ISSN 1808-6136

ISSN on-line 2674-7499

SISTEMAS INSTRUMENTADOS DE SEGURANÇA IMPLEMENTADOS EM DISPOSITIVOS LÓGICOS RECONFIGURÁVEIS: UMA REVISÃO SISTEMÁTICA

ANDRÉ TIAGO SANTOS[1], ALEXANDRE SIMIÃO CAPORALI[2]

[1] Mestre. Professor de Educação Básica, Técnica e Tecnológica do Instituto Federal de Educação, Ciência e Tecnologia de São Paulo – *campus* Registro. andretisantos@bol.com.br.
[2] Doutor. Professor Titular do Instituto Federal de Educação, Ciência e Tecnologia de São Paulo – *campus* São Paulo. andretisantos@bol.com.br.

RESUMO

O objetivo deste trabalho é identificar, classificar e selecionar trabalhos sobre desenvolvimentos de Sistemas Instrumentados de Segurança (SIS's) implementados em Arranjo de Portas Programáveis em Campo (FPGA). Um protocolo de pesquisa foi formalizado e executado para conduzir uma revisão sistemática de literatura. Assim, os desenvolvimentos de SIS baseados e implementados em FPGA são atípicos, indicando-se que pesquisas nesta área devem ser amplamente desenvolvidas e apresentadas no sentido de se incrementar, não somente o quantitativo de tais trabalhos, como também, a qualidade de tais trabalhos em termos de arquiteturas, desenvolvimento com Dispositivos Lógicos Reconfiguráveis e implementações, testes e validações de Sistemas Instrumentados de Segurança para uso em processos industriais. Os dados obtidos foram analisados e são apresentadas abordagens para desenvolvimento de SISs baseados em FPGA.

Palavras-chave: Arranjo de Portas Programáveis em Campo; Revisão Sistemática; Sistemas Instrumentados de Segurança.

INSTRUMENTED SAFETY SYSTEMS IMPLEMENTED IN RECONFIGURABLE LOGICAL DEVICES: A SYSTEMATIC REVIEW

ABSTRACT

This research intends to identify, classify and select this work on developments of Safety Instrumented Systems (SISs) implemented in Field Programmable Gate Array (FPGA). A research protocol was formalized and conducted to conduct a systematic literature review. Thus, SISs developments based on and implemented in FPGA are atypical, indicating that research in this area should be widely developed and presented in order to increase, not only the quantity of such works, but also, the quality of such works in terms of architectures, development with Reconfigurable Logic Devices and implementations, tests and validations of Safety Instrumented Systems for use in industrial processes. The data obtained have been released and are examined for the development of FPGA-based SISs.

Keywords: Field Programmable Gate Arrays; Safety Instrumented Systems; Systematic Review.

1 INTRODUÇÃO

Recebido em 20/11/2020 e aprovado para publicação em 26/03/2021.

Os Sistemas de Seguranças Instrumentados (SIS) são utilizados para monitorar a condição de valores e parâmetros de uma planta, em conformidade com os limites operacionais, estes definidos por uma equipe multidisciplinar fabril (Manutenção, Operação, Engenharias, Saúde e Segurança no Trabalho, entre outros), e, quando houver condições de riscos, devem gerar alarmes e colocar a planta básica de controle de processos em uma condição segura ou, mesmo, na condição de *shutdown* (desligamento – desacionamento).

De acordo com Cassiolato (2012), os Sistemas Instrumentados de Segurança (SIS) são os responsáveis pela segurança operacional e que asseguram a parada de emergência dentro dos limites considerados seguros, sempre que a operação ultrapassar estes limites. O objetivo maior é se evitar acidentes dentro e fora das fábricas, como incêndios, explosões, danos aos equipamentos, proteção da produção e da propriedade e, mais do que isso, evitar riscos de vidas ou danos à saúde individual e impactos catastróficos para a comunidade. Deve-se ter de forma evidente que nenhum sistema é totalmente imune a falhas e sempre se impõe proporcionar mesmo em caso de falha, uma condição segura.

Estes são compostos por subsistemas semelhantes a um sistema de controle de processos, com Sensor (ou conjunto de Sensores), um Resolvedor Lógico (Controlador e/ou Arquitetura de Controle com dotação de agente inteligente) e Atuador (ou conjunto de atuadores). Esses subsistemas estão aparte do Sistema Básico de Controle de Processos (BPCS – *Basic Process Control Systems*) no sentido de, ao se tratar alguns tipos de falhas (randômicas de *hardware*, sistemáticas e/ou de causas comuns) no BPCS, com todo tratamento e especificações regidos pela norma IEC 61508, os SIS's trabalham no sentido de se garantir um estado seguro a planta industrial.

De acordo com Costa (2014), os FPGAs (*Field Programmable Gate Arrays* - Matrizes de Portas Programáveis por Campo) são definidos como Dispositivos de Lógica Programável Complexa (CPLDs – *Complex Programmable Logic Devices*) que são providos de caracteres de dinâmica reconfiguração de sua estrutura lógica interna, diferentemente dos Controladores microcontrolados/microprocessados, que têm uma estrutura de processamento hierárquico de dados. Suas arquiteturas internas consistem de arranjos de células lógicas formadas por blocos de memória do tipo LUT (*look-up table*), *flip-flops* (biestáveis) e multiplexadores, que podem ser utilizadas na implementação de funções lógicas. Basicamente, um FPGA/CPLD apresenta na sua arquitetura: blocos lógicos, blocos de E/S (entrada/saída) e chaves de interconexão. Os blocos lógicos formam arranjos bidimensionais e as chaves de interconexão são organizadas como canais de roteamento horizontal e vertical entre as linhas e colunas de células lógicas.

Esses canais de roteamento possuem chaves programáveis que permitem conectar os blocos lógicos de maneira conveniente, em razão das necessidades de cada *design* e, para conexão entre as células e os blocos de saída, os FPGAs possuem estruturas conhecidas como barramentos.

Assim, numa arquitetura baseada em lógica programável estruturada, por exemplo, FPGA, um algoritmo é implementado por *hardware*, sem a necessidade de ciclos de busca e execução de instruções, como é em sistemas microcontroladores/microprocessadores.

A questão básica de pesquisa é determinar o que caracteriza um método (ou métodos) de desenvolvimento de SIS baseado em FPGA. Pretende-se chegar a um conjunto fundamental de características que são necessárias para que um método (ou métodos) possa(m) ser classificado(s) como método apropriado de SIS baseado em FPGA, investigando-se através de revisão sistemática de literatura (estudo secundário) (BIOLCHINI *et al.*, 2005 *apud* MAFRA; TRAVASSOS, 2005), quais são as características de projeto no contexto dos métodos de desenvolvimento. Como se desenvolve SIS implementado em FPGA? Será adotada uma abordagem que estrutura a questão de pesquisa em 4 elementos básicos: população, intervenção, comparação e resultado (PAI *et al*., 2004 *apud* MAFRA; TRAVASSOS, 2005). Tendo em vista ser o objetivo deste estudo realizar uma caracterização da área, não haverá comparação e nem será possível aplicação de meta-análise. Dessa forma, podemos definir este tipo de estudo secundário, apesar de sistemático, como uma "quase" revisão sistemática.

A motivação desta pesquisa é servir de apoio à busca de entendimento e à solução a outras questões envolvendo o processo de desenvolvimento de Sistemas Instrumentados de Segurança implementados com Dispositivos Lógicos Reconfiguráveis (FPGA). Este artigo contempla apenas uma síntese dos resultados da revisão e está estruturado da seguinte forma: na seção 2, é apresentado um protocolo elaborado especificamente para essa revisão sistemática; na seção 3, descreve-se a execução do protocolo apresentado na seção 2; na seção 4, são apresentados e analisados os dados obtidos; na seção 5, apresentam-se algumas propostas de desenvolvimento de SIS implementado em FPGA em termos de Resultados e Discussões, e, na seção 6, são apresentadas as conclusões.

2 PROTOCOLO DE REVISÃO SISTEMÁTICA DE LITERATURA

O objetivo da revisão sistemática é identificar, classificar e selecionar trabalhos sobre desenvolvimentos de Sistemas Instrumentados de Segurança implementados em Arranjo de Portas Programáveis em Campo (FPGA - *Field Programmable Gate Array*), de um modo geral. As perguntas formuladas são: Quais trabalhos utilizam Sistemas Instrumentados de Segurança? Quais trabalhos empregam os SISs baseados em FPGA? Quais são os autores? Quais as fontes de publicação? Quando foram publicados? O problema considerado é encontrar propriedades ou características de projetos de SISs baseados em FPGA. A aplicação da revisão sistemática é servir de base ou apoiar pesquisas envolvendo (1) atividades de projeto de Sistemas Instrumentados de Segurança e (2) desenvolver metodologia de implementação de SISs com base em Dispositivos Lógicos Reconfiguráveis.

A população considerada foram os grupos de publicações que têm Sistemas Instrumentados de Segurança como tema (fontes primárias). A intervenção considerada são os estudos que discutem aspectos relativos ao desenvolvimento e experimentos com SISs baseados em FPGA. Não houve comparação. E o resultado considerado foi a extração, a agregação e a apresentação dos dados da revisão sistemática. Uma visão abrangente dos desenvolvimentos realizados de SISs projetados em FPGA. Foram utilizados como controle os artigos das fontes primárias.

As fontes selecionadas foram as bases de dados eletrônicas, disponíveis no portal CAPES, incluindo documentos indexados por *IEEE Xplore*, *Science Direct*, *Scopus* e *Web of Science*. O idioma escolhido foi o Inglês, por ser maioria nas bases de dados pesquisadas. Além disso, textos em português, embora se reconheça a sua importância, muitas vezes não se encontram indexados, o que aumenta o esforço ou impede sua busca. Considerou-se qualquer tipo de trabalho ou artigo com texto completo que fizesse abordagem sobre desenvolvimentos e/ou experimentos com SIS concebidos em FPGA.

As palavras-chave escolhidas para a população foram *"Field Programmable Gate Array" e "safety instrumented systems"* em seus exatos termos.

Como critérios de inclusão e exclusão, considerou-se que os documentos devem estar disponíveis na *web*, de modo integral, e contemplar características de experimentos e/ou desenvolvimentos de SISs e que sejam implementados em FPGA. Como estratégia de extração de informações, considerou-se que, para cada artigo selecionado, serão extraídas as seguintes informações: título do documento, autor(es), fonte, ano de publicação e propriedades ou características que identifiquem desenvolvimento e/ou experimento de SISs baseados em FPGA.

Na medida do possível, a *string* de busca será a mesma para todas as máquinas de busca. Contudo, poderá haver adaptações para se adequar a restrições de máquinas de busca específicas, observando-se as seguintes diretrizes: (1) a *string* derivada deverá ser logicamente equivalente à *string* original, ou (2) na impossibilidade de se manter equivalência exata, deverá a *string* derivada ser mais abrangente para evitar perda de documentos potencialmente relevantes. Segue-se a principal *string* de busca para os trabalhos nas bases: *"Field Programmable Gate Array" AND "safety instrumented systems*".

3 EXECUÇÃO DE BUSCAS

As buscas foram realizadas utilizando máquinas de busca de editoras ou bibliotecas digitais disponíveis no portal CAPES. Durante o mês de Outubro de 2020 (1º ao 31º dias), período registrado da referida busca, foi estruturada a *string* "'*Field Programmable Gate Array' AND 'safety instrumented systems'*" inserida nos parâmetros de busca nas bases *IEEE Xplore, Science Direct, Scopus* e *Web of Science*. Somente a base *Scopus* necessitou de adaptação para a operação lógica "*ALL ('Field Programmable Gate Array') AND ALL ('Safety Instrumented Systems')*", pois, na base, esta estrutura lógica de busca forneceu um número adequado de artigos (14, no caso).

Atingiu-se a quantidade de 31 referências, sendo 17 para *Science Direct*, e 14 para *Scopus*. Nenhum trabalho foi indicado pelas bases *IEEE Xlpore* e *Web of Science.* Não foram utilizadas ferramentas para auxílio do tratamento das referências.

As réplicas foram eliminadas, mantendo-se o artigo remanescente e contabilizando-se para a biblioteca digital com maior quantidade de itens recuperados.

Em uma avaliação superficial preliminar (trabalho completo), foram excluídas as referências que tratavam de outros trabalhos não pertinentes à metodologia da pesquisa (índices remissivos e resumos de trabalhos p.e.).

Posteriormente, em uma avaliação mais apurada e detalhada, foram selecionados os documentos candidatos a fazer parte da revisão sistemática: total de 17 referências, sendo 7 para *Science Direct* e 10 para *Scopus*. A tabela 1 mostra, de modo detalhado, as referências utilizadas nesta Revisão Sistemática com seus critérios de inclusão/exclusão.

TABELA 1 – Referências selecionadas na execução da RS.

id	Nome da Obra	Ano	Autores	Comentários	*Status*	Critério
1	Risk-informed approach to the safety improvement of the reactor protection system of the AGN-201K research reactor	2020	Ibrahim Ahmed; Enrico Zio; Gyunyoung Heo.	Aborda identificação dos pontos fracos no projeto e operação do reator de pesquisa e avalia possíveis melhorias de segurança. Não trata de SIS.	Excluído	1
2	A safety instrumented system for rolling stocks: Methodology, design process and safety analysis.	2015	David Macii; Stefano Dalpez; Roberto Passerone; Michele Corrà; Manuel Avancini; Luigi Benciolini.	Aborda o projeto, as principais características e a análise de segurança de um dispositivo de vigilância de homem morto para veículos ferroviários.	Incluído	
3	Distortion of process values by N-multiplet Reconciliation.	2010	Gus Tibazarwa.	Aborda análise de algoritmos de reconciliação genéricos escaláveis para combate de falhas aleatórias. Não aborda SIS de modo profuso.	Excluído	1
4	Periodic surveillance test strategies to effectively enhance the availability of safety-critical systems in NPPs using the multi-state based availability model.	2015	Kwang Seop Son, Seung Hwan Seong, Gwi Sook Jang, Hyun Gook Kang.	Aborda estratégias eficazes de teste de vigilância periódica que aumentam a disponibilidade de sistemas de segurança nuclear. Não trata de base FPGA.	Excluído	2
5	Reliability analysis of subsea blow out preventer control systems subjected to multiple error shocks.	2012	Baoping Cai, Yonghong Liu, Zengkai Liu, Xiaojie Tian, Hang Li, Congkun Ren.	São abordadas análises de duas configurações para sistemas de controle distribuído em prevenção de explosão submarina. Não aborda base FPGA.	Excluído	2
6	Prospects for Model-Based Testing of Discrete Safety Systems.	2007	Patrick Salaün, François Cheriaux, Denis Trognon.	Aborda a descrição das perspectivas para a validação de Sistemas de Segurança Discretos (lógicos). Não trata de SIS nem de base FPGA.	Excluído	1, 2
7	SIL Attachment Paradigm from the Perspective of Quantitative Hazards Rates.	2018	Dogruguven, E. H.; Ustoglu, I.	Abordagens usadas na indústria ferroviária de análises quantitativas de risco são discutidas. Não trata de SIS.	Excluído	1
8	Safety fuzzy logic controller with 2oo3 architecture implemented in FPGA.	2016	Fatima Ezzahra Nadir, Mohammed Bsiss, Mohammed Jbilou, Benaissa Amami.	Aborda análise de controlador difuso de segurança com arquitetura 2oo3 implementado em FPGA.	Incluído	
9	A fault tolerant architecture to avoid the effects of Single Event Upset (SEU) in avionics applications.	2014	Lorenzo Ciani, Marcantonio Catelani.	Aborda técnicas de tolerância a falhas para dispositivos aviônicos baseados em FPGA na presença de distúrbios de radiação induzidos por partículas incidentes. Não trata de SIS.	Excluído	1

Id	Nome da Obra	Ano	Autores	Comentários	Status	Critério
10	Uncertainty handling in fault tree based risk assessment: State of theart and future perspectives.	2019	Mohammad Yazdia, Sohag Kabirb, Martin Walker.	Aborda estado da arte com foco no tratamento da incerteza na análise de árvore de falhas (FTA) com base na avaliação de risco. Não trata de SIS nem de FPGA.	Excluído	1, 2
11	A quantified Safety Analysis for Safety Fuzzy Logic Controller 1oo2 Reliability Block Diagrams.	2012	Mohammed Bsiss, Hadj Baraka Ibrahim, Amami Benaissa.	Aborda um estudo analítico para quantificar a integridade de segurança num Controlador de Segurança em Lógica difusa implementado em FPGA. Não trata de SIS.	Excluído	1
12	Toward automated FMEDA for complex electronic products.	2015	Eugene Babeshko, Vyacheslav Kharchenko, Oleg Odaruschchenko, Volodymyr Skylar.	Aborda desafios na aplicação da FMEDA e técnicas de análise relacionadas para produtos eletrônicos baseados em FPGA. Não trata de SIS.	Excluído	1
13	First Approach of Diversity Design for FPGA Based on Energy Management.	2015	Kenichi Morimoto, Yuichiro Shibata, Yudai Shirakura, Hidenori Maruta, Fujio Kurokawa, Masanori Nobe, Masaharu Tanaka.	Aborda a apresentação da primeira abordagem que aplica a compilação do FPGA a se gerar diversidades em sistemas de alta confiabilidade. Não trata de SIS.	Excluído	1
14	Implementing state machines in distributed event-based systems.	2017	Holger Zipper , Marco Meiery, Eike Hintzez, Christian Diedrich.	Aborda descrição de fatores complicadores nas máquinas de estado com base em eventos e soluções. Não trata de SIS nem de FPGA.	Excluído	1, 2
15	Towards MPSoC Enabled Subsea Embedded Systems for Fault Tolerant Applications.	2019	Juliano Pimentel, Tanya Vladimirova.	Trata de sistemas eletrônicos para submarinos incorporados usando a flexibilidade de multiprocessador programável em vez de conjuntos de placa de circuito impresso sob medida. Não aborda SIS.	Excluído	1
16	FPGA Implementation of Fuzzy Interpreted Petri Net.	2020	Zbigniew Hadjuk, Jolanta Wojtowicz.	Trata de introduzir um novo método de implementação de redes de Petri interpretadas em lógica difusa baseada em FPGA. Não trata de SIS.	Excluído	1
17	Modelling Common Cause Failures In Systems with Triple Modular Redundancy and Repair	2020	Matthew J. Cannon, Andrew M. Keller, Andrés Pérez-Cellis, Michael J. Wirthlin.	Introduz uma nova cadeia de Markov a modelar as causas comuns de falhas em sistemas de reparo com redundância tripla modular. Não aborda SIS.	Excluído	1

Fonte: dados da pesquisa.

Considerando-se, dessa forma, ambas bases de acesso aos trabalhos, 45,2% do total de resultados foi excluído com base no terceiro critério de exclusão e, 6,5% da quantidade total foi agregada em conformidade com os critérios de inclusão (primeiro e segundo).

Observa-se que os trabalhos que abordam, por exemplo, análise de algoritmos de reconciliação genéricos escaláveis para combate de falhas aleatórias (TIBAZARWA, 2010);

usos na indústria ferroviária de análises quantitativas de risco (DOGRUGUVEN; USTOGLU, 2018); técnicas de tolerância a falhas para dispositivos aviônicos baseados em FPGA na presença de distúrbios de radiação induzidos por partículas incidentes (CIANI; CATELANI, 2014); não tratam de SIS.

Os artigos que tratavam de estado da arte com foco no tratamento da incerteza na análise de árvore de falhas (FTA) e com base na avaliação de risco (YAZDI; KABIR; WALKER, 2018); ou descrição de fatores complicadores nas máquinas de estado com base em eventos (ZIPPER *et al*., 2017); ou análises de duas configurações para sistemas de controle distribuídos em prevenção de explosão submarina (PIMENTEL; VLADIMIROVA, 2019), não abordam base de implementação com FPGA.

Conclui-se que, assim, pesquisas que, de modo factível, desenvolvem e projetam configurações distintas para Sistemas Instrumentados de Segurança implementados com Dispositivos Lógicos Reconfiguráveis do tipo FPGA, são atípicas, apresentando-se uma pequena fração de trabalhos agregados a esta pesquisa.

5 DISCUSSÕES E RESULTADOS

Nessa seção, inicialmente, serão mostradas algumas discussões sobre os trabalhos obtidos nesta pesquisa tipificada como “quase” Revisão Sistemática de Literatura. Após, os resultados serão apresentados e demonstrados.

O trabalho de Macii *et al*. (2015) abordou sobre um equipamento moderno para transporte ferroviário que deve ser compatível com a confiabilidade, disponibilidade, requisitos de manutenção e segurança de ambos os regulamentos nacionais e padrões internacionais como EN 50126-1: 1999 e EN 50126-2: 2007. Neste artigo (MACII *et al.*, 2015), o processo de design de um novo DMVD foi totalmente descrito com ênfase especial nas questões de segurança. Este processo pode ser do interesse de projetistas, engenheiros e profissionais que desenvolvem segurança em sistemas de diagnóstico para aplicações ferroviárias. No particular, apenas componentes de *hardware* e módulos de nível de transferência de registro sintetizados em FPGAs são usados, a operação correta de ambas funções de segurança e diagnóstico podem ser verificadas por meio de técnicas normalmente utilizadas apenas para sistemas de *hardware*.

Macii *et al.* (2015) concluiu que o sistema proposto é modular, flexível (ou seja, adequado para diferentes tipos de trens e contextos) e capaz de atender aos requisitos de

segurança desejados. Além do que, é caracterizado por custos de desenvolvimento mais baixos do que outras soluções existentes, uma vez que não inclui programáveis dispositivos ou núcleos executando rotinas de *software*, que requerem atividades de validação e verificação longas e caras. Descreveu-se completamente e foram justificadas todas as etapas de desenvolvimento e as opções de *design* de um ponto de vista orientado para a segurança, a fim de cumprir os requisitos normativos em função do Nível de integridade de segurança (SIL).

A pesquisa de Nadir *et al.* (2016) retrata que o setor industrial requer não apenas o desempenho dos sistemas em termos de qualidade, produtividade e confiabilidade, mas também em termos de segurança. A implementação de Controlador de Lógica Difusa (*Fuzzy Logic Controller* - FLC), desenvolvido em FPGA, que não permite apenas a confiabilidade do sistema e reduz o ciclo de vida de concepção do controlador, mas também garante um nível de integridade de segurança (SIL) que é exigido pelo campo de aplicação e relacionados com a arquitetura do sistema de controle. Análise de um controlador de lógica nebulosa de segurança implementado em FPGA pode ser realizada por diferentes métodos que estão relacionados aos padrões internacionais (IEC 61508 e ISA TR 84.0.0.2), que são padrões que tratam de Sistemas Instrumentados de Segurança - SIS. Este artigo (NADIR *et al.*, 2016) propôs a análise de um controlador de lógica *fuzzy* de segurança implementado em FPGA com arquitetura de votação 2 de 3 (2oo3) usando uma análise qualitativa e quantitativa fornecida por esses padrões. A análise quantitativa é realizada pelo cálculo da probabilidade média de falha sob demanda (PFDavg – PFDméd) do sistema relacionado à segurança para definir seu Nível de integridade de segurança (SIL). A análise qualitativa é baseada no Método de confiabilidade baseado em Diagrama de Bloco e Análise de Árvore de Falhas.

Portanto, Nadir *et al*. (2016) inferiu em sua pesquisa que, em termos de análise qualitativa, A Análise da Árvore de Falhas (*Fault Tree Analysis* – FTA) pode fornecer uma representação binária das causas que levam ao sistema relacionado à segurança para falha perigosa. Em termos de análise quantitativa, a análise FTA é baseada nos padrões ISA TR84.0.0.2 padrão no cálculo do PFDavg. Este padrão não considera o fator de fração de segurança (SFF) e a fração de falhas não detectadas que têm uma causa comum e a taxa de falha detectada perigosa no caso de arquitetura de votação 1 de 1 (1oo1). Além disso, este padrão não faz um diferença entre os dois tipos de componentes A e B. No entanto, a análise do Diagrama de Blocos de Confiabilidade é baseada no padrão internacional IEC 61508 para o cálculo da PFDméd. Esta norma considera todos os parâmetros definidos anteriormente e há

uma diferença entre os dois tipos componentes A e B. O tipo de componentes permite identificar o fator de segurança que contribui diretamente para o cálculo da PFDavg. Apesar dessa diferença entre ambos os padrões, ambos os métodos de análise fornecem os mesmos resultados. O Sistema de Controle de Lógica Difusa de Segurança, de arquitetura de votação 2oo3, possui um arranjo de votação para maioria do resultado dos sinais indicadores de falha, assim, se apenas um dispositivo provê um resultado discordante dos outros dois, o estado da saída não é alterado.

No que tange aos resultados obtidos, extraídos resultados de exclusão conforme o terceiro critério, 11,7% dos artigos foram incluídos neste trabalho, cada qual com 5,8%, sendo estes (MACII *et al*., 2015) e (NADIR *et al*., 2016), representando uma pequena fração de referências que tratam de desenvolvimento de SISs implementados em FPGA.

Ambos artigos abordam questões, como nos trabalhos de Santos *et al*. (2017) e Sekiou *et al*. (2013), que abordam SIS baseados em FPGA para ambientes industriais, relativas às Normas IEC 61508, ISA TR 84.0.0.2, intertravamentos para sistemas de segurança, arquiteturas de votação para disponibilidade/confiabilidade de Sistemas de Segurança, bem como as análises quanti/qualitativas dos sistemas em ração da Probabilidade de Falha na Demanda média.

No entanto, mesmo que os Sistemas não estejam contemplados como Instrumentados de Segurança e, ainda, em ambientes industriais, como os desenvolvimentos descritos nos trabalhos de (SANTOS *et al.*, 2017) e (SEKIOU *et al.*, 2013), ainda assim, os caracteres, descritos anteriormente, que são abordados nos trabalhos anteriores, estão abordados nestas referências escolhidas para a composição nesta *quasi*-Revisão Sistemática.

Deste modo, os desenvolvimentos de SIS baseados e implementados em FPGA são atípicos, indicando-se que pesquisas nesta área devem ser amplamente desenvolvidas e apresentadas no sentido de se incrementar, não somente o quantitativo de tais trabalhos, como também, a qualidade de tais trabalhos em termos de arquiteturas, desenvolvimento com Dispositivos Lógicos Reconfiguráveis e implementações, testes e validações de Sistemas Instrumentados de Segurança para uso em processos industriais.

6 CONSIDERAÇÕES FINAIS

De fato, os Sistemas Instrumentados de Segurança são relevantes e têm sua importância destacada no que tange a proteção de processos diversos, pessoas e comunidades

onde estão instalados tais sistemas. Como os Dispositivos Lógicos Reconfiguráveis têm grande flexibilidade na configuração, são os selecionados para que se componham como Solucionadores Lógicos cujos dados não perpassam por rotinas computacionais caracterizadas por microprocessadores/micro controladores digitais.

Espera-se que a caracterização acima, resultado de estudo secundário (*quasi-revisão* sistemática) cuja síntese foi apresentada neste artigo, possa permitir algum direcionamento nos trabalhos e pesquisas relacionadas a obtenção de projetos de Sistemas Instrumentados de Segurança implementados em FPGA para ambientes industriais e processos produtivos. Em particular, o interesse dos autores está relacionado a metodologia de desenvolvimento de SIS baseados em FPGA, principalmente quando aplicados no contexto da engenharia de automação e controle de processos.

Pretende-se evoluir e atualizar o trabalho aqui apresentado. Além da inclusão de novas fontes de busca, há a possibilidade do aperfeiçoamento da pesquisa de modo que o conceito de Sistemas Supervisórios de Segurança seja adicionado ao desenvolvimento e projeto de SISs baseados em FPGA, haja vista que são linhas de desenvolvimento paralelas. Há a possibilidade de que, em trabalhos futuros, a revisão aqui descrita sirva de base para que uma nova ou mais ampla pesquisa seja realizada em busca de modelos e procedimentos metodológicos, baseados nos dispositivos normativos internacionais e/ou nacionais, para tais sistemas tolerantes a falhas.

Uma das dificuldades encontradas durante a realização da pesquisa é o fato de ser notável que as pesquisas na área de Sistemas Instrumentados de Segurança baseados em Dispositivos Lógicos Reconfiguráveis são escassas. Por isso, é valorizado todo documento que faça um levantamento do estado da arte relacionado ao estabelecimento de qualidade desse tipo de aplicação. A *quasi*-RS apresentada é valorizada por configurar o armazenamento contínuo das informações e a garantia de abrangência da pesquisa por partes de pesquisadores interessados no tema, o que constitui sólida contribuição.

7 REFERÊNCIAS

BIOLCHINI *et al*. (2005) "**Systematic Review in Software Engineering"**, COPPE / UFRJ, Relatório Técnico, ES-679/05.

CASSIOLATO, C. **SIS - Sistemas Instrumentados de Segurança - Uma visão prática - Parte 1**. 2012. Disponível em: https://www.instrumatic.com.br/artigo/sis-sistemas-instrumentados-de-seguranca-uma-visao-pratica-parte-1. Acesso em: 05 nov. 2020.

CIANI, L; CATELANI, M. A fault tolerant architecture to avoid the effects of Single Event Upset (SEU) in avionics applications, **Measurement**, v. 54, 2014, p.. 256-263.

COSTA, C. **Implementação de Controlador Lógico baseado em Lógica Programável Estruturada (FPGA**), 2014. Disponível em: http://professorcesarcosta.com.br/upload/imagens_upload/Artigo_Implementa%c3%a7%c3%a3o%20de%20Controlador%20L%c3%b3gico%20Program%c3%a1vel%20em%20FPGA.pdf. Acesso em: 05 nov. 2020.

DOGRUGUVEN, E.H.; USTOGLU I. SIL Attachment Paradigm from the Perspective of Quantitative Hazard Rates. **IFAC-PapersOnLine**, v. 51, n. 9, 2018, p. 112-117.

PIMENTEL, J.; VLADIMIROVA, T.. **Towards MPSoC Enabled Subsea Embedded Systems for Fault Tolerant Applications**. 1-8. 10.1109/AHS.2019.000-7. 2019.

MACII, D.; DALPEZ, S.; PASSERONE, R.; CORRÀ, M.; AVANCINI, M.; BENCIOLINI, L. A safety instrumented system for rolling stocks: methodology, design process and safety analysis. **Measurement**, [S.L.], v. 67, p. 164-176, maio 2015. Elsevier BV. http://dx.doi.org/10.1016/j.measurement.2015.01.002.

MAFRA, S. N.; TRAVASSOS, G. H. Técnicas de Leitura de Software: Uma Revisão Sistemática. In: Simpósio Brasileiro de Engenharia de Software, 2005, Uberlândia. **Anais do 19o SBES - Simpósio Brasileiro de Engenharia de Software**, 2005. v. 1. p. 72-87.

NADIR, F. E.; BSISS, M.; JBILOU, M.; AMAMI, B.. Safety Fuzzy Logic Controller with 2oo3 architecture implemented in FPGA. **2016 5Th International Conference On Systems And Control (Icsc),** [S.L.], p. 186-191, maio 2016. IEEE. http://dx.doi.org/10.1109/icosc.2016.7507070.

PAI, M. M., M. GORMAN, J.D. *et al*. (2004) "Systematic Reviews and meta-analyses: An illustrated, step-by-step guide", **The National Medical Journal of India**, vol. 17, n.2.

SANTOS, A. T.; COSTA, C.; CAPORALI, A. S.. **Desenvolvimento de Sistema Instrumentado de Segurança baseado em FPGA.** São Paulo: 2º Congresso de Pós-Graduação do Instituto Federal de Educação, Ciência e Tecnologia de São Paulo – IFSP. [s.n.], 2017.

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.

TIBAZARWA, G.. Distortion of process values by N-multiplet Reconciliation. **ISA transactions**. 49. 433-42. 10.1016/j.isatra.2010.04.008. (2010).

YAZDI, M.; KABIR, S.; WALKER, M.. Uncertainty handling in fault tree based risk assessment: State of the art and future perspectives, P**rocess Safety and Environmental Protection**, v. 131, 2019, p.. 89-104.

ZIPPER, H.; MEIER, M.; HINTZE, E; DIEDRICH, C. "Implementing state machines in distributed event-based systems," **2017 3rd International Conference on Event-Based Control, Communication and Signal Processing (EBCCSP)**, Funchal, 2017, pp. 1-7, doi: 10.1109/EBCCSP.2017.8022809.