UM MÉTODO PARA A IMPLEMENTAÇÃO DE SISTEMAS INSTRUMENTADOS DE SEGURANÇA EM PROCESSOS CRÍTICOS A PARTIR DE REDES DE PETRI DE ALTO NÍVEL

JEFERSON A.L.SOUZA, DIOLINO J. SANTOS FILHO, PAULO E. MIYAGI, LUCAS A. MOSCATO, FABRÍCIO JUNQUEIRA

Laboratório de Sistemas de Automação,Departamento de Engenharia Mecatrônica e de Sistemas Mecânicos, Escola Politécnica da Universidade de São Paulo
Av Prof. Mello Moraes, 2231, Cidade Universitária, 05508-030, São Paulo, SP, Brasil
E-mails: jeferson.souza@usp.br, diolinos@usp.br, pemiyagi@usp.br, lamoscat@usp.br, fabri@usp.br

Abstract— The inherent complexity of critical production systems, inserted in a context of sustainability policies and environmental preservation and protection of the people, are the motivation for the design of safety control systems, which aim to reduce the risk, inherent of any production system, to a safe level. According to the experts, the concept of Safety Instrumented Systems (SIS) is a solution in that promotes the reduction of risk through hierarchical layers to prevent and / or mitigate faults. Standards such as IEC 61508/61511 refer to the performance requirements, but do not mention implementation methods. Whereas the occurrence of a failure may be associated with the occurrence of an event, Petri nets become an efficient tool for design the detection and treatment of the effects of the occurrence of faults. This paper proposes a method for implementing the SIS in critical production systems from risk analysis techniques, fuzzy logic and High Level Petri nets.

Keywords—Critical Production Systems, Faults, Safety Instrumented Systems, High Level Petri nets.

Resumo— A complexidade inerente dos sistemas críticos de produção, inseridos em um contexto de políticas de sustentabilidade e de preservação ambiental e proteção das pessoas, são a motivação para o projeto de sistemas de controle de segurança, que têm por objetivo a redução do risco, inerente a qualquer sistema produtivo, a um nível seguro. De acordo com os especialistas, o conceito de Sistemas Instrumentados de Segurança (SIS) é uma solução, na medida em que promove a redução do risco por meio de camadas hierárquicas a fim de prevenir e / ou mitigar falhas. Normas como a IEC 61508/61511 fazem referência aos requisitos de desempenho, mas não mencionam métodos de implementação. Considerando que a ocorrência de uma falha pode estar associada à ocorrência de um evento, as redes de Petri tornam-se uma ferramenta eficiente para a modelagem da detecção e do tratamento dos efeitos da ocorrência de falhas. Este trabalho propõe um método para a implementação do SIS em sistemas críticos a partir de técnicas de análise de risco, lógica fuzzy e redes de Petri de Alto Nível.

Palavras-chave— Sistemas Produtivos Críticos, Falhas, Sistemas Instrumentados de Segurança, redes de Petri de Alto Nível.

1 Introdução

No cenário globalizado e competitivo no qual as organizações estão inseridas, torna-se fundamental a adoção de planejamentos estratégicos e práticas operacionais que assegurem a capacidade para uma rápida adaptação e consequente mudança dos sistemas produtivos até então concebidos. A expectativa é de que além de resultar num processo com redução efetiva de custos, alta qualidade do produto e flexibilidade das linhas de produção, e redução dos tempos de desenvolvimento de novos produtos e de entrega (Santos Filho, 2000) (Chen & Dai, 2004) (Wu, *et al.*, 2008), também provoque a redução de impactos ambientais do processo. Os resultados obtidos neste novo cenário são Sistemas Produtivos (SPs) que executam processos altamente complexos (Sampaio, 2011) (Ferreira, *et al.*, 2014) que não poderiam ser exequíveis por meio de métodos convencionais de produção (Mazzolini, *et al.*,2011). Em função desta complexidade inerente a qualquer sistema produtivo moderno, alguns estados, embora indesejados, podem ser alcançados, podendo-se citar: os estados de falha de componentes, falhas de projeto, ou ainda erros operacionais, incluindo-se os intencionais, além de eventos do ambiente que envolvem o sistema. Tais ocorrências podem resultar, dependendo da complexidade do SP, em sérios riscos à integridade física das pessoas, ao meio ambiente e a perdas econômicas decorrentes de danos ao próprio equipamento (Sallak, et al., 2008). Embora muitos trabalhos tenham sido apresentados, tanto para o diagnóstico quanto para o tratamento de uma determinada classe de falhas (Morales, et al., 2007) (Ru & Hadjicostis, 2008) (Wang, *et al.*, 2008) (Zhang & Jiang, 2008) (Summers & Raney, 1999) (Sallak, *et al.*, 2008), os acidentes continuam ocorrendo.

Dentro deste contexto, o uso de Sistemas Instrumentados de Segurança – SIS são, de acordo com especialistas, uma solução para este problema, na medida em que as ações de controle desempenhadas por um SIS provêm mecanismos de reação aos eventos indesejados, por meio da inserção de camadas sucessivas de redução de riscos para prevenir e/ou mitigar os efeitos da ocorrência de falha de um SP. Os SIS são referenciados em normas, tais como a IEC 61508 e a IEC 61511, que referenciam os requisitos de desempenho e o ciclo de vida para o projeto de um SIS. No entanto, as normas não fazem menção a métodos para implementação de SIS.

Em função da relevância do tema, diversos trabalhos vêm sendo publicados. (Squillante JR, 2013) propõe um método para a implementação do SIS de prevenção, em que o risco de um SP é avaliado por meio de um estudo HAZOP (*Hazard and Operability)*. Os resultados são refinados por meio de redes Bayesianas (BN) e o algo-

ritmo de controle para detecção, diagnóstico e tratamento das falhas são implementados por meio de redes de Petri clássicas. (Souza, 2014) propõe uma sistemática para o SIS de mitigação, em que os elementos críticos do SP são definidos a partir de técnicas de análise de riscos, e as ações de mitigação são determinadas por meio de lógica fuzzy. Assim como (Squillante Jr, 2013) os algoritmos de controle também são modelados por meio das redes de Petri clássicas, tendo-se como resultado grafos de elevada complexidade em função do inter-relacionamento dos arcos orientados da rede. Outro fato observado foi a limitada integração dos modelos de prevenção e mitigação, revelando lacunas para a implementação real de um SIS.

O presente trabalho propõe um método para a implementação de SIS em SPs críticos com referência às normas IEC 61508 e IEC 61511, considerando a integração do SIS de prevenção e mitigação, a partir do uso das redes de Petri de Alto Nível – HLPN para a modelagem formal dos algoritmos de controle.

2 Conceitos Fundamentais

2.1 Sistemas Instrumentados de Segurança

Sistema Instrumentado de Segurança (SIS) constitui um sistema de controle de segurança que tem por objetivo reduzir os riscos inerentes a SPs. De uma forma geral a função de um SIS é monitorar através de sensores de segurança, eventos críticos no processo industrial e indicar alarmes ou executar ações pré-programadas, por meio de atuadores de segurança, para a prevenção de acidentes ou mitigação das consequências geradas pela ocorrência desses eventos (Goble, 1998).

De acordo com a norma IEC 61508, um SIS é composto por camadas independentes e sucessivas de redução de riscos, que podem ser implementadas por sistemas de controle de segurança, que atuam de forma independente do Sistema Básico de Controle de Processo - BPCS. A estrutura de um SIS, com referência às normas IEC 61508 / 61511, é ilustrada na Figura 1.

Figura 1. Camadas de redução de riscos (adaptado da IEC 61511-1).

2.2 Técnicas de Análise de Riscos

Esta seção introduz conceitos fundamentais de algumas técnicas de análise de riscos, tais como o FMEA, FTA, HAZOP e a técnica *What-If.*

A técnica FMEA, descrita na IEC 60812 (IEC, 2006), consiste em um estudo detalhado e sistemático das possíveis falhas dos componentes de um sistema. Os modos de falha de cada componente são identificados, e um nível de severidade é associado ao seu efeito, além de avaliar a probabilidade de sua ocorrência. O FMEA também aborda ações para eliminar, mitigar e controlar as causas e as consequências das falhas. (Lewis, 1995).

Outra técnica utilizada é a Árvore de Falhas – FTA, metodologia de raciocínio dedutivo, descrita na IEC 62025 (2008) que parte de um evento topo, que é a ocorrência de uma falha específica em um sistema, e que tem por objetivo determinar as relações lógicas de falhas de componentes e/ou erros humanos operacionais que podem estar associados à ocorrência do evento topo. A análise é feita a partir da construção de uma árvore lógica. Desta maneira, obtém-se um grafo que pode ser utilizado para identificar todas as causas potenciais para a ocorrência de uma falha (Modarres, et al., 2010). O grafo permite uma análise do tipo “top-down”, do que resulta no entendimento de como o evento ocorreu. Já na análise “bottom-up” tem-se “o porquê” da ocorrência. A vantagem do FTA sobre o FMEA é que pode-se ter a combinação de vários elementos ou vários modos de falha, conectados no grafo por elementos lógicos do tipo “e” e “ou”.

O estudo de operabilidade e riscos, ou HAZOP (HAzard and OPerability studies) definido na IEC 61882 (IEC, 2001) foi desenvolvido para o exame eficiente e detalhado das variáveis de um processo, possuindo uma forte semelhança com o FMEA. Por meio do Hazop identificam-se os caminhos nos quais os equipamentos de processos podem falhar ou ser inadequadamente operados. É desenvolvida por uma equipe multidisciplinar, sendo guiada pela aplicação de palavras específicas – palavras guia – a cada variável do processo. Desta forma, geram-se os desvios dos padrões operacionais, os quais são analisados em relação às suas causas e consequências.

Como forma complementar a outras técnicas de análise de riscos, a técnica What-If é implementada a partir de questionamentos do tipo “O que.....se.....?” à equipe de especialistas no processo, no intuito de se identificar os riscos inerentes e propor ações para prevenir e/ou mitigar os efeitos da ocorrência de falhas.

2.3 Lógica Fuzzy

A lógica fuzzy vem se tornando útil na modelagem de sistemas não-lineares, ou quando o uso de equações diferenciais se torna muito complexo, ou mesmo em processos cujo conhecimento do comportamento dinâmico ainda não é totalmente compreendido (Lee, 1990).

Sistemas fuzzy têm por base o conhecimento humano ou em um conjunto de regras que têm por objetivo imitar o raciocínio humano em decisões de controle (Zadeh, 1996). Questões do tipo “Se...(condicional) Então...

(consequente)" são formuladas a especialistas do processo em análise, e as ações de controle são definidas a partir das respostas, sendo, em sua maioria, sistemas de múltiplas entradas para uma única saída (Zadeh, 1965), (Lee, 1990), (Popa, et al., 2008). Todas as regras são processadas em paralelo, com a consequente ser ativo com o seu grau de pertinência na saída do sistema. Ao contrário da lógica booleana, os números fuzzy estão contidos em um intervalo fechado 0 e 1, podendo assumir valores dentro deste intervalo (Zadeh, 1965).

O uso da lógica fuzzy em CPs é referenciado na norma IEC61131-7, que trata da conversão da lógica fuzzy em linguagem implementável em CPs comerciais.

2.3 Redes de Petri

Rede de Petri (PN), como uma ferramenta gráfica e matemática, provê uma forma uniforme para modelagem, análise e projeto de Sistemas a Eventos Discretos - SEDs (Adam, *et al.,*1998; Nassar, et al., 2008; Zurawski & Zhou, 1994), sendo efetiva como técnica de descrição e especificação de processos (Hamadi & Benatallah, 2003; Morales, *et al.,* 2007; Yoo, *et al.,*2010). Fornece uma representação que pode ser usada tanto como modelo conceitual quanto modelo funcional de um sistema em que se pode analisar e validar o funcionamento do sistema em cada fase de seu ciclo de desenvolvimento. A PN pode também ser utilizada como uma ferramenta de projeto, permitindo uma fácil interpretação e identificação dos processos e seu comportamento dinâmico e/ou dos sistemas que estão sendo modelados (Nassar et al., 2008). Os modelos baseados em PN podem ser usados para avaliação qualitativa e quantitativa, envolvendo a análise das propriedades comportamentais e medida de desempenho, respectivamente. Além disso, com o desenvolvimento de softwares simuladores (Zurawski & Zhou, 1994), tem-se à disposição ferramentas para edição e análise destes modelos. Possibilita a representação da dinâmica do sistema e sua estrutura em diversos níveis de abstração, de acordo com a complexidade do sistema (Nassar, et al., 2008). É capaz de modelar a sincronização de processos, a ocorrência de eventos assíncronos, de operações concorrentes e de conflitos, ou do compartilhamento de recursos (Adam, *et al.*, 1998; Nassar, et al., 2008).

Dentre as extensões das PN pode-se citar as redes de Petri de Alto Nível – HLPN (Smith, 1998)(ISO/IEC 15909, 2000) e as redes de Petri Coloridas – CPN (Jensen, 1997), nas quais a representação gráfica do modelo seja reduzida, sem contudo perder o formalismo da modelagem das PN clássicas, aumentando-se com isso o nível de abstração e o poder de modelagem de processos, em que os lugares da rede possuem marcas individualizadas e separadas por tipo, podendo ser declarada a identidade de cada variável. Os arcos possuem inscrições e filtros que selecionam o tipo da marca que pode fluir por este arco, e as transições, que ocorrem em diferentes modos restritos à regra de localidade de seu preset e pós-set. O comportamento dinâmico do grafo é resultado, portanto, do conjunto grafo, inscrições e declaração.

3 Proposta

O método proposto é representado por meio do fluxograma mostrado na Figura 2.

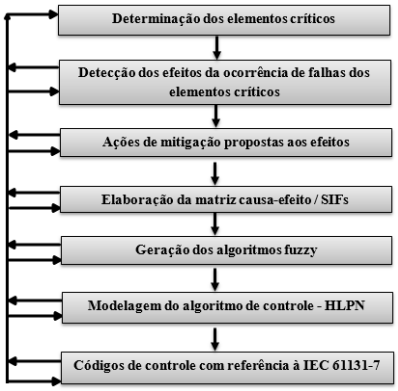


Figura 2. Fluxograma de implementação de SIS em SPs críticos

Os itens 3.1 a 3.7 detalham cada passo, utilizando como exemplo uma estação de compressão de gás, ilustrada na Figura 3.

Figura 3. Estação de compressão de gás – ECOMP

O gás natural é uma mistura de hidrocarbonetos altamente inflamável, e está presente na natureza a baixas pressões, misturado a impurezas.

Estações de compressão de gás têm como objetivo retirar o gás combustível da natureza, filtrar e pressurizar, de modo com que o possa ser encaminhado a centros consumidores por meio de gasodutos. A geração de energia elétrica e o combustível que alimenta os compressores vêm de uma parte do gás extraído, de forma com que o processo é classificado como crítico, uma vez que a ocorrência de uma falha pode resultar em uma catástrofe.

O método foi aplicado a partir de informações obtidas de uma equipe de especialistas no processo, em fornecedores de peças e equipamentos e em instalações similares, conforme os requisitos das normas IEC 61508/61511.

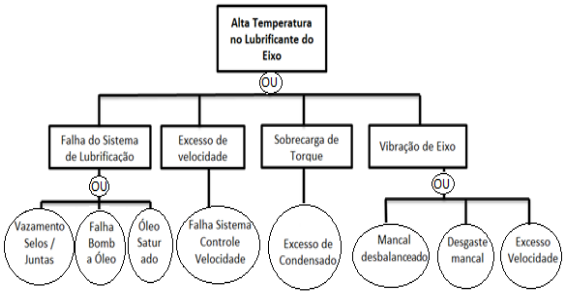
3.1 Determinação dos Elementos Críticos

Aplicando-se as técnicas de Análise de Riscos ao processo verifica-se, a partir dos resultados do FMEA e FTA, que as unidades compressoras representam elementos críticos do processo, pois são responsáveis pela

pressurização do gás extraído da natureza, e operam em elevados níveis de pressão, velocidade e temperatura.

Aplicando-se as técnicas FMEA e FTA, verifica-se um potencial modo de falha associado à lubrificação do mancal do compressor, podendo ocasionar danos à instalação e até incêndios, na medida em que o gás natural é utilizado para a própria alimentação dos compressores. A Tabela 1 representa o respectivo FTA com o evento topo de alta temperatura no lubrificante.

Tabela 1. FTA para "Alta Temperatura no Lubrificante do Eixo"



3.2 Detecção dos efeitos da ocorrência de falhas nos elementos críticos

Para os efeitos das falhas apresentadas na etapa anterior, foram inseridos termopares, com os Tags TET 211 A a TET 211D, respectivamente a cada uma das quatro unidades compressoras.

3.3 Ações de Mitigação propostas aos efeitos

Para mitigar os efeitos causados pela ocorrência da falha listada nos estudos FMEA e FTA, sugere-se, além da ação de *shutdown* prevista no SIS de prevenção, a ação do resfriamento forçado dos compressores a partir da liberação de gás carbônico proveniente de cilindros já instalados no processo. Além do resfriamento, o gás carbônico será responsável por retirar o oxigênio, evitando uma eventual combustão do gás natural.

3.4 Elaboração da Matriz Causa-Efeito / Identificação das SIFs.

Para cada evento inicializador, representado pelos sinais dos sensores, determina-se as respectivas ações de mitigação, fazendo-se a representação em uma matriz, em que as causas são elencadas nas colunas e os efeitos, associados às ações de mitigação (atuadores), nas respectivas linhas.

Eventos inicializadores comuns podem ser agrupados, representando, de acordo com a IEC 61508, as funções instrumentadas de segurança – SIFs. Ações de mitigação também podem ser comuns para diferentes SIFs. A matriz causa-efeito para a SIF 1, representada pelos sinais dos sensores TET211, é ilustrada na Tabela 2.

Tabela 2. Matriz Causa Efeito para a SIF 1

	EFEITOS	PARADA TCA	PARADA TCB	PARADA TCC	PARADA TCD	GASCARB A	GASCARB B	GASCARB C	GASCARB D
CAUSAS									
TET-211A		X				X			
TET-211B			X				X		
TET-211C				X				X	
TET-211D					X				X

Analisando-se todo o processo, a matriz causa-efeito resultou em 6 SIFs, 72 eventos inicializadores (causas), e 108 ações (efeitos).

3.5 Geração dos Algoritmos Fuzzy

A partir dos eventos inicializadores e das respectivas ações de mitigação, elaboradas de forma qualitativa na matriz causa-efeito, o próximo passo consiste na elaboração quantitativa destes sinais. A partir dos resultados da técnica *What-If* da equipe de especialistas, a lógica fuzzy pode ser utilizada para associar as respectivas ações dos atuadores para os intervalos das variáveis de processo ou de variáveis associadas a algum parâmetro de falha de um componente.

Para ilustrar o algoritmo, o especialista relata que para um valor entre 10% e 30% acima do *set-point* da temperatura TET211 o *shutdown* deve ser realizado. Já um valor acima de 50% seria inaceitável, o que requer uma ação de mitigação além do *shutdown* proposto. A Figura 4 representa este resultado em uma função de pertinência fuzzy implementada no *toolbox fuzzy* do *MatLab*®. Note que podemos ter intervalos em que duas ações podem estar ocorrendo, com proporções distintas.

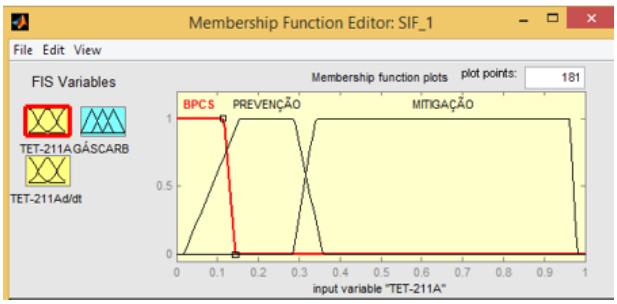


Figura 4. Funções de pertinência fuzzy para temperatura

A Figura 5 representa a edição das regras fuzzy, de acordo com os resultados da técnica *What-If*.

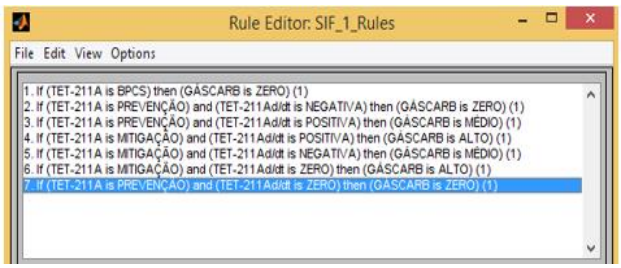


Figura 5. Conjunto de regras fuzzy para as funções de pertinência

O conjunto de estados para todas os valores das variáveis de entrada, e seus respectivos valores da saída, representado pela válvula associada ao cilindro de gás carbônico para uma unidade compressora está representado na Figura 6.

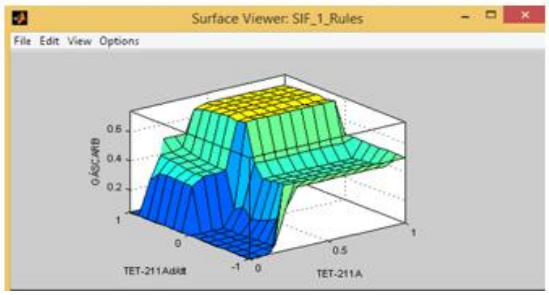


Figura 6.Saída do atuador de mitigação

Aplicando-se a lógica fuzzy para todo o processo obteve-se como resultado um total de 180 regras fuzzy, cujo entendimento ficou bastante comprometido devido ao inter-relacionamento dos eventos inicializadores com os atuadores, comuns a diferentes regras.

3.5 Modelagem do Algoritmo de Controle – HLPN

A partir dos resultados obtidos em lógica fuzzy, o próximo passo consiste no uso das redes de Petri para a modelagem formal do algoritmo de controle e verificação das propriedades de *vivacidade*, *reiniciabilidade e segurança* a partir do resultado da edição dos modelos em *softwares*, como por exemplo o PIPE2. A utilização das redes de Petri clássicas, embora exequíveis, resultou em grafos de difícil edição e compreensão em função do elevado inter-relacionamento dos arcos entre atuadores comuns a diferentes SIFs.

Para contornar tal problema sem, no entanto, incorrer na perda de informações dos modelos fuzzy, optou-se pelas redes de Petri de Alto Nível – HLPN, a partir de modelos hierárquicos.

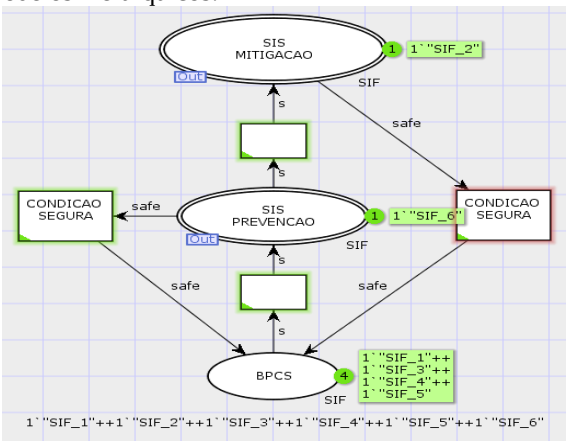


Figura 7. Modelo em HLPN de SIS, em referência à IEC 61508

A edição dos modelos foi feita com o auxílio da ferramenta CPNtools, e a Figura 7 ilustra o modelo em HLPN de um SIS, com referência à norma IEC 61508/61511.

As funções de pertinência fuzzy, elaboradas a partir das técnicas de análise de riscos, foram implementadas nos modelos HLPN a partir da distinção de marcas (multisets) nos respectivos lugares da rede, e da utilização de funções algébricas para o disparo dos respectivos arcos. Outra vantagem, como já mencionado, foi o fato de se trabalhar com modelos hierárquicos de prevenção e mitigação, em que os intervalos dos eventos inicializadores das respectivas SIFs foram representados de forma sintética em uma rede principal, e as respectivas ações de prevenção / mitigação, associadas às linhas da matriz causa-efeito, foram representadas em as redes secundárias. As ações de prevenção / mitigação são executadas até que a condição de verificação segura de todos os sensores seja satisfeita, reinicializando o modelo para o nível de controle básico do sistema – BPCS.

As propriedades de *vivacidade*, *reiniciabilidade e segurança* foram verificadas no modelo clássico. Pelo fato da rede Alto Nível ser derivada da rede clássica (dobramento), pode-se considerar que as propriedades são mantidas. A Figura 8 ilustra o modelo do algoritmo de controle para os eventos inicializadores TET211. Os demais modelos são estruturas isomorfas e independentes, na medida em que não foram considerados neste trabalho o inter-relacionamento de falhas.

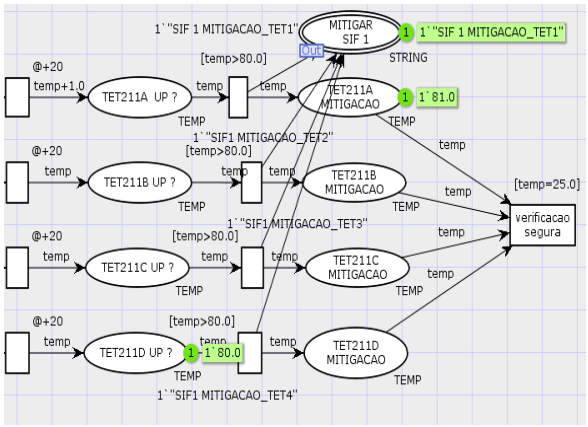


Figura 8. Modelo em HLPN para o SIS de mitigação

3.6 Códigos de Controle - Referência à IEC61131-7

Os códigos de controle, implementáveis em controladores comerciais, podem ser escritos a partir dos resultados da lógica fuzzy, com base na evolução dinâmica da rede HLPN. A norma IEC 61131-7 referencia a conversão da lógica fuzzy em linguagem texto estruturado. A Figura 9 ilustra um pequeno trecho da implementação do código.

```
FUNCTION_BLOCK FUZZYCONTROL
VAR_INPUT
        temperature : REAL;
        dtemperature : REAL;
VAR_OUTPUT
        valvule : REAL; END_VAR
FUZZIFY temperature
TERM Basiccontrol := (0,1) (200,1) (250,0);
TERM prevent := (200,0) (250,1) (300,1) (350,0);
TERM mitigate := (300,0) (350,1) (1000,1);
END_FUZZIFY
```

```
DEFUZZIFY valvule
TERM zero := 0;
TERM medium := (0,0) (20,1) (55,1) (95,0);
TERM high := (40,0) (100,1);
ACCU : MAX;
METHOD : COG;
DEFAULT := 0; END_DEFUZZIFY
RULEBLOCK No1
        AND : MIN;
RULE 1 : IF temperature is mitigate THEN valvule IS high;
RULE 2 : IF temperature is BasicControl THEN valvule IS zero;
RULE 3 : IF (temperature is prevent) and (dtemperature is P)
         THEN valvula IS medium;
RULE 4 : IF (temperature is mitigate) and (dtemperature is N)
         THEN valvula IS medium;
```

Figura 9 – Exemplo de código, com referência à IEC 61131-7

4 Conclusão

O trabalho apresenta um método para a implementação de SIS para a mitigação de falhas em SPs críticos, com referência às normas IEC 61508 / 61511. Com o auxílio de uma equipe de especialistas no processo, técnicas de análises de riscos são utilizadas para a determinação dos elementos críticos. O passo seguinte consiste na determinação de sinais de controle (sensores) que possam estar associados à ocorrência de falhas dos elementos críticos, podendo ou não estar associadas a variáveis de processo. Lógica fuzzy é utilizada para determinar os intervalos dos respectivos sinais dos sensores para indicar a necessidade de promover o *shutdown* e ativar os respectivos atuadores de mitigação. As redes de Petri são utilizadas para a modelagem e verificação formal do modelo. No entanto, em função da complexidade do modelo obtido, a modelagem passa a ser feita por meio das redes de Petri de Alto Nível, que resultam em modelos mais simplificados e de fácil edição, sem contudo perder a complexidade do modelo e os resultados da lógica fuzzy. Outra vantagem foi a geração de modelos hierárquicos, que podem contribuir para trabalhos futuros na medida em que ações de mitigação podem ser proporcionais à ocorrência da falha, isto é, no modelo atualmente proposto, todos os atuadores de mitigação são acionados na ocorrência de uma determinada SIF. Um modelo hierárquico pode avaliar quais atuadores seriam necessários em função da severidade do efeito da ocorrência e da localização geográfica da falha no processo.

Agradecimentos

Os Autores deste trabalho gostariam de agradecer às agências do governo brasileiro CNPq, FAPESP e CAPES pelo suporte financeiro à realização deste trabalho.

Referências Bibliográficas

Bell, R., 2005. “Introduction to IEC 61508”. In Proceedings of ACS Workshop on Tools and Standards. Sydney, Australia.

Chen, C. and Dai, J., 2004. Design and high-level synthesis of hybrid controller. In Proc. of IEEE Conference.

IEC, I.E.C., “Programmable Controllers IEC 61131-7: Fuzzy Control programming”, 2000.

IEC, I.E.C., 2003a. “Functional safety - safety instrumented systems for the process industry sector - part 1 (IEC 61511)”

IEC, I.E.C., 2010. “Functional safety of electrical / electronic / programmable electronic safety-related systems (IEC 61508)”.

ISO/IEC 15.909, “High Level Nets: Concepts, Definitions and Graphical Notations”, Final Draft, v. 4.7.1, 2000.

Jensen, K., “Coloured Petri Nets. Basic Concepts, Analysis Methods and Paractical Use.”, Springer-Verlag, 1997.

Lee, C. C.: “Fuzzy logic in control system: fuzzy logic controller Part 1”. In IEEE Transactions n System, Man and Cybernetic, Vol 20, n^{0}2, p. 404-418, 1990.

Lewis, E.E., 1995. Introduction to Reliability Engineering. 2^0 Ed., John Wiley&Sons.

Lundteigen, M.-A.; Rausand, M. Architectural constraints in IEC 61508: Do they have the intended effect ?Reliability Engineering and System Safety, pp. 520-525, Elsevier Science Publisher Ltd., 2009.

Modarres, M., Kaminskiy, M., Krivstov, V., 2010. Reliability Engineering and Risk Analysis:a practical guide.,CRC Press.

Popa, D. D., Craciunescu, A, Kreindler, L.: “A PI-Fuzzy controller designated for industrial motor control applications”. In ISIE IEEE International Symposium on Applications, Industrial Eletronics, 2008.

Sallak, M.; Simon, C.; Aubry, J., A fuzzy probabilistic approach for determining safety integrity level, IEEE Transaction on Fuzzy Systems, vol 16, n. 1, pp. 239-248, 2008.

Smith, E.; “Principles of High Level Petri Nets”, LNCS 1491, pp. 174-210.

Souza, J.A.L., “Mitigação de Falhas Críticas em Sistemas Produtivos”. Dissertação de Mestrado. Escola Politécnica da Universidade de São Paulo. 2014.

Squillante Jr, R.; Santos Fo, D.J.; Souza, J.A.L.; Junqueira, F,; Myiagi, P.E. “Safety in Supervisory Control for Critical Systems”. IFIP International Federation for Information Processing (DoCEIS 2013), vol 394, pp. 261-270,

Summers, A.; Raney, G. Common cause and common sense, designing failure out of your safety instrumented systems (SIS). In: ISA Transactions, vol 38, pp. 291-299, 1999.

Wu, B; Xi, L.-F; Zhuo, B.-H. Service-oriented communication architecture for automated manufacturing system integration. International Journal of Computer Integrated Manufacturing, vol 21, n. 5, pp. 599-615, 2008.

Zadeh, L. A.: Fuzzy Sets. Information and Control, Vol 8, p. 338-353, 1965.

Zhang, Y; Jiang, J. Bibliographical review on reconfigurable fault-tolerant control systems, Annual Reviews in Control, vol 32, pp. 229-252, 2008.