e Sequera (2017, p.118), como consequência desse novo paradigma, o ensino de conteúdos relacionados a automação e controle de processos industriais também vem se adaptando. Alguns laboratórios tradicionais, onde os alunos executam experimentos apenas presencialmente já estão absorvendo conceitos novos, como IoT e IIoT, conexão remota a equipamentos físicos, microcomputadores embarcados, virtualização de sistemas reais, sensores inteligentes, entre outros conceitos atuais (TAWFIK et al., 2014). Alguns autores chamam esse movimento de inserção de novas tecnologias no processo de ensino-aprendizagem de educação 4.0.

Entre os representantes dessa nova geração de tecnologias e plataformas para ensino na Engenharia estão os laboratórios remotos. O próximo subcapítulo traz exemplos de casos onde as tecnologias expostas em 2.1 são aplicadas no campo da educação para produzir laboratórios remotos focados em temas relacionados a teoria de controle, redes de comunicação digitais, instrumentação de processos e automação.

2.3 LABORATÓRIOS REMOTOS PARA ENGENHARIA

A ideia de laboratórios de experimentos remotos não é recente e surgiram com o advento da Internet, na década de 1980. Essa categoria de plataformas de ensino se fortaleceu com a popularização das TIC e da modalidade de e-learning e atualmente há diversos casos de cursos de engenharia que aproveitam dos recursos de compartilhamento de arquivos, comunicação instantânea e interação em tempo real e à distância com equipamentos físicos para tornar as disciplinas práticas mais flexíveis quanto a tempo e local para realização dos experimentos (CAMINERO et al., 2016).

Além dessa gama de recursos online, o mercado requer profissionais com habilidades e competências de trabalhar com ambientes digitais. Por essa razão, algumas instituições de ensino já adotam cursos baseados em ambiente e-learning e m-learning em suas grades curriculares. As vantagens dos laboratórios remotos incluem, de acordo com Iannucci et al. (2018, p. 1142):

- a) Flexibilidade quanto a tempo e local para realização dos experimentos;
- b) Os alunos obtêm e analisam dados reais, assim como em laboratórios tradicionais;
- c) Diminuição no custo de aquisição de licenças e hardware;
- d) Escalabilidade, pois mais alunos podem realizar experimentos a distância;
- e) Em alguns casos, laboratórios remotos são mais seguros que os presenciais;
- f) O laboratório remoto não sobrecarrega os professores e tutores com a preparação de equipamento e o andamento do laboratório.

A primeira categoria de laboratórios remotos que surgiram foram via Internet, através dos portais de aplicação via web (BELLMUNT, 2006). Até hoje, inúmeros exemplos de laboratórios web são implementados em diversos campos da educação: desde a engenharia a medicina, biologia, ciências da computação, entre outros. O foco deste subcapítulo é nos exemplos nas áreas de controle e automação.

Lopes et al. (2017) desenvolveram uma aplicação web a partir da qual os alunos conseguem controlar robôs móveis através de comandos simples. A página é desenvolvida em HTML5 e CSS3, está hospedada em um servidor Apache e os comandos inseridos pelos alunos são processados em requisições AJAX para o servidor

do laboratório. Este servidor processa os comandos e os envia para os robôs através de uma interface serial.

Chevalier et al. (2017) introduzem outro portal online para uma disciplina de engenharia de controle. Os alunos se autenticam em uma página web criada para o curso, agendam um horário para se conectarem ao laboratório remoto e realizam experimentos com duas plataformas: uma plataforma de Stewart, onde os alunos controlam a posição de uma bola em um prato; e um sistema com quatro reservatórios de água, para controlar seus níveis. Em ambos, os usuários escolhem via web a estratégia de controle e os parâmetros dos controladores.

Há diversos trabalhos recentes descrevendo portais web por onde os alunos conseguem monitorar e controlar equipamentos reais. Jiménez, Avilés e Mauledoux (2018) implementam um laboratório remoto através do qual os alunos enviam comandos que são processados por um Arduino MEGA e controlam dois braços robóticos. Shyr, Su e Lin (2013) utilizam uma arquitetura muito parecida com a descrita anteriormente, contudo, um servidor web se comunica com um CLP para realizar o controle de uma esteira sincronizada com um braço cartesiano. Kalúz et al. (2015) implementa um servidor web para controle de múltiplas bancadas no mesmo laboratório, assim, os alunos podem realizar experimentos com equipamentos diferentes na mesma disciplina.

Nos casos anteriores, os laboratórios remotos utilizam uma solução muito parecida: aplicar servidores web, baseados em arquitetura cliente-servidor, através dos quais os alunos podem controlar e monitorar sistemas físicos simples. Há soluções que utilizam a arquitetura web, porém, permitem hospedar laboratórios de diferentes disciplinas, assuntos e universidades, são os sistemas de gerenciamento de laboratório remoto. Alguns casos são o MIT iLAB (MENDES et al., 2016), o WebLab Deusto (ORDUÑA et al., 2011) e o NCSLab (LEI et al., 2018), cujo website está representado na Figura 7, repositórios de laboratórios remotos através dos quais os alunos se cadastram e acessam cursos em variadas áreas de conhecimento, não somente da engenharia. Há autores, como Tawfik (2014, p.15), que classificam essa modalidade como Laboratory as a Service (LaaS).

Figura 7 – WebLab Deusto: exemplo de sistema de gerenciamento de laboratórios remotos.

Fonte: <https://weblab.deusto.es> (2018).

Apesar de populares, os laboratórios web não permitem que os alunos tenham controle integral do processo ou equipamento que eles controlam. Por exemplo, os alunos conseguem alterar parâmetros, escolher via interface web qual a estratégia de controle mais adequada e monitorar o processo, contudo, o algoritmo que interpreta os comandos enviados por eles e os transforma em sinal para os atuadores é implementado do lado do servidor. Os alunos também não mapeiam as entradas e saídas dos dispositivos conectados ao controlador nem os protocolos de comunicação entre eles, isso é configurado pelos projetistas do laboratório remoto.

Com o surgimento de novas TIC, novas soluções de laboratórios remotos surgiram, com destaque para o uso da computação em nuvem, infraestrutura para virtualização de desktop e redes privadas virtuais. Jana et al. (2017) implementa um laboratório remoto para monitoramento de sensores wireless. Esses sensores armazenam seus dados na Google App Engine, um provedor de serviços de computação em nuvem, a partir da qual os alunos podem acessar o laboratório de qualquer dispositivo com conexão à Internet.

Alagappan, Venkataraman e Sivakumar (2016) discutem a viabilidade, os desafios e os benefícios de implementar um VDI para que os alunos possam acessar seu próprio desktop virtualizado e instalado com as aplicações necessárias a partir de qualquer máquina. Kist et al. (2014) descrevem uma solução onde usuários podem compartilhar experimentos remotos criados nas áreas de ciência, tecnologia e engenharia em servidores web. Para acessar esse servidor, o usuário deve se conectar à VPN da University of South Queensland, Austrália.

Apesar das alternativas para desenvolvimento de laboratórios remotos, a literatura envolvendo soluções que não envolvam exclusivamente portais web ainda é incipiente, principalmente na área de controle e automação, cujos ambientes e-learning existentes estão predominantemente em portais web.

Conforme explicitado no subcapítulo 3.3, este trabalho implementa uma solução técnica diferente da apresentada por muitos trabalhos que compõem o estado da arte em laboratórios remotos, baseados exclusivamente em portais online. Neste caso, os alunos têm acesso direto ao ambiente do servidor virtualizado em suas máquinas, desenvolvem e carregam as suas aplicações diretamente no hardware do controlador e supervisionam e controlam as malhas como em um laboratório presencial. Portanto, este laboratório remoto complementa a bibliografia sobre o assunto e guia trabalhos futuros a implementarem melhorias para esta solução ou se basearem nela para a construção de outros laboratórios com arquiteturas alternativas às existentes.

2.4 METODOLOGIA PBL PARA DISCIPLINAS PRÁTICAS

As disciplinas práticas, remotas ou presenciais, são fundamentais na grade curricular dos cursos de engenharia porque expõem os alunos a situações e problemas reais e os fazem aplicar conceitos que eles só haviam aprendido em aulas teóricas. Além de habilidades técnicas, empresas e organização buscam por profissionais com habilidades sociais: trabalho em equipe, comunicação e liderança. Aulas expositivas estimulam o aluno a resolver individualmente problemas teóricos, porém, disciplinas experimentais estimulam os alunos a trabalhar em grupo, resolver problemas em conjunto e compartilhar conhecimento (FERNANDES, 2016).

Por esses motivos, uma das abordagens mais utilizadas em disciplinas práticas é a PBL. Conforme Efstratia (2014, p. 1256), essa abordagem consiste em apresentar projetos e desafios reais com objetivos bem definidos aos alunos. Durante o desenvolvimento do projeto, os alunos se deparam com falhas e problemas e devem se organizar de forma a resolvê-las e concluir o projeto. Por meio da troca de experiências e dos processos de experimentação e tentativa-erro, os alunos ganham conhecimento. É uma dinâmica diferente de aulas expositivas, onde o conhecimento é transmitido principalmente por meio de um professor.

Os tutores e responsáveis pela disciplina desempenham um papel diferente em disciplinas práticas em relação às teóricas: neste caso, eles atuam como facilitadores, auxiliando no esclarecimento de dúvidas (ALVES; BRANDÃO; OLIVEIRA, 2018). Em laboratórios exclusivamente remotos, contudo, os alunos realizam experimentos práticos em suas próprias máquinas em locais e horários distintos. A interação entre grupos diferentes é menor, assim como o contato entre alunos e professores. A implementação de chats online e de ambientes virtuais de aprendizagem (AVA) com fóruns de discussão pode ajudar a reduzir esse isolamento, porém, os laboratórios presenciais são mais vantajosos no quesito interação e troca de experiências.

Este trabalho implementa um laboratório remoto como suporte ao presencial. Portanto, os alunos ainda interagem entre si e com os tutores durante o período das aulas práticas, porém não estão restritos a elas para concluir seus experimentos. Essa abordagem híbrida ainda é favorável para aplicação da metodologia PBL e possui vantagens em relação aos laboratórios exclusivamente presenciais e exclusivamente remotos.

3 DESCRIÇÃO DOS MÉTODOS E FERRAMENTAS

O desenvolvimento do laboratório remoto considerou as necessidades dos alunos que cursaram a disciplina presencialmente em 2016, as limitações técnicas de se implementar a ferramenta de acesso remoto a uma planta cujos únicos equipamentos com interface de rede são os CLPs e os desafios quanto a segurança durante as práticas remotas. Em cada etapa da construção da ferramenta de acesso remoto, o autor justifica suas escolhas e sugere melhorias para as próximas turmas. Toda a metodologia aplicada ao longo deste trabalho está resumida pela Figura 8.

Figura 8 – Cronograma com a metodologia do desenvolvimento do laboratório remoto.

Fonte: Próprio autor (2018).

3.1 CONTEXTO DO TRABALHO

A disciplina SEL0431 tem como objetivo proporcionar aos alunos o contato direto com equipamentos de campo industriais, malhas de controle e redes de comunicação digitais. Sua grade é composta por experimentos práticos em uma planta industrial de

escala reduzida, sobre a qual os alunos desenvolvem projetos para controle de processos industriais e supervisão das variáveis de processo. Os alunos são responsáveis por todas as etapas de seus projetos: desde o mapeamento de entradas e saídas de cada CLP e desenvolvimento das aplicações em ladder a sintonia dos ganhos dos controladores (ALVES; BRANDÃO; OLIVEIRA, 2018).

Para esta disciplina, é adotada a metodologia PBL, ou seja, os alunos colocam em prática os conceitos aprendidos em aulas teóricas sobre automação, instrumentação, controle e redes de comunicação industrial, realizam práticas diferentes na mesma unidade industrial e trocam conhecimento durante as aulas. O professor e o tutor desta disciplina atuam como auxiliadores, esclarecendo dúvidas sobre os projetos e avaliando o desempenho dos alunos.

Esta disciplina é optativa e ministrada para os alunos do segundo, terceiro, quarto e quinto anos das turmas de Engenharia Elétrica da USP. O subcapítulo 3.2 detalha a planta didática e a organização da disciplina, enquanto este subcapítulo discute a motivação para o desenvolvimento do laboratório remoto.

Basicamente, os alunos desenvolvem 4 projetos diferentes ao longo da disciplina SEL0431 e cada projeto possui um prazo de conclusão de 3 semanas. Contudo, os grupos cumprem diversas etapas para concluir um projeto: entender o objetivo da prática, mapear as variáveis envolvidas e entender como elas se comunicam com o CLP, aprender a trabalhar com o ambiente de desenvolvimento das aplicações, desenvolver e testar a aplicação e lidar com dúvidas e obstáculos durante os testes. Nas práticas iniciais, este tempo foi extrapolado e o semestre foi estendido para alguns grupos. Ademais, para completar a prática os grupos dividiam suas tarefas entre os membros, e em alguns casos, alguns alunos ficaram restritos a etapas específicas do projeto.

Durante 2016, quando a prática era exclusivamente presencial, alguns alunos tentaram explorar os ambientes de configuração e programação de CLPs em casa. Contudo, a maioria dos softwares industriais exigem licenças custosas para serem adquiridas, assim como os CLPs e outros equipamentos de campo, e o contato dos alunos com estes elementos é restrito às aulas no laboratório.

De acordo com Alves, Brandão e Tietz (2018), os intuitos do laboratório remoto são diminuir a restrição de tempo e local para que os alunos operem a planta e concluam

seus projetos com mais qualidade, disponibilizar o acesso a recursos utilizados em plantas industriais reais e dispendiosos de adquirir e prover contato com tecnologias de acesso remoto a equipamentos industriais, uma das tendências no mercado de trabalho no contexto de Indústria 4.0.

3.2 A DISCIPLINA DE LABORATÓRIO DE CONTROLE DE PROCESSOS INDUSTRIAIS

Este subcapítulo descreve com detalhes como os alunos foram organizados durante a disciplina, quais são os projetos desenvolvidos por eles e a ferramenta sobre a qual eles realizam os experimentos.

3.2.1 Organização da disciplina

A disciplina é composta por aulas práticas semanais e comporta duas turmas de 16 alunos cada, uma às quartas-feiras e outra às quintas-feiras. Cada turma de 16 alunos é dividida em 4 grupos com 4 alunos cada, os quais devem desenvolver 4 projetos diferentes ao longo do semestre. Ao final do prazo de 3 semanas, os grupos trocam os projetos entre si e entregam um relatório técnico contendo detalhes da implementação do projeto, resultados e conclusões. São estes relatórios que o professor e tutor da disciplina utilizam para avaliar o desempenho do grupo como um todo.

Neste trabalho, os projetos são denominados Projeto 1, 2, 3 e 4, assim como os grupos. A sequência dos projetos para cada grupo ao longo do semestre é mostrada pela Tabela 4.

Tabela 4 – Sequência de projetos para cada grupo.

Grupos/rodada	1ª	2ª	3ª	4ª
Grupo 1	Projeto 1	Projeto 2	Projeto 3	Projeto 4
Grupo 2	Projeto 2	Projeto 3	Projeto 4	Projeto 1
Grupo 3	Projeto 3	Projeto 4	Projeto 1	Projeto 2
Grupo 4	Projeto 4	Projeto 1	Projeto 2	Projeto 3

Fonte: Próprio autor (2018).

A planta didática é uma unidade industrial de escala reduzida que possui inúmeros equipamentos de campo e opera com água. O projeto 1 tem como objetivo principal controlar a vazão de água pela planta. Os alunos estabelecem um setpoint, mapeiam as entradas e saídas conectadas ao respectivo controlador, determinam uma estratégia de controle e implementam no CLP. O grupo também é responsável por ajustar os ganhos do controlador, de forma a obter um controle estável do sistema. No painel principal da planta, há chaves manuais através das quais os alunos podem acionar o atuador manualmente e escolher se o seu acionamento será manual ou automático. Neste caso, o sinal de saída para o atuador é determinado pelo algoritmo de controle. Em resumo, os objetivos principais deste projeto são:

- a) Determinar um setpoint para controlar o fluxo de água pelo sistema;
- b) Implementar no código uma entrada para a chave manual, a qual decide qual o modo de controle do atuador: manual ou automático;
- c) Implementar no código uma entrada para a chave manual que, quando acionada, deve ativar ou desativar o atuador. Esta ação é válida somente quando o modo manual de controle está ativo;
- d) Quando o atuador estiver acionado, um LED presente no painel deve ser ligado;
- e) Quando o modo manual for escolhido, outro LED no painel deve ser ligado.

Além dos objetivos principais, o professor e tutor da disciplina recomendam os grupos a comparar os parâmetros do controlador de forma a ajustá-lo com os melhores valores.

No projeto 2 os alunos controlam a temperatura da água que sai de uma caldeira e circula pelo reservatório. Neste caso, o grupo deve manter a água dentro de uma faixa de temperatura a ser escolhida pelos próprios alunos. Por questão de segurança, esta temperatura não excede 50° C, um relê de segurança desativa a resistência da caldeira neste caso. O painel elétrico principal contém duas chaves e dois LEDs, cujos propósitos são escolher o modo de controle, acionar ou desativar manualmente o atuador e sinalizar quando as chaves estão comutadas. Os grupos devem atingir os seguintes objetivos:

- a) Estipular uma faixa na qual a temperatura da água que sai da caldeira deve ser mantida;

- b) Implementar no código uma entrada representando a chave manual que comuta os modos de controle: manual ou automático;
- c) Implementar no código uma entrada para a chave manual que aciona o atuador do sistema quando é comutada. Esta ação vale somente quando o modo de controle é manual;
- d) Quando o atuador estiver acionado, seu respectivo LED deve acender. A mesma regra é válida para o LED que indica o estado da chave que seleciona o modo de controle.

Como objetivo extra, o tutor e o professor recomendam aos alunos incluir na malha de controle o sensor que mede a temperatura da água no reservatório 2 e a válvula solenoide que conecta a saída da caldeira à entrada deste reservatório. A válvula deve permitir ou bloquear o fluxo de água aquecida ao reservatório conforme a temperatura medida pelo sensor.

O projeto 3 tem como objetivo principal controlar o nível de um dos dois reservatórios de água presentes na planta. O grupo pode escolher entre o reservatório 1 e o reservatório 2, cada um possui um instrumento de medição diferente, contudo, o atuador é o mesmo e o painel possui duas chaves dedicadas ao controle dessa malha. De forma análoga aos projetos 1 e 2, o grupo possui os seguintes objetivos:

- a) Determinar qual reservatório será controlado, assim como o setpoint para controle do seu nível de água;
- b) Implementar no código uma entrada para a chave manual, a qual decide qual o modo de controle do atuador: manual ou automático;
- c) Implementar no código uma entrada para a chave manual que, quando acionada, deve ativar ou desativar o atuador;
- d) Quando o atuador estiver acionado, um LED presente no painel deve ser ligado;
- e) Quando o modo manual for escolhido, outro LED no painel deve ser ligado.

Os responsáveis pela disciplina sugerem como objetivo extra controlar o nível em ambos os reservatórios utilizando a mesma aplicação e ajustar os ganhos do controlador.

O projeto 4 envolve o desenvolvimento de um sistema supervisório, através do Elipse SCADA, que lê as variáveis de cada CLP e representa seus estados através de elementos gráficos em uma aplicação, que é dividida em duas partes principais: uma para

autenticação, onde o grupo pode definir o nível de acesso de grupos de usuário; outra para visualizar em tempo real os dados dos CLPs na planta. Os elementos a serem representados são:

- a) Cada setpoint das malhas de controle;
- b) As variáveis manipuladas, que correspondem às saídas dos atuadores principais de cada malha de controle;
- c) As variáveis de processo, que correspondem às entradas de cada malha de controle.

Além dos elementos da aplicação principal, os tutores recomendam que os grupos representem as variáveis de processo em um gráfico de tendência, gerem relatórios a partir das medições das variáveis e representem as demais entradas e saídas dos controladores.

Apesar de cada projeto ter seus próprios objetivos, eles não são totalmente independentes. O funcionamento de um sistema de controle representa um distúrbio aos demais sistemas de controle e o funcionamento do sistema supervisório desenvolvido no projeto 4 depende do funcionamento destes sistemas para que ele leia os valores das variáveis. Portanto, durante as práticas os alunos de diferentes grupos interagem entre si para trocar informações e obter conclusões em conjunto.

3.2.2 Planta didática multitarefa

A planta didática multitarefa é uma unidade industrial de escala reduzida construída por alunos do Laboratório de Automação Industrial da Escola de Engenharia de São Carlos e utilizada pela primeira vez como plataforma para ensino de controle de processos industriais em 2016. Ela contém dois painéis elétricos: o principal, com os CLPs, conversores de protocolo de rede, fontes de energia, chaves e LEDs; e o secundário, que contém um switch de rede e dois inversores de frequência. Cada CLP controla um sistema diferente e estes sistemas podem funcionar simultaneamente, por isso a planta é denominada multitarefa. A Figura 9 mostra este equipamento.

Ao todo são 4 CLPs: três deles são configurados pelos alunos durante as aulas, e o quarto é um CLP dedicado a garantir a segurança da planta. Este controlador não é

acessado pelos alunos e sempre que ele detecta uma situação anormal, como nível alto dos reservatórios, ele aciona a luz vermelha de uma sinaleira e desativa os atuadores da planta até que a situação seja reestabelecida. O painel também conta com um botão de emergência, que também desativa os atuadores da planta ao ser acionado. Contudo, quando este botão é destravado, os atuadores não voltam a operar automaticamente.

Os controladores são listados abaixo:

- a) CLP Siemens S7-1200 com cartão de entrada analógica para controle da malha de temperatura. O software de configuração utilizado é o TIA Portal v11;
- b) CLP Siemens S7-1200 com cartão para entrada de rede PROFIBUS e conversor de redes PROFIBUS DP-PA para controle da malha de nível;
- c) CLP Fertron com módulos de entrada e saída digitais e analógicas para controle da malha de vazão. O software de configuração utilizado é o Citrino Tools;
- d) CLP Siemens S7-1200 para segurança da planta.

Figura 9 – Planta didática multitarefa.

Fonte: Próprio autor (2018).

O controlador Siemens S7-1200 está ligado a entradas digitais, como as chaves do painel elétrico, e analógicas, as quais são termorresistências, cuja resistência elétrica varia de acordo com a temperatura da água dentro da caldeira. Um circuito com uma resistência fixa em série e alimentada por 24V dissipa uma tensão sobre a resistência variável e há uma tabela que relaciona temperatura da água na caldeira e a tensão emitida à entrada analógica do CLP.

Um dispositivo sensor e indicador mostra o valor da temperatura da água dentro da caldeira no painel principal e possui uma função de segurança importante: ele desativa a resistência da caldeira sempre que a temperatura da água dentro dela ultrapassar 50° C. A Tabela 5 mostra as variáveis conectadas a este CLP.

Tabela 5 – Variáveis da malha de controle de temperatura.

Malha de controle de temperatura	
Entradas	Saídas
I0.0 - Botão de parada de emergência	Q0.0 - Contator que aciona o resistor na caldeira
I0.4 - Chave para acionamento manual do atuador	Q0.1 - Válvula solenoide que liga a saída da caldeira à entrada do reservatório 2
I0.5 - Chave para seleção do modo de controle	Q0.2 - LED indicador do modo de controle
IW64 - Sensor de temperatura da água na caldeira	Q0.3 - LED indicador do funcionamento do atuador
IW65 - Sensor de temperatura de água no reservatório 2	

Fonte: Próprio autor (2018).

A malha de controle de nível possui mais elementos conectados ao controlador. Os elementos que medem os níveis dos reservatórios 1 e 2 são, respectivamente, um sensor de medição por pressão diferencial, demonstrado à esquerda da Figura 10, e um sensor ultrassônico que se comunica através do protocolo PROFIBUS PA, mostrado ao centro da Figura 10. Um Coupler DP-PA, como o mostrado à direita na Figura 10, faz a conversão para PROFIBUS DP, cujo sinal é lido por um cartão conectado ao CLP.

Figura 10 – Da esquerda à direita, o instrumento de medição de nível por diferencial de pressão, o sensor ultrassônico e o Coupler DP/PA da Siemens.

Fonte: Próprio autor (2016).

Os sinais obtidos por esses elementos são algumas das entradas do CLP. Ele processa esses sinais e calcula uma saída para o atuador, uma bomba d'água como a representada à esquerda na Figura 11. Porém, a bomba aceita corrente alternada, portanto, um inversor de frequência tem a função de interface entre CLP e atuador. Ele lê o sinal analógico emitido pelo CLP e envia um sinal AC para a bomba proporcional ao sinal recebido em sua entrada analógica. Este driver está representado à direita na Figura 11 e a Tabela 6 mostra as variáveis dessa malha de controle.

Figura 11 – Bomba d'água centrífuga do fabricante Ferrari, à esquerda, e inversor de frequência CFW-08, à direita.

Fonte: Próprio autor (2016).

Tabela 6 – Variáveis da malha de controle de nível.

Malha de controle de nível	
Entradas	Saídas
I0.1 - Chave para acionamento manual do atuador	Q0.1 - Bit para habilitar o inversor de frequência
I0.2 - Chave para seleção do modo de controle	Q0.2 - LED indicador do funcionamento da bomba
I0.5 - Botão de parada de emergência	Q0.3 - Válvula solenoide da entrada do reservatório 1
IW64 - Sensor diferencial de pressão	Q0.4 - Válvula solenoide da entrada do reservatório 2
ID266 - Sensor ultrassônico	Q0.5 - LED indicador do modo de controle
	QW80 - Sinal analógico para o inversor de frequência

Fonte: Próprio autor (2018).

A malha de controle de vazão possui entradas digitais e uma entrada analógica, que é um transmissor volumétrico via protocolo HART. Este elemento envia sinal ao CLP Fertron e este envia um sinal analógico a outro inversor de frequência, idêntico ao inversor na Figura 11. Assim como a malha de controle de nível, o inversor é um elemento intermediário entre o CLP e o atuador AC, outra bomba d'água. A Tabela 7 mostra as entradas e saídas conectadas a este controlador.

Tabela 7 – Variáveis da malha de controle de vazão.

Malha de controle de vazão	
Entradas	Saídas
AI1 - Transmissor volumétrico	AO1 - Sinal analógico para o inversor de frequência
DI3 - Chave para acionamento manual do atuador	DO2 - Bit para habilitar o inversor de frequência
DI4 - Botão de parada de emergência	DO3 - LED indicador do modo de controle

DI5 - Chave para seleção do modo de controle	DO4 - LED indicador do funcionamento do atuador
---	--

Fonte: Próprio autor (2018).

Além dos elementos descritos neste subcapítulo, há outros sensores e componentes responsáveis pela segurança da planta didática durante a operação e há duas caixas que armazenam a água que circula pelo sistema. As bombas centrífugas atuam em conjunto com as caixas e caso elas estejam com nível acima ou abaixo do permitido, o sistema para de funcionar. Para facilitar a visualização das falhas ou situações de risco que ocorrem durante a operação da planta, uma sinaleira luminosa está montada sobre o painel principal. Essa descrição é encontrada também em Alves, Brandão e Oliveira (2018).

3.3 DESENVOLVIMENTO DO LABORATÓRIO REMOTO

A escolha da solução para implementação do laboratório remoto foi feita de acordo com os requisitos do projeto, que estão detalhados na seção 3.3.1, e de acordo com as limitações da planta didática. Os únicos elementos que possuem interface de rede são os CLPs e o switch Ethernet e é através deles que os alunos obtêm os dados de sensores e atuadores. No laboratório presencial, os alunos acessam e configuram os CLPs através da rede local e o switch redireciona os pacotes de acordo com o IP que o usuário informa no software de configuração do CLP.

O primeiro desafio é acessar os IPs privados dos controladores na rede local através de uma rede externa e assim configurá-los e monitorá-los através da Internet. O segundo desafio é implementar uma solução segura, que garanta a confiabilidade, integridade e disponibilidade dos dados, considerando métodos e protocolos apresentados no subcapítulo 2.1.4. O terceiro desafio é garantir que os alunos acessem e obtenham facilmente os dados da planta, portanto, recursos adicionais são acrescentados para auxiliá-los no uso da ferramenta.

Os próximos subcapítulos detalham e justificam quais foram as ferramentas escolhidas para desenvolver a ferramenta de conexão remota.

3.3.1 Requisitos de projeto e implementação do laboratório remoto

O primeiro requisito para este projeto é utilizar ferramentas abertas e de uso intuitivo pelos alunos, garantindo que eles acessem os programas para configurar e programar os CLPs da planta de qualquer lugar e em qualquer momento que ela esteja ligada. O laboratório remoto é uma extensão do laboratório presencial, portanto, este projeto tem como objetivo disponibilizar o mesmo ambiente a que os alunos têm acesso durante as aulas. A solução mais apropriada para este caso é o uso de tecnologias de virtualização de desktop, seja através de VDI por alguma plataforma de computação em nuvem ou através de algum aplicativo de acesso remoto (PORNTROY, 2012; PANDEY et al., 2017).

Ao implementar instâncias de desktop virtuais na nuvem, cada aluno teria seu próprio ambiente e hardware virtuais dedicados, porém, ainda seria necessário um servidor ou algum gateway físico para se comunicar com os CLPs na planta. Apesar de escalável, este tipo de solução em nuvem tem um custo de manutenção da infraestrutura e acréscimo na latência da comunicação entre clientes e servidor (JANA et al., 2017).

Alguns aplicativos de acesso remoto, como o TeamViewer permitem com que a máquina do usuário se conecte diretamente ao servidor conectado à Internet. Porém, o acesso direto contorna algumas camadas de segurança da aplicação. Há outros requisitos além de segurança: a solução precisa ser multiplataforma, gerenciar acessos simultâneos, apresentar latência menor que 100ms, considerado um valor aceitável para processos industriais não-críticos (JANA et. al, 2017), aplicar políticas de autenticação e autorização e limitar as permissões dos usuários no servidor.

A solução implementada neste trabalho aproveitou a infraestrutura de rede do campus de São Carlos da USP. Uma máquina com processador i7 e 8GB de memória RAM foi instalada com as aplicações que os alunos precisam para realizar seus experimentos com a planta didática. Esta máquina é o gateway entre a rede local e a rede WAN da USP, a USPNet.

Porém, ela não conecta a rede privada do laboratório à Internet. Ela está dentro da zona perimetral, ou seja, o firewall da rede bloqueia o acesso direto ao servidor. Para acessá-lo por uma rede externa, é necessário primeiramente conectar-se a uma VPN

através do aplicativo Cisco AnyConnect Secure Mobility Client, cuja interface é mostrada pela Figura 12.

Figura 12 – Interface do aplicativo Cisco AnyConnect para Windows.

Fonte: Próprio autor (2018).

Esta aplicação aplica duas medidas de segurança: a primeira é a autenticação, ou seja, somente alunos e membros da Universidade conseguem se conectar à rede WAN; a segunda é a utilização do protocolo IPsec, que implementa criptografia na camada de rede, e evita que mensagens interceptadas sejam decifradas.

Após a etapa de conexão à WAN da Universidade, o usuário está na mesma rede do servidor e precisa acessá-lo através de um aplicativo ou protocolo. A Tabela 2 traz uma comparação entre os programas de conexão remota mais populares e, através dela, o autor optou por utilizar o protocolo RDP.

Apesar de ser nativo para Windows, há aplicações clientes gratuitas para outras plataformas: Remmina para Linux, Microsoft Remote Desktop para MacOS e Remote Desktop Connection para clientes mobile. O suporte a transferência de arquivos, múltiplas sessões e baixa/média latência em relação a outros protocolos foram fatores determinantes na escolha. A Figura 13 mostra a interface do aplicativo Remote Desktop Client, para Windows, e a interface do Chrome RDP, um plug-in web do aplicativo.

Figura 13 – Aplicativo e extensão web do protocolo RDP.

Fonte: Próprio autor (2018).

Após a conexão com a VPN, qualquer aplicação baseada no protocolo RDP consegue acessar o servidor, basta acessar o IP fixo e a porta correta. O firewall libera somente a porta 3389 para conexões remotas com este servidor, porém, o endereço no formato “IP: porta” é substituído por um nome. No-IP é um site que fornece domínios gratuitos para máquinas e o servidor RDP do laboratório é acessível através do endereço “sel0431.ddns.net”.

Através da interface da aplicação de acesso remoto, o aluno escolhe a qual usuário padrão ele quer se conectar: VAZAO, TEMPERATURA, NIVEL ou SUPERVISAO, os quais possuem os programas necessários para desenvolver os projetos 1, 2, 3 e 4, respectivamente, além de ferramentas adicionais de apoio ao laboratório remoto. O aluno autorizado possui uma senha e um nome de usuário sem os quais ele não consegue acessar o servidor, é a última etapa de verificação antes de concretizar o acesso.

Além dos requisitos para definir uma solução de acesso remoto seguro ao servidor, há os requisitos de configuração do próprio servidor. Para gerenciamento de acesso remoto, as versões do Windows Server são as mais apropriadas, contudo, nem todos os softwares de configuração de CLP funcionam nesta versão de sistema operacional. Os únicos sistemas operacionais suportados por todas as aplicações são o Windows 7, XP, 8 e 10. Para manter o ambiente de trabalho semelhante ao ambiente das máquinas do laboratório, este autor optou por instalar o Windows 7.

Todas as conexões à planta são feitas através deste servidor. Para este caso, onde a máquina recebe no máximo 4 conexões simultâneas, centralizar o processamento

das tarefas dos usuários é factível. A partir de mais acessos concorrentes, a melhor solução é distribuir o processamento e centralizar somente o gerenciamento dos acessos. Neste cenário, o uso de VDI é recomendável. No caso deste trabalho, a máquina possui um usuário administrador do sistema e 4 usuários comuns. Para testar a latência na comunicação com o servidor, um teste de conexão foi realizado: 4 máquinas em uma rede externa à USPNet conectaram-se simultaneamente ao servidor via Remote Desktop Connection sobre VPN e executaram tarefas diversas: desde abrir o navegador a abrir um projeto no TIA Portal. Estas máquinas estavam conectadas a uma rede de 10MB via WiFi e os testes de conectividade foram repetidos 50 vezes. A Tabela 8 mostra a média dos resultados, dos tempos máximos, mínimos e o desvio-padrão dos valores médios, em milissegundos.

Tabela 8 – Valores médios dos tempos mínimo, máximo e médio, em milissegundos, da conexão com o servidor por uma rede privada de 10MB.

Mínimo	Médio	Máximo	Desvio-padrão do valor médio
23,2	32,6	49,3	5,42

Fonte: Próprio autor (2018).

O teste revelou um valor aceitável na latência da comunicação entre cliente e servidor via VPN. Usuários distintos podem acessar contas distintas ao mesmo tempo, contudo, não podem acessar o mesmo usuário simultaneamente. Essa característica não é inerente ao protocolo RDP, o qual permite que usuários capturem sessões ativas de outros. Scripts em PowerShell, presentes no apêndice A, gerenciam múltiplas conexões. Um usuário só pode abrir uma sessão se ela estiver livre. Outras características do servidor estão listadas abaixo:

- a) O tempo máximo de sessão por usuário é de 2 horas;
- b) O usuário comum só tem acesso ao navegador, aos aplicativos do desktop, e às opções de fazer “logout” ou se desconectar. Ao escolher a primeira opção, a sessão é automaticamente liberada para outros usuários;

- c) Caso o usuário somente se desconecte, a sessão fica ativa por mais 2 minutos. O motivo: instabilidade na conexão da rede do cliente. Caso a conexão se perca involuntariamente, ele ainda pode se reconectar à sessão;
- d) O tempo ocioso máximo com a sessão ativa é de 10 minutos. Depois desse período, a sessão é automaticamente liberada.

Os itens a), b) e d) acima são configurados no próprio servidor, enquanto a opção c) é configurada no script. Todas as configurações foram feitas e podem ser alteradas pelo administrador do sistema e são transparentes aos usuários. Seus únicos passos são conectar-se à USPNet e posteriormente ao servidor via qualquer aplicação baseada no protocolo RDP para realizar os experimentos.

3.3.2 Arquitetura do laboratório remoto

A arquitetura do laboratório remoto, após a definição das tecnologias utilizadas para sua implementação, é representada pela Figura 14. Caso o aluno esteja em uma rede externa, seu acesso é feito via RDP sobre a VPN da USP através de qualquer dispositivo conectado à Internet. A rede local do laboratório é separada da rede externa pela zona desmilitarizada, própria da infraestrutura de rede da Universidade, e pelo servidor.

3.3.3 Ferramentas adicionais

A interação remota com a unidade industrial tende a diminuir a sensação de controle sobre os experimentos. Ademais, em práticas a distância a obtenção de dados não é tão fácil quanto em práticas presenciais, portanto, algumas ferramentas adicionais são implementadas na rede local para providenciar uma experiência melhor aos alunos. Algumas ferramentas são de uso dos usuários do laboratório, enquanto outras são de uso dos administradores do sistema.

Três webcams são posicionadas de forma a mostrar os pontos principais da planta: o painel principal, os reservatórios e o transmissor volumétrico, conforme a Figura 15

demonstra. As imagens são iniciadas como serviços do Windows, e sempre que um usuário se conecta ao servidor, elas surgem aparecem na tela da máquina do cliente.

Figura 14 – Arquitetura de implementação do laboratório remoto.

Fonte: Próprio autor (2018).

Figura 15 – Diferentes ângulos da planta vistos pela webcam.

Fonte: Próprio autor (2017).

Ainda que as webcams mostrem valores das variáveis de processo, elas não mostram o valor de todas as variáveis dos CLPs. O aluno consegue visualizá-las em uma tabela de entradas e saídas quando o CLP está online, contudo, essa não é uma tarefa intuitiva. Um sistema supervisório redundante, disponível em um portal web, também é iniciado automaticamente quando o usuário inicia a conexão com o servidor.

Este sistema é um trabalho envolvendo outros tipos de tecnologia e outra implementação técnica: é um segundo gateway, construído com o microcomputador Raspberry Pi, o qual lê ciclicamente os valores de cada CLP e os publica em um broker MQTT. Um serviço web consome esses dados e os atualiza em um website, disponível apenas para visualização dos alunos. A Figura 16 mostra a aplicação web lendo os valores das variáveis do CLP responsável pelo controle da malha de temperatura.

Figura 16 – Dashboard online para supervisão das variáveis do CLP de controle de temperatura.

Fonte: Próprio autor (2017).

Além de visualizar os valores das variáveis, os alunos devem ser capazes de alterá-los. No modo automático de controle, essa tarefa é realizada exclusivamente via software, entretanto, no modo manual de controle o acionamento físico das chaves é

impossível. Tutoriais explicam como alterar via TIA Portal e Citrino Tools o estado de variáveis de entrada.

Esse e outros materiais de suporte estão presentes em um ambiente virtual de aprendizagem, o Moodle. Através dele, os alunos acessam conteúdos explicativos sobre como configurar os ambientes de programação de CLPs e desenvolvimento de sistemas SCADA, como acessar remotamente a planta didática e as especificações técnicas dos dispositivos, conforme Figura 17.

Figura 17 – Ambiente Moodle com instruções sobre a disciplina e os equipamentos.

Fonte: Próprio autor (2017).

A última ferramenta de apoio ao laboratório instalada no servidor é útil para os administradores do sistema e para os usuários. Ela registra as informações sobre cada sessão, como o usuário ao qual o aluno se conectou, os horários de início e fim de cada sessão, o tempo de duração de cada conexão, IP e nome de usuário do cliente. Essa ferramenta é o UserLock, um software tem suporte para web, e por onde os alunos conseguem consultar pelo endereço <http://sel0431.ddns.net/uladmin> se o usuário padrão que ele deseja acessar está desocupado. Caso esteja, o aluno se conecta ao ambiente do servidor, como na Figura 18; caso contrário, ele recebe uma mensagem negando a conexão.

Figura 18 – Desktop do servidor virtualizado em uma máquina com Windows 10.

Fonte: Próprio autor (2017).

Caso o aluno queira agendar uma conexão, ele deve contatar o administrador do sistema. Os próprios scripts de gerenciamento de acesso permitem com que conexões sejam agendadas por um período máximo de 2 horas.

Em resumo, os alunos se conectam à VPN quando suas máquinas estão em uma rede externa à USPNet, por meio de um aplicativo gratuito, para então se conectarem ao servidor do laboratório, por meio de outro aplicativo baseado no protocolo RDP. Além do ambiente virtual com os programas necessários, eles monitoram em tempo real seus experimentos e podem requisitar ao tutor da disciplina o agendamento de um acesso.

3.3.4 Segurança a nível físico e de aplicação

A segurança da aplicação é aplicada em diversos níveis, desde a camada física por meio do CLP de segurança à camada de aplicação por meio do aplicativo Cisco AnyConnect. A Tabela 9 resume todas as medidas aplicadas neste projeto.

Tabela 9 – Resumo das medidas de segurança implementadas no laboratório remoto.

Componente do laboratório remoto	Medidas
Cisco AnyConnect	*Autenticação para acesso à VPN *Mensagens encapsuladas com o protocolo IPsec
Zona desmilitarizada	*Firewall da própria infraestrutura de rede da USP
Servidor RDP	*Autorização *Política de acesso dos usuários padrão aos recursos da máquina *Monitoramento de conexões
Planta didática	*CLP dedicado à segurança dos equipamentos da planta

Fonte: Próprio autor (2018).

3.4 MÉTODO PARA AVALIAÇÃO DO DESEMPENHO TÉCNICO DOS ALUNOS

Este trabalho analisa os efeitos da implementação do laboratório remoto sob duas ópticas diferentes: a dos alunos e a dos tutores da disciplina. No primeiro caso, os usuários do laboratório remoto avaliam a ferramenta de acordo com vários aspectos, como facilidade de uso, de conexão e de aquisição dos dados, enquanto no segundo caso, o autor deste trabalho compara os desempenhos dos alunos em 2016, quando o laboratório era exclusivamente presencial, e em 2017, com a adição do laboratório remoto. As métricas são as seguintes:

- a) Tempo médio para conclusão das práticas;
- b) Desempenho na disciplina de acordo com a avaliação dos relatórios.

Quanto ao item b), em 2016 e em 2017 os relatórios foram avaliados por pessoas diferentes, portanto, o autor deste trabalho coletou todos eles e estipulou o mesmo critério

para corrigi-los novamente. O critério do autor considera quais etapas cada grupo concluiu, considerando cada projeto em particular e, ao todo, são 3: as etapas básicas, os objetivos principais e as tarefas extra propostas durante as práticas. Cada projeto tem as suas próprias etapas, descritas na Tabela 10, porém todas são avaliadas qualitativamente neste trabalho e 3 avaliações são possíveis: a etapa não foi concluída, foi concluída em partes, ou foi totalmente concluída. Os resultados e discussões a respeito da avaliação segundo este critério são apresentados no subcapítulo 4.1.1.

Tabela 10 – Etapas de cada projeto, segundo os critérios adotados neste trabalho.

Projeto	Etapas
1 (Vazão)	*Básico: Mapeamento das entradas, saídas e protocolos de comunicação com o CLP *Objetivo principal: configurar o ambiente de programação e escrever uma aplicação funcional para ambos os modos de controle *Objetivo extra: comparar e ajustar os ganhos do controlador
2 (Temperatura)	*Básico: Mapeamento das entradas, saídas e protocolos de comunicação com o CLP *Objetivo principal: configurar o ambiente de programação e escrever uma aplicação funcional para ambos os modos de controle *Objetivo extra: controlar a temperatura da água no reservatório 2
3 (Nível)	*Básico: Mapeamento das entradas, saídas e protocolos de comunicação com o CLP *Objetivo principal: configurar o ambiente de programação e escrever uma aplicação funcional para ambos os modos de controle *Objetivo extra: controlar o nível de ambos os reservatórios
4 (Supervisório)	*Básico: estabelecer comunicação entre a aplicação e os CLPs da planta *Objetivo principal: desenvolver um sistema SCADA que lesse as variáveis de processo de todos os CLPs *Objetivo extra: gerar relatórios e gráficos de tendência na aplicação

Fonte: Próprio autor (2018).

3.5 MÉTODO PARA AVALIAÇÃO DO USO DO LABORATÓRIO REMOTO

A avaliação da implementação do laboratório remoto pelos estudantes é feita através de um questionário envolvendo perguntas e sentenças de naturezas diferentes, que estão divididas em 3 seções. A primeira seção é a identificação do grupo ao qual o aluno pertence; a segunda seção é composta majoritariamente por afirmações onde o aluno escolhe uma nota de 0 a 10, onde 0 representa que ele discorda totalmente da afirmação, e 10 indica que ele concorda totalmente. Questões e questionários dessa natureza são do tipo escala de Likert (IANNUCCI et al., 2018). Finalmente, a terceira seção está aberta a sugestões e críticas ao laboratório remoto.

O questionário com as sentenças está no subcapítulo 4.2, o qual apresenta e disserta sobre o ponto de vista dos alunos sobre a ferramenta, e segue o modelo aplicado em outros trabalhos que coletam opiniões dos alunos sobre o uso do laboratório, como Chevalier et al. (2017), que compara as visões dos discentes por três anos consecutivos para medir o efeito da aplicação de um laboratório remoto a uma turma de engenharia.

4 RESULTADOS E DISCUSSÕES

O capítulo 4 está dividido em dois subcapítulos principais: o primeiro demonstra o impacto da ferramenta no processo de aprendizagem de controle de processos industriais; o segundo, a visão discente sobre a implementação do laboratório remoto. Esse ponto de vista é importante porque expõe os pontos de melhorias da ferramenta e ajudam a proporcionar uma experiência melhor para as turmas dos próximos anos. As sugestões são coletadas e discutidas no capítulo 6.

4.1 EFEITOS DA IMPLEMENTAÇÃO DO LABORATÓRIO REMOTO

Os subcapítulos 4.1.1, 4.1.2 e 4.1.3 exibem métricas que auxiliam este trabalho a concluir como a implementação do laboratório remoto influencia na dinâmica de uma disciplina prática de controle de processos industriais. Em 4.1.1 e 4.1.3 há uma comparação entre os desempenhos dos alunos nas turmas de 2016 e 2017 quanto a entrega dos projetos e tempo de conclusão de curso que torna explícito o efeito da adição de tal ferramenta. Esse monitoramento é feito após o final de cada entrega de projeto, então o autor observou a evolução dos grupos ao longo do semestre em ambos os anos. O subcapítulo 4.1.2 não tem o intuito de comparar os grupos de diferentes turmas, mas de mostrar a aceitação ou não pelos alunos de uma ferramenta nova para a disciplina.

4.1.1 Comparação do desempenho acadêmico dos estudantes

Este trabalho adota um critério diferente daqueles adotados pelos responsáveis da disciplina em 2016 e 2017 para avaliar o desempenho dos grupos. Originalmente, os relatórios técnicos foram avaliados por pessoas diferentes seguindo critérios distintos em ambos os anos. Eles recebiam uma nota que varia de 0 a 10 de acordo com o conteúdo que os grupos apresentavam. Neste caso, o conteúdo também é o principal ponto de avaliação, contudo, a nota é quantitativa e o critério é unificado para as turmas.

A Tabela 10 divide cada projeto em 3 etapas, e cada etapa é um conjunto de tarefas que os grupos precisam concluir para finalizar uma parte do projeto. Caso o grupo

não tenha finalizado uma tarefa sequer, a etapa é considerada não concluída; caso parte das tarefas tenham sido concluídas, a etapa é considerada parcialmente concluída; caso todas as tarefas tenham sido finalizadas, a etapa é avaliada como totalmente atingida.

O gráfico da Figura 19 mostra a evolução dos grupos ao longo do semestre, contabilizando o número total de etapas básicas, principais e extras concluídas por semana em 2016 e 2017. O eixo vertical representa o número de relatórios, ao todo são 8 por semana, enquanto o eixo horizontal, o número de etapas básica, principal e extra que foram concluídas totalmente, parcialmente ou não foram concluídas.

Figura 19 – Comparação do desempenho dos grupos quanto à entrega das tarefas nos projetos em 2016 e 2017.

Fonte: Próprio autor (2018).

O autor faz a mesma correlação demonstrada no gráfico anterior para cada projeto, como mostra a Figura 20. O eixo vertical representa o número de relatórios e o eixo horizontal, o número de etapas básicas, principais e extras concluídas ou não.

Figura 20 – Desempenho dos grupos em cada um dos projetos em 2016 e 2017.

Fonte: Próprio autor (2018).

Comparando os desempenhos dos grupos na Figura 19, observa-se que o desempenho geral de ambas as turmas melhora ao longo do semestre. Nas primeiras semanas, as turmas se adaptam aos equipamentos e programas para configuração das aplicações ladder e SCADA e enfrentam desafios até então novos para elas. O volume

de dúvidas é maior e os grupos consomem mais tempo superando eventuais obstáculos que aparecem durante o desenvolvimento dos projetos, portanto, algumas etapas não são concluídas.

Contudo, conforme os alunos ganham experiência ao trabalhar com o equipamento, eles interagem entre si e fazem, em alguns momentos, o papel de facilitadores para outros alunos ajudando os tutores da disciplina. Isso é uma característica da abordagem PBL e ajudar a explicar a melhora no desempenho geral ao longo do semestre. A quantidade de perguntas durante as aulas tende a diminuir e os grupos trabalham de forma mais autônoma, sem depender exclusivamente dos tutores para esclarecer dúvidas.

Comparando os desempenhos entre os anos, este trabalho expõe uma melhora nas turmas de 2017. Todas as etapas principais foram concluídas e os alunos fizeram experimentos mais complexos com a planta, logo, apresentaram resultados mais completos. A melhoria na documentação sobre os equipamentos e nos tutoriais em 2017 facilitou o desenvolvimento dos projetos também.

A implementação do laboratório remoto foi um fator importante para que os grupos entregassem resultados mais elaborados ao final dos projetos. Enquanto que, em 2016, somente o horário de aula era disponível para que eles entendessem o funcionamento do equipamento, esclarecem dúvidas, realizassem testes e superassem obstáculos, em 2017, havia mais tempo disponível para cumprir alguns passos e o local não era restrito ao laboratório.

Outro aspecto importante da implementação do laboratório remoto é que cada aluno possui seu próprio ambiente de trabalho. Durante as aulas práticas, os grupos se dividiram em passos bem definidos para entregar o projeto dentro do prazo, portanto, cada aluno tinha uma função específica, ao passo que, com a ferramenta de acesso à distância, cada aluno pode cumprir todos os passos: estudar o funcionamento dos dispositivos, configurar o software de programação de CLP e realizar testes com as malhas de controle. Portanto, a experiência individual na disciplina é mais completa. Cada pessoa de um grupo pode realizar seus próprios experimentos e debater com o grupo durante a aula presencial, ou não precisa esperar uma semana para remover impedimentos do projeto.

Nesse sentido, há um ponto de melhoria para avaliar as próximas turmas: aplicar testes individuais para medir o conhecimento de cada aluno durante o semestre. Alguns autores, além da avaliação grupal, aplicam testes antes do início da disciplina e após seu término para medir a evolução no aprendizado de cada pessoa.

4.1.2 Quantidade de acessos realizados durante o semestre

O uso do acesso remoto à planta industrial não é obrigatório para os alunos. O uso do equipamento ocorre pela necessidade em terminar etapas do projeto, pela curiosidade em trabalhar com uma ferramenta nova ou pela comodidade em poder trabalhar em um ambiente virtualizado individual. Este trabalho mediu o volume do uso do laboratório remoto ao longo do semestre através do programa UserLock, e a Figura 21 mostra o número de acessos ao longo das semanas pelos alunos. Os alunos tiveram 14 semanas úteis para concluir a disciplina, contudo, na 7ª e 10ª semanas houve feriado na sexta, e o laboratório ficou indisponível.

Figura 21 – Quantidade de acessos remotos à planta por semana.

Fonte: Próprio autor (2018).

Ao todo, foram registrados 57 acessos de 15 máquinas diferentes, uma média de quase 4 acessos por máquina. O número de acessos aumentou consideravelmente ao longo do semestre e dois fatores explicam esse crescimento. O primeiro é que a ferramenta de acesso remoto foi submetida a testes-piloto no início da disciplina, portanto, algumas das suas ferramentas como o sistema supervisorio online e o gerenciamento e visualização de acessos ao servidor foram consolidados a partir da segunda semana.

Outro fator é a prioridade de escolha dos alunos. No início do semestre, a maior necessidade dos grupos é entender o funcionamento da unidade industrial e realizar os primeiros testes com as malhas de controle o sistema SCADA. Os alunos preferem fazê-lo presencialmente, pois sentem que há o controle de fato sobre a operação da planta. Quando eles não concluem as etapas dentro do tempo esperado ou querem realizar um experimento individualmente, eles utilizam o laboratório remoto. Portanto, ao ganhar confiança em acessar presencialmente a planta, os grupos começaram a diluir suas atividades entre horário de aula e experimentos a distância.

Em média, cada acesso durou 38 minutos, e a maioria deles foi direcionada ao usuário NIVEL, com 22 acessos, seguido pelos usuários VAZAO, SUPERVISAO e TEMPERATURA, com 16, 12 e 7 acessos, respectivamente. Há uma correlação entre o número de projetos com objetivos concluídos, conforme a Figura 22, e o número de acessos. Os projetos em que os grupos apresentaram melhor desempenho tiveram menos acessos, portanto, é possível comparar qual o grau de dificuldade técnica de cada projeto. A lista com os acessos à planta está presente no apêndice B.

4.1.3 Comparação dos tempos de conclusão dos projetos

A métrica apresentada por este subcapítulo também tem caráter comparativo. Uma das motivações para este trabalho foi flexibilizar o tempo e o local de trabalho dos alunos, de modo a evitar que eles ultrapassassem o prazo de entrega dos projetos. Como o início de projeto de um grupo depende que o grupo anterior o tenha terminado, o atraso na entrega prejudica o andamento de toda a disciplina. Este trabalho mediu os tempos de conclusão médios de cada projeto em ambos os anos, e obteve a Figura 22.

Figura 22 – Tempo médio de conclusão das práticas em 2016 e 2017.

Fonte: Ferreira, Brandão e Tietz (2018).

O tempo médio para concluir a disciplina foi reduzido em 0,4 semanas, em média. Em ambos os anos, este tempo naturalmente diminui porque os grupos se auto-organizam para solucionar problemas e aprender a trabalhar com os equipamentos e programas. Em 2017, em relação a 2016, esse decréscimo ocorreu pelos mesmos motivos pelos quais o desempenho dos alunos melhorou: documentos melhorados sobre a unidade industrial e a não-restrição à sala de aula para concluir os objetivos. A diminuição no tempo para conclusão dos projetos pelas turmas de 2017 é mais notória nas rodadas finais, as quais apresentaram mais acessos remotos.

A introdução da ferramenta como suporte à disciplina, portanto, teve um impacto geral positivo no desempenho dos grupos e no processo de aprendizagem prática de controle de processos industriais.

4.2 RESULTADOS DA AVALIAÇÃO DOS ALUNOS SOBRE O LABORATÓRIO REMOTO

O professor e monitor da disciplina aplicam, ao final de cada projeto, um questionário para os alunos avaliarem o uso do laboratório remoto quanto a vários

aspectos. O mesmo aluno responde o mesmo questionário para avaliar projetos diferentes porque eles possuem etapas, obstáculos e objetivos diferentes. Ao todo foram registradas 39 respostas diferentes e elas são resumidas pela Tabela 11. As questões baseadas na escala Likert têm o número de vezes que cada nota foi marcada e uma média ponderada no final, enquanto que, para as questões dissertativas, as três respostas mais relevantes são mostradas.

Tabela 11 – Questionário de avaliação do uso do laboratório remoto com o resumo das respostas.

Identificação	Qual é o seu projeto?	1 (vazão)			2 (temperatura)			3 (nível)			4 (supervisão)		
		10			6			15			8		
	Dia da turma	Quarta-feira						Quinta-feira					
Questões de múltipla escolha	1. É a sua primeira experiência com laboratório remoto?	22						17					
		Não						Sim					
		0						39					
	2. A disponibilidade de tempo e local para realizar as práticas aumentou com a introdução do laboratório remoto.	0	1	2	3	4	5	6	7	8	9	10	Média
		0	0	0	0	0	0	1	5	11	14	8	8,6
	3. Você se sente mais seguro operando a planta remotamente.	2	1	2	3	5	9	8	3	3	1	2	5,2
	4. Os programas e tutoriais são fáceis de acompanhar.	0	0	0	0	0	0	0	3	6	12	18	9,2
	5. É fácil se conectar à planta via acesso remoto.	0	0	0	0	0	0	0	2	5	14	18	9,2
	6. É fácil obter os dados da planta e observar o que está acontecendo.	0	0	0	0	1	4	5	12	8	6	3	7,3
	7. Tenho a sensação de controle sobre meu experimento, e não tive dificuldades em operar e interagir com a planta, mesmo remotamente	0	0	0	0	0	2	4	11	12	4	6	7,8
	8. Senti-me motivado a realizar o experimento prático proposto com a planta via acesso remoto.	0	0	0	0	0	0	0	2	12	10	15	9,0
9. Senti-me confortável/confiante em operar a planta didática mesmo a distância	0	0	0	0	0	0	3	6	8	12	10	8,5	

	10. O acesso remoto foi útil para conclusão do projeto.	0	0	0	0	0	0	2	7	6	14	10	8,6
	11. Eu recomendo a implementação de laboratórios remotos para outras disciplinas práticas.	0	0	0	0	0	0	0	1	7	17	14	9,1
	12. Minha experiência com o laboratório remoto foi proveitosa. Contribuiu para o meu aprendizado.	0	0	0	0	0	1	3	5	11	12	7	8,3
Questões abertas		3 respostas mais comuns											
	13. Quais as vantagens de usar a ferramenta de acesso remoto?	*Ferramenta simples e ajudou a agilizar a conclusão da prática. *Não é preciso instalar software pago. *Mobilidade para realizar a prática e facilidade de acesso.											
	14. Quais as desvantagens de usar a ferramenta de acesso remoto?	*Dificuldade de mudar algumas variáveis da planta, como os botões. *Falta de interação com o grupo e o professor. *Dificuldade em interagir com a planta porque alguns detalhes não estão disponíveis para se observar.											
	15. Sugestões adicionais.	*Melhorar a qualidade e aumentar a quantidade de webcams. *Tornar a planta acessível por mais tempo. *Facilitar a mudança de estado dos botões do painel.											

Fonte: Próprio autor (2018).

As maiores notas dadas pelos alunos são nos quesitos de facilidade de acesso, flexibilidade para uso da planta e utilidade para esta e outras disciplinas. Os alunos envolvidos neste curso estão matriculados em outras disciplinas práticas, nas quais eles encaram os mesmos problemas: limitação de tempo, recursos físicos ou recursos humanos para auxiliá-los a concluir suas práticas. Os alunos estão restritos a experimentos com equipamentos físicos em horários e locais determinados, em turmas numerosas, onde eles precisam gerenciar quem é responsável por qual tarefa.

A implementação de uma plataforma baseada em aplicações gratuitas e utilizando a infraestrutura de rede da própria universidade lida com alguns obstáculos de cursos experimentais, proporciona ao aluno uma réplica do laboratório físico em sua própria máquina e os estimula a explorar mais a fundo e/ou menos tempo os recursos do laboratório. Devido a tais vantagens, a questão foi avaliada com nota 9,1.

Neste caso, a disciplina SEL0431 adotou uma abordagem híbrida porque tanto o laboratório presencial quanto o remoto foram adotados. Em laboratórios exclusivamente remotos, há alguns pontos de atenção para não prejudicar a experiência do usuário, e

estes pontos foram indicados pelos alunos no questionário. Apesar das ferramentas adicionais permitirem com que os alunos visualizem os dados da planta em tempo real, a facilidade em obter informação é limitada, pois as webcams focam em pontos específicos da planta, que são o painel, os reservatórios e o transmissor volumétrico. Em comparação com o laboratório presencial, a sensação de controle e interação com os equipamentos é menor.

Trabalhar com chaves e elementos comutados manualmente foi outra dificuldade relatada pelos estudantes. Ainda que os softwares de configuração do CLPs permitissem que os alunos mudassem o estado dos botões, esta não é uma tarefa intuitiva, exigiu um tutorial a mais e é mais complexa que simplesmente girar uma chave. Para as práticas envolvendo sistemas SCADA e o controle automático das malhas o desenvolvimento não foi prejudicado.

Finalmente, há uma característica de disciplinas cursadas presencialmente que é a interação entre pessoas. Há trabalhos que implementam chat online e fóruns de discussão em ambientes virtuais de aprendizagem, contudo, a troca de experiência e conhecimento em tempo real durante a execução dos testes é mais intensa nos laboratórios presenciais.

De maneira geral, o laboratório trouxe impactos positivos para o processo de aprendizagem dos alunos, colocou-os em contato com uma das tecnologias que compõem o novo movimento de revolução industrial e recebeu uma avaliação positiva dos discentes. O processo representado pela Figura 8 é iterativo, e cabe aos responsáveis pelo desenvolvimento do laboratório remoto analisarem as sugestões dos aprendizes, estudarem o estado da arte em laboratórios experimentos à distância e implementarem alterações para os próximos anos.

5 CONCLUSÕES

Neste capítulo, o autor apresenta as considerações finais sobre a implementação do laboratório remoto em uma disciplina prática de controle de processos industriais, e também reserva um subcapítulo para discutir melhorias para esta ferramenta a partir da experiência de uso dos alunos.

Este trabalho apresentou uma nova abordagem pedagógica para uma disciplina no campus e também utilizou tecnologias e arquitetura diferentes das soluções utilizadas por outros laboratórios remotos, mas ainda baseada em aplicações gratuitas. Enquanto a maioria destes é baseada em web services e portais online, esta solução providencia controle maior dos alunos às aplicações instaladas diretamente na máquina servidora, contudo, sem deixar de aplicar políticas de segurança. A solução é baseada no protocolo remoto RDP sobre a VPN da Universidade, ferramentas adicionais de suporte ao uso do laboratório e técnicas de segurança implementadas em todas as camadas da arquitetura da solução.

As razões principais pelas quais esta ferramenta foi desenvolvida e implementada foram a necessidade dos alunos de lidar com restrições de tempo, local, orçamento e recursos físicos para aprender na prática os conceitos de controle de processos industriais e a tendência da indústria em se adaptar à nova realidade de Indústria 4.0, e assim exigir com que seus profissionais tenham contato com tecnologias de acesso remoto.

O uso de laboratórios remotos vem substituindo ou se mesclando com os laboratórios tradicionais, com a vantagem de que os estudantes não precisam de diversas máquinas físicas, licenças custosas ou mesmo um laboratório espaçoso. Basta um equipamento físico no laboratório, sua própria máquina e uma infraestrutura que o permita conectar-se de forma segura ao laboratório para que o aluno tenha um ambiente individual para aprender através de experimentos.

A solução que este trabalho detalha é replicável a qualquer disciplina que tenha algum equipamento com acesso a rede. Ainda que os únicos dispositivos com interface de rede na planta sejam os CLPs, isso não impossibilita o acesso às suas variáveis pela

rede externa. Neste caso, o gateway entre planta e rede WAN é um notebook do laboratório, contudo, poderia ser um microcomputador, como a Raspberry Pi.

Outra possibilidade é ampliar o número de alunos que a disciplina comporta ou mesmo torna-la acessível a alunos de outras universidades, como é o caso dos sistemas de gerenciamento de laboratórios remotos. Porém, algumas mudanças na solução seriam necessárias. A primeira é adotar uma ferramenta de agendamento automático, independente do administrador do sistema, visto que atualmente os usuários só conseguem visualizar quem está acessando o servidor. A segunda é tornar a solução independente da infraestrutura de rede da USP, e para isso, soluções de VDI são recomendáveis, devido a sua escalabilidade. Finalmente, implementar melhorias sugeridas pelos alunos que tornem a experiência com o laboratório remoto próxima à experiência com um laboratório presencial. Essas sugestões variam desde melhorar aspectos básicos, como a obtenção de dados e manipular manualmente alguns dispositivos, a implementar aplicações por onde os alunos do mesmo grupo ou de grupos distintos e tutores possam se comunicar e trocar informações.

O laboratório remoto é uma ferramenta que auxiliou na aprendizagem dos alunos e, combinada com as vantagens do laboratório presencial, é uma abordagem recomendada a outras disciplinas experimentais. Os estudantes cursam uma quantidade grande de disciplinas por semestre e o apoio de outras iniciativas como esta podem contribuir para uma experiência mais completa em um curso. Toda a literatura e implementação desenvolvidas em torno do laboratório não são a finalidade deste trabalho, mas o meio de demonstrar como ele impacta positivamente na aprendizagem ao longo do semestre.

5.1 SUGESTÕES DE TRABALHOS FUTUROS

Este trabalho propõe uma melhoria contínua da solução de acesso remoto apresentada. Para a próxima turma, as mudanças com maior grau de prioridade são:

- a) Melhorar a qualidade de visualização da planta didática e obtenção dos seus dados. Para isso, recomenda-se aumentar o número de câmeras ou adquirir

câmeras de qualidade melhor, focar a imagem na planta como um todo e mostrar outros pontos importantes da planta, como os inversores de frequência;

- b) Tornar o acesso remoto disponível em outros dias. Atualmente, os alunos utilizam o laboratório remoto somente às sextas;
- c) Utilizar alguma plataforma, como a do sistema supervisório redundante, para permitir o acionamento dos elementos manuais da planta de forma mais intuitiva;
- d) Aplicar testes pré e pós-laboratório para medir a evolução individual dos alunos. Atualmente, só há avaliação em grupo e isso mascara o desempenho particular de cada aluno para o desenvolvimento do projeto;
- e) Implementar uma ferramenta de agendamento automático online;
- f) Implementar ferramentas de comunicação em tempo real, como chats online.

Há ainda outras sugestões a longo prazo que permitam utilizar este e outros laboratórios remotos por turmas maiores e de universidades diferentes:

- a) Tornar a solução independente da infraestrutura de rede de computadores da USP. Isso limita o uso da planta a estudantes vinculados à universidade;
- b) Criar um repositório de laboratórios remotos, como o MIT iLAB, porém aplicando uma arquitetura de solução apropriada a portais online;
- c) Mudar a arquitetura da solução de forma a torna-la mais escalável. Por exemplo, o uso de plataformas de computação em nuvem para implementar VDI tornam a solução independente da rede privada da Universidade e podem manter o uso de protocolos como o RDP para acesso a instâncias do ambiente do servidor.

Portanto, este subcapítulo aborda diferentes aspectos de alterações cabíveis a este trabalho. Desde incrementar a forma de avaliação da disciplina e melhorar a experiência de uso do laboratório remoto a mudar sua arquitetura de forma a torna-lo escalável.

REFERÊNCIAS BIBLIOGRÁFICAS

ALAGAPPAN, Annamalai; VENKATARAMAN, Sivakumar; SIVAKUMAR, Subitha. Virtual Desktop Infrastructure for Rendering Education Technology In Multifaceted Learning Platforms – A Case Study at Botho University. In: **IEEE International Conference on Signal Processing, Communication, Power and Embedded System**, 2016, India, p. 1717-1720.

ALVES, L. F.; BRANDÃO D.; TIETZ, F. Desenvolvimento de Laboratório Remoto para Suporte ao Ensino de Controle de Processos Industriais para Estudantes de Engenharia Elétrica. In: CONGRESSO INTERNACIONAL DE EDUCAÇÃO E TECNOLOGIAS, 4., Julho 2018. **Anais...** São Carlos, Brasil, 2018.

ANGULO, Ignacio; RODRIGUEZ-GIL, Luis; GARCIA-ZUBIA, Javier. Scaling up the Lab: An Adaptable and Scalable Architecture for Embedded Systems Remote Labs. **IEEE Access**, [s.l.], v. 6, p.16887-16900, 2018. Institute of Electrical and Electronics Engineers (IEEE). <http://dx.doi.org/10.1109/access.2018.2812925>.

ALVES, Luiz F; BRANDÃO, Dennis; A OLIVEIRA, Marcelo. A multi-process pilot plant as a didactical tool for the teaching of industrial processes control in electrical engineering course. **International Journal Of Electrical Engineering Education**, [s.l.], 9 jul. 2018. SAGE Publications. <http://dx.doi.org/10.1177/0020720918787455>.

BELLMUNT, O. G. et al. A Distance PLC Programming Course Employing a Remote Laboratory Based on a Flexible Manufacturing Cell. **IEEE Transactions On Education**, [s.l.], v. 49, n. 2, p.278-284, maio 2006. Institute of Electrical and Electronics Engineers (IEEE). <http://dx.doi.org/10.1109/te.2006.873982>.

BUYYA, Rajkumar; DASTJERDI, Amir Vahid. Internet of Things Principles and Paradigms. Cambridge: Morgan Kaufmann, 2016. 380 p.

CAMINERO, Agustin C. et al. VirTual remoTe labORatories Management System (TUTORES): Using Cloud Computing to Acquire University Practical Skills. **IEEE Transactions On Learning Technologies**, [s.l.], v. 9, n. 2, p.133-145, 1 abr. 2016. Institute of Electrical and Electronics Engineers (IEEE). <http://dx.doi.org/10.1109/tlt.2015.2470683>.

CHEVALIER, Amelie et al. A Three-Year Feedback Study of a Remote Laboratory Used in Control Engineering Studies. **IEEE Transactions On Education**, [s.l.], v. 60, n. 2, p.127-133, maio 2017. Institute of Electrical and Electronics Engineers (IEEE). <http://dx.doi.org/10.1109/te.2016.2605080>.

EFSTRATIA, Douladeli. Experiential Education through Project Based Learning. **Procedia - Social And Behavioral Sciences**, [s.l.], v. 152, p.1256-1260, out. 2014. Elsevier BV. <http://dx.doi.org/10.1016/j.sbspro.2014.09.362>.

ENCALADA, Washington; SEQUERA, José. Model to Implement Virtual Computing Labs via Cloud Computing Services. **Symmetry**, [s.l.], v. 9, n. 7, p.117-131, 13 jul. 2017. MDPI AG. <http://dx.doi.org/10.3390/sym9070117>.

FERNANDES, Marcelo Ac. Project-based learning applied to an embedded systems course. **International Journal Of Electrical Engineering Education**, [s.l.], v. 54, n. 3, p.223-235, 5 dez. 2016. SAGE Publications. <http://dx.doi.org/10.1177/0020720916675830>.

FERRATER-SIMON, Coia et al. A Remote Laboratory Platform for Electrical Drive Control Using Programmable Logic Controllers. **IEEE Transactions On Education**, [s.l.], v. 52, n. 3, p.425-435, ago. 2009. Institute of Electrical and Electronics Engineers (IEEE). <http://dx.doi.org/10.1109/te.2008.930095>.

GEANEY, Gerard; O'MAHONY, Tom. Design and evaluation of a remote PLC laboratory. **International Journal Of Electrical Engineering Education**, [s.l.], v. 53, n. 3, p.212-223, 27 dez. 2015. SAGE Publications. <http://dx.doi.org/10.1177/0020720915622468>.

IANNUCCI, Leonardo et al. IHomeX: An Internet-Enabled Laboratory for Long-Term Experiment Management. **IEEE Transactions On Instrumentation And Measurement**, [s.l.], v. 67, n. 5, p.1142-1149, maio 2018. Institute of Electrical and Electronics Engineers (IEEE). <http://dx.doi.org/10.1109/tim.2017.2786740>.

IONESCU, Clara M. et al. A Remote Laboratory as an Innovative Educational Tool for Practicing Control Engineering Concepts. **IEEE Transactions On Education**, [s.l.], v. 56, n. 4, p.436-442, nov. 2013. Institute of Electrical and Electronics Engineers (IEEE). <http://dx.doi.org/10.1109/te.2013.2249516>.

JAGADEESH, R.; SIDDARAJU, C.; RANGANATHA, R. Design and Implementation of an Architecture for a Remotely Operated PLC Laboratory Using Labview. **International Journal Of Mechanical And Production Engineering Research And Development**, [s.l.], v. 8, n. 2, p.419-426, 2018. Transstellar Journal Publications and Research Consultancy Private Limited. <http://dx.doi.org/10.24247/ijmperdapr201847>.

JANA, Gopal C. et al. Enactment of Remote Laboratory Management Model Based on Mobile Cloud Computing. In: **2nd IEEE International Conference on Recent Trends in Electronics Information and Communication Technology (RTEICT)**, 19-20 Maio 2017, India, 1396-1401.

JIMÉNEZ, Robinson; SANCHEZ, Oscar Avies; MAULEDEOX, Mauricio. Remote Lab for Robotics Applications. **International Journal Of Online Engineering (ijoe)**, [s.l.], v. 14, n. 01, p.186-192, 25 jan. 2018. International Association of Online Engineering (IAOE). <http://dx.doi.org/10.3991/ijoe.v14i01.7674>.

KALUZ, Martin et al. A Flexible and Configurable Architecture for Automatic Control Remote Laboratories. **IEEE Transactions On Learning Technologies**, [s.l.], v. 8, n. 3,

p.299-310, 1 jul. 2015. Institute of Electrical and Electronics Engineers (IEEE). <http://dx.doi.org/10.1109/tlt.2015.2389251>.

KIST, Alexander A. et al. Overlay network architectures for peer-to-peer Remote Access Laboratories. **2014 11th International Conference On Remote Engineering And Virtual Instrumentation (rev)**, [s.l.], p.274-280, Fev. 2014. IEEE. <http://dx.doi.org/10.1109/rev.2014.6784274>.

LOPES, Maisa Soares dos Santos et al. Web Environment for Programming and Control of a Mobile Robot in a Remote Laboratory. **IEEE Transactions On Learning Technologies**, [s.l.], v. 10, n. 4, p.526-531, 1 out. 2017. Institute of Electrical and Electronics Engineers (IEEE). <http://dx.doi.org/10.1109/tlt.2016.2627565>.

LEI, Zhongcheng et al. Modular Web-Based Interactive Hybrid Laboratory Framework for Research and Education. **IEEE Access**, [s.l.], v. 6, p.20152-20163, 2018. Institute of Electrical and Electronics Engineers (IEEE). <http://dx.doi.org/10.1109/access.2018.2821713>.

LUTHON, Franck; LARROQUE, Benoit. LaboREM—A Remote Laboratory for Game-Like Training in Electronics. **IEEE Transactions On Learning Technologies**, [s.l.], v. 8, n. 3, p.311-321, 1 jul. 2015. Institute of Electrical and Electronics Engineers (IEEE). <http://dx.doi.org/10.1109/tlt.2014.2386337>.

MELKONYAN, Arsen; AKOPYAN, David; CHEN, Philip. Work in Progress – Real-Time Remote Internet-Based Communication Laboratory. **39th ASEE/IEEE Frontiers in Education Conference**, 18-21 Oct. 2009, San Antonio, USA, p.1-6.

MENDES, Luciano A. et al. Experiment Lab Server Architecture: A Web Services Approach to Supporting Interactive LabVIEW-based Remote Experiments under MIT's iLab Shared Architecture. In: **13th IEEE International Conference on Remote Engineering and Virtual Instrumentation (REV)**, 24-26 Feb. 2016, Madrid, Spain, p. 293-305.

MORAES, Cícero Couto de; CASTRUCCI, Plínio de Lauro. Engenharia de Automação Industrial. 2. ed. Rio de Janeiro: Ltc, 2013. 346 p.

MORIMOTO, Carlos E.; Redes, um guia prático. 2. ed. São José: Gdh Press e Sul Editores, 2011. 448 p.

ORDUÑA, Pablo et al. Adding New Features to New and Existing Remote Experiments through their Integration in WebLab-Deusto. **International Journal Of Online Engineering (ijoe)**, [s.l.], v. 7, n. 2, p.33-39, 19 out. 2011. International Association of Online Engineering (IAOE). <http://dx.doi.org/10.3991/ijoe.v7is2.1774>.

PANDEY, Atul et al. An Automation Framework for Benchmarking and Optimizing Performance of Remote Desktops in the Cloud. **2017 International Conference On High**

Performance Computing & Simulation (hpcs), [s.l.], p.745-752, jul. 2017. IEEE. <http://dx.doi.org/10.1109/hpcs.2017.113>.

PORTNOY, Matthew. **Virtualization Essentials**. Indianapolis: John Wiley & Sons, Inc., 2012. 286 p.

SHYR, Wen-jye; SU, Te-jen; LIN, Chia-ming. Development of Remote Monitoring and a Control System Based on PLC and WebAccess for Learning Mechatronics. **International Journal Of Advanced Robotic Systems**, [s.l.], v. 10, n. 2, p.97-104, fev. 2013. SAGE Publications. <http://dx.doi.org/10.5772/55363>.

SOUPPAYA, Murugiah P; A SCARFONE, Karen. Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security. [s.l.], p.1-53, jul. 2016. National Institute of Standards and Technology. <http://dx.doi.org/10.6028/nist.sp.800-46r2>.

TANENBAUM, Andrew; WETHERALL, David. **Redes de Computadores**. 5. ed. São Paulo: Pearson Prentice Hall, 2011. 582 p.

TAWFIK, Mohamed et al. Laboratory as a Service (LaaS): a Novel Paradigm for Developing and Implementing Modular Remote Laboratories. **International Journal Of Online Engineering (IJOE)**, [s.l.], v. 10, n. 4, p.13-21, 8 jun. 2014. International Association of Online Engineering (IAOE). <http://dx.doi.org/10.3991/ijoe.v10i4.3654>.

VICENTE, Alfredo Gardel et al. Remote Automation Laboratory Using a Cluster of Virtual Machines. **IEEE Transactions On Industrial Electronics**, [s.l.], v. 57, n. 10, p.3276-3283, out. 2010. Institute of Electrical and Electronics Engineers (IEEE). <http://dx.doi.org/10.1109/tie.2010.2041131>.

XU, Lei; JIANG, Chunxiao; WANG, Jian. Information Security in Big Data: Privacy and Data Mining. **IEEE Access**, [s.l.], v. 2, p.1149-1176, 2014. Institute of Electrical and Electronics Engineers (IEEE). <http://dx.doi.org/10.1109/access.2014.2362522>.

APÊNDICE A – SCRIPT PARA GERENCIAMENTO DE ACESSOS REMOTOS AO SERVIDOR

<#

VERSION DATE AUTHOR

1.0 2015-03-10 Tony Pombo
- Initial Release

1.1 2015-03-11 Tony Pombo
- Added enum Rights, and configured functions to use it
- Fixed a couple typos in the help

1.2 2015-11-13 Tony Pombo
- Fixed exception in LsaWrapper.EnumerateAccountsWithUserRight when SID cannot be resolved
- Added Grant-TokenPrivilege
- Added Revoke-TokenPrivilege

1.3 2016-10-29 Tony Pombo
- Minor changes to support Nano server
- SIDs can now be specified for all account parameters
- Script is now digitally signed

1.3.1 2017-02-16 Tony Pombo
- Fixed dash/hyphen typo in Get-AccountsWithUserRight and Get-UserRightsGrantedToAccount

Changed here for the author of this work

#> # Revision History

#Requires -Version 3.0

Set-StrictMode -Version 2.0

Add-Type @'

using System;

namespace PS_LSA

{

using System.ComponentModel;
using System.Runtime.InteropServices;
using System.Security;
using System.Security.Principal;
using LSA_HANDLE = IntPtr;

public enum Rights

{

SeTrustedCredManAccessPrivilege, // Access Credential Manager as a trusted caller
SeNetworkLogonRight, // Access this computer from the network
SeTcbPrivilege, // Act as part of the operating system
SeMachineAccountPrivilege, // Add workstations to domain
SeIncreaseQuotaPrivilege, // Adjust memory quotas for a process
SeInteractiveLogonRight, // Allow log on locally
SeRemoteInteractiveLogonRight, // Allow log on through Remote Desktop Services
SeBackupPrivilege, // Back up files and directories
SeChangeNotifyPrivilege, // Bypass traverse checking
SeSystemtimePrivilege, // Change the system time
SeTimeZonePrivilege, // Change the time zone
SeCreatePagefilePrivilege, // Create a pagefile
SeCreateTokenPrivilege, // Create a token object
SeCreateGlobalPrivilege, // Create global objects

```

SeCreatePermanentPrivilege,    // Create permanent shared objects
SeCreateSymbolicLinkPrivilege, // Create symbolic links
SeDebugPrivilege,              // Debug programs
SeDenyNetworkLogonRight,       // Deny access this computer from the network
SeDenyBatchLogonRight,         // Deny log on as a batch job
SeDenyServiceLogonRight,       // Deny log on as a service
SeDenyInteractiveLogonRight,    // Deny log on locally
SeDenyRemoteInteractiveLogonRight, // Deny log on through Remote Desktop Services
SeEnableDelegationPrivilege,    // Enable computer and user accounts to be trusted for delegation
SeRemoteShutdownPrivilege,      // Force shutdown from a remote system
SeAuditPrivilege,              // Generate security audits
SeImpersonatePrivilege,         // Impersonate a client after authentication
SeIncreaseWorkingSetPrivilege,  // Increase a process working set
SeIncreaseBasePriorityPrivilege, // Increase scheduling priority
SeLoadDriverPrivilege,         // Load and unload device drivers
SeLockMemoryPrivilege,         // Lock pages in memory
SeBatchLogonRight,             // Log on as a batch job
SeServiceLogonRight,           // Log on as a service
SeSecurityPrivilege,           // Manage auditing and security log
SeRelabelPrivilege,            // Modify an object label
SeSystemEnvironmentPrivilege,   // Modify firmware environment values
SeManageVolumePrivilege,       // Perform volume maintenance tasks
SeProfileSingleProcessPrivilege, // Profile single process
SeSystemProfilePrivilege,       // Profile system performance
SeUnsolicitedInputPrivilege,    // "Read unsolicited input from a terminal device"
SeUndockPrivilege,             // Remove computer from docking station
SeAssignPrimaryTokenPrivilege,  // Replace a process level token
SeRestorePrivilege,            // Restore files and directories
SeShutdownPrivilege,           // Shut down the system
SeSyncAgentPrivilege,          // Synchronize directory service data
SeTakeOwnershipPrivilege       // Take ownership of files or other objects
}

[StructLayout(LayoutKind.Sequential)]
struct LSA_OBJECT_ATTRIBUTES
{
    internal int Length;
    internal IntPtr RootDirectory;
    internal IntPtr ObjectName;
    internal int Attributes;
    internal IntPtr SecurityDescriptor;
    internal IntPtr SecurityQualityOfService;
}

[StructLayout(LayoutKind.Sequential, CharSet = CharSet.Unicode)]
struct LSA_UNICODE_STRING
{
    internal ushort Length;
    internal ushort MaximumLength;
    [MarshalAs(UnmanagedType.LPWStr)]
    internal string Buffer;
}

[StructLayout(LayoutKind.Sequential)]
struct LSA_ENUMERATION_INFORMATION
{
    internal IntPtr PSid;
}

internal sealed class Win32Sec
{
    [DllImport("advapi32", CharSet = CharSet.Unicode, SetLastError = true)]

```

```

internal static extern uint LsaOpenPolicy(
    LSA_UNICODE_STRING[] SystemName,
    ref LSA_OBJECT_ATTRIBUTES ObjectAttributes,
    int AccessMask,
    out IntPtr PolicyHandle
);

[DllImport("advapi32", CharSet = CharSet.Unicode, SetLastError = true)]
internal static extern uint LsaAddAccountRights(
    LSA_HANDLE PolicyHandle,
    IntPtr pSID,
    LSA_UNICODE_STRING[] UserRights,
    int CountOfRights
);

[DllImport("advapi32", CharSet = CharSet.Unicode, SetLastError = true)]
internal static extern uint LsaRemoveAccountRights(
    LSA_HANDLE PolicyHandle,
    IntPtr pSID,
    bool AllRights,
    LSA_UNICODE_STRING[] UserRights,
    int CountOfRights
);

[DllImport("advapi32", CharSet = CharSet.Unicode, SetLastError = true)]
internal static extern uint LsaEnumerateAccountRights(
    LSA_HANDLE PolicyHandle,
    IntPtr pSID,
    out IntPtr /*LSA_UNICODE_STRING[]*/ UserRights,
    out ulong CountOfRights
);

[DllImport("advapi32", CharSet = CharSet.Unicode, SetLastError = true)]
internal static extern uint LsaEnumerateAccountsWithUserRight(
    LSA_HANDLE PolicyHandle,
    LSA_UNICODE_STRING[] UserRights,
    out IntPtr EnumerationBuffer,
    out ulong CountReturned
);

[DllImport("advapi32")]
internal static extern int LsaNtStatusToWinError(int NTSTATUS);

[DllImport("advapi32")]
internal static extern int LsaClose(IntPtr PolicyHandle);

[DllImport("advapi32")]
internal static extern int LsaFreeMemory(IntPtr Buffer);
}

internal sealed class Sid : IDisposable
{
    public IntPtr pSid = IntPtr.Zero;
    public SecurityIdentifier sid = null;

    public Sid(string account)
    {
        try { sid = new SecurityIdentifier(account); }
        catch { sid = (SecurityIdentifier)(new NTAccount(account)).Translate(typeof(SecurityIdentifier)); }
        Byte[] buffer = new Byte[sid.BinaryLength];
        sid.GetBinaryForm(buffer, 0);
    }
}

```



```

        pSid = Marshal.AllocHGlobal(sid.BinaryLength);
        Marshal.Copy(buffer, 0, pSid, sid.BinaryLength);
    }

    public void Dispose()
    {
        if (pSid != IntPtr.Zero)
        {
            Marshal.FreeHGlobal(pSid);
            pSid = IntPtr.Zero;
        }
        GC.SuppressFinalize(this);
    }
    ~Sid() { Dispose(); }
}

public sealed class LsaWrapper : IDisposable
{
    enum Access : int
    {
        POLICY_READ = 0x20006,
        POLICY_ALL_ACCESS = 0x00F0FFF,
        POLICY_EXECUTE = 0X20801,
        POLICY_WRITE = 0X207F8
    }

    const uint STATUS_ACCESS_DENIED = 0xc0000022;
    const uint STATUS_INSUFFICIENT_RESOURCES = 0xc000009a;
    const uint STATUS_NO_MEMORY = 0xc0000017;
    const uint STATUS_OBJECT_NAME_NOT_FOUND = 0xc0000034;
    const uint STATUS_NO_MORE_ENTRIES = 0x8000001a;

    IntPtr IsaHandle;

    public LsaWrapper() : this(null) { } // local system if systemName is null
    public LsaWrapper(string systemName)
    {
        LSA_OBJECT_ATTRIBUTES IsaAttr;
        IsaAttr.RootDirectory = IntPtr.Zero;
        IsaAttr.ObjectName = IntPtr.Zero;
        IsaAttr.Attributes = 0;
        IsaAttr.SecurityDescriptor = IntPtr.Zero;
        IsaAttr.SecurityQualityOfService = IntPtr.Zero;
        IsaAttr.Length = Marshal.SizeOf(typeof(LSA_OBJECT_ATTRIBUTES));
        IsaHandle = IntPtr.Zero;
        LSA_UNICODE_STRING[] system = null;
        if (systemName != null)
        {
            system = new LSA_UNICODE_STRING[1];
            system[0] = InitLsaString(systemName);
        }

        uint ret = Win32Sec.LsaOpenPolicy(system, ref IsaAttr, (int)Access.POLICY_ALL_ACCESS, out IsaHandle);
        if (ret == 0) return;
        if (ret == STATUS_ACCESS_DENIED) throw new UnauthorizedAccessException();
        if ((ret == STATUS_INSUFFICIENT_RESOURCES) || (ret == STATUS_NO_MEMORY)) throw new
OutOfMemoryException();
        throw new Win32Exception(Win32Sec.LsaNtStatusToWinError((int)ret));
    }

    public void AddPrivilege(string account, Rights privilege)
    {
        uint ret = 0;

```

```

using (Sid sid = new Sid(account))
{
    LSA_UNICODE_STRING[] privileges = new LSA_UNICODE_STRING[1];
    privileges[0] = InitLsaString(privilege.ToString());
    ret = Win32Sec.LsaAddAccountRights(IsaHandle, sid.pSid, privileges, 1);
}
if (ret == 0) return;
if (ret == STATUS_ACCESS_DENIED) throw new UnauthorizedAccessException();
if ((ret == STATUS_INSUFFICIENT_RESOURCES) || (ret == STATUS_NO_MEMORY)) throw new
OutOfMemoryException();
throw new Win32Exception(Win32Sec.LsaNtStatusToWinError((int)ret));
}

public void RemovePrivilege(string account, Rights privilege)
{
    uint ret = 0;
    using (Sid sid = new Sid(account))
    {
        LSA_UNICODE_STRING[] privileges = new LSA_UNICODE_STRING[1];
        privileges[0] = InitLsaString(privilege.ToString());
        ret = Win32Sec.LsaRemoveAccountRights(IsaHandle, sid.pSid, false, privileges, 1);
    }
    if (ret == 0) return;
    if (ret == STATUS_ACCESS_DENIED) throw new UnauthorizedAccessException();
    if ((ret == STATUS_INSUFFICIENT_RESOURCES) || (ret == STATUS_NO_MEMORY)) throw new
OutOfMemoryException();
    throw new Win32Exception(Win32Sec.LsaNtStatusToWinError((int)ret));
}

public Rights[] EnumerateAccountPrivileges(string account)
{
    uint ret = 0;
    ulong count = 0;
    IntPtr privileges = IntPtr.Zero;
    Rights[] rights = null;

    using (Sid sid = new Sid(account))
    {
        ret = Win32Sec.LsaEnumerateAccountRights(IsaHandle, sid.pSid, out privileges, out count);
    }
    if (ret == 0)
    {
        rights = new Rights[count];
        for (int i = 0; i < (int)count; i++)
        {
            LSA_UNICODE_STRING str = (LSA_UNICODE_STRING)Marshal.PtrToStructure(
                IntPtr.Add(privileges, i * Marshal.SizeOf(typeof(LSA_UNICODE_STRING))),
                typeof(LSA_UNICODE_STRING));
            rights[i] = (Rights)Enum.Parse(typeof(Rights), str.Buffer);
        }
        Win32Sec.LsaFreeMemory(privileges);
        return rights;
    }
    if (ret == STATUS_OBJECT_NAME_NOT_FOUND) return null; // No privileges assigned
    if (ret == STATUS_ACCESS_DENIED) throw new UnauthorizedAccessException();
    if ((ret == STATUS_INSUFFICIENT_RESOURCES) || (ret == STATUS_NO_MEMORY)) throw new
OutOfMemoryException();
    throw new Win32Exception(Win32Sec.LsaNtStatusToWinError((int)ret));
}

public string[] EnumerateAccountsWithUserRight(Rights privilege)
{

```

```

uint ret = 0;
ulong count = 0;
LSA_UNICODE_STRING[] rights = new LSA_UNICODE_STRING[1];
rights[0] = InitLsaString(privilege.ToString());
IntPtr buffer = IntPtr.Zero;
string[] accounts = null;

ret = Win32Sec.LsaEnumerateAccountsWithUserRight(lsaHandle, rights, out buffer, out count);
if (ret == 0)
{
    accounts = new string[count];
    for (int i = 0; i < (int)count; i++)
    {
        LSA_ENUMERATION_INFORMATION LsaInfo =
(LSA_ENUMERATION_INFORMATION)Marshal.PtrToStructure(
    IntPtr.Add(buffer, i * Marshal.SizeOf(typeof(LSA_ENUMERATION_INFORMATION))),
    typeof(LSA_ENUMERATION_INFORMATION));

        try {
            accounts[i] = (new SecurityIdentifier(LsaInfo.PSid)).Translate(typeof(NTAccount)).ToString();
        } catch (System.Security.Principal.IdentityNotMappedException) {
            accounts[i] = (new SecurityIdentifier(LsaInfo.PSid)).ToString();
        }
    }
    Win32Sec.LsaFreeMemory(buffer);
    return accounts;
}
if (ret == STATUS_NO_MORE_ENTRIES) return null; // No accounts assigned
if (ret == STATUS_ACCESS_DENIED) throw new UnauthorizedAccessException();
if ((ret == STATUS_INSUFFICIENT_RESOURCES) || (ret == STATUS_NO_MEMORY)) throw new
OutOfMemoryException();
throw new Win32Exception(Win32Sec.LsaNtStatusToWinError((int)ret));
}

public void Dispose()
{
    if (lsaHandle != IntPtr.Zero)
    {
        Win32Sec.LsaClose(lsaHandle);
        lsaHandle = IntPtr.Zero;
    }
    GC.SuppressFinalize(this);
}
~LsaWrapper() { Dispose(); }

// helper functions:
static LSA_UNICODE_STRING InitLsaString(string s)
{
    // Unicode strings max. 32KB
    if (s.Length > 0x7ffe) throw new ArgumentException("String too long");
    LSA_UNICODE_STRING lus = new LSA_UNICODE_STRING();
    lus.Buffer = s;
    lus.Length = (ushort)(s.Length * sizeof(char));
    lus.MaximumLength = (ushort)(lus.Length + sizeof(char));
    return lus;
}

}

public sealed class TokenManipulator
{
    [StructLayout(LayoutKind.Sequential, Pack = 1)]
    internal struct TokPriv1Luid

```

```

{
    public int Count;
    public long Luid;
    public int Attr;
}

internal const int SE_PRIVILEGE_DISABLED = 0x00000000;
internal const int SE_PRIVILEGE_ENABLED = 0x00000002;
internal const int TOKEN_QUERY = 0x00000008;
internal const int TOKEN_ADJUST_PRIVILEGES = 0x00000020;

internal sealed class Win32Token
{
    [DllImport("advapi32.dll", ExactSpelling = true, SetLastError = true)]
    internal static extern bool AdjustTokenPrivileges(
        IntPtr htok,
        bool disall,
        ref TokPriv1Luid newst,
        int len,
        IntPtr prev,
        IntPtr relen
    );

    [DllImport("kernel32.dll", ExactSpelling = true)]
    internal static extern IntPtr GetCurrentProcess();

    [DllImport("advapi32.dll", ExactSpelling = true, SetLastError = true)]
    internal static extern bool OpenProcessToken(
        IntPtr h,
        int acc,
        ref IntPtr phtok
    );

    [DllImport("advapi32.dll", SetLastError = true)]
    internal static extern bool LookupPrivilegeValue(
        string host,
        string name,
        ref long pluid
    );

    [DllImport("kernel32.dll", ExactSpelling = true)]
    internal static extern bool CloseHandle(
        IntPtr phtok
    );
}

public static void AddPrivilege(Rights privilege)
{
    bool retVal;
    int lasterror;
    TokPriv1Luid tp;
    IntPtr hproc = Win32Token.GetCurrentProcess();
    IntPtr htok = IntPtr.Zero;
    retVal = Win32Token.OpenProcessToken(hproc, TOKEN_ADJUST_PRIVILEGES | TOKEN_QUERY, ref
htok);
    tp.Count = 1;
    tp.Luid = 0;
    tp.Attr = SE_PRIVILEGE_ENABLED;
    retVal = Win32Token.LookupPrivilegeValue(null, privilege.ToString(), ref tp.Luid);
    retVal = Win32Token.AdjustTokenPrivileges(htok, false, ref tp, Marshal.SizeOf(tp), IntPtr.Zero, IntPtr.Zero);
    Win32Token.CloseHandle(htok);
    lasterror = Marshal.GetLastWin32Error();
}

```

```

        if (lasterror != 0) throw new Win32Exception();
    }

    public static void RemovePrivilege(Rights privilege)
    {
        bool retVal;
        int lasterror;
        TokPriv1Luid tp;
        IntPtr hproc = Win32Token.GetCurrentProcess();
        IntPtr htok = IntPtr.Zero;
        retVal = Win32Token.OpenProcessToken(hproc, TOKEN_ADJUST_PRIVILEGES | TOKEN_QUERY, ref
htok);
        tp.Count = 1;
        tp.Luid = 0;
        tp.Attr = SE_PRIVILEGE_DISABLED;
        retVal = Win32Token.LookupPrivilegeValue(null, privilege.ToString(), ref tp.Luid);
        retVal = Win32Token.AdjustTokenPrivileges(htok, false, ref tp, Marshal.SizeOf(tp), IntPtr.Zero, IntPtr.Zero);
        Win32Token.CloseHandle(htok);
        lasterror = Marshal.GetLastWin32Error();
        if (lasterror != 0) throw new Win32Exception();
    }
}
}
'@ # This type (PS_LSA) is used by Grant-UserRight, Revoke-UserRight, Get-UserRightsGrantedToAccount, Get-
AccountsWithUserRight, Grant-TokenPrivilege, Revoke-TokenPrivilege

```

```

function Grant-UserRight {
    [CmdletBinding()]
    param (
        [Parameter(Position=0, Mandatory=$true, ValueFromPipelineByPropertyName=$true,
ValueFromPipeline=$true)]
        [Alias('User','Username')][String[]] $Account,
        [Parameter(Position=1, Mandatory=$true, ValueFromPipelineByPropertyName=$true)]
        [Alias('Privilege')][PS_LSA.Rights] $Right,
        [Parameter(ValueFromPipelineByPropertyName=$true, HelpMessage="Computer name")]
        [Alias('System','ComputerName','Host')][String] $Computer
    )
    process {
        $lsa = New-Object PS_LSA.LsaWrapper($Computer)
        foreach ($Acct in $Account) {
            foreach ($Priv in $Right) {
                $lsa.AddPrivilege($Acct,$Priv)
            }
        }
    }
} # Assigns user rights to accounts

```

```

function Revoke-UserRight {
    [CmdletBinding()]
    param (
        [Parameter(Position=0, Mandatory=$true, ValueFromPipelineByPropertyName=$true,
ValueFromPipeline=$true)]
        [Alias('User','Username')][String[]] $Account,
        [Parameter(Position=1, Mandatory=$true, ValueFromPipelineByPropertyName=$true)]
        [Alias('Privilege')][PS_LSA.Rights] $Right,
        [Parameter(ValueFromPipelineByPropertyName=$true, HelpMessage="Computer name")]
        [Alias('System','ComputerName','Host')][String] $Computer
    )
    process {
        $lsa = New-Object PS_LSA.LsaWrapper($Computer)
    }
}

```

```

        foreach ($Acct in $Account) {
            foreach ($Priv in $Right) {
                $lsa.RemovePrivilege($Acct,$Priv)
            }
        }
    }
} # Removes user rights from accounts

$flag_temp = 0

while (1)
{
    $Computer = $env:COMPUTERNAME
    $Users = query user /server:$Computer 2>&1

    $Users = $Users | ForEach-Object {
        (($_trim() -replace ">" -replace "(?m)^\s+([A-Za-z0-9]{3,})\s+(\d{1,2})\s+(\w+)", '$1 none $2' -replace "\s{2,}", ", " -
        replace "none", $null))
    } | ConvertFrom-Csv
    foreach ($User in $Users)
    {
        [PSCustomObject]@{
            ComputerName = $Computer
            Username = $User.USERNAME
            SessionState = $User.STATE.Replace("Disc", "Disconnected")
            SessionType = $($User.SESSIONNAME -Replace '#', " " -Replace "[0-9]+", "")
        }
    }
    if ($Users.USERNAME.Contains('temperatura') -and ($flag_temp -eq 1))
    {
        $flag_temp = 0
        Grant-UserRight "Usuario-PC\TEMPERATURA" SeDenyRemoteInteractiveLogonRight
    }
    elseif (-not $Users.USERNAME.Contains('temperatura') -and ($flag_temp -eq 0))
    {
        $flag_temp = 1
        Revoke-UserRight "Usuario-PC\TEMPERATURA" SeDenyRemoteInteractiveLogonRight
    }
    Write-Host($flag_temp)
    Start-Sleep -s 120 #Wait 2 minutes to close a disconnected session
}

```

APÊNDICE B – LISTA DE ACESSOS AO SERVIDOR

Tabela 12 – Lista de acessos, com duração, a cada usuário padrão.

Logon Time	Logoff Time	User Account
01/09/2017 08:35	01/09/2017 09:40	NIVEL
01/09/2017 13:32	01/09/2017 14:02	NIVEL
15/09/2017 10:57	15/09/2017 11:31	VAZAO
15/09/2017 11:29	15/09/2017 11:56	SUPERVISAO
15/09/2017 17:43	15/09/2017 18:45	NIVEL
22/09/2017 12:20	22/09/2017 12:43	NIVEL
22/09/2017 12:41	22/09/2017 13:09	TEMPERATURA
22/09/2017 15:12	22/09/2017 15:39	VAZAO
22/09/2017 17:02	22/09/2017 17:41	NIVEL
06/10/2017 10:12	06/10/2017 10:51	NIVEL
06/10/2017 14:41	06/10/2017 15:30	NIVEL
06/10/2017 12:34	06/10/2017 12:57	VAZAO
20/10/2017 09:59	20/10/2017 10:14	TEMPERATURA
20/10/2017 10:23	20/10/2017 11:01	NIVEL
20/10/2017 13:45	20/10/2017 14:08	TEMPERATURA
20/10/2017 14:20	20/10/2017 14:58	VAZAO
20/10/2017 14:12	20/10/2017 14:42	TEMPERATURA
20/10/2017 14:59	20/10/2017 15:23	VAZAO
27/10/2017 11:17	27/11/2017 11:58	NIVEL
27/10/2017 11:41	27/11/2017 12:10	VAZAO
27/10/2017 13:00	27/11/2017 13:39	NIVEL
27/10/2017 13:34	27/11/2017 14:02	SUPERVISAO
27/10/2017 14:56	27/11/2017 15:27	NIVEL
27/10/2017 16:10	27/11/2017 16:58	NIVEL
27/10/2017 17:03	27/11/2017 17:36	SUPERVISAO
10/11/2017 12:56	10/11/2017 13:21	VAZAO
10/11/2017 13:58	10/11/2017 14:09	NIVEL
10/11/2017 14:54	10/11/2017 15:23	SUPERVISAO
10/11/2017 16:01	10/11/2017 16:32	SUPERVISAO
10/11/2017 16:25	10/11/2017 17:04	VAZAO
10/11/2017 16:42	10/11/2017 17:19	NIVEL
10/11/2017 17:32	10/11/2017 18:00	VAZAO
10/11/2017 17:35	10/11/2017 18:11	SUPERVISAO
17/11/2017 08:57	17/11/2017 09:31	VAZAO
17/11/2017 09:34	17/11/2017 09:58	SUPERVISAO
17/11/2017 10:10	17/11/2017 10:26	SUPERVISAO
17/11/2017 13:46	17/11/2017 14:51	VAZAO
17/11/2017 14:48	17/11/2017 15:35	NIVEL
17/11/2017 15:43	17/11/2017 16:12	SUPERVISAO
17/11/2017 16:43	17/11/2017 17:12	NIVEL

17/11/2017 17:10	17/11/2017 17:32	SUPERVISAO
17/11/2017 17:13	17/11/2017 18:02	NIVEL
20/11/2017 09:43	20/11/2017 10:09	TEMPERATURA
20/11/2017 11:24	20/11/2017 11:56	NIVEL
20/11/2017 11:25	20/11/2017 11:49	TEMPERATURA
20/11/2017 13:50	20/11/2017 14:28	SUPERVISAO
20/11/2017 14:43	20/11/2017 15:36	NIVEL
20/11/2017 15:02	20/11/2017 16:17	VAZAO
20/11/2017 15:41	20/11/2017 16:10	TEMPERATURA
27/11/2017 10:13	27/11/2017 10:54	NIVEL
27/11/2017 10:35	27/11/2017 11:42	VAZAO
27/11/2017 10:57	27/11/2017 11:23	NIVEL
27/11/2017 13:02	27/11/2017 13:47	VAZAO
27/11/2017 13:58	27/11/2017 14:29	VAZAO
27/11/2017 14:22	27/11/2017 15:01	NIVEL
27/11/2017 14:34	27/11/2017 15:06	SUPERVISAO
27/11/2017 15:40	27/11/2017 16:03	VAZAO

Fonte: Próprio autor (2018).