ASPECTOS DE SEGURANÇA DO CONTROLADOR PROSAFE RS QUE IMPACTAM EM SEGURANÇA DO PROCESSO

Luth Augusto Matos Gagliano[1], Oberdan Rocha Pinheiro[2]

[1] Senai Cimatec, E-mail: luthaugusto@hotmail.com

[2] Senai Cimatec, E-mail: oberdan.pinheiro@fieb.org.br

SAFETY ASPECTS OF CONTROLLER PROSAFE RS THAT IMPACTS ON PROCESS SAFETY

Resumo: Em processos industriais, segurança é um assunto muito relevante. A confiabilidade em sistemas de controle determina a segurança em processos críticos, por isso a seleção desses sistemas deve ser criteriosa. Ter conhecimento dos critérios de segurança e certificações que classificam um controlador é essencial para direcionar o equipamento adequado ao processo. O avanço no desempenho dos controladores programáveis resultou em mais robustez e confiabilidade de informações processadas e sistemas com nível de segurança SIL3, como a aplicação através do Prosafe RS da Yokogawa, são largamente utilizados em indústrias.

Palavras chave: *Controlador lógico programável; Segurança em processo; Certificações de segurança em automação.*

Abstract: In industrial process, safety is a topic really relevant. The reliability in control systems defines the safety in critical processes, so system selection must be careful. Understand the safety criteria and certifications that classifies the programmable controller is essential to orientate the suitable equipment to the process. The improvement in programmable controllers performance resulted in more robustness and data process reliability in a way that SIL3 safety level applications as Prosafe RS from Yokogawa are widely used in industries.

Keywords: *Programmable logical controller; Process safety; Safety automation certifications.*

1. INTRODUÇÃO

Sistemas de automação flexíveis permitem constantes mudanças na configuração do controle do processo de produção. A aplicação do Clp (controlador lógico programável) se encaixa nessa classificação de automação e teve sua origem na necessidade da indústria de obter uma forma de se adaptar rapidamente a produção de novos produtos sem um custo e trabalho elevado.

Um controlador programável tem a função de receber sinais nas suas portas de entrada, executar um programa que contém a sua lógica determinada e atualizar suas saídas enviando sinais aos dispositivos conectados. Esse dispositivo utiliza uma memória programável para armazenar instruções que são determinadas de acordo com as necessidades do usuário. Segundo Martins (2007) em um controlador "pode-se utilizar inúmeros pontos de entrada de sinal para controlar pontos de saída de sinal (cargas). Desta forma são implementadas funções lógicas que controlam máquinas e processos através de módulos de entrada e saída de dados. "

Para atuar em ambientes industriais, controladores programáveis são elaborados com diversas aplicações de segurança, o objetivo dos fabricantes além de permitir o controle de processos através de um computador robusto, é que ele trabalhe de modo confiável, evitando falhas e atuando de forma segura quando o erro ocorra. De acordo com IEC (2015), tais erros podem ser provenientes de falhas aleatórias de sistema do hardware ou software, erro humano, influências ambientais como temperatura, chuva, interferências eletromagnéticas, falha por queda de energia ou diversas outras variáveis que possam afetar o controlador.

É importante relevar que a falha pode ser caracterizada como falha do controlador ou falha do processo, de acordo com Wang (2012), falha do controlador inclui erros de software e falha de hardware, enquanto que as falhas do processo são provindas externamente do controlador, exemplificadas como a inabilidade do processo atuar como a forma esperada. Esse artigo aborda exclusivamente falhas relacionadas ao controlador, excluindo a abrangência de falhas de processo.

Ao longo do texto são detalhados critérios de controladores lógico programáveis que impactam na confiabilidade de informações e consequentemente na segurança que o equipamento provê ao processo, relevando assim aspectos do hardware e do software utilizado por fornecedores para oferecer ao mercado equipamentos mais seguros. Por fim são detalhadas as características do controlador Prosafe RS da Yokogawa e suas características que podem influenciar na segurança do processo.

1.1. Certificações de segurança aplicáveis a controladores lógicos programáveis.

Algumas normas e certificações devem ser relevadas quando se trata de segurança e confiabilidade em controladores programáveis. Dentre as mais

importantes estão a norma internacional IEC 61850, a norma de segurança internacional ISO 13849-1 e a certificação TUV.

Uma das formas dos fornecedores de assegurar a qualidade de seus equipamentos é através da comprovação da qualidade de seus componentes através da certificação da norma internacional IEC 61850. Essa norma é aplicada para dispositivos elétricos, eletrônicos e eletrônicos programáveis, sendo assim, define em controladores programáveis os requerimentos para que o projeto, elaboração, construção e atuação do dispositivo atenda a quesitos de segurança que devem determinar o seu nível de segurança SIL (safety integrity level).

A escala de classificação varia em quatro níveis, de acordo com Magnetrol (2009), “o nível de integridade de segurança é uma forma de indicar tolerância da taxa de falha de uma particular função de segurança”. A seguir uma tabela exemplifica os quatro níveis de classificação SIL, considerando que a disponibilidade é definida como a probabilidade que o equipamento vai executar sua tarefa e PFDmed é a média de PFD (Probabilidade de falha em requisição), relacionada a probabilidade da falha do sistema responder sob um requisição de ação de uma potencial condição de perigo.

Tabela 1 – SIL e Medidas Relacionadas. Fonte: (Adaptado de Magnetrol, 2009)

SIL	Disponibilidade	PFDmed	Redução de Risco	Consequência Qualitativa
4	>99.99%	10^{-5} to $<10^{-4}$	100,000 to 10,000	Potencial de fatalidades na comunidade
3	99.9%	10^{-4} to $<10^{-3}$	10,000 to 1,000	Potencial de múltiplas fatalidades on-site
2	99 to 99.9%	10^{-3} to $<10^{-2}$	1,000 to 100	Potencial de danos maiores ou fatalidades on-site
1	90 to 99%	10^{-2} to $<10^{-1}$	100 to 10	Potencial para danos menores on-site

A norma ISO 13849-1 é abrangente para soluções de segurança em dispositivos elétricos, mecânicos, pneumáticos e hidráulicos. De acordo com Carlson (2013), “a norma utiliza análise estatística para fazer uma determinação probabilística da confiabilidade dos componentes, dispositivos e circuitos utilizados em partes relacionadas à segurança nos sistemas de controle de máquinas industriais. Essa determinação representa a probabilidade de uma falha de perigo ao longo do tempo e é representada por um indicador denominado Performance level (PL)”.

Sendo assim, PL é um nível de desempenho que determina a confiabilidade do sistema. Cinco patamares são separados para indicar o nível de segurança apropriado, níveis de “a” à “e”, sendo que o equipamento certificado com “PLe” tem a maior confiabilidade e o mais indicado para sistemas críticos com alto nível de risco. O índice é calculado a partir da classificação de quatros categorias, que compreendem exigência estrutural, tempo médio até a deficiência perigosa (MTTFd), grau de cobertura de diagnóstico (DC) e erros de causa conjunta (CCF).

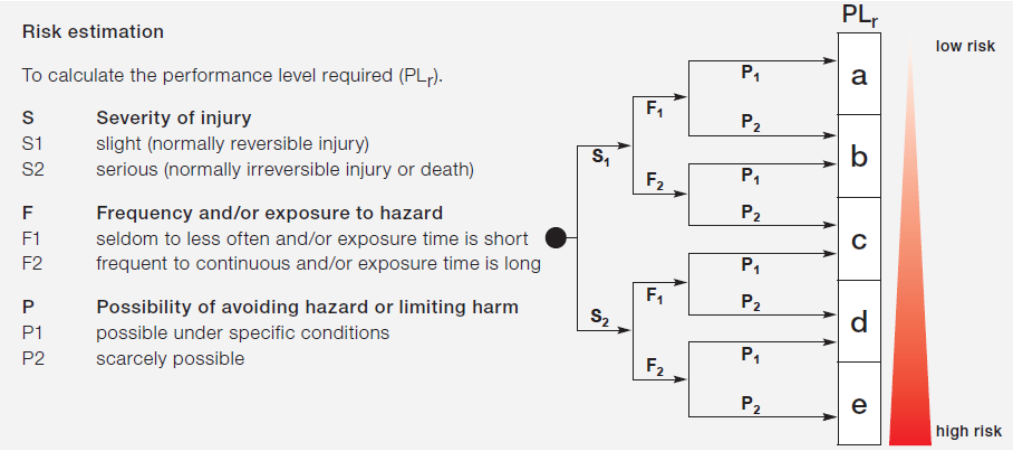

Figura 1 – Estimativa de risco para nível de desempenho. Fonte: (Safety in control systems according to EN ISO 13849-1, 2011)

Além das normas ISO e IEC, outro critério de segurança é relevante por diversos países europeus e recentemente os EUA, a certificação TÜV é emitida através de uma agência independente que certifica sistemas instrumentados de segurança. De acordo com Adamski (2008), TÜV Rheinland é autorizada para atuar com engenharia de segurança para plantas industriais, processos e produtos durante manufatura e utilização. Se o produto testado está de acordo com rigorosos requisitos técnicos e de desempenho, ele é aprovado e certificado para uma classe AK do nível 1 ao 8.

Diversas características no Clp influenciam em sua performance e consequentemente no seu nível de segurança, a seguir são detalhados assuntos relacionados ao software e hardware no equipamento que influenciam na sua confiabilidade.

1.2. Aspectos de segurança do hardware do controlador.

Um dos critérios de segurança do hardware de um controlador é o seu nível de proteção a intempéries, as normas brasileiras NBR 6146 e NBR 9884 definem os critérios para classificação de equipamentos elétricos quanto a proteção do seu invólucro à materiais líquidos e sólidos.

O IP (índice de proteção) é composto por dois números, o primeiro número se refere à proteção de materiais sólidos, dentro de uma escala de 0 à 6, o nível zero indica nenhuma proteção e o nível 6 como totalmente protegido contra poeira. O segundo número determina a proteção quanto a umidade, sendo o nível 0 como proteção nula e o nível 8 com proteção a submersão.

Um dos pontos considerados na elaboração de um controlador industrial é a manutenção do equipamento, em muitas indústrias o processo depende da atuação do Clp, é muito importante que em caso de falha a manutenção desses equipamentos seja simples e rápida. Atualmente, são encontrados dois

tipos de construção de controladores, eles podem ser classificados como modulares ou fixos.

Os controladores fixos são equipamentos menos robustos e com um custo menor, são projetados para atuar em sistemas mais simples e o seu funcionamento depende da interligação de todos os seus componentes. Ou seja, uma falha na sua fonte de energia compromete todo o sistema, isso porque todos os seus componentes estão agregados em uma unidade e são dependentes.

Os controladores modulares são montados em racks e elaborados para executar tarefas complexas, sua montagem permite a instalação de diversos componentes independentes e em muitos equipamentos é permitida a troca de algumas partes com o controlador em funcionamento, ou seja, sem a necessidade de parada do processo. Essa configuração além de permitir que o usuário selecione a melhor combinação de componentes para o seu controlador, permite a instalação de componentes reservas que podem atuar em redundância, tornando o sistema de controle mais confiável.

Outra característica que destaca a vantagem da implantação do controlador modular sobre o fixo é a possibilidade de expansão de dispositivos conectados. No Clp fixo a quantidade de I/Os é limitada e a expansão do sistema determina a troca do hardware, diferente do modular que permite a ampliação do sistema com a instalação de novos componentes ao rack.

A redundância é uma forma de assegurar a disponibilidade de sistemas, ela consiste na aplicação de componentes duplicados como fontes de alimentação, processadores ou até mesmo outro sistema de controlador completo. É uma estratégia muito utilizada para controladores programáveis que atuam com funções de segurança, porém o nível de redundância deve ser avaliado de acordo com a criticidade do processo.

De acordo com Scheneider (2008), a redundância em automação pode ser classificada em três níveis, frio, morno e quente. A redundância fria é caracterizada em processos onde o tempo de resposta não é crítico e possa necessitar da atuação do operador. A redundância morna é resumida em um processo onde o tempo é um fator crítico, porém uma pausa momentânea é aceitável, durante essa parada, motores, válvulas e outros dispositivos podem se desligar e os instrumentos podem não se comunicar com o Clp. A redundância quente é determinada quando o processo não possa ser parado nem por um instante em qualquer circunstância.

Segmentos da indústria nuclear e exploração espacial atuam com o nível máximo de confiabilidade, onde há a presença de três controladores dos quais dois ficam em operação e um em modo reserva. Para que essa configuração ocorra corretamente é necessário que todos os controladores estejam com a mesma lógica de programação determinada para suas entradas e saídas, assim, a cada ciclo as informações dos dois controladores atuantes são comparadas, em caso de alguma discordância de informação o sistema é alarmado. É essencial também a máxima eficiência de transferência de I/Os entres sistemas, exigindo que a comunicação entre processadores primários e secundários esteja muito bem configurada.

1.3. Aspectos de segurança de software para sistemas de controle industriais.

De acordo com Williamson (1998) “um sistema crítico de segurança deve ser seguro, deve estar disponível, ser confiável, fidedigno e rodar em tempo real. O software deve ser livre de erros. O Sistema deve estar de acordo com a especificação e a especificação deve estar correta”. Para que o software atue em tempo real a resposta do sistema deve estar de acordo com a necessidade de requisição de informação, Maziero (2014) explica que “sua característica essencial é ter um comportamento temporal previsível (ou seja, seu tempo de resposta deve ser conhecido no melhor e pior caso de operação)”.

O desenvolvimento de códigos para sistemas críticos tem o objetivo de simplificar ao máximo o programa evitando erros ao longo do desenvolvimento do código. Além disso, aspectos como prevenção de falhas, análise de segurança, anulação e detecção de falhas, devem ser tópicos bastante aprofundados através de diversos métodos disponíveis para a configuração de um processo que exige alto nível de segurança.

O recente surgimento de ameaças a sistemas de controle de processos industriais tem alertado executivos quanto à importância da segurança da proteção de suas redes SCADA. Programas maliciosos já são uma ameaça real que podem reprogramar controladores programáveis e esconder suas mudanças, ou mesmo roubar dados de processo de uma indústria. Os vírus Stuxnet e Duqu são casos de programas projetados para afetar especificamente sistemas de controladores industriais.

Solomon (2012) afirma que a vulnerabilidade nesses sistemas é devida a diversos fatores, as empresas estão sedentas por obter informação em qualquer lugar, suas redes de sistema de controle estão cada vez mais conectadas na internet, a rede SCADA não recebe o devido investimento em segurança e os engenheiros de controle de processo e o departamento de TI geralmente não tem as mesmas prioridades na empresa. Além disso, as ameaças estão cada vez mais sofisticadas, com ataques complexos e difícil identificação.

1.4. Aplicação do controlador Prosafe RS da Yokogawa em planta industrial petroquímica

Na planta da Braskem em Camaçari na Bahia, um dos controladores selecionados para umas das funções de controle de processo crítico é o Clp Prosafe RS fabricado pela Yokogawa. As características do controlador fornecem ao processo a segurança e os requisitos de manutenção necessários para assegurar a supervisão continua dos dados do processo da planta industrial instalada.

O controlador é classificado como de grande porte, sendo assim pode atender ao controle de diversos processos simultaneamente, sua característica modular permite a configuração do usuário das entradas e saídas de acordo

com a necessidade de segurança de seu processo, inclusive a seleção de redundância de cartões de acordo com critérios de cada projeto. O seu hardware do tipo modular montado em um rack, garante que durante paradas de manutenção seja possível à troca de módulos ligados ao CLP sem que todo o controlador seja retirado do processo para análise. Sendo assim, a depender da criticidade do processo, o usuário pode escolher se no seu rack há uma redundância de cartões de entrada, dois cartões que coletam informação do campo trabalhando simultaneamente, redundância de cartões de saída, dois cartões que enviam informação a partir da lógica dos processadores para o processo, ou mesmo dois cartões de processadores atuando simultaneamente.

O sistema completo do Prosafe RS consiste em uma estação de controle de segurança, um servidor de design de automação, uma estação de engenharia de segurança e componentes de rede que se comunicam com cada equipamento. A certificação IEC 61508 garante a eficiência e assertividade na coleta e emissão de dados que podem alcançar o padrão SIL3, essas aplicações são implantadas quando há a possibilidade de múltiplas fatalidades e habilita uma disponibilidade do controlador de 99,9%, ou seja, essas são as chances de um equipamento executar as atividades programadas pelo usuário. Independente da redundância de cartões do sistema, todas as aplicações do equipamento têm arquitetura dupla, sendo assim, mesmo com a utilização de apenas um cartão de entrada de dados é garantido o nível de segurança SIL3.

Quanto à segurança na configuração do equipamento para prevenção de mudanças realizadas por usuários não autorizados, configurações podem ser restringidas por senha e acessos a estações de engenharia podem ser restringidos, além disso, o sistema PROSAFE RS é embutido com funções de segurança que previnem vírus e acessos indevidos através de redes conectadas.

2. CONCLUSÃO

Foi descrito ao longo do artigo características que garantem a confiabilidade de execução de atividades que os controladores programáveis são destinados a executar. Aspectos de hardware e da programação devem influenciar na execução da rotina do controlador e seu desempenho sobre situações críticas pode ser avaliada através de algumas certificações no mercado.

Porém é importante relevar que o nível de segurança do controlador não garante a segurança do processo. Ao exemplo, um controlador com a maior certificação de segurança do mercado deve executar sua ação programada sobre uma válvula de bloqueio, porém a válvula deve também ter um nível de confiabilidade tão distinto quanto para que o processo seja equivalente em nível de resposta. Ou seja, nesse caso o que está certificado não é o fechamento da válvula, mas sim o envio do sinal para o instrumento. Cassiolato (2011) chama atenção que um sistema seguro de controle faz uma função de controle e não de segurança, sendo que nenhum sistema é completamente resistente a falhas.

Foi demonstrado o controlador PROSAFE RS que reúne todas as características de segurança necessárias para um sistema crítico de uma indústria petroquímica e quais os fatores são relevados para a escolha desse equipamento. Um ponto importante em projetos de controladores com funções de segurança e robustez é o custo elevado de equipamentos com tais especificações. Quanto maior o nível de confiabilidade exigido mais custoso será a aquisição do sistema, se torna necessário então uma avaliação aprofundada do nível de segurança exigido para cada projeto específico.

Sendo assim o profissional responsável para seleção de algum sistema de controle precisa avaliar a criticidade do seu processo e o impacto que a falha dos equipamentos pode proporcionar para as pessoas e para o seu negócio, compreender os critérios de segurança dos controladores programáveis, suas certificações e suas limitações são essências para escolha da solução mais apropriada.

3. REFERÊNCIAS

MARTINS, Geomar Machado. **Princípios de Automação Industrial**. Universidade Federal de Santa Maria. 2007.

IEC. **Functional safety, Essential to overall safety**. International Electrotechnical Commission, Geneva, Switzerland. 2015.

WANG, Ginam. QIN, Shiming. **A Study of Fault Detection and Diagnosis for PLC Controlled Manufacturing System.** ICSC 2012, Part 1, CCIS 326, pp.373-282. 2012

MAGNETROL. **Understanding Safety Integrity Level.** Magnetrol International, Bulletin: 41-299.2, USA, 2009.

CARLSON, Mike. **The Buzz About ISO 138491: The Good, the Bad and the Ugly (and a Possible Alternate Solution).** EHS Today, 2013.

ADAMSKI , Bob. **Is The Risk Worth It? Beware of the New Safety Instrumented Suppliers.** Invensys Systems, 2008.

HEMERT, Grant Van. **Water/Wastewater: Achieving The Three Levels Of Redundancy**. Schneider Electric, 2008.

WILLIAMSON, Louise M. **Analysis of safety critical plc code against IEC 1508 development techniques.** Durham theses, Durham University, 1998.

MAZIERO Carlos A. **Sistemas Operacionais: Conceitos e Mecanismos.** DAINF – UTFPR, 2014.

SOLOMON, Marc. **Vírus em rede SCADA: proteção garante o faturamento.** Mecatrônica Atual. Ed. 58, pp 38-39, 2012.

CASSIOLATO, César. **SIL ou não SIL, eis a questão.** Mecatrônica Atual. Ed. 58, pp 40-41, 2012.

YOKOGAWA. **Safety Instrumented System PROSAFE RS.** Yokogawa Electric Corporation, Bulletin 32S01B10-01E, 2005