



Grupo de Estudo de Proteção, Medição, Controle e Automação em Sistemas de Potência – GPC

AValiação de Sistemas de Proteção Através da Ferramenta de Modelagem e Verificação Formal Estatística

**Felipe Crestani dos Santos (1); Guilherme de Oliveira Kunz (2); Jonas Roberto Pesente (3);
FPTI(1); UNIOESTE(2); IB(3);**

RESUMO

Este informe técnico tem por objetivo a avaliação do emprego da técnica de modelagem e Verificação Formal Estatística como ferramenta de suporte ao projeto, simulação, validação e implementação de sistemas de proteção. A metodologia avaliada é apresentada e aplicada em um sistema de proteção teste baseado em redes *Ethernet*, evidenciando os principais benefícios que a abordagem baseada em Verificação Formal Estatística pode proporcionar para o processo de projeto e análise de sistemas de proteção, principalmente no sentido de comprovar se a estratégia atende ao comportamento determinístico temporal esperado.

PALAVRAS-CHAVE

Sistemas de Proteção, Sistemas de Tempo Real Críticos, Autômatos Híbridos, Verificação Formal Estatística.

1.0 - INTRODUÇÃO

A evolução tecnológica nas mais diversas áreas do conhecimento, principalmente na área da “Ciência da Computação”, tem estimulado a competitividade industrial através da implantação de processos mais eficientes e autônomos (1). Dentro do escopo dos Sistemas de Energia Elétrica (SEEs), um dos aspectos que caracteriza essa evolução é o conceito de *Smart Grids*, no qual se propõe o uso de uma camada de informação ao sistema elétrico que proporciona a implementação de funcionalidades como controle, proteção, reconfiguração, acompanhamento da demanda, redução de perdas, entre outras, de maneira coordenada e interoperável (2). A adequação destas funcionalidades levanta questões importantes sobre o planejamento, operação, controle e proteção dos SEEs.

No âmbito da proteção, o conceito *Smart Grids* proporciona aos relés de proteção (agora IEDs – *Intelligent Electronic Devices*) características multifuncionais relacionadas à proteção, monitoramento e controle, além de integrar estas funções distribuídas sobre uma rede local (3). Essa nova característica acrescenta mais um aspecto a ser avaliado durante o seu funcionamento, que é o atraso de tempo inerente na transmissão dos dados.

A bibliografia consultada indica a necessidade de uma abordagem formal que sistematize o projeto e validação de dos sistemas de proteção (4, 5). Em geral, esse processo é realizado mediante simulações computacionais envolvendo diversos cenários de operação e distúrbios. Ainda que sejam considerados um número significativo de simulações, não há garantias formais de que o sistema apresente comportamento indesejável logo em sua primeira atuação em campo (5).

Uma das ferramentas que vem ganhando destaque é a modelagem e verificação formal. Inicialmente adotada na área da Ciência da Computação, esta abordagem é indicada para verificação de propriedades em sistemas com elevada criticidade temporal, também denominados na área em questão como Sistemas de Tempo Real Críticos (6).

Uma metodologia baseada em Modelagem e Verificação Formal é proposta por Kunz (2012). No trabalho em questão, o autor aplica a metodologia para o projeto efetivo de um sistema automático de transporte de passageiros (Sistema Aeromóvel). Em Siqueira (2014), o processo de Modelagem e Verificação Formal é utilizado para modelagem de um Sistema Hidráulico de Regulação de Velocidade (SHRV) de geradores síncronos. Sengupta et al. (2015) avalia a coordenação das funções de proteção de corrente e distância em um sistema de geração.

Assim como os trabalhos supracitados, o presente trabalho tem como objetivo a aplicação de uma metodologia formal para modelagem de sistemas de proteção, de forma a subsidiar o processo de projeto e verificação de desempenho destes. Como formalismo de modelagem, o trabalho adota os Autômatos Temporizados Híbridos, o qual permite-se a representação da natureza híbrida (discreta e contínua) da nova característica dos sistemas de proteção. Além disso, este formalismo permite a aplicação de uma abordagem estatística sobre os modelos, característica necessária quando se acrescenta o processo não determinístico inerente ao processo de comunicação de dados. Desta forma, o trabalho é organizado da seguinte maneira: a Seção 2.0 apresenta os aspectos considerados no processo de Modelagem e Verificação Formal de sistemas críticos; a Seção 3.0 apresenta a descrição da metodologia aplicada à Sistemas de Proteção; um exemplo de aplicação é discutido na Seção 4.0; e por fim, a Seção 5.0 apresenta as conclusões do trabalho.

2.0 - MODELAGEM E VERIFICAÇÃO FORMAL ESTATÍSTICA

O processo de Modelagem e Verificação Formal é basicamente segmentado em três principais etapas: “Modelagem”, “Especificação” e “Verificação” (7), conforme ilustrado pela Figura 1. A etapa de modelagem consiste na abstração de determinada realidade para a linguagem formal empregada pelo verificador de modelos. Após a modelagem, é necessário que sejam elencadas propriedades as quais se deseja verificar. A especificação das propriedades neste trabalho é feita através da lógica temporal, a qual permite a descrição de afirmativas sobre a evolução do comportamento de um sistema no decorrer do tempo [ref]. Por fim, algoritmos de verificação avaliam exaustivamente os estados do modelo de entrada em busca de estados que satisfaçam (ou não) as propriedades descritas na etapa de especificação.

Em específico neste trabalho, o mecanismo de verificação é baseado em um processo estocástico, sendo o resultado da verificação uma distribuição de probabilidade do modelo em atender determinada propriedade. Este processo é discutido melhor nas subseções seguintes.

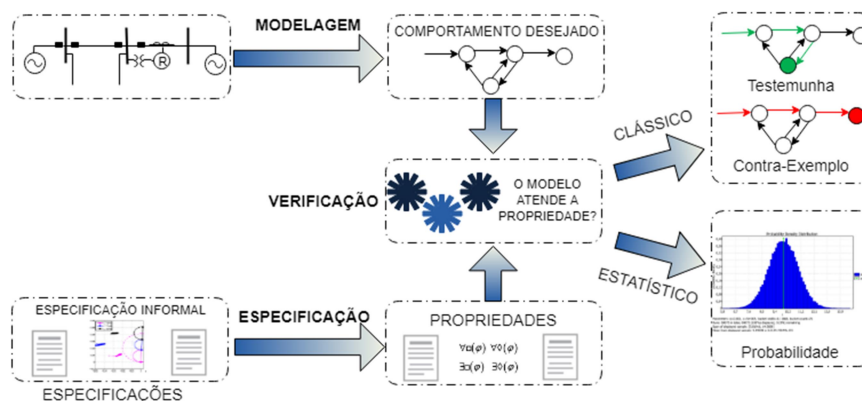


Figura 1 – Processo de Modelagem e Verificação Formal Estatística

2.1 Etapa de Modelagem: Formalismo de Apoio

Neste trabalho, os Sistemas de Proteção são representados através de uma abstração de Sistemas Dinâmicos a Eventos Discretos (SDEDs). Esta escolha é naturalmente justificada pela ocorrência síncrona e assíncrona de eventos discretos que, em sequência específica, levam o sistema a um estado pré-determinado. Mais especificamente, o formalismo de apoio adotado neste trabalho é baseado no conceito de Autômatos Temporizados Híbridos, os quais permitem a abstração do sistema de proteção por modelos com características discreta e contínua. Esta característica híbrida é essencial para representação da característica não determinística dos sistemas de comunicação (8).

No contexto deste trabalho, um Autômato Híbrido é definido como uma Tupla $H = (Q \times X, Q_0 \times X_0, \hat{\alpha}, \Sigma, Inv, G)$ onde: i) $Q \times X$ denota o espaço de estados híbridos, sendo Q um conjunto de estados discretos $\{q_1, q_2, \dots, q_N\}$ e $X \subseteq \mathbb{R}^n$ espaço de estados das variáveis contínuas; ii) $Q_0 \times X_0 \subseteq Q \times X$ é o conjunto de condições iniciais do autômato; iii)

$\{\varepsilon_q\}_{q \in Q}$ associa a cada estado discreto a dinâmica das variáveis contínuas através de equações diferenciais de primeira ordem. iv) $\Sigma \subseteq Q \times Q$ denota o conjunto de transições (ou alfabeto) do autômato. Cada transição $e \in \Sigma$ relaciona dois estados, sendo o estado de saída denotado por $s(e)$ e o de chegada $t(e)$; v) Inv denota as invariantes de cada estado; e vi) $\{G_e\}_{e \in \Sigma}$ associa cada transição a um guarda $G_e \subseteq Inv_{s(e)}$ (9, 10).

2.2 Etapa de Especificação – Lógica Temporal

Lógicas temporais são formalismos que permitem descrever as especificações do sistema através de operadores temporais e quantificadores de caminhos combinados aos operadores da lógica clássica. A semântica dos operadores temporais é definida a partir de um caminho de computação específico e tem por objetivo a ordenação temporal de ocorrência de eventos sobre este caminho. Os quantificadores de caminho são utilizados para determinar o ramo de estados que será abrangido. As proposições atômicas são usadas para formalizar as condições de interesse nos estados do sistema (11). A lógica CTL (*Computation Tree Logic*) utiliza a composição destes três operadores para definição das propriedades. A seguir apresenta-se a descrição semântica das principais propriedades descritas pela lógica CTL. A interpretação gráfica para cada propriedade é apresentada na Figura 2.

- $\forall \Box(\varphi)$ – Para todos os caminhos, em todos os estados, φ deve ser satisfeito. Esta propriedade denota um comportamento global em todos os caminhos e estados possíveis da computação;
- $\forall \Diamond(\varphi)$ – Para todos os caminhos, no futuro, φ deve ser satisfeito. Esta propriedade denota a existência de um ou mais estados que satisfaçam φ em dado momento, para todos os caminhos de computação;
- $\exists \Box(\varphi)$ – Existe um caminho em que φ é satisfeito em todos os estados. A propriedade demonstra a ocorrência de pelo menos um caminho de computação em que φ é sempre atendido;
- $\exists \Diamond(\varphi)$ – Existe um caminho onde, no futuro, em pelo menos um estado φ é atendido, Para a propriedade ser válida, deve haver pelo menos um estado que satisfaça φ .

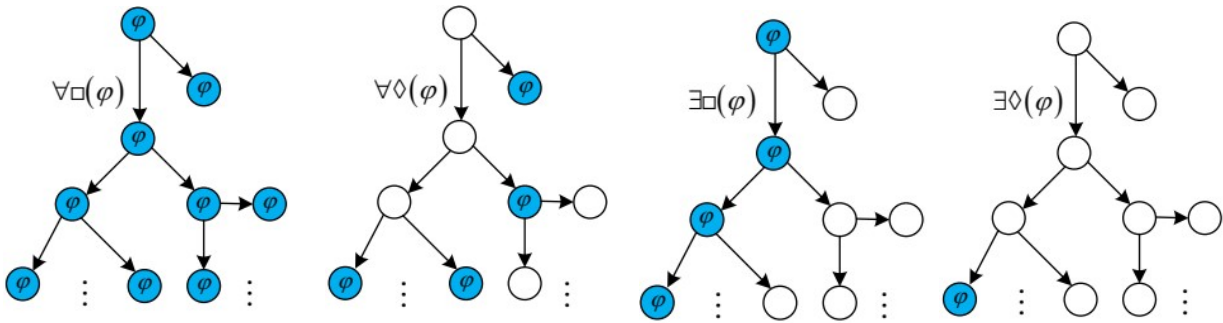


Figura 2 – Visualização da semântica das fórmulas CTL

Da definição de Autômatos Híbridos descrita na subseção anterior, observa-se que o sistema não pode ser representado por meio de um conjunto de estado finitos, uma vez que para cada estado discreto Q , existem infinitos valores de X para o estado híbrido $Q \times X$. Isto introduz um problema de não-decidibilidade ao sistema, não sendo possível a aplicação da lógica clássica de CTL. Nesse contexto, o verificador de modelos deve ser capaz de lidar com este problema.

2.3 Etapa de Verificação – Verificador de Modelos UPPAAL STRATEGO

O verificador de modelos adotado neste trabalho é o UPPAAL STRATEGO (9). O UPPAAL consiste em uma suíte poderosa que agrega ferramentas para modelagem (gráfica), simulação (gráfica) e verificação (via conferência automática de modelos) em um mesmo ambiente. Por se tratar de uma ferramenta que está se consolidando na área de modelagem e verificação de sistemas concorrentes de tempo real (desde 1995), o UPPAAL tem sido alvo de um investimento contínuo pelas universidades envolvidas em seu desenvolvimento, sendo a última versão datada em 19 de fevereiro de 2019 (4.1.20-5).

O formalismo de base empregado pelo UPPAAL é uma extensão dos Autômatos Temporizados Híbridos: cada autômato é definido por um *template* ou *process*. Os estados são representados por *locations* e as transições por *edges*. As restrições de tempo são realizadas através de variáveis do tipo relógio (*clock*). Além destes componentes, há um conjunto de ampliações da linguagem de modelagem que permite a representação de comportamentos mais sofisticados, como guardas de transições (*guard*) e canais de sincronização (*chan*).

Na Figura 3 é apresentada uma rede de autômatos exemplificando a representação gráfica do UPPAAL. Do modelo, identifica-se canais de sincronização, atualizações de relógios em transições, guardas e invariantes de estados. O funcionamento da rede de autômatos da Figura 3 é interpretado da seguinte maneira: o autômato *relay*

envia sinais aleatórios de *trip* através da transição com etiqueta *Trip!*. O transição *Trip?* ocorre no autômato *circuit breaker*, a qual reseta o relógio *t*. O autômato permanece no estado *arcing* em um intervalo entre 2 e 5 unidades de tempo. Por fim, o autômato *circuit breaker* retorna para sua condição inicial.

A especificação das propriedades é realizada através da TCTL (Timed Computation Tree Logic), na qual consiste em uma extensão à linguagem CTL apresentada na subseção anterior. Através desta linguagem é possível expressar a variável tempo nos caminhos de computação possíveis.

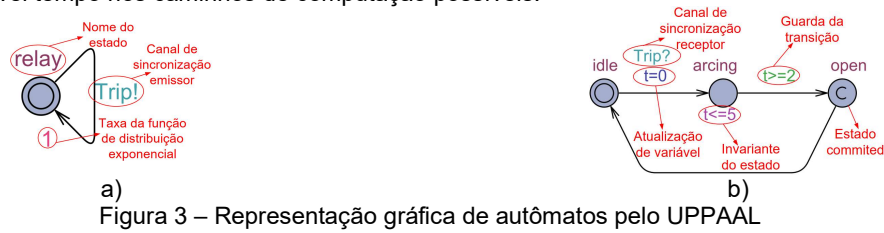


Figura 3 – Representação gráfica de autômatos pelo UPPAAL

3.0 - METODOLOGIA APLICADA AOS SISTEMAS DE PROTEÇÃO

Em virtude do aumento de complexidade na operação dos sistemas de proteção, associado principalmente à crescente utilização de redes *Ethernet* para comunicação e implementação de funcionalidades distribuídas em uma rede local da subestação, este trabalho avalia a aplicação de uma abordagem sistemática para modelagem de sistemas de proteção. A abstração é baseada em Autômatos Híbridos, que, conforme discutido anteriormente, se apresentam como uma abstração natural do comportamento dos sistemas de proteção e possuem como vantagem a decomposição do problema em subsistemas.

Nesse contexto, a obtenção de um modelo de uma subestação automatizada por ser pensada como uma composição de modelos mais simples. A Figura 4 apresenta a abstração de uma subestação implementada de acordo com a norma IEC 61850.

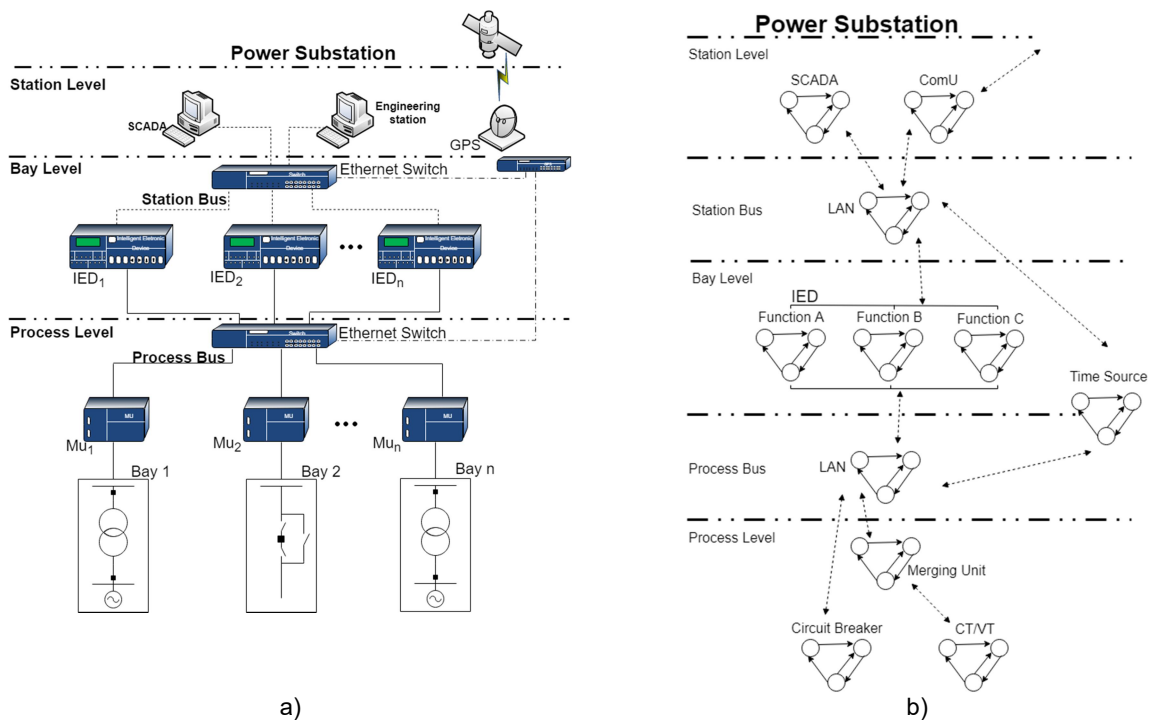


Figura 4 – a) Estrutura de uma subestação digital e b) sua respectiva representação em redes de autômatos

Considerando o processo de desenvolvimento de cada autômato da Figura 4.b, cada modelo pode ser submetido à metodologia adaptada de Kunz (2012), representada pela Figura 7 e detalhada a seguir (6):

1. **Levantamento de requisitos:** especificação dos requisitos do equipamento ou controlador a ser modelado;
2. **Modelagem:** desenvolvimento dos modelos do equipamento/controlador na forma de autômatos híbridos;
3. **Simulação:** a etapa de simulação tem como objetivo verificar se o sistema possui comportamento esperado conforme o especificado;
4. **Verificação:** a etapa de verificação tem por objetivo verificar formalmente se os requisitos do modelo são completamente atendidos. No caso de não atender aos requisitos, volta-se à etapa de modelagem;

5. **Simplificação:** existe a possibilidade de realizar simplificações nos modelos de forma a reduzir o esforço computacional no processo de verificação. Esta simplificação é necessária na integração entre dois modelos previamente validados individualmente.

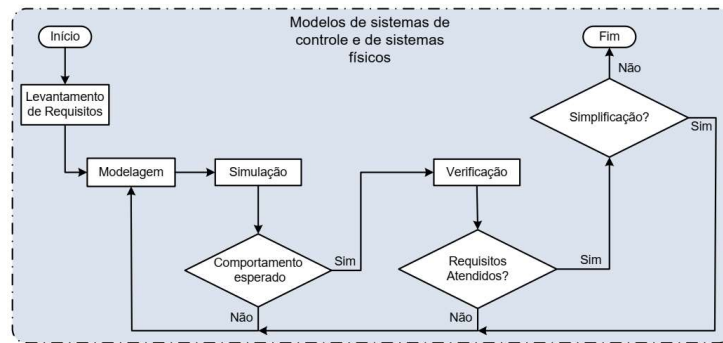


Figura 5 – Fluxograma para validação dos modelos.
Adaptado de Kunz (2012).

A validação do comportamento dos modelos é realizada através da comparação entre os requisitos comportamentais definidos por normas, testes de conformidade em equipamentos/protocolos e trabalhos acadêmicos vinculados à área.

4.0 - EXEMPLO DE APLICAÇÃO

Esta seção apresenta a aplicação da metodologia discutida na seção anterior. O subsistema adotado como exemplo é uma simplificação da interação entre um relé digital e dois disjuntores através de um barramento de comunicação. Um exemplo de abstração seria a atuação de uma função de proteção diferencial em uma subestação com barramento de comunicação entre relé e disjuntores, assim como proposta pela IEC 61850. Salienta-se que o modelo desenvolvido aqui apenas tem a finalidade de demonstração da metodologia proposta, logo, de forma a se reduzir a complexidade de desenvolvimento dos modelos, foram desconsideradas funções mais complexas como processo de amostragem e condicionamento dos sinais elétricos, lógica da função de proteção e o comportamento detalhado no sistema de proteção.

Relativo à etapa de Modelagem, o problema é dividido inicialmente em três subsistemas (Figura 6): Modelo Relé, Modelo LAN e Modelo Disjuntor. Conforme observado na Figura 6, a interação entre os modelos é realizada dos canais de sincronização s_Trip e r_Trip . O relé faz a verificação de falta a cada ciclo de scan (uma unidade de tempo). Se uma falta é detectada dentro do período de scan, o relé envia um sinal de trip ao modelo da LAN. A LAN é representada apenas por um atraso de tempo definido por uma função de distribuição uniforme entre 0 e 1 unidades de tempo. Após o atraso de tempo, o pacote de *trip* é recebido pelo disjuntor, o qual inicia o processo de abertura de seus terminais. Considera-se a possibilidade de que o disjuntor falhe no processo de abertura dos terminais, sendo representado através de pesos nas transições após o estado *arcing*.

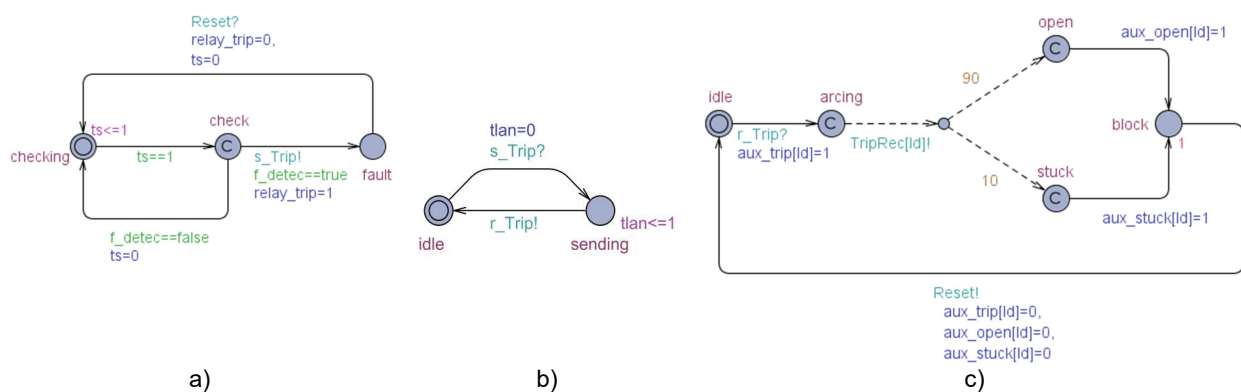


Figura 6 – Etapa 1 – Modelagem. a) Modelo Relé; b) Modelo LAN; c) Modelo Disjuntor.

A próxima etapa da metodologia consiste na avaliação do comportamento dos modelos através de simulações. A Figura 7 apresenta os resultados para os modelos Relé e Disjuntor. Salienta-se que este processo é realizado individualmente para cada modelo, logo, é necessário o desenvolvimento de modelos que fazem a interação com os modelos em análise. Estes modelos não são apresentados neste trabalho, no entanto, basicamente consistem de funções que geram eventos aleatórios e modelos que fazem a observação de variáveis e estados dos modelos em análise para ajudar no processo de verificação formal.

Com relação à simulação do Modelo Relé, da Figura 7.a observa-se que o relé realiza o processo de verificação de falta a cada ciclo de *scan*. Em torno de 5 unidades de tempo, uma falta foi inserida (aleatoriamente) ao sistema. Logo, no próximo ciclo de *scan* (sexto), o relé detecta a falta e envia um comando de *trip*. O tempo de permanência de falta é representado pela variável *t_fault*. Com relação ao Modelo Disjuntor, a Figura 7.b apresenta a resposta do disjuntor para comandos de *trip* gerados aleatoriamente. A cada comando de *trip* recebido, o disjuntor sai do estado inativo (*idle*) para aberto ou em falha.

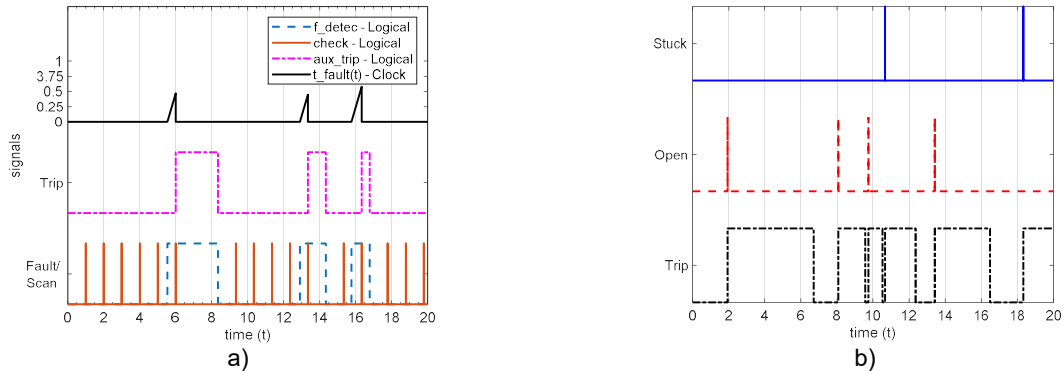


Figura 7 – Etapa 2 – Simulação. a) Modelo Relé; b) Modelo Disjuntor.

Após o processo de validação do comportamento do modelo através da análise da simulação, a metodologia segue através da etapa de verificação formal. A Tabela 1 apresenta o resultado da verificação formal aplicada individualmente aos modelos Relé e Disjuntor. Como a finalidade deste exemplo é apenas a demonstração da metodologia, apenas foram verificados o comportamento básico dos modelos.

Tabela 1 – Etapa 3 – Verificação formal dos modelos

Modelo Relé			Modelo Disjuntor		
Descrição Informal	Descrição Formal	Resultado	Descrição Informal	Descrição Formal	Resultado
Verifica a conformidade de geração de comandos de trip	$\text{Pr}[\leq 1000] ([\text{Relay.fault} \text{ imply } \text{f_detec} == \text{true}])$	100%	Verifica a conformidade no comportamento básico do disjuntor:	$\text{Pr}[\leq 1000] (<> \text{CB1.open})$	100%
	$\text{Pr}[\leq 1000] (<> \text{Relay.fault} \text{ and } \text{f_detec} == \text{false})$	0%		$\text{Pr}[\leq 1000] (<> \text{CB1.stuck})$	100%
Verifica a conformidade de tempo de detecção de falta	$\text{Pr}[\leq 1000] ([\text{Fault_Detec.fault_cond} \text{ imply } \text{tfault} \leq 1])$	100%	- Abertura	$\text{Pr}[\leq 1000] (<> \text{CB1.open} \text{ and } \text{CB1.stuck})$	0%
	$\text{Pr}[\leq 1000] (<> (\text{Fault_Detec.fault_cond} \text{ and } (\text{tfault} > 1)))$	0%	- Travamento	$\text{Pr}[\leq 1000] ([\text{CB1.open} \text{ or } \text{CB1.stuck}] \text{ imply } \text{aux_trip}[0] == 1)$	100%
		- Inconsistência			
			- Resposta ao comando trip		

Os resultados da simulação e verificação formal apresentados anteriormente indicam que o comportamento individual dos componentes do sistema exemplo estão modelados corretamente. A partir desta etapa, os modelos são integrados através dos canais de sincronização e as etapas da metodologia são aplicadas novamente. O sistema é então composto pelo autômato que modela o Relé, o autômato da LAN e dois autômatos que modelam os disjuntores. Além disso, assim como nas etapas anterior, autômatos auxiliares são desenvolvidos para excitar e avaliar os modelos sob teste. O resultado da simulação da rede de autômatos é apresentada na Figura 8.

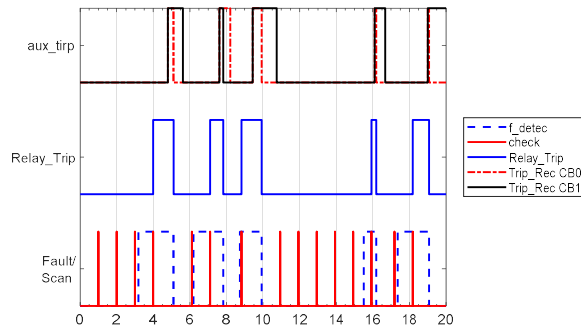


Figura 8 – Etapa 2 – Simulação do sistema composto pela rede de autômatos

Da simulação em questão, observa-se que o estado de *trip* do relé persiste até o primeiro evento de *reset* ser enviado pelos disjuntores. De forma a avaliar o impacto deste evento, uma propriedade de sincronismo foi verificada sobre o modelo. Esta propriedade implica que o mesmo evento de *trip* deve estar associado à abertura dos disjuntores. A verificação formal aplicada ao sistema completo é apresentada na Tabela 2. Observa-se que para o sistema original esta propriedade de sincronismo não está em conformidade. Através do contra-exemplo gerado por esta propriedade, a perda de sincronismo acontece na determinada sequência de eventos: Um dos disjuntores dispara o evento de reset ao relé, que retorna para o estado de *check* de falta. Na ocorrência de uma falta antes de que o segundo disjuntor retorne para o estado *idle*, o relé dispara o comando de *trip*, que é recebido apenas pelo disjuntor que enviou o primeiro comando de reset. Isto acontece pois os canais de sincronização do tipo *broadcast* do UPPAAL não são bloqueantes. Salienta-se que este é um problema de modelagem apenas, e não representa necessariamente a lógica que seria aplicada em campo.

Propõe-se então uma correção ao Modelo Relé de forma com que o mesmo retorne ao seu modo funcional de operação apenas após o evento de reset dos dois disjuntores. O modelo corrigido é apresentado na Figura 9. A metodologia sugere que uma nova simulação seja realizada de forma a verificar o comportamento do modelo, no entanto, apenas apresenta-se o resultado da verificação formal. Verifica-se através da Tabela 2 que a propriedade de sincronismo é atendida para o novo modelo, indicando que os modelos desenvolvidos e sua respectiva integração representam, de acordo com os requisitos operacionais desejados, o comportamento desejado.

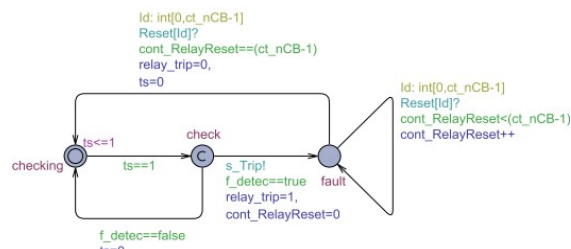


Figura 9 – Correção no Modelo Relé

Tabela 2 – Etapa 3 – Verificação formal sobre a rede de autômatos

Integração dos Modelos			
Descrição Informal	Descrição Formal	Resultado	
		Original	Corrigido
Verifica o comportamento básico da rede de autômatos: - Atuação dos disjuntores durante falta - Sincronismo de operação entre disjuntores e relé	$\text{Pr}[\leq 1000] ([] (\text{Relay.fault and LAN.tlan} > 1) \text{ imply not}(\text{CB0.idle or CB1.idle}))$	100%	100%
	$\text{Pr}[\leq 1000] ([] (\text{CB0.block and CB1.block}) \text{ imply } (\text{cont_Trip} == \text{cont_TripReceiver}[0] \text{ and } \text{cont_Trip} == \text{cont_TripReceiver}[1]))$	0%	100%

Cabe salientar aqui que estes modelos foram simplificados de forma a exemplificar a aplicação da metodologia baseada em modelagem e verificação formal. Este exemplo indica que a metodologia pode ser empregada na modelagem completa de uma subestação automatizada através da norma IEC 61850. Estudos provenientes dos modelos podem ser realizados, conforme será abordado na próxima seção.

5.0 - CONCLUSÕES

Em resposta à necessidade de ferramentas mais sofisticadas na área de validação de Sistemas de Proteção, este informe técnico apresentou o emprego da técnica de Modelagem e Verificação Formal Estatística como ferramenta de suporte à proposição e validação de novas estratégias de proteção. A metodologia foi empregada em um sistema teste envolvendo a interação entre um relé digital e dois disjuntores através de um barramento de comunicação.

O exemplo avaliado indica que a metodologia pode ser vantajosa para o desenvolvimento de novas ferramentas e processos de projeto e verificação de desempenhos em Sistemas de Proteção com sistema de comunicação baseado em redes *Ethernet*, se apresentando como uma abordagem promissora para linhas de pesquisas futuras.

Além disso, da revisão bibliográfica realizada, identificou-se três linhas de pesquisa onde os modelos desenvolvidos possam ser integrados em metodologias em diferentes aspectos. Estas aplicações são apresentadas na Figura 10 e sumarizadas a seguir: i) na etapa que antecede a implementação de controle da nova estratégia de proteção proposta, onde os modelos desenvolvidos são traduzidos para uma linguagem de programação que será embarcada em um controlador; ii) na etapa de testes de desempenho da estratégia proposta, onde a verificação das propriedades do modelo representam o funcionamento global da estratégia; e iii) em testes de conformidade em equipamentos, onde um modelo da rede de autômatos é substituído por um equipamento físico real, com finalidade de avaliar o seu comportamento juntamente com a rede de autômatos através do conceito de *Hardware-in-the-Loop* (HIL).

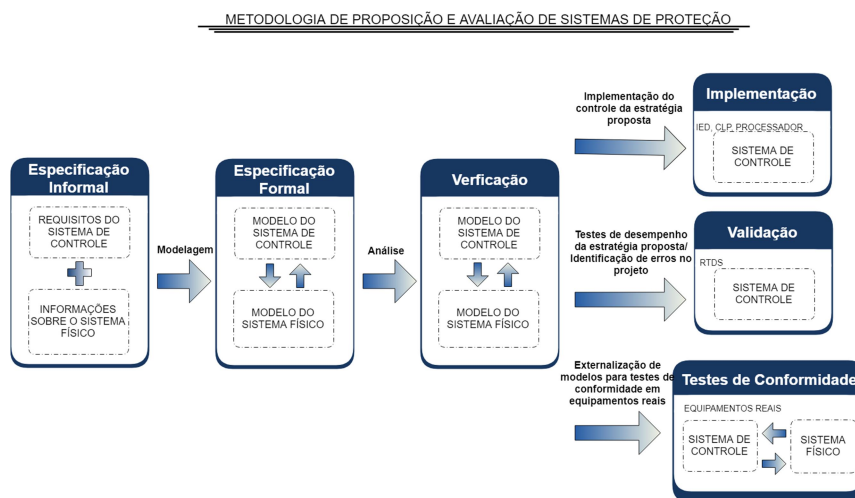


Figura 10 – Aplicações possíveis da ferramenta de modelagem e verificação formal

6.0 - REFERÊNCIAS BIBLIOGRÁFICAS

- (1) Cecilia, A. A. & Sudarsanan, K. (2016). A Survey in Smart Grid, 2016 International Conference on Emerging Trends in Engineering, Technology and Science (ICETETS), pp. 1–7.
- (2) Isa, N. B. M., Wei, T. C. & Yatim, A. H. M. (2015). Smart Grid Technology: Communications, Power Electronics and Control System, Sustainable Energy Engineering and Application (ICSEEA), 2015 International Conference on, pp. 10–14.
- (3) Laaksonen, H. & Suomi, F. (2013). New Functionalities and Features of IEDs to Realize Active Control and Protection of Smart Grids, Electricity Distribution (CIRED 2013), 22nd International Conference and Exhibition on, pp. 1–4.
- (4) Siqueira, R. A. (2014). Metodologia para Modelagem e Análise de Sistemas para Controle de Geração de Energia Elétrica. Tese de Doutorado. Universidade de São Paulo. 2014
- (5) Sengupta, A., Mukhopadhyay, S. & Sinha, A. K. (2015a). Automated Verification of Power System Protection Schemes - Part I: Modelling and Specifications, 2015 IEEE Power Energy Society General Meeting, pp. 1–1.
- (6) Kunz, G. O. (2012). Metodologia para Desenvolvimento de Sistema de Controle de APM (Automated People Movers) com Aplicação ao Sistema Aeromovel de Transporte de Passageiros. Tese de Doutorado. Universidade Federal do Rio Grande do Sul, 2012.
- (7) Baier, C. & Katoen, J.-P. (2008). Principles of Model Checking (Representation and Mind Series), The MIT Press.
- (8) Cassandra, C. G. & Lafortune, S. (2010). Introduction to Discrete Event Systems, 2nd edn, Springer Publishing Company, Incorporated.

- (9) David, A., Jensen, P. G., Larsen, K. G., Mikucionis, M. & Taankvist, J. H. (2015). Uppaal Stratego, in C. Baier & C. Tinelli (eds), Tools and Algorithms for the Construction and Analysis of Systems, Vol. 9035 of Lecture Notes in Computer Science, Springer Berlin Heidelberg, pp. 206–211.
- (10) Susuki, Y., Koo, T. J., Ebina, H., Yamazaki, T., Ochi, T., Uemura, T. & Hikiyara, T. (2012). A Hybrid System Approach to the Analysis and Design of Power Grid Dynamic Performance, Proceedings of the IEEE 100(1): 225–239.
- (11) Rondon, M. E. S. (2012). Verificação Formal de Aplicações Concorrentes em Sistemas Elétricos de Potência. Tese de Doutorado. Universidade Federal do Rio de Janeiro, 2012.

7.0 - DADOS BIOGRÁFICOS



Autor de Contato: Felipe Crestani dos Santos

Formação Acadêmica: Engenharia Elétrica (UTFPR, 2014). Mestrado em Engenharia Elétrica e Computação (Unioeste, 2017).

Experiência Profissional: Atualmente é colaborador da Fundação Parque Tecnológico Itaipu (FPTI-BR) junto ao Laboratório de Automação e Simulação de Sistemas Elétricos (LASSE)..



Autor: Guilherme de Oliveira Kunz

Formação Acadêmica: Engenharia Mecânica (UFRGS, 2001). Mestrado em Engenharia Mecânica (UFRGS, 2006). Doutorado em Engenharia Mecânica (UFRGS, 2012; UMINHO, 2012).

Experiência Profissional: Atualmente é professor na Universidade Estadual do Oeste do Paraná – Campus de Foz do Iguaçu.



Autor: Jonas Roberto Pesente

Formação Acadêmica: Engenharia Elétrica (UNIOESTE, 2005). Mestrado em Engenharia Mecânica (ITA, 2009). Mestrado em Engenharia Elétrica (UFSC, 2009). Doutorado em Engenharia Elétrica (UFSC, 2018).

Experiência Profissional: Atualmente é colaborador da Usina Hidrelétrica de Itaipu, junto à divisão de Estudos Elétricos e Normas.