Revista Estação Científica

# SISTEMAS INSTRUMENTADOS DE SEGURANÇA BASEADOS EM FPGA: UMA REVISÃO BIBLIOGRÁFICA

## *SAFETY INSTRUMENTED SYSTEMS BASED ON FPGA: A REVIEW*

**André Tiago Santos**[1]
**Alexandre Simião Caporali**[2]

**RESUMO**

Este estudo tem como objetivo discutir o emprego dos Sistemas Instrumentados de Segurança (SISs) baseados em Dispositivos Lógicos Reconfiguráveis (FPGAs) em plantas industriais, observando os parâmetros normativos, modos de aplicação e o mecanismo pelo qual o SIS age na planta. Trata-se de uma revisão bibliográfica baseada na literatura especializada através de consulta a artigos científicos selecionados, basicamente, através de busca no banco de dados do Scielo, da IEEE *Xplore* e da CAPES CAFe. Os estudos encontrados sobre o emprego de SIS apontaram que este modelo de controle mitiga efeitos indesejáveis em Processos Produtivos. Os parâmetros normativos proporcionam um próprio desenvolvimento na redução destes efeitos. Os tipos de SIS mais aplicados foram os que usaram Controladores Lógicos CLPs, Controles Difusos (*Fuzzy*) e integrações com Sistemas Supervisórios. As arquiteturas de FPGA empregadas foram para que se comparassem as velocidades de processamento com CLPs, que se diferenciassem as arquiteturas de votação e emprego em Controladores *Fuzzy*. Um dos estudos explicou o mecanismo de atuação da arquitetura baseada em FPGA em SIS. Ainda é necessário robustecer os estudos sobre o emprego dessa modalidade de Controle e Automação, já que os parâmetros normativos são de relevante importância e permitem o uso deste modo de Arquitetura de Solucionador Lógico.

[1] Mestre Profissional em Automação e Controle de Processos pelo IFSP (2017). Professor do Ensino Básico, Técnico e Tecnológico do IFSP – câmpus Registro.
[2] Doutor em Engenharia Mecânica pela Universidade de São Paulo - USP (2003). Professor do Ensino Básico, Técnico e Tecnológico do IFSP – câmpus São Paulo. Artigo com área temática de Engenharias.

**PALAVRAS-CHAVE:** Automação, Processos Industriais, Sistemas Instrumentados de Segurança, FPGA, Revisão bibliográfica.

## 1 – INTRODUÇÃO

Os Sistemas Instrumentados de Segurança (SISs) são sistemas de automação capazes de prevenir e/ou mitigar consequências indesejáveis de eventos perigosos ocasionados por falhas detectadas e tratadas, de acordo com Santos *et al*. (2017). Acidentes e incidentes são condições indesejáveis para o andamento de um processo produtivo, pois, podem representar um sério risco no que diz respeito à integridade física das pessoas, ao meio ambiente e à estrutura econômico-financeira no qual a empresa está instalada. Daí se evidencia a importância dos SIS.

Em automação e controle, especificamente, existem diversas alternativas para implementação de sistemas controladores, inclusive de programação embarcada de SIS, dentre elas, os dispositivos FPGA (*Field Programmable Gate Array*), que são circuitos programáveis capazes de implementar módulos digitais e podem ser alterados, praticamente, em qualquer instante durante o desenvolvimento, através de programação reconfigurável e de modo dinâmico, ou seja, que representa a possibilidade de se modificar, de modo total ou parcial, a funcionalidade de um sistema, formatando-se uma boa escolha para implementação de sistemas.

No sentido de se consolidar estudos envolvendo arquiteturas flexíveis de sistemas embarcados implementados em SIS, é de considerável relevância pesquisar os trabalhos realizados e os estudos experimentais concluídos, com resultados convergentes aos objetivos, bem como estabelecer o relacionamento entre os tópicos em aplicações industriais em Sistemas de Automação e Controle de Processos.

Este trabalho, portanto, tem como objetivo realizar uma revisão de literatura sobre a correlação entre trabalhos experimentais realizados entre Sistemas Instrumentados de Segurança e suas implementações com Sistemas de Eletrônica Embarcada FPGA.

## 2 – METODOLOGIA

O presente artigo foi elaborado a partir de uma revisão bibliográfica nas bases de dados: IEEE Xplore (Explorador de publicações na revista Internacional de Engenharia Eletroeletrônica), SciELO, CAPES CAFe (Comunidade Acadêmica Federada vinculada a Coordenação de Aperfeiçoamento de Pessoal de Nível Superior) e nas bases que contemplam artigos de congressos e/ou publicações conclusivas de teses e/ou dissertações. As palavras-chave empregadas foram “Sistemas Instrumentados de Segurança”, “SIS”, “FPGA” e “SIL” (*Safety Integrity Level* – Nível de Integridade de Segurança, em inglês) e seus correspondentes em inglês “*Safety Instrumented System*” e demais siglas. Definiram-se como critérios de exclusão artigos publicados antes do ano 2000 e que não se demonstrassem artigos utilizados em aplicações destinadas a plantas de controle de processo. A pesquisa dos artigos foi realizada em duas fases: entre março de 2016 e março de 2017 e; durante o mês de março de 2020, esta última para que se consolide um estado da arte.

A busca nos bancos de dados foi realizada utilizando as terminologias e notações de Engenharia de Automação, Instrumentação Industrial e de Sistemas em tópicos multidisciplinares comuns em português e inglês. As palavras-chave utilizadas na busca foram Sistemas Instrumentados de Segurança, Nível de Integridade de Segurança, Função Instrumentada de Segurança e FPGA.

Os critérios de inclusão para os estudos encontrados foram à abordagem do emprego de SIS em plantas de processos industriais, de ensaio ou não, com base na Arquitetura implementada com dispositivos reconfiguráveis FPGA. Foram excluídos estudos que relatavam o emprego de outras modalidades de implementação, que não os SIS baseados em FPGA.

A seguir, buscou-se estudar e compreender os principais parâmetros e forma de aplicação empregados nos estudos encontrados, de acordo com os parâmetros normativos e as bases eletroeletrônicas para a utilização de SIS, bem como o mecanismo e modelo de Dispositivo Reconfigurável pelos quais o SIS atua na planta produtiva industrial.

## 3 – DISCUSSÕES E RESULTADOS

Serão apresentadas, a seguir, as sínteses analíticas de alguns trabalhos que foram fundamentais na realização de tal pesquisa no sentido de se consolidar os resultados e as discussões a respeito da revisão. Resumidamente, abordaram-se 10 (dez) artigos sobre SIS e 8 (oito) artigos que versaram sobre FPGA e que ambos temas tiveram relação direta em aplicações industriais.

### 3.1 – Sistemas Instrumentados de Segurança - SIS.

Sekiou *et al.* (2013) explanam o conceito de falhas, diagnósticos, níveis intrínsecos de falhas, arquitetura de um SIS e os resultados de simulação de um forno em um processo industrial de manutenção da gaseificação. As normas da Comissão Eletrotécnica Internacional 61508 e 61511 são os documentos norteadores de tais sistemas que envolvem programação em plataforma de computação e de sinais eletrônicos para equipamentos de segurança.

Sekiou *et al.* (2013), basicamente, definem SIS, como segue: Sistemas Instrumentados de Segurança (SIS) são dispositivos de elétrica/eletrônica programável relacionada à segurança eletrônica de sistemas que se destinam a alcançar ou manter um estado seguro para o Equipamento sob Controle (EUC – sigla em inglês), a respeito de um evento perigoso específico.

Um sistema bem projetado pode aumentar a disponibilidade do EUC e reduzir o número de falhas espúrias causadas por um SIS que não avaliar adequadamente a situação de segurança e, desnecessariamente, desligar um processo. Os dados sugerem que 90% dos problemas nos SIS podem ser atribuídos aos elementos finais e sensores (SEKIOU *et al.*, 2013).

Este artigo (SEKIOU *et al.*, 2013) apresenta os resultados de uma simulação e estudo experimental baseado no diagnóstico de falhas do SIS componentes (especialmente sensores). O EUC é um forno em indústria de processamento de gás. Foi demonstrado que adicionar um segundo sensor para o SIS pode melhorar seu desempenho, denotado de Nível de integridade de segurança: SIL.

Considerando o desenvolvimento do Sistema, em (FANG *et al.*, 2008), o planejamento, desenho e a arquitetura de tal devem seguir procedimentos e métodos descritos pelas Normas e Dispositivos Legais. Em função desta dissertação, o diagrama em V (Figura 1) para desenvolvimento de programa de computador compatível para um SIS é o elemento normativo norteador para a especificação, desenvolvimento, testes e validação de tal dispositivo. É importante salientar, também, as definições de estado seguro do Sistema, na qual, o Equipamento sob Controle opera em condições seguras em caso de falha detectada pelo SIS (JIN *et al.*, 2011). Neste caso, as condições de estudo e análise de falha deste sistema dependerão da probabilidade de ocorrência de desvios operacionais por hora (*PFH – Probability of Failure per Hour* – tradução livre) e da quantização dos Níveis de Integridade e Segurança (*SIL – Safety Integrity Level* – tradução livre) dadas variáveis constantes para a obtenção do modelo de Markov. Não será tratado deste método como objeto desta edição.

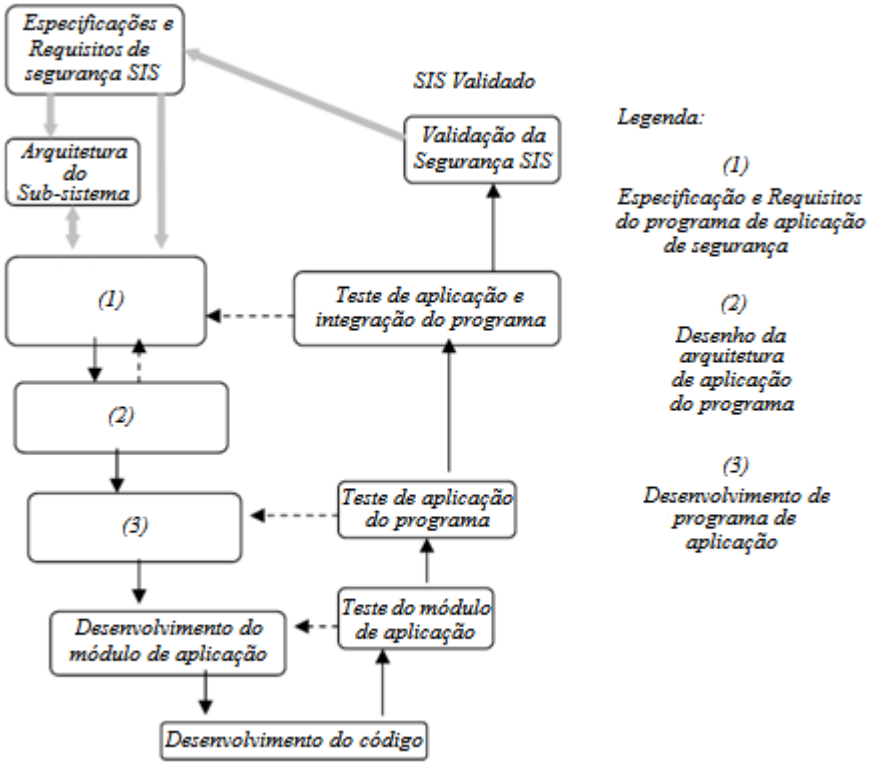


**Figura 1: Diagrama em V para desenvolvimento de programa computacional para SIS**

Assim, foi apresentado, em Fang *et al*. (2008), procedimento e método para o projeto e desenvolvimento do Sistema Instrumentado de Segurança (SIS) em processos industriais. Foi introduzida uma técnica para análise de risco do sistema e avaliação de risco inicial foi usada para determinação da Função Instrumentada de Segurança (SIF). Procedimento e métodos de Nível de Integridade de Segurança (SIL) seleção são pesquisados em detalhes. Planejar e projetar o SIS foram investigados.

Cerrando este estudo de Fang *et al*., (2008), propuseram-se métodos de análise de risco do sistema e avaliação de risco. E depois foram apresentadas abordagens de seleção, plano e engenharia do Nível de Integridade de Segurança (SIL) para o SIS conforme as normas referenciadas.

Os Padrões Internacionais e Diretrizes propõem metodologias qualitativas e quantitativas para a segurança avaliação do sistema de instrumentos de segurança (SIS). No entanto, algumas dessas metodologias costumam ser complexas e não são muito fáceis de aplicar. De fato, algumas críticas são encontradas pelos técnicos votados na segurança funcional, como o estudo do SIS para arquiteturas complexas, o cálculo dos parâmetros de segurança, como a identificação do subsistema SIS durante a revisão do projeto para garantir os requisitos de segurança, e assim por diante (CATELANI *et al.*, 2011).

Assim, Catelani *et al*. (2011) abordam método menos complexo para determinação do nível de segurança de uma planta, baseado nas diretrizes das normas internacionais (IEC 61508 e IEC 61511), nos modelos básicos de Sistemas Instrumentados de Segurança – SIS e na determinação das Probabilidades de Falha na Demanda (PFD) de cada Subsistema desenvolvido e do Sistema total.

Com relação a topologia do Sistema de Segurança, dependendo da configuração no qual o Sistema é construído na Malha de Controle, se tem um modelo de análise de falha distinto para cada configuração, conforme padrões internacionais. Neste caso, a topologia de arquitetura em série de sistemas permite que a saída de cada Sistema seja conectada diretamente a entrada da mesma. A configuração em paralelo permite que todas as entradas dos equipamentos sejam interconectadas bem como todas as saídas. Há, ainda, uma terceira via de topologia denominada KooN (*K outs of N nodes* – K saídas

de N nós de entrada – tradução livre), de configuração complexa em função das anteriores, que garante de modo criterioso o funcionamento do Sistema de acordo com os nós de entrada conectados aos diversos ramos de saída (CATELANI *et al*., 2011).

O modelo adotado e normatizado para análise de falha do Sistema é denominado Probabilidade média de Falha na Demanda (*Probability of Failure on Demand - PFD*), no qual define o Nível de Integridade de Segurança (SIL, em inglês) a ser implementado no Sistema (CATELANI *et al*., 2011).

Concluindo, o objetivo do artigo produzido por Catelani *et al.*, (2011) é propor uma metodologia simplificada e mais eficiente para a avaliação da segurança SIS eletromecânico em conformidade com as normas IEC 61508 e IEC 61511. A técnica proposta baseia-se numa implementação alternativa da abordagem do Diagrama de Blocos de Confiabilidade (RBD – sigla em inglês) para a análise de desempenho do sistema de instrumentos de segurança. É considerado, a fim de demonstrar as vantagens da proposta, um estudo de caso de algumas das funções de segurança. Com relação a outras metodologias normalmente utilizadas para a análise de segurança, os resultados provaram que a abordagem proposta é mais fácil na aplicação e economiza tempo. Além disso, tais resultados são comparativamente próximos daqueles obtidos usando o Padrão dos métodos.

Ainda tomando o quesito analítico para este artigo, Lundteigen e Rausand (2007) abordaram o tópico da Causa Comum de Falhas (*Common Cause Failure* – CCF – tradução livre) em SIS para processos produtivos em indústrias de Óleo e Gás, de modo a implementar medições para níveis SIL e atribuições SIF eficazes dentro do período do teste das funções de instrumentação das plantas (malhas de controle: transmissores, controladores, elementos finais e seus componentes), especificamente para os processos produtivos citados e extensivamente a qualquer processo produtivo instrumentado.

As CCF, definida, segundo a norma, estritamente: *as a failure which is the result of one or more events, causing failures of two or more separate channels in a multiple channel system, leading to a system failure* (IEC 61511, 2003 *apud* LUNDTEIGEN, RAUSAND, 2007), traduzindo: como uma falha da qual é resultado de um ou mais eventos, causando falhas em dois ou mais canais

separados em um sistema de múltiplos canais, indicando a uma falha de sistema (tradução livre).

Deste modo, Lundteigen e Rausand (2007) apresentam uma abordagem de defesa de Causa Comum de Falhas (CCF) para sistemas instrumentados de segurança (SISs) na indústria de petróleo e gás. O SIS normalmente opera no modo de baixa demanda, o que significa que testes e inspeções regulares são necessários para revelar possíveis falhas no SIS. A abordagem de intervenção para as CCF compreende listas de verificação e ferramentas analíticas que podem ser integradas com as abordagens atuais para a função de teste, inspeção e acompanhamento (por diagramas de influência, análise de tarefas e matrizes de causa-efeito simplificadas). O documento enfoca como as medidas de salvaguarda podem ser implementadas para aumentar a conscientização sobre melhorar a capacidade de detectar CCFs e evitar a introdução de novos CCFs. A abordagem de defesa do CCF também pode ser aplicável a outros setores da indústria.

O artigo intitulado: Modelagem e otimização de políticas de testes de prova para Sistemas Instrumentados de Segurança, de Torres-Echeverría *et al.* (2009), introduzem um novo desenvolvimento para modelos de determinação de probabilidade de falha na demanda, dependentes do tempo, para arquiteturas dispostas em paralelo, e ilustra tal aplicação para otimização multiobjetiva em políticas de testes de prova para SIS. O modelo é baseado no ciclo médio de testes, que incluem diferentes intervalos em avaliação dos quais o módulo caminha no tempo de serviço: testes, reparos e tempo mensurado entre testes. O modelo destina-se a avaliar explicitamente os efeitos de diferentes frequências e estratégias de teste (ou seja, simultânea, sequencial e escalonada). Inclui a quantificação de falhas detectadas e não detectadas e coloca especial ênfase na quantificação da contribuição da falha de causa comum na probabilidade do sistema de falha na demanda como componente adicional. Posteriormente, o artigo apresenta a otimização multiobjetiva de políticas de teste de prova com algoritmos genéticos, usando este modelo para quantificar a probabilidade média de falha na demanda como um dos objetivos. Os outros dois objetivos são a taxa de erros espúrios e o custo do ciclo de vida do sistema. Isso permite equilibrar os aspectos mais importantes da implementação do sistema de segurança. A

abordagem aborda os requisitos da norma IEC 61508, bem como à sua aderência. A metodologia geral é ilustrada através de um caso de aplicação prática de um sistema de proteção contra altas temperaturas e pressão de um reator químico.

Os resultados obtidos na publicação de (TORRES-ECHEVERRÍA *et al.*, 2009) foram o de aproximação do modelo esperado com a otimização obtida no que tange às políticas de testes de prova e o de provimento de benefícios ao gestor (tomador de decisões) em termos das otimizações em si e do melhor conhecimento do comportamento do Sistema de Segurança, se fazendo uma ferramenta poderosa em aplicações práticas para análises em sistemas industriais.

Conforme relatam Wang, Chen e Yu (2017) os sistemas de supervisão da segurança de fornos (FSSSs, sigla em inglês) desempenham papel importante na proteção de perigos em caldeiras de centrais térmicas. Para avaliar o desempenho do próprio FSSS, as teorias de segurança funcional estão aplicadas no artigo para alcançar a adequada análise de risco, atingir o nível de integridade da segurança (SIL) determinado e avaliar a segurança funcional. A Função instrumentada de segurança mais importante (SIF) de FSSS - vazão de combustível do mestre (MFT) é considerada. A probabilidade de falha na demanda (PFD) é calculada com base no método de análise de árvore de falhas (FTA). De acordo com o resultado da análise, o alvo SIL para o FSSS é 2 (dois), mas o sistema atual não atende aos requisitos. Através de medidas corretivas de votação um-de-dois (1oo2) - configuração redundante para cada atuador - e comprimindo o ciclo de testes funcionais, o índice de segurança da MFT finalmente atinge o valor alvo, em conformidade com os resultados esperados para tal modelo.

Conforme o trabalho retratado por Qi *et al* (2020), os sistemas instrumentados de segurança (SISs), usados em várias indústrias, são projetados para executar funções específicas de segurança para evitar possíveis cenários de acidentes. Entretanto, a ativação espúria ocorre quando um SIS é ativado em um momento oportuno, de modo potencial, resultando em interrupção da produção, perda econômica, bem como o risco de se apresentar durante a restauração do sistema. Portanto, é necessário quantificar a taxa de

ativação espúria para reduzir este número (taxa) de ativações e alcançar o mais alto nível geral de redução de riscos. Este estudo analisa possíveis cenários levando a uma falha espúria nos subsistemas do SIS e apresenta um desenvolvimento adicional das fórmulas para calcular a Taxa de Falha Espúria (*Spurious Trip Rate* - STR) para qualquer configuração do KooN. As fórmulas propostas são comparadas aos existentes modelos para evidenciar as melhorias e são aplicados em cálculos numéricos para investigar a integridade operacional dos subsistemas do SIS. Os resultados indicam que a falha de causa comum contribui para a maioria do STR em elementos de entrada e solucionadores lógicos, e configurações ideais com PFDavg (Probabilidade de Falha na Demanda média, sigla em inglês) inferior e STR menor é identificado em cada subsistema. A abordagem geral é ilustrada através de um simples estudo de caso e algumas conclusões são tiradas: possíveis cenários de falha que contribuem para a ativação espúria em dois diferentes tipos de configurações KooN (K - 1 <N - K e K - 1 ≥ N - K) e diferentes subsistemas do SIS são analisados, e o STR estimado fórmulas para qualquer configuração do KooN são propostas com base no análise de cenário e a suposição de que uma combinação de falhas do tipo *Spurious Operation* – SO (operação espúria – tradução livre) e *Dangerous Detected* - DD (perigosa detectada – tradução livre) leva a um lapso operacional espúrio. Os cálculos das Causas Comuns de Falha (CCF) estão resumidos e envolvido nas fórmulas STR e verifica-se que a CCF contribui para na maioria das configurações STR em KooN, onde 1 <K <N da entrada elementos e solucionadores de lógica. A análise das fórmulas propostas em subsistemas indica que existe uma seleção ideal de K e N em um Configuração KooN que leva a um PFDavg mais baixo (alta integridade de segurança) e um STR menor (alta integridade operacional). Os resultados podem ser úteis para pesquisas adicionais relacionadas à otimização da configuração e concepção do SIS, considerando os aspectos de confiabilidade e disponibilidade.

O sistema instrumentado de segurança (SIS) é um dispositivo essencial para proteger as indústrias de situações perigosas. A confiabilidade do SIS é medida pela análise da probabilidade de falha sob demanda (PFD), que é uma parte integrante da avaliação quantitativa de risco e segurança para determinar

o nível de integridade de risco e segurança. O PFD varia de local para local devido aos efeitos atmosféricos. Neste artigo, novos modelos matemáticos propõem-se calcular a probabilidade de falha do equipamento devido à corrosão considerando três fatores atmosféricos: temperatura, umidade e velocidade do vento. Os modelos são resolvidos pelo método de mínimos quadrados e usa-se este padrão de dados para identificar os parâmetros envolvidos nos modelos. Finalmente, a comparação entre os dois modelos propostos é feita para selecionar o melhor modelo para calcular a probabilidade de falha. Os modelos fornecem boa correlação com os dados de referência. Deste modo, esses modelos podem ser usados para calcular o PFD em qualquer localização geográfica (OUACHE; KABIR, 2016).

O trabalho realizado por Redutskiy (2017) dá um panorama dos processos da indústria de petróleo e gás, que estão associados a gastos e riscos significativos. Adequação das decisões sobre medidas de segurança tomadas nas fases iniciais do planejamento das instalações e processos contribui para evitar incidentes tecnológicos e perdas correspondentes. São propostas formulação de requisitos simples para sistemas instrumentados de segurança que são seguidos mais adiante durante o projeto de engenharia detalhado e as operações, bem como um modelo matemático para projeto de sistema de segurança é apresentado de forma generalizada. O modelo visa refletir as perspectivas divergentes das principais partes envolvidas em projetos de petróleo e gás; e, portanto, é formulado como um problema multi-objetivo. Aplicação de otimização de caixa preta é sugerido, para resolver instâncias da vida real. Um modelo de Markov é aplicado e leva em conta falhas de dispositivo, incidentes tecnológicos, restaurações contínuas e manutenção para um determinado processo e configuração do sistema de segurança. Esta pesquisa é relevante a departamentos de engenharia e empreiteiros, especializados em planejar e projetar a solução tecnológica. A análise da computação (o resultado do experimento) revela que o desenho proposto abordagem de otimização pode sugerir esquemas de redundância aconselhável para os subsistemas e para restringir os especialistas no sentido de prover os componentes de sistema necessários. A aplicação do modelo proposto não é limitado a formular apenas os requisitos e pode também ser aplicado como ponto de partida para

desenvolvimento de engenharia detalhada ou para fins de pesquisa para soluções de engenharia razoáveis.

Sistemas de Segurança (ou Interfaces de Segurança) são equipamentos de extrema importância em ambientes industriais diversos, desde metalúrgicas até petroquímicas e indústrias nucleares. Os Sistemas Instrumentados de Segurança (SISs) são utilizados para monitorar a condição de valores e parâmetros de uma planta industrial, dentro dos limites operacionais e quando houver condições de riscos devem gerar alarmes e colocar a planta em uma condição segura ou mesmo na condição de desligamento (*shutdown*). Seu objetivo principal é evitar acidentes dentro e fora das fábricas, como incêndios, explosões, danos aos equipamentos, proteção da produção e da propriedade e mais do que isto, evitar riscos de vidas ou danos à saúde pessoal e impactos catastróficos para a comunidade. Este trabalho apresenta um estudo sobre um Sistema Instrumentado de Segurança (SIS) de arquitetura 1oo1, a partir de simulação, testes experimentais e o desenvolvimento de um protótipo, constituído por *hardware* e *software* embarcado em dispositivo de lógica reconfigurável (FPGA), que em conjunto, permitiram analisar e determinar as condições de riscos e diagnóstico de falhas do SIS. Os resultados obtidos demonstraram que o sistema proposto funcionou satisfatoriamente em função dos requisitos de segurança estabelecidos (SANTOS *et al*., 2017).

Portanto, os 10 (dez) autores dos quais descreveram os Sistemas Instrumentados de Segurança e as Funções Instrumentadas de Segurança trabalharam com a abundância suficiente de informações relativas às normas vigentes, métodos de desenvolvimento do SIS, arquitetura do Sistema e, bem como, a implementação do Nível de Integridade de Segurança requerido para cada Sistema desenvolvido à aplicação desejada. Apenas 1 (um) destes implementou um SIS com FPGA.

### 3.2 – Dispositivos Lógicos Reconfiguráveis baseados em FPGA.

Tratando-se de sistemas reconfiguráveis, o trabalho realizado por Ichikawa e demais (2011) explanaram que, embora, um controlador lógico programável (CLP) tenha sido amplamente adotado para o controle sequencial de maquinário industrial, seu desempenho nem sempre satisfaz os requisitos

recentes em sistemas grandes e altamente responsivos. Com o estado da arte tecnologia FPGA (*Field Programmable Gate Array*), é possível implementar um programa de controle com lógica *hard-wired* para resposta e redução do custo/espaço de implementação. Esta abordagem também vale a pena para a transmigração de legado de *software* de CLP no futuro *hardware* de controle baseado em FPGA. Este estudo apresenta um método sistemático para implementar uma sequência controle do software do CLP. As instruções de CLP são convertidas em códigos VHDL - ou "VHSIC *Hardware Description Language*" (Linguagem de descrição de hardware VHSIC "*Very High Speed Integrated Circuits*") que é uma linguagem utilizada para facilitar o projeto/concepção de circuitos digitais em FPGA - e, em seguida, implementadas como circuito lógico com várias funções periféricas. Programas de CLP produtivos foram examinados com o Mitsubishi Electric FX2N PLC e o Altera Stratix II FPGA, e foram mostrados para caber em um chip FPGA comum. Um projeto sequencial simples foi estimado em 184 vezes mais rápido que o CLP, enquanto um *design* de plano orientado para desempenho foi estimado em 44 vezes mais rápido do que o projeto Sequencial (ou seja, 8050 vezes mais rápido que o CLP). Um sistema prático de enrolamento de camada foi realmente construído e operado com sucesso com a placa de controle FPGA, cujo desenho lógico foi implementado com nossas ferramentas. (ICHIKAWA *et al.*, 2011).

O artigo apresentado por (BÖRCSÖK, 2008) retrata como os sistemas embarcados são cada vez mais utilizados. Em aplicações industriais, FPGAs estão sendo usados em conjuntos complexos de sistemas críticos. O objetivo foi o de apresentar as ideias básicas por trás da arquitetura do sistema 1oo2 relacionado à segurança na plataforma FPGA. Desde sistemas com um único processador (1oo1) fornecem consumo relativo para entradas efetivas com uma classificação de integridade de segurança de SIL2, uma arquitetura dupla (1oo2) que oferece alta segurança. A integridade de uma classificação de SIL3, é apresentada. Na primeira fase, o design completo de um simples Processador FPGA 16 bits RISC e um projeto de sistema *on-chip* sintetizável. O VHDL é apresentado e as exigências de segurança para a arquitetura 1oo2 é fornecida. Na segunda metade, a implementação da arquitetura RISC e da arquitetura 1oo2 e alguns aplicativos executáveis são exibidos.

O FPGA que foi empregado neste projeto é o Xilinx XC2V500-6FG456C. XC2V indica o tipo de dispositivo que é Virtex2, 500 mostra o número de portas lógicas, -6 mostra grau de velocidade, FG mostra tipo de pacote, 456 mostra o número de pinos e C é faixa de temperatura (0 ° C a + 85 ° C). Virtex2 é projetado para alta performance com alta velocidade e baixa potência consumo. Os FPGAs da Xilinx Virtex são baseados na configuração de Tabelas tipo *Look up Tables* (LUTs).

Os resultados obtidos no trabalho de (BÖRCSÖK, 2008) mostraram que os ganhos obtidos para uma arquitetura baseada em sistema de votação 1oo2 foram expressivos em razão da arquitetura 1oo1 e as chances de encontrar falhas na arquitetura proposta pelo artigo são maiores. Já o consumo do número de blocos lógicos na programação VHDL aumentou, somente, 24% em função da arquitetura anteriormente avaliada.

Nadir *et al*. (2016) propõem a análise de um controlador de segurança com lógica difusa implementado em FPGA com arquitetura 2oo3 utilizando uma análise qualitativa e quantitativa fornecida por esses padrões. A análise quantitativa é realizada pelo cálculo da probabilidade média de falha na demanda (PFDavg) do sistema relacionado à segurança para definir o seu nível de integridade de segurança (SIL). A análise qualitativa baseia-se nos Método do Diagrama de Blocos de Confiabilidade e Análise de Árvore de Falhas, cujos resultados definiram que a análise qualitativa baseada na Análise da Árvore de Falhas se obtiveram resultados triviais com relação ao Diagrama de Blocos de Confiabilidade, no qual se devem considerar todos os coeficientes e fatores para a obtenção do nível de integridade de segurança.

O componente utilizado para o desenvolvimento do projeto no artigo de Nadir *et al*. (2016) é o *Spartan 3E Starter Kit Board* da fabricante *Xilinx* (família *Spartan3-E* xc5s500e-4fg320).

Assim, o Controlador de Segurança baseado em Lógica Difusa (*Safety Fuzzy Logic Controller* – SFLC) de arquitetura de votação 2oo3, possui uma arquitetura de redundância com três controladores dotados de Controladores de Lógica Difusa (*Fuzzy Logic Controller* – FLC) e o temporizador *watchdog,* para monitoramento de processamentos indesejados no sistema computacional. Esta arquitetura tem um arranjo de votação por maioria para os sinais de saída. Se

somente um dos FLC der um resultado discordante com os dois demais, o estado de saída para a SIF não mudará (NADIR *et al*., 2016).

No trabalho retratado por Maerani *et al*. (2018), o processo de verificação é muito importante para o novo processo de desenvolvimento ou reengenharia da Instrumentação e Controle (I&C) na Usina Nuclear (*Nuclear Power Plants* - NPP). Devido ao fato de o componente de recurso de segurança de engenharia do Sistema de Controle (*Engineered Safety Feature-Component Control System*, sigla ESF-CCS) é um sistema crítico de segurança, é necessário especificar uma abordagem sistemática para verificar o desempenho do desenho de desenvolvimento. Para esse processo de verificação, uma abordagem de engenharia de sistema é usada e refere-se ao ciclo de vida do projeto de código computacional para verificar o código VHDL na implementação do ESF-CCS baseado em matriz de portas reconfiguráveis (FPGA). Embora o FPGA não use *software*, o FPGA precisa de um Linguagem de Descrição de *Hardware* (*Hardware Description Language* - HDL) para descrever os sinais digital e misto para um sistema integrado. Portanto, o código VHDL deve ser verificado para garantir que esse nível de código não cause erros no sistema baseado em FPGA, especialmente para o desenvolvimento do ESF-CCS. O método de verificação é iniciado observando-se a análise dos requisitos, verificação das saídas projetadas, desenvolvimento dos testes do código de processamento computacional para verificar a confiabilidade do código que é para apoiar o ESF-CCS baseado em FPGA. O teste de caixa branca é usado para que se teste de *software* para demonstrar as respostas do código VHDL, se o desenho é bem-sucedido ou não, e o estado do teste de cobertura está em sua totalidade (100%). Dentro Além disso, a Análise da Temporização Estática (*Static Timing Analysis* - STA) é aplicada para verificar o tempo de atraso. Depois de todas as etapas de verificação realizadas, os resultados do projeto podem ser validados. Neste artigo, o ESF-CCS baseado em FPGA usando código VHDL é verificado e habilita o código computacional a responder adequada e normalmente às entradas e condições propostas devido ao fato de serem cobertas em sua integralidade.

Já o uso de FPGAs (*Field Programmable Gate Arrays*) em sistemas críticos de segurança nas usinas nucleares significa que esses sistemas devem

passar por uma análise detalhada de confiabilidade e segurança. A Análise de Árvores de Falhas (*Fault Tree Analysis* - FTA) tem sido amplamente utilizada na indústria de energia nuclear. No entanto, a FTA é anterior aos sistemas digitais de I&C e realiza apenas análises estáticas. Portanto, metodologias dinâmicas (dependentes do tempo) foram criadas para modelar e analisar sistemas digitais de I&C. Um destes é a Metodologia Fluxográfica Dinâmica (*Dynamic Flowgraph Methodology* - DFM). O DFM pode modelar malhas de controle e realimentação, que são propriedades inclusas aos sistemas baseados em FPGA. Este trabalho apresenta uma comparação dos métodos de análise FTA e DFM, para analisar a confiabilidade de um laço lógico de inconsistência operacional de reator baseado em FPGA genérico, de um parâmetro e um canal. O sistema foi analisado para duas condições de falha separadas, com os resultados do DFM e do FTA sendo comparados. Os resultados do DFM e do FTA foram semelhantes para sistemas simples usando uma etapa de tempo, no entanto, os resultados foram mais diferentes para várias etapas de tempo e/ou sistemas de teste complexos. Problemas com o FTA foram descobertos pertencentes aos estados de sincronismo temporal (*clock*) oscilante, levando ao impossível retorno do MCS (Conjunto Mínimo de Corte, sigla em inglês) pelo FTA. São discutidas as razões potenciais para os diferentes resultados retornados por dois métodos, assim como as orientações para futuras comparações entre esses métodos (McNELLES *et al*., 2016).

Seguindo a mesma analogia, Hsu e Yang (2016) versam sobre a importância dos desenvolvimentos com Matrizes de portas programáveis – reconfiguráveis - (FPGAs), como dispositivos de lógica programável (*Programmable Logic Devices* - PLDs), que ganharam interesse em implementações e aplicações em I&C de segurança em usinas nucleares devido às vantagens específicas dos FPGAs sobre as aplicações digitais microprocessadas de I&C, atualmente, mais comuns. Existem pontos em comum entre Desenvolvimentos de aplicativos de I&C Baseados em FPGA e em microprocessador/microcontrolador. Os FPGAs são visualizados como uma mistura de configuração física e lógica. O ciclo de vida de desenvolvimento de *software* e *hardware*, portanto pode ser implementado às aplicações de I&Cs baseadas em FPGA como no caso para aplicativos baseados em

microprocessadores. Alcançar alta confiabilidade nas implementações de aplicativos com FPGAs, é necessário que se siga o processo de desenvolvimento do ciclo de vida que seja consistente com o IEEE *Std.* 1074, Padrão IEEE para Ciclo de Vida do Desenvolvimento de Processos de Recursos Computacionais e as rigorosas Metodologias de V&V (Verificação e Validação) definidas no dispositivo normativo IEEE *Std*. 1012, Padrão IEEE para Verificação e Validação dos tais Recursos, tanto nas implementações baseadas em microprocessadores. No entanto, a implementação específica dos aplicativos de I&C baseados em FPGA é muito original e com características próprias que também são ditados pelos fabricantes de FPGA. As atividades de implementação da arquitetura e do projeto do FPGA envolvem a programação do Dispositivo, bem como sua codificação, simulação e processos de geração de arquivos binários. O artigo apresenta uma descrição detalhada processo de implementação do FPGA para aplicações de I&C de segurança à luz de um caso de sucesso para um dos NPPs, uma atualização desta aplicação usando componentes de Dispositivos Reconfiguráveis para substituir o obsoleto Controlador Intel, baseado no microprocessador 8085, onde os FPGAs emulam os processos dos microprocessadores e interpretadores existentes na execução do processamento da CPU. Para validar a implementação e garantir que os requisitos do usuário final funcionem e sejam totalmente atendidos, é crítico que as partes funcional e estrutural, bem como testes de simulação, sejam realizados com projetos/casos bem sucedidos de teste e as ferramentas do fabricante do Dispositivo devem ser avaliadas e qualificadas pela sua adequação ao uso. O teste de simulação da Matriz Reconfigurável é parte essencial da implementação da configuração. Assim, em razão dos testes de simulação da referida Matriz, a qualificação relacionadas às ferramentas de simulação é integral.

As técnicas tradicionais de tolerância a falhas baseadas em redundância espacial e temporal geralmente implicam alta potência, atraso e área despesas gerais. As soluções econômicas geralmente dependem do design do sistema e da plataforma de hardware disponível. Especialmente para Arranjos de Portas Reconfiguráveis (FPGAs), erros leves na memória de configuração são uma ameaça significativa à confiabilidade. Nesse trabalho, apresenta-se um mecanismo de tolerância a falhas estendido e abrangente, especialmente

adequado para lidar com configurações falhas em sistemas baseados em FPGA que devem lidar com vários modos de falha. Cada modo de falha pode apresentar diferentes criticidade e probabilidade de ocorrência, e essas propriedades são medidas e exploradas para fornecer soluções de baixo custo quando comparadas às abordagens padrão, como redundância modular tripla. As propriedades exploradas são normalmente encontradas no monitoramento crítico de sistemas que podem acionar alarmes e avisos críticos ou de segurança em geral. Nesses sistemas, a falha em acionar um aviso, quando necessário, é frequentemente considerada mais crítica do que fornecer um falso alarme ocasional. Por exemplo, Correspondência de Expressão Regular (*Regular Expression Matching* - REM), um mecanismo de uso intensivo da computação usado para executar a Inspeção Profunda de Pacotes em situações críticas em aplicativos de rede, apresenta essas propriedades, e pode ser muito acelerado pelos FPGAs para atender às restrições de desempenho em redes de alto rendimento. Portanto, usamos mecanismos REM baseados em FPGA como um estudo de caso para demonstrar a eficácia das técnicas propostas. Além disso, é introduzido um mecanismo de posicionamento e reinício com reconhecimento mútuo para reduzir o tempo de reparo, melhorando a confiabilidade e disponibilidade do sistema. Resultados experimentais mostram que a taxa de falhas e o reparo o tempo pode ser reduzido em 95 e 90%, respectivamente, evitando, de modo incremental, os custos (LEIPNITZ, NAZAR; 2018).

Ainda a versar sobre Dispositivos Lógicos Reconfiguráveis, Kharchenko e Illiashenko (2016) se posicionam em função de os sistemas críticos de instrumentação e controle (I&Cs) de segurança industrial estraem enfrentando mais ameaças e ataques à segurança da informação (em geral e cibernética, em particular). A aplicação de lógica de computação programável, em primeiro lugar, os arranjos de portas lógicas reprogramáveis (FPGA) em sistemas críticos causa déficits de segurança específicos. As técnicas de avaliação de segurança para esses sistemas são baseadas em conhecimentos heurísticos e no julgamento de especialistas. O principal desafio é como levar em consideração os recursos da tecnologia FPGA para I&Cs críticos de segurança, incluindo sistemas nos quais a abordagem da diversidade é aplicada para minimizar os riscos de falha de causa comum. Tais sistemas são chamados sistemas multi-versão (MV). O

objetivo do artigo está na descrição da técnica e ferramenta para casos baseados em casos avaliação de segurança de I&Cs baseados em MV-FPGA. Destarte, o caso de garantia de segurança tende a reduzir incerteza da avaliação de segurança, levando em consideração influência da segurança (cibersegurança) no sistema. É caracterizado pela introdução da técnica de tomada de decisão, fácil de dimensionar, modificar e está em conformidade com os requisitos das normas e padronizações.

Portanto, em razão de se empregar os Dispositivos de Lógica Reconfigurável tipo FPGA, tais trabalhos descrevem implementações de diversas arquiteturas para procedimentos de votação para falhas de componentes/sistemas de controle (inclui-se instrumentação) e/ou de segurança, bem como desenvolvimentos de memoriais de cálculo para os Níveis de Integridades de Segurança (SILs) dadas informações consistentes para que se construíssem estes memoriais. No entanto, nenhum destes programou, de fato, aplicação em que se dispusesse um SIS que fosse desenvolvido baseado em Arquitetura obtida com Dispositivos Lógicos Reconfiguráveis (FPGAs) para Sistemas de Controle de Processos Industriais. Deste modo, evidencia-se a necessidade de se robustecer tal construção, desenvolvimento, implementação e homologação.

## 4 – CONCLUSÃO

Ao analisar as pesquisas revisadas, percebe-se que há um consenso entre os autores na concordância entre os dispositivos normativos e as aplicações de engenharia na área, e, de maneira geral, os componentes de atuação nas SIFs, não obstante, terem utilizado abordagens e denominações distintas.

Nos estudos analisados, grande parte dos autores não descreveu sobre a concepção de SIS baseados em FPGA, mas, com emprego de dispositivos controladores lógicos programáveis de maneira formal ou clássica de programação. Apenas (SANTOS *et al*., 2017) adotaram um desenvolvimento de SIS baseado em FPGA.

Nesse contexto, grande parte dos pesquisadores não se referiram aos desenvolvimentos, implementações e validações de Sistemas Instrumentados de Segurança que se utilizem de Dispositivos Lógicos Reconfiguráveis (FPGAs), com uso simultâneo, que se denota como uma engenharia de automação com um viés distinto de aplicação.

As identificações de componentes de controles automáticos entrelaçados com SIS em distintas arquiteturas de votação e Nível de Integridade de Segurança foram importantes contribuições para gestores industriais e engenheiros de diversas áreas que estão envolvidos diretamente com estes modelos de Sistemas de Segurança.

Com base na revisão apresentada, pode-se afirmar que poucos estudos têm sido realizados nestas áreas, e que a maioria massiva de pesquisadores utilizou uma metodologia de implementação de SIS e FPGA distinta.

Salienta-se, não obstante, a importância de realizar outras pesquisas sobre este tema para que os gestores de plantas produtivas tenham pleno conhecimento técnico sobre os modelos de segurança em sua área de atuação e possam arguir, de modo assertivo, acerca do desenvolvimento de tais sistemas com a arquitetura proposta, principalmente na ocorrência de mudanças e intercorrências indesejadas nas plantas industriais de processo, bem como as atualizações tecnológicas.

Revista Estação Científica

**AGRADECIMENTOS**

Agradeço, primeiramente, ao Pai das luzes por todas as coisas. Aos meus pais, Vivaldo (*in memorian*) e Marta, pela boa formação familiar e pessoal, e, aos meus professores, Dr. Alexandre Simião Caporali e Dr. César da Costa, pelos ensinamentos, paciência e apoio nesta pesquisa.

***ABSTRACT***

*The objective of this study is to discuss the use of Safety Instrumented Systems (SISs) based on Reconfigurable Logic Devices (FPGAs) in industrial plants, observing the normative parameters, modes of application and the mechanism by which the SIS acts in the plant. This is a literature review based on the specialized literature through consultation of selected scientific articles through search in the database of Scielo, IEEE Xplore and CAPES CAFe, basically. The studies found on the use of SIS pointed out that this control model mitigates undesirable effects in Productive Processes. Normative parameters provide their own development in reducing these effects. The most applied types of SIS were those using Logic Controllers PLCs, Fuzzy Controls and Integrations with Supervisory Systems. The FPGA architectures used were to compare the processing speeds with PLCs, which differentiated the voting and employment architectures in Fuzzy Controllers. One of these has explained the performance mechanism of the FPGA-based architecture in SIS. Further studies are needed and must be strengthen on the use of this kind of Control and Automation, since the normative parameters are of relevant importance and allow the use of this mode of Logical Resolver Architecture.*

***KEYWORDS:*** *Automation, Industrial Processes, Safety Instrumented Systems, FPGA, Literature Review.*

## REFERÊNCIAS

BÖRCSÖK, J.; HAYEK, A.; UMAR, M. ***Implementation of a 1oo2-RISC-Architecture on FPGA for Safety Systems.*** Revista *IEEE Transactions* (2008). 6 p.

CATELANI, M.; CIANI, L.; LUONGO, V. ***A simplified procedure for the analysis of Safety Instrumented Systems in the process industry application.*** Microelectronics Reliability 51 (2011): 1503-1507.

FANG, L.; WU, Z.; WEI, L.; LIU, J. ***Design and Development of Safety Instrumented System*.** Revista *Proceedings of the IEEE International Conference on Automation and Logistics*. Qingdao, China, 2008. 6 p.

HSU, A; YANG, S. *FPGA* ***Implementation for Safety I&C Applications.*** Revista *Nuclear Plant Journal.* Jan./Fev., 2016. 4p.

ICHIKAWA, S.; AKINAKA, M.; HATA, H.; IKEDA, R.; YAMAMOTO, H. ***An FPGA implementation of Hard-Wired sequence control system based on PLC Software.*** Revista *IEEJ Transactions on Electrical and Electronic Engineering.* n. 6, p. 367-375, 2011.

JIN, H.; LUNDTEIGEN, M. A.; RAUSAND, M. ***Reliability performance of safety instrumented systems. A common approach for both low– and high-demand mode of operation*.** *Reliability Engineering and System Safety* 96 (2011): 365-373.

KHARCHENKO, V.; ILLIASHENKO, O. ***Fault Tolerance Mechanisms for FPGA-Based Regular Expression Matching.*** Conferência *MATEC Web of Conferences.* 76 (2016). 9p.

LEIPNITZ, M. T.; NAZAR, G. L. ***Fault Tolerance Mechanisms for FPGA-Based Regular Expression Matching.*** Revista *Journal of Electronic Testing.* 34 (2018): 487–506.

LUNDTEIGEN, M. A.; RAUSAND, M. ***Common cause failures in safety-instrumented systems on oil and gas installations: Implementing defense measures through function testing.*** Revista *Journal of Loss Prevention in the Process Industries* 20 (2007): 218-229.

MAERANI, R; MAYAKA, J. K.; JUNG, J. C. ***Software verification process and methodology for the development of FPGA-based engineered safety features system. Revista Nuclear Engineering and Design.*** 330 (2018): 325-331.

McNELLES, P; ZENG, Z. C.; RENGANATHAN, G; LAMARRE, G; AKL, Y; LIXUAN, L. ***A comparison of Fault Trees and the Dynamic Flowgraph Methodology for the analysis of FPGA-based safety systems Part 1:***

***Reactor trip logic loop reliability analysis.*** Revista *Reliability Engineering and System Safety.* 153 (2016): 135–150.

NADIR, F. E.; JBILOU, M.; BSISS, M.; AMAMI, B. ***Safety fuzzy logic controller with 2oo3 architecture implemented in FPGA.*** 5° Conferência Internacional em Sistemas e Controle, Universidade Cadi Ayyad, Marrocos, 2009: 6 p.

OUACHE, R.; KABIR, M. N. ***Models of probability of failure on demand for safety-instrumented system using atmospheric elements.*** Revista *Safety Science.* 87 (2016): 38-46.

QI, M.; YUFENG, K.; XUN, L.; XIAOYING, W.; DONGFENG, Z.; IL, M. ***Spurious activation and operational integrity evaluation of redundant safety instrumented systems.*** Revista Reliability Engineering and System Safety. 197 (2020), 17p.

REDUTSKIY, Y. ***Optimization of safety instrumented system design and maintenance frequency for oil and gas industry processes. Revista Management and Production Engineering.*** Vol. 1, Número 8, Março 2017: 46 – 59.

SANTOS, A. T.; CAPORALI, A. S.; COSTA, C. **Desenvolvimento de sistema instrumentado de segurança baseado em dispositivo reconfigurável.** 2° Congresso de Pós-Graduação do Instituto Federal de São Paulo. IFSP (2017): 3p.

SEKIOU, S.; CHIREMSEL, Z.; DRID, S.; SAID, R. N. ***Failures diagnostic of Safety Instrumented System:*** Simulation and Experimental Study. IEEE *Transactions* – CoDIT'13 (2013). 6 p.

TORRES-ECHEVERRÍA, A. C.; MARTORELL, S.; THOMPSON, H. A. ***Modelling and optimization of proof testing policies for safety-instrumented systems. Revista Reliability Engineering and System Safety.*** 94 (2009): 838-854.

WANG, P.; CHEN, X.; YU, L. ***Application of Functional Safety Theories in Furnace Safety Supervisory Systems.*** 9° Conferência Internacional de Tecnologia de Medições e Automação Mecatrônica. IEEE (2017): 4p.