# MODELAGEM FUNCIONAL PRELIMINAR DO LABORATÓRIO DE SEGURANÇA CIBERNÉTICA DE SISTEMAS ELÉTRICOS EM AMBIENTE DE TECNOLOGIA DE INFORMAÇÃO, COMUNICAÇÕES E AUTOMAÇÃO

**Roberto Miranda Gomes**
Cognify Consultoria
Av. Almirante Barroso, 90 - Centro, Rio de Janeiro - RJ, 20031-909
roberto.gomes@cognify.com.br

**José Augusto Sigmund Maciel de Araujo Costa**
2º. CTA
Praça Duque de Caxias, 25 - Urca, Rio de Janeiro - RJ, 20221-260
sigmund@2cta.eb.mil.br

**Cícero Roberto Garcez**
Instituto Militar de Engenharia
Praça Gen. Tibúrcio, 80 - Urca, Rio de Janeiro - RJ, 22290-270
garcez@ime.eb.br

## RESUMO

O objetivo do presente trabalho é elaborar uma modelagem funcional preliminar do Laboratório de Segurança Cibernética de Sistemas Elétricos em Ambiente de Tecnologias de Informação, Comunicação e Automação (LaSC). O Laboratório será ambiente de simulação do tipo *hardware in the loop* incluindo dispositivos físicos industriais que representam infraestruturas críticas na área de Sistemas Elétricos e de Potência e de Tecnologia de Automação. O ambiente de simulação deverá prover condições, nas áreas de Tecnologia da Informação e Comunicação e Segurança Cibernética aplicadas à Tecnologia de Automação de Infraestruturas Críticas, permitindo o desenvolvimento de estudos e análises de segurança cibernética de infraestruturas críticas.

**Palavra-chave:** LaSC; Infraestruturas críticas; Sistemas Elétricos e de Potência; Tecnologia da Automação; Ataques Cíber-físicos; Ameaças Cibernéticas; Segurança Cibernética; Defesa Cibernética.

## ABSTRACT

The objective of the present work is to elaborate a preliminary functional modeling of the Laboratory of Cyber Security of Electrical Systems in Environment of Information, Communication and Automation Technologies (LaSC). The Laboratory will be a hardware in the loop simulation environment including industrial physical devices that represent critical infrastructures in the area of Electrical and Power Systems and Automation Technology. The simulation environment shall provide conditions in the areas of Information and Communication Technology and Cyber Security applied to Critical Infrastructure Automation

Technology, enabling the development of cyber security studies and analysis of critical infrastructures.

**Keywords:** Cybersecurity of Electrical Systems; Automation Technologies; Cyber-Physical Attacks; Cyber Threats; Cyber Security; Cyber Defense.

**Como Citar:**
GOMES, Roberto Miranda; COSTA, José Augusto Sigmund Maciel De Araujo; GARCEZ, Cícero Roberto. Modelagem Funcional Preliminar Do Laboratório De Segurança Cibernética De Sistemas Elétricos Em Ambiente De Tecnologia De Informação, Comunicações E Automação. *In*: SIMPÓSIO DE PESQUISA OPERACIONAL E LOGÍSTICA DA MARINHA, 19., 2019, Rio de Janeiro, RJ. **Anais** […]. Rio de Janeiro: Centro de Análises de Sistemas Navais, 2019.

## 1. INTRODUÇÃO

As sociedades modernas, seja em âmbito nacional ou seja na vida em comunidades menores, como as cidades, dependem de uma espinha dorsal de infraestruturas críticas. Independente do setor, economia, transportes, abastecimentos de energia, água etc., todas essas infraestruturas críticas apoiam parte de suas operações em recursos de tecnologia da informação (TI). Boa parte das operações nas indústrias mencionadas é realizada de maneira descentralizada, a partir de pontos remotos, necessitando de comunicação entre eles. Esta interconexão no mundo moderno se dá por meio das redes de computadores, que são comumente suportadas pela Internet. É importante considerar, para melhor compreensão deste cenário, que o termo computador tem um sentido bastante amplo, abrangendo os mais diversos dispositivos, sensores e atuadores nas mais variadas indústrias.

De forma geral, essas indústrias estão em risco de ataque cibernético malicioso, considerando o cenário de operações apresentado e o consequente aumento da superfície de exposição de seus recursos operacionais. A proteção efetiva contra esses ataques requer soluções flexíveis, capazes de se adaptar a contextos industriais específicos e robustos o suficiente para impedir a presença do adversário mais persistente ou avançado e resilientes para se recuperar, caso o ataque se concretize.

Abordagens para a proteção de infraestrutura crítica, na qual os sistemas de tecnologia da informação (TI) e de tecnologia de automação (TA) sejam gerenciados separadamente tendem a não ser eficientes. Todos os níveis de um ambiente de controle industrial devem ser tratados, desde os dispositivos de interface com os operadores até os ambientes mais estratégicos que contenham dados sensíveis. A defesa contra ataques cibernéticos deve considerar:

- a proteção dos sistemas operacionais ao mesmo tempo que permite conexões seguras e comunicações com sistemas de TA e TI, voltados para a eficiência operacional;
- a movimentação segura de dados entre os sistemas de TA e TI, ainda que fisicamente segregados, reduzindo o risco de comprometimento em ambos;
- a proteção dos sistemas de negócios voltada também para o ser humano, com proteção das pessoas e dados de dispositivos de usuário final.

Problemas de segurança em Sistemas de Controle Industrial (ICS) têm sido noticiados pelo mundo, provocando mudanças em toda a cadeia de fornecimento global. Existe uma necessidade premente de aprendizado sobre falhas, vulnerabilidades,

gerenciamento de risco, resposta a incidentes, recuperação e continuidade do negócio, dentre outros relacionados ao cenário de ameaças cibernéticas em constante mudança.

Ambientes de ICS simulados e interativos proporcionam um ambiente seguro, porém realista, para aquisição de experiências em termos de defesa, preservando a confiabilidade, a integridade e a disponibilidade das operações. Equipamentos de TI e industriais como Controladores Lógicos Programáveis (PLC), Interfaces Homem-Máquina (IHM), Unidades de Telemetria Remota (RTU), atuadores, podem ser integrados para simular um ambiente realista e iterativo de modo a auxiliar os profissionais da área no desenvolvimento de habilidades necessárias para a proteção dos sistemas reais.

O Brasil materializou efetivamente sua preocupação com suas Infraestruturas Críticas quando publicou a Política Nacional de Segurança das Infraestruturas Críticas, pelo Decreto Nº 9.573, de 22 de novembro de 2018, tendo como finalidade "garantir a segurança e a resiliência das infraestruturas críticas do País e a continuidade da prestação de seus serviços" [4].

Anteriormente, o Brasil já havia publicado a Estratégia Nacional de Defesa (END), aprovada em sua primeira versão pelo Decreto Nº 6.703, DE 18 de dezembro de 2008, desenvolvida para, dentre outros objetivos, reorganizar a base industrial de defesa para assegurar o atendimento às necessidades de equipamento das Forças Armadas apoiado em tecnologias sob domínio nacional, preferencialmente as de emprego dual (militar e civil). A END menciona a necessidade de transformação das Forças Armadas para melhor defenderem o Brasil, citando como um de seus princípios a "independência nacional, alcançada pela capacitação tecnológica autônoma, inclusive nos estratégicos setores espacial, cibernético e nuclear" [3].

Ao Exército Brasileiro (EB) foi atribuído o encargo de estruturar o Setor Cibernético. Por meio da Portaria Nº 666, de 4 de agosto de 2010, o EB criou o Centro de Defesa Cibernética (CDCiber) [5] a partir da ativação do Núcleo do Centro de Defesa Cibernética (Nu CDCiber), subordinado ao Departamento de Ciência e Tecnologia, em 02 de agosto de 2010. O Nu CDCiber foi o responsável pela Implantação do Centro, conforme estabelecido na Portaria Nº 667, de 04 de agosto de 2010 [6]. Desde então vários projetos estruturantes foram desdobrados, até que em 2014 o Ministério da Defesa (MD) criou o Comando de Defesa Cibernética (ComDCiber) pela Portaria Nº 2.777/MD, de 27 de outubro de 2014, como uma iniciativa do governo para reforçar a estratégia de defesa cibernética nacional. Segundo a portaria, o Estado-Maior Conjunto das Forças Armadas (EMCFA) ficaria responsável por supervisionar a implantação do Comando de Defesa Cibernética (ComDCiber) e da Escola Nacional de Defesa Cibernética (ENaDCiber), subordinados ao Comando do Exército [1].

Aliando as iniciativas da esfera federal voltadas para o setor cibernético com as voltadas para a proteção das infraestruturas críticas, a Usina Hidrelétrica Itaipú Binacional e o Exército Brasileiro, formalizaram um Memorando de Entendimentos e de um Acordo de Cooperação, em 2014. Em 2018, o Instituto Militar de Engenharia (IME) submeteu um Formulário de Apresentação de Proposta de Projeto com objetivo de instalar um laboratório que permita o desenvolvimento de estudos e análises de segurança cibernética de infraestruturas críticas. O IME criou, em 2017, no seu Programa de Pós-Graduação em Engenharia de Defesa, uma Linha de Pesquisa em Computação e Defesa e Segurança Cibernéticas e conta com modernos laboratórios de computação de alto desempenho e de controle, automação e robótica industrial recentemente implantados, dentre os quais se destaca o Laboratório de Automação e Simulação de Sistemas Elétricos (LASSE), que detém vocação natural para apoiar tecnicamente o projeto.

A proposta de Projeto foi aprovada com o objetivo, descrito resumidamente, de implantar um ambiente de simulação do tipo *hardware in the loop* incluindo dispositivos

físicos industriais que representam infraestruturas críticas na área de Sistemas Elétricos e de Potência (SEP) e de Tecnologia de Automação (TA). O ambiente de simulação deverá prover condições, nas áreas de Tecnologia da Informação e Comunicação (TIC) e Segurança Cibernética aplicadas à Tecnologia de Automação de Infraestruturas Críticas. O desafio atual é criar um modelo funcional do Laboratório que vai ser denominado LaSC - Laboratório de Segurança Cibernética de Sistemas Elétricos em Ambiente de Tecnologias de Informação, Comunicação e Automação e este trabalho versa exatamente sobre esta iniciativa.

O Projeto de criação do LaSC é tempestivo e possui extremo senso de oportunidade devido ao modelo vigente de Indústria 4.0 [7]:

"As preocupações de segurança aumentaram consideravelmente após a revolução da Indústria 4.0, já que a tendência de conectar equipamentos ICS (*Industrial Control System*) à Internet cresceu significativamente nas indústrias. A estratégia de defesa via *air gap*, que é a separação completa entre a rede de tecnologia de automação (TA) e a rede de tecnologia da informação (TI) já não parece mais tão viável em vista da necessidade de comunicação entre as diversas entidades que participam de um sistema, como ocorre no setor elétrico, por exemplo."

Além disso, o Projeto de criação do LaSC encontra amparo na Política Nacional de Defesa conforme descrito em [2,p.9]:

"Para se opor a possíveis ataques cibernéticos, é essencial aperfeiçoar os dispositivos de segurança e adotar procedimentos que minimizem a vulnerabilidade dos sistemas que possuam suporte de tecnologia da informação e comunicação ou permitam seu pronto restabelecimento."

## 2. METODOLOGIA

A abordagem empregada para confecção de um modelo funcional preliminar iniciou-se com uma análise estratégica do Laboratório com intuito de se compreender os desafios a serem enfrentados, considerando tanto o ambiente interno como o externo. Da mesma forma buscou-se enxergar os pontos fortes e as oportunidades a serem exploradas, o que resultou na elaboração de uma matriz *SWOT*.

O trabalho prosseguiu com tarefas voltadas para a gestão das atividades a serem realizadas visando alcançar os objetivos de elaboração do modelo funcional. Com esse objetivo montou-se uma Estrutura Analítica de Projeto (EAP).

Os pacotes de tarefas elencados passaram por uma análise de esforço versus resultado, tipo curva ABC, de maneira a se criar uma priorização para maximização da eficiência do trabalho dentro do tempo previsto porque sabia-se da dificuldade de esgotar o assunto. Então, a partir da EAP e da priorização e precedência das tarefas levantandas, montou-se um *Program Evaluation and Review Technique* (PERT) e *Critical Path Method* (CPM) para identificação do caminho crítico e orientação da diretriz a ser seguida no trabalho.

Considerando o objetivo de criação de um modelo funcional, ainda que preliminar, o foco primário concentrou-se no levantamento dos envolvidos (*stakeholders*) com o Projeto de criação do LaSC, bem como na identificação das tarefas demandadas para o Laboratório. Com base nesses levantamentos, alguns diagramas foram construídos com o objetivo de ampliar o entendimento sobre as funcionalidades do Laboratório.

O arcabouço metodológico utilizado como base para montagem dos diagramas foi o SysML, que é uma linguagem de modelagem de arquitetura de propósito geral voltada para

Engenharia de Sistemas. O SysML é capaz de apoiar as fases de especificação, análise, projeto, verificação e validação de uma ampla gama de sistemas e sistemas de sistemas. Esses sistemas podem incluir hardware, software, informações, processos, pessoal e instalações. O SysML é uma tecnologia muito aderente às aplicações [11].

O SysML organiza seus diagramas basicamente em duas categorias: diagramas de comportamento e de estrutura. Considerando esta organização, buscou-se, a fim de abordar o problema de maneira mais ampla, empregar diagramas de ambas as categorias. Optou-se pelo Diagrama de Blocos para mostrar a estrutura de uma rede genérica de Sistemas de Controle Industrial nos moldes do que é comumente encontrado na indústria atualmente. Já na categoria dos diagramas de comportamento, selecionou-se o Diagrama de Casos de Uso, capaz de mostrar, ainda que estaticamente, as principais "histórias de usuário" (*user story*, em referência à terminologia adotada em metodologias ágeis) e considerando os *stakeholders* levantados como usuários do "sistema LaSC".

Para visualização da dinâmica comportamental do LASC, durante a fase de planejamento, pensou-se também na elaboração do diagrama de atividades, o que acabou sendo prejudicado pelo pouco tempo para a realização do trabalho e pelo grau de incerteza no esgotamento da identificação das atividades que o Laboratório deverá realizar. Os diagramas elaborados foram:

- Entidade-Relacionamento;
- Contexto;
- Blocos;
- Casos de uso.

Sobre o histórico de SysML, cabe destacar que a decisão de definir uma linguagem de modelagem de propósito geral baseada na *Unified Modeling Language* (UML) e dedicada a Engenharia de Sistemas partiu do *International Council on Systems Engineering* (INCOSE), que entrou em contato com *Object Management Group* para formar um grupo denominado *Systems Engineering Domains Special Interest Group* (SE DSIG). O objetivo dessa linguagem é definido da seguinte forma [8,p.2]:

“Uma linguagem de modelagem padrão para engenharia de sistemas para analisar, especificar, projetar e verificar sistemas complexos, que se destina a sistemas de qualidade, melhorar a capacidade de trocar informações de engenharia de sistemas entre ferramentas e ajudar a cobrir a lacuna semântica entre sistemas, software e outras disciplinas de engenharia”.

O SysML é uma tecnologia bastante aderente ao que é conhecido como *Model-Based Systems Engineeering* (MBSE), ou seja, Engenharia de Sistemas Baseada em Modelos, o que se julgou bastante alinhado com a proposta do presente trabalho e da disciplina.

## 3. RESULTADOS

Neste capítulo serão apresentados os diagramas provenientes da modelagem preliminar, definidos na proposta do trabalho. O objetivo geral por trás da modelagem é estabelecer um quadro que facilite a compreensão do espaço do problema, a síntese de possíveis soluções e análise dessas soluções identificadas [12].

### 3.1. ANÁLISE ESTRATÉGICA

Petrova, dentre várias definições apresentadas em seu livro *Genesis of Strategic Management* [10], define **estratégia** como sendo um "método para estabelecer objetivos – corporativos, de negócio e funcionais". Esta definição se enquadra no intento proposto por este trabalho preliminar. O LASC, como um laboratório ainda em fase de implantação, necessita de estudo para estabelecimento de seus objetivos frente as demandas e expectativas de seus *stakeholder*, sobretudo os patrocinadores. Tendo em vista o exposto, elaborou-se uma Matriz *SWOT* visando ampliar a compreensão sobre tais objetivos.

A análise *SWOT* combina a análise do ambiente externo e interno da organização. O ambiente interno caracteriza os pontos fortes e fracos de uma organização, enquanto o ambiente externo caracteriza os impactos em uma organização - as oportunidades e ameaças decorrentes do exterior. A Matriz *SWOT* elaborada é apresentada na Figura1.

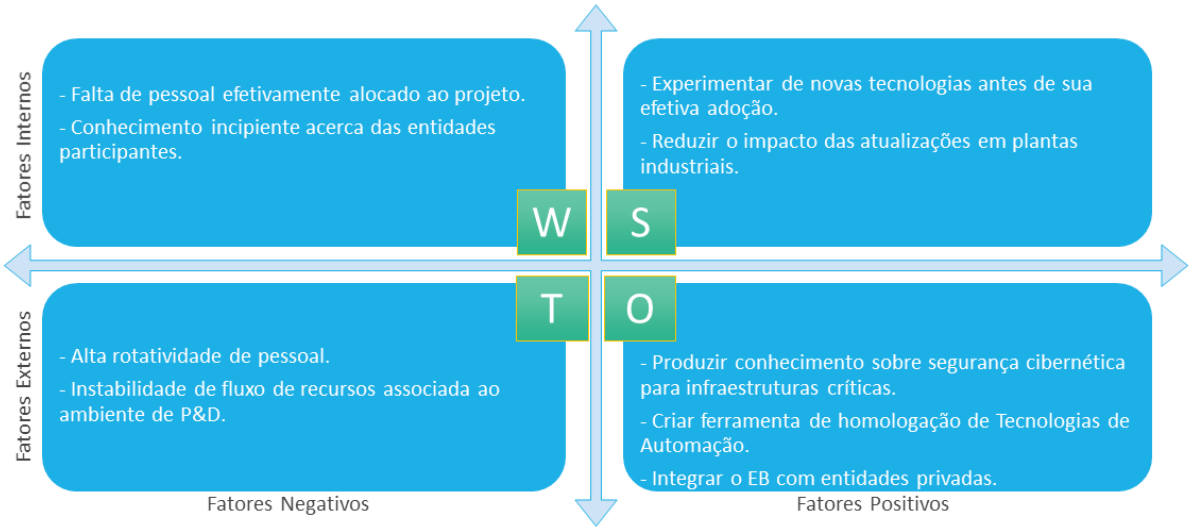


*Figura 1: Matriz SWOT da implantação do LaSC*

Os **pontos fortes** (*strenghts* - S) são determinados como capacidades organizacionais, vantagens competitivas ou recursos disponíveis que podem ser usados. As **fraquezas** (*weaknesses* - W) são definidas como a ausência de habilidades, baixos níveis de competência, fraquezas, deficiências ou falta de recursos. As **oportunidades** (*opportunities* - O) são representadas como situações em que os benefícios externos são absolutamente claros e existe uma grande oportunidade sucesso se a organização adota as ações corretas. As **ameaças** (*Threats* - T) são representadas como situações que levam a eventos e resultados externos potencialmente prejudiciais à organização, se as ações apropriadas não forem tomadas. [10].

### 3.2. GERENCIAMENTO DAS ATIVIDADES

Petrova, define em seu livro *Genesis of Strategic Management* [10], dentre diversas áreas funcionais da gestão, o **gerenciamento de processos de negócios** como sendo "uma abordagem de gerenciamento holística, concentrada na sincronização de todos os aspectos de uma organização com os desejos e necessidades dos clientes".

Ampliada a compreensão dos objetivos do LASC a partir da Matriz *SWOT* e considerando ainda a necessidade de identificação dos processos de negócio, clientes (dentro

da categoria de *stakeholders*) e demais aspectos da organização e suas respectivas demandas, ainda em fase de planejamento montou-se uma Estrutura Analítica de Projeto (EAP). Encarou-se essa estrutura hierárquica de organização das tarefas como uma forma de gerenciar as atividades a serem exercidas e seus respectivos artefatos a serem entregues. As atividades levantadas foram as seguintes (já considerando os códigos hierarquicamente estabelecidos na EAP):

1. Compreender as relações existentes entre *Stakeholders*
   - 1.1 Elencar stakeholders
   - 1.2 Elaborar Diagrama Entidade-Relacionamento
   - 1.3 Elaborar Diagrama de Contexto
2. Compreender as funções e atividades desenvolvidas pelo Laboratório
   - 2.1 Levantar Funções do Laboratório
   - 2.2 Confecção do *PERT/CPM*
   - 2.3 Diagrama de Blocos
   - 2.4 Diagrama de Casos de Uso
   - 2.5 Diagrama de Atividades
3. Gerenciamento Acadêmico
   - 3.1 Definição da equipe e esclarecimentos sobre o tema
   - 3.2 Pesquisa bibliográfica
   - 3.3 Definição dos diagramas
   - 3.4 Apresentações
   - 3.5 Confecção do relatório

A título de priorização das atividades, adotou-se como convenção o emprego das letras "A", "B" e "C", como referência à Curva ABC. As atividades elencadas foram analisadas, além da ótica de precedência, também pela perspectiva do esforço empregado versus resultado alcançado, como um exercício analítico de causa e efeito. A EAP resultante é apresentada na Figura 2.

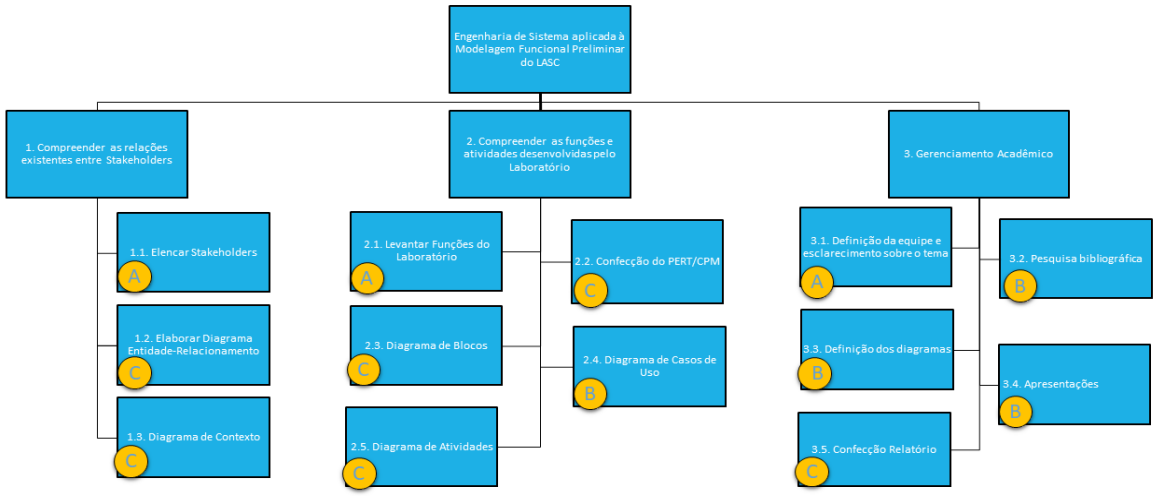


*Figura 2: EAP para a Modelagem Funcional Preliminar do LASC*

O prof. dr. Olaf Passenheim, em seu livro *Project Management* [9], cita que as "técnicas de agendamento (em formato de rede) formam a base para todo planejamento e ajudam nas decisões gerenciais sobre como é melhor utilizar os recursos para alcançar as restrições de tempo e custo".

Nesta modelagem preliminar, contou-se apenas com os dois alunos redatores do presente trabalho como recursos, sem a necessidade de cálculos de custo. Porém, para efeito de prática acadêmica em consonância com boas práticas de gerenciamento de projeto, elaborou-se um *PERT/CPM*, que é técnica de agendamento em formato de rede. O diagrama para disposição das atividades no tempo e observância do caminho crítico é apresentado na Figura 3.

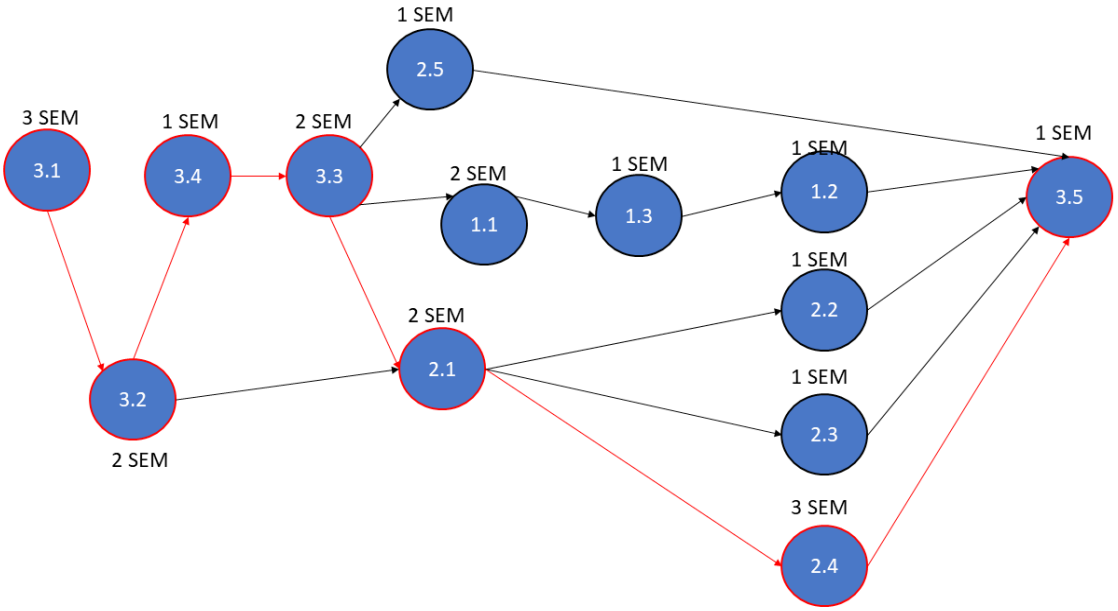


*Figura 3: PERT/CPM para a Modelagem Funcional Preliminar do LASC*

### 3.3. DIAGRAMA DE ENTIDADE-RELACIONAMENTO

Diagramas de Entidade-Relacionamento (ER) têm a finalidade de exibir como as entidades de um sistema se relacionam, no formato de fluxograma. Em geral, são utilizados para projetar bancos de dados relacionais, porém, no trabalho em questão, utilizou-se como ferramenta de gestão para melhor compreensão acerca dos papéis exercidos pelos *stakeholders* e seus relacionamentos, incluindo o próprio LASC, conforme a Figura 4.

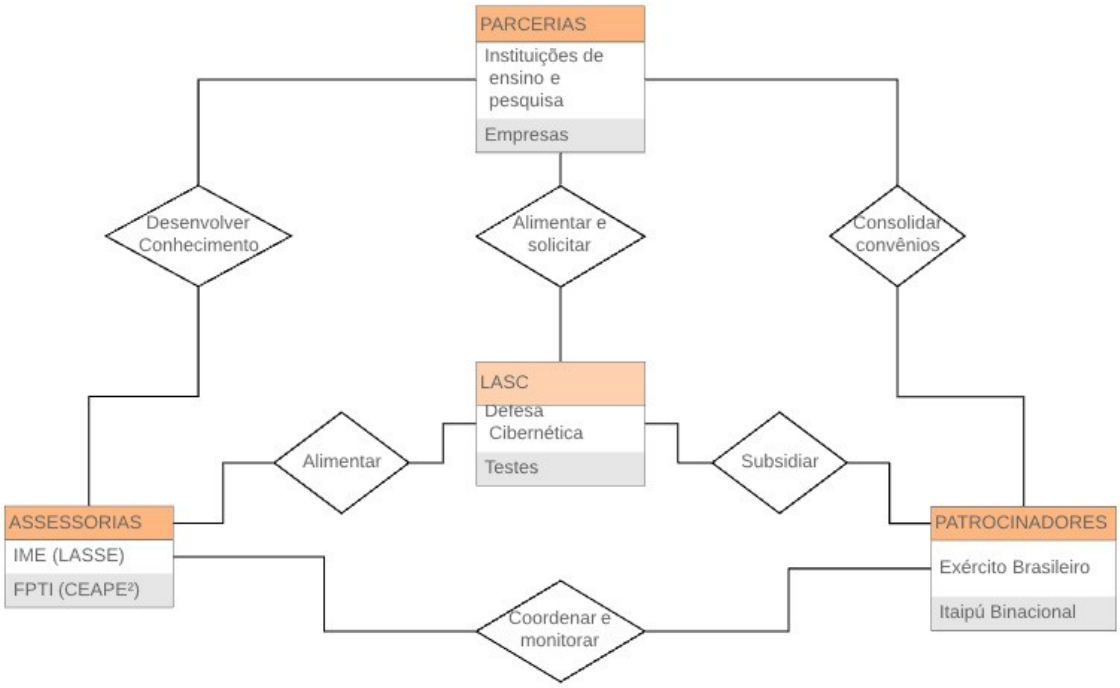


*Figura 4: Diagrama de Entidade-Relacionamento dos stakeholders dos LaSc*

O levantamento dos *stakeholder* consolidou-se em uma lista bastante extensa de envolvidos e, de certa maneira, incerta a respeito do esgotamento deles. Por este motivo optou-se por agrupá-los em categorias e tratá-lo de forma conjunta, conforme apresentado no Diagrama de Entidade-Relacionamento.

### 3.4. DIAGRAMA DE CONTEXTO

Diagrama de Contexto é um diagrama que representa todo o fluxo de dados do sistema, atuando como um recurso para modelar os escopos do sistema. Elaborou-se este diagrama como primeira atividade orientada à modelagem do domínio, conforme a Figura 5.

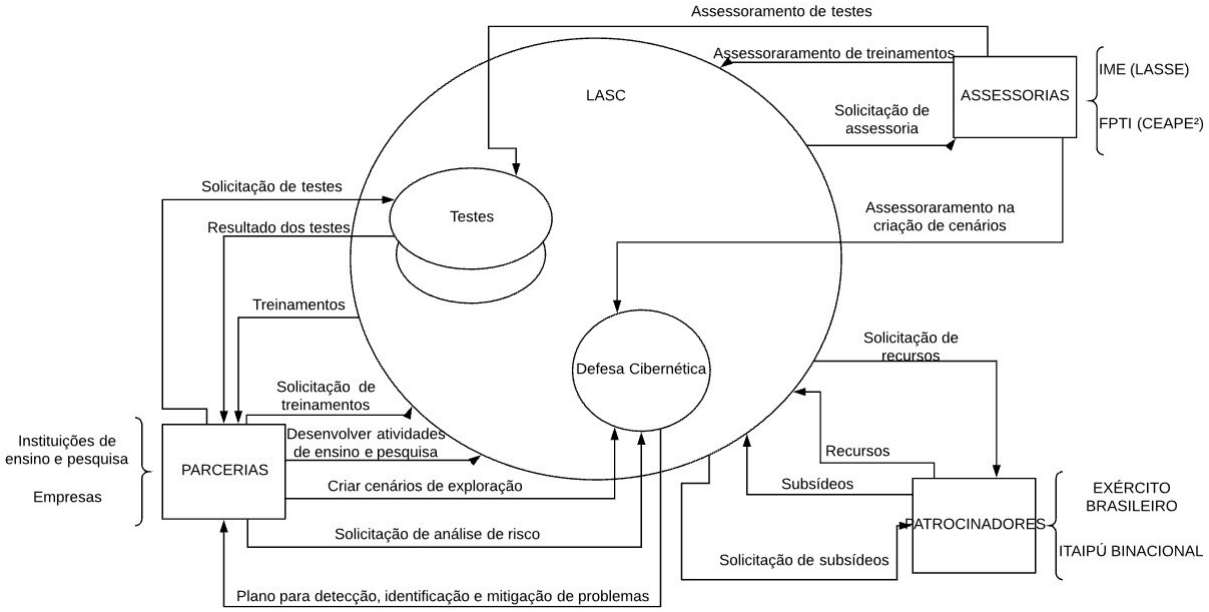


*Figura 5: Diagrama de Contexto das atividades do LaSC*

Como atividade primária na modelagem do domínio, este artefato descreve o que o sistema e seu ambiente são e captura componentes de alto nível do sistema e do seu ambiente operacional e estabelece a estrutura referencial particularmente importante para organizações multidisciplinares de partes interessadas [12].

Importante destacar os ainda não mencionados órgãos de assessoria identificados: LASSE – Laboratório de Automação e Simulação de Sistemas Elétricos, situado no IME; e o CEAPE$^2$ – Centro de Estudos Avançados em Proteção de Estruturas Estratégicas, localizado no Parque Tecnológico de Itaipú (PTI).

### 3.5. DIAGRAMA DE BLOCOS

O diagrama de blocos (*Block Definition Diagrama - BDD*, como é conhecido em SysML) pertence a categoria de diagramas de estrutura e fornece uma representação em caixa preta de um bloco do sistema. Pode conter blocos de qualquer natureza, incluindo *software* ou *hardware* e tende a ser o diagrama primário a ser construído para instruir o restante da modelagem em um sistema de sistemas. SysML define outro tipo específico de diagrama de bloco (conhecido como *Internal Block Diagram - IBD*) que fornece a caixa branca ou a visão interna de um bloco do sistema e é geralmente instanciado a partir do BDD para representar a montagem final de todos blocos interiores ao bloco do sistema principal [8].

O modelo genérico de uma rede com sistemas de controle industrial, incluindo a rede de TI e TA é apresentado na Figura 6. A rede corporativa representada pode ser compreendida com uma rede de TI comum. Sua comunicação com a rede costuma empregar algum esquema de segurança como VPN, por exemplo. O segmento da Central SCADA normalmente contém uma DMZ (zona desmilitarizada) com perímetro protegido para os servidores. E as subestações remotas podem se conectar por redes de comunicação industrial apartadas com protocolo específico Modbus. Porém, em tempos de indústria 4.0, grande parte dos equipamentos utiliza TCP ou mais especificamente Modbus/TCP.

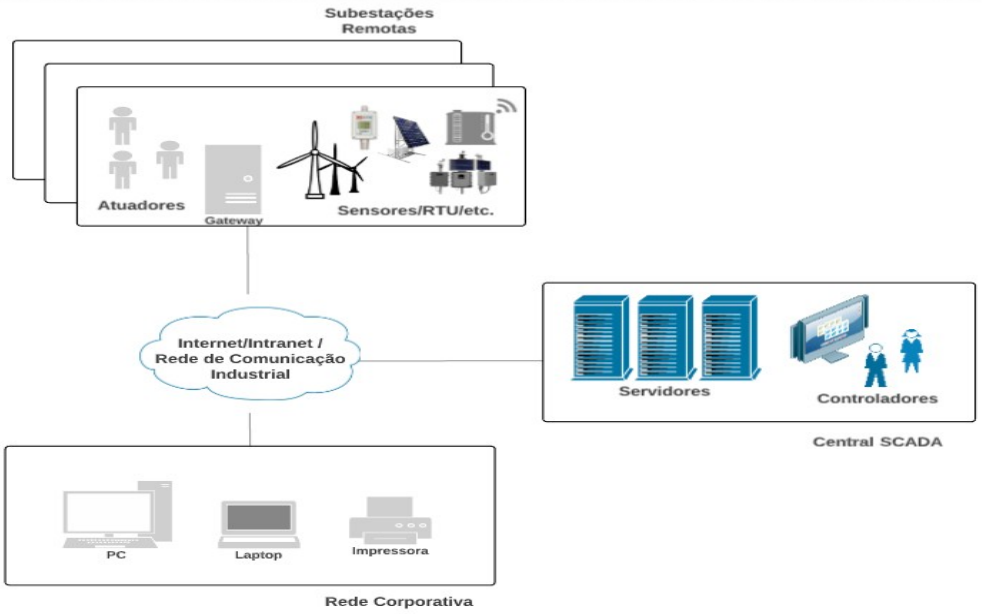


*Figura 6: Diagrama de Blocos de uma rede genérica de comunicação de ICS*

Um cenário como este demonstra que, nos dias de hoje, com Internet das Coisas, a superfície de ataques cibernéticos está bastante ampliada, ou seja, as indústrias tendem a se tornar mais vulneráveis.

### 3.6. DIAGRAMA DE CASOS DE USO

O Diagrama de Casos de Uso relaciona as principais funcionalidades do sistema com os respectivos usuários que as executam (atores), documentando o que o sistema realiza, de fato, do ponto de vista dos usuários. Está representado na Figura 7.

O Diagrama de Casos de Uso apresenta as descrições do papel do sistema, seus comportamentos esperados e suas interações com atores externos [12]. A descrição detalhada de cada Caso de Uso fica como sugestão para trabalhos futuros.

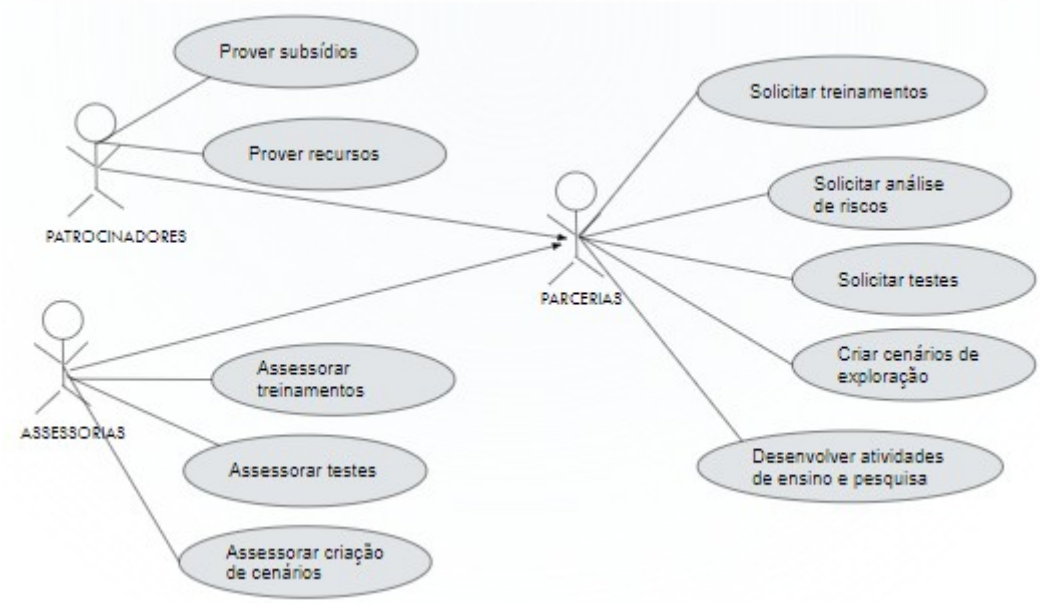


*Figura 7: Diagrama de Casos de Uso do LaSC*

## 4. CONCLUSÕES E TRABALHOS FUTUROS

O trabalho teve por finalidade prover uma modelagem funcional preliminar do LASC. Nesse sentido, foi elaborado um conjunto de diagramas de modo a alcançar o intento em alinhamento com o aprendizado da disciplina.

Atividades preparatórias aos diagramas foram executadas como o levantamento dos principais *stakeholders*, agrupamento deles em classes, e definição as principais funções do LaSC, dividindo-as nas categorias estratégicas, operacionais e de gestão. Visando melhor alcançar os objetivos, o diagrama de atividades foi removido do escopo do trabalho, visto a complexidade de definição das atividades agregadoras das principais funções do LaSC no prazo estipulado.

Assim, pode-se concluir que os objetivos do trabalho foram atingidos, pois os diagramas previstos foram confeccionados conforme o levantamento das necessidades dos envolvidos. Para trabalhos futuros que visem a complementar esta modelagem preliminar do sistema, sugere-se a confecção do diagrama de atividades, bem como aprofundar e esmiuçar as funções e seus atores, descrevendo os fluxos de cada caso de uso.

Um modelo funcional de um sistema descreve como o sistema atingirá seus objetivos. Ele vai além dos casos de uso, quebrando-os em maior detalhe e mostrando atividades, fluxos e transições de estado entre seus componentes (podendo ser outro sistema no caso de um sistema de sistemas).

É uma característica cada vez mais comum dos sistemas complexos a existência de funcionalidades complexa, o que não é fácil de abordar usando técnicas tradicionais de avaliação. Por este motivo, é tão importante a utilização de um conjunto de artefatos capazes de habilitar e aprimorar a análise, teste e avaliação de sistemas complexos, que sejam difíceis de se avaliar usando metodologias e ferramentas analíticas tradicionais.

## 5. REFERÊNCIAS BIBLIOGRÁFICAS

[1] Ministério da Defesa. Criação do comando de defesa cibernética - portaria no2.777/md, de 27 de outubro de 2014.

[1] Ministério da Defesa. Política nacional de defesa.

[2] Presidência da República. Estratégia nacional de defesa - decreto no6703 de 18 de dezembro de 2008.

[3] Presidência da República. Política nacional de segurança das infraestruturas críticas - decreto no9.573, de 22 de novembro de 2018.

[4] Comando do Exército. Criaçao do centro de defesa cibernética - portariano666 de 04 de agosto de 2010.

[5] Comando do Exército. Criação do núcleo do centro de defesa cibernética - portaria no667 de 04 de agosto de 2010.

[6] Roberto Miranda Gomes. Sistemas de controle industrial (ics) e demandas de segurança.

[7] INCOSE.SysML Modeling Language, 2006.

[8] PASSENHEIM, Olaf. Project Management. Bokboon, 2014.

[9] PETROVA, Elitsa. Genesis of Strategic Management. Bokboon, 2017.

[10] SysML Open Source Project. Sysml open source project index page.

[11] J. Stephen Topper and Nathaniel C. Horner. Model-based systems engi-neering in support of complex systems development.John Hopkins APLTechinical Digest, 32(1), 2013.