
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
DE SÃO PAULO – IFSP

MAURICIO GARCIA

# Diagnóstico e tratamento de falhas em Sistemas Instrumentados de Segurança utilizando Redes Digitais de comunicação

São Paulo – Brasil

2015

MAURICIO GARCIA

# DIAGNÓSTICO E TRATAMENTO DE FALHAS EM SISTEMAS INSTRUMENTADOS DE SEGURANÇA UTILIZANDO REDES DIGITAIS DE COMUNICAÇÃO

Dissertação apresentada ao Instituto Federal de Educação, Ciência e Tecnologia de São Paulo para obtenção do título de Mestre em Automação e Controle de Processos.

Área de Concentração:
Controle e Automação

Orientador:
Prof. Dr. Alexandre Simião Caporali

São Paulo
2015

G21d Garcia, Mauricio.
Diagnóstico e tratamento de falhas em sistemas instrumentados de segurança utilizando redes digitais de comunicação / Mauricio Garcia. São Paulo: [s.n.], 2015.
61 f.: il.

Orientador: Prof. Dr. Alexandre Simião Caporali.

Dissertação (Mestrado Profissional em Automação e Controle de Processos) - Instituto Federal de Educação, Ciência e Tecnologia de São Paulo, IFSP, 2015.

1. Sistema instrumentado de segurança - SIS 2. IEC61508
3. Nível de integridade segura – (SIL) I. Instituto Federal de Educação, Ciência e Tecnologia de São Paulo.
II. Título

CDU 681.0

a

MINISTÉRIO DA EDUCAÇÃO
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SÃO PAULO
*CAMPUS* SÃO PAULO
DIRETORIA GERAL DO *CAMPUS* SÃO PAULO
Coordenadoria de Registros Escolares de Pós-Graduação

# ATA DE EXAME DE DEFESA DE DISSERTAÇÃO

Nome do Programa: **Mestrado Profissional em Automação e Controle de Processos**

Nome do(a) Aluno(a): Mauricio Garcia

Nome do Orientador: Prof. Dr. Alexandre Simião Caporali

Nome do Co-orientador:

Título do Trabalho: "Diagnóstico e Tratamento de Falhas em Sistemas Instrumentados de Segurança Utilizando Redes Digitais de Comunicação"

Abaixo o resultado de cada participante da Banca Examinadora

| **Nome completo dos Participantes Titulares da Banca** | **Sigla da Instituição** | **Aprovado / Não Aprovado** |
|---|---|---|
| Prof. Dr. Alexandre Simião Caporali – Orientador | IFSP – SPO | Aprovado |
| Prof. Dr. Dennis Brandão – Membro Externo | USP - EESC | aprovado |
| Prof. Dr. Victor Juliano De Negri – Membro Externo | UFSC | Aprovado |
| **Nome completo dos Participantes Suplentes da Banca** | **Sigla da Instituição** | **Aprovado / Não Aprovado** |
| Prof. Dr. Eduardo Alves da Costa – Membro Interno | IFSP - SPO | |
| Prof. Dr. Alexandre Brincalepe Campo – Membro Interno | IFSP - SPO | |

Considerando-o: [X] APROVADO
[ ] NÃO APROVADO

Assinaturas

São Paulo, 31 de Março de 2015

Alexandre S. Caporali
Presidente da Banca

Membro Externo

Membro Externo

Observações:

# Agradecimentos

Registro meus agradecimenos à aqueles que de forma direta ou indireta contribuiram para o desenvolvimento e conclusão deste trabalho.

Pelo incentivo motivacional e apoio incondicional, ao meu orientador e Coordenador do curso de Mestrado em Automação e Controle de Processo do Instituto Federal de São Paulo, Prof. Dr. Alexandre Simião Caporali, que além do acompanhamento técnico científico no desenvolvimento do trabalho me apoiou nos momentos de dificuldade e conflitos com minha atividade profissional.

Ao corpo docente do curso de Mestrado em Automação e Controle de Processo do Instituto Federal de São Paulo pelo apoio e suporte em suas areas de concentração durante os dois anos de aulas e atividades desenvolvidas.

A AscoNumatics – Brazil, em especial na pessoa de nosso Gerente Geral, Eng. Ignácio De La Rosa, pelo apoio, equipamentos e instalações cedidas para o desenvolvimento e construção do protótipo de estudo.

A minha esposa Cássia, meus filhos Lucas e André, pela compreensão e apoio durante o período de ausência e também pelo apoio e motivação.

“alguns homens estudam durante toda uma vida para adquirir conhecimento. Outros, dedicam toda uma vida à arte de ensinar e nos mostram o verdadeiro significado de ser um Mestre. Dedico este trabalho à todos aqueles que fazem da docência não só uma profissão, mas uma opção de vida.”

Mauricio Garcia

# *DIAGNÓSTICO E TRATAMENTO DE FALHAS EM SISTEMAS INSTRUMENTADOS DE SEGURANÇA UTILIZANDO REDES DIGITAIS DE COMUNICAÇÃO*


## Resumo:

Este trabalho apresenta uma proposta para o diagnóstico e tratamento de falhas nos projetos de Sistemas Instrumentados de Segurança – SIS, utilizados principalmente na indústria de processos. O diagnóstico e tratamento de falhas fazem parte dos requisitos necessários para a determinação do Nível de Integridade Segura – SIL de uma planta de acordo com a norma internacional IEC61508. Através de um protótipo de estudo, os alarmes de falhas puderam ser monitorados em um terminal inteligente de válvulas com protocolo de comunicação digital. Os tempos de resposta apurados entre sinais simulados e seus respectivos diagnósticos nos módulos de entradas e saídas digitais, apresentaram velocidades adequadas à sua utilização em escala industrial.



**Palavras-chave:**

*Sistema Instrumentado de Segurança – SIS, IEC61508, Nível de Integridade Segura –( SIL).*

# *DIAGNOSIS AND FAULT TREATMENT ON SAFETY INSTRUMENTED SYSTEM USING A DIGITAL COMMUNICATION NETWORK*


## Abstract

This work presents a proposal to diagnosis and fault treatment in Safety Instrumented Systems – SIS design, mainly used in the process industry. Diagnosis and fault treatment are part of the requirements for determining the plant Safety Integrity Level – SIL, according to the international standard IEC61508. Through a constructed study prototype, fail alarms could be monitored in a smart valve terminals using digital protocol communication. The measured response time between simulated signals and its diagnosis in the digital input and output modules presented suitable speeds for use in industrial scale.



**Keywords:**

*Safety Instrumented System – SIS, IEC61508, fail, Safety Integrity Level – SIL.*

# LISTA DE FIGURAS

# LISTA DE TABELAS

# LISTA DE ABREVIATURAS E SIGLAS

ANSI ..... American National Standards Institute

C..... ..... taxa de consequência da falha perigosa

$C_A$ ..... Falha coberta

CPF ..... Família de Perfis de Comunicação, *(Comunication Profile Family)*

CSP ..... reserva fria, *(cold spare)*

DFT ..... Estrutura de Falhas Dinâmicas, *(Dinamic Fault Tree)*

E/EE/EP..... Elétrico/Eletro-Eletrônico/Eletrônico Programável

EUC..... Equipamento sob Controle *(Equipment Under Control)*

fail safe ..... falha segura

failure on demand ..... falha sob demanda

FDEP ..... Dependência Funcional

FMEDA .... Análise Modos Falha, Efeitos e Diagnósticos (*Failure Modes Effects& Diagnostic Analysis*)

$F_{np}$..... taxa de demanda de um sistema seguro de proteção

$F_p$ ..... frequência de risco com medidas de proteção

$F_t$ ..... frequência tolerável de perigo de falha

FTA ..... Análise da Arquitetura de Falhas, *(Fault Tree Analysis)*

HFT ..... Tolerância de Falha do Equipamento, *(Hardware Fault Tolerance)*

IAC1 ..... entrada analógica 1 de contrôle

IAF1 ..... entrada analógica 1 de vazão

IAF2 ..... entrada analógica 2 de vazão

IAP1 ..... entrada analógica 1 de pressão

IAP2 ..... entrada analógica 2 de pressão

IAT1 ..... entrada analógica 1 de temperatura

IAT2 ..... entrada analógica 2 de temperatura

IAV1..... entrada analógica 1 de verificação

ID1 ..... entrada digital 1

ID2 ..... entrada digital 2

IEC ..... International Electrotechnical Commission

ISA ..... International Society of Automation

l/min ..... litros/minuto

MC ..... Cadeias Markov

OAC1 ..... Sinal de Saída Analógico de Controle 1

$PFD_{avg}$ ..... Probabilidade de Falha sob Demanda média

SCL ..... Camadas de Segurança na Comunicação, *(Safety Communication Layer)*

SDCD ..... Sistemas Digitais de Controles Distribuidos

SF ..... Função de Segurança

SFF ..... Fração de Falha Segura, (Safe Failure Fraction)

$S_i$ ..... estado inicial

SIF ..... Função Instrumentada de Segurança

SIL ..... Safety Integrety Level

SIS ..... Sistemas Instrumentados de Segurança

TIV ..... Terminal Inteligente de Válvulas

VAux ..... Válvula Auxiliar

VCDR ..... Válvula de Contrôle Direcional Redundante

$\Delta p$ ..... Delta P, diferença de pressão

$\Delta R$ ..... Fator de Redução de Risco

$\gamma^{D}$ ..... Taxa de Falha sob Demanda

$\gamma^{DD}$ ..... Taxa de Falha sob Demanda detectada

$\gamma^{DU}$ ..... Taxa de Falha sob Demanda não detectada

$\gamma^{S}$ ..... Taxa de Falha Segura

$\gamma^{SD}$ ..... Taxa de Falha Segura detectada

$\gamma^{SU}$ ..... Taxa de Falha Segura não detectada

$\gamma_{TOT}$ ..... Taxa Total de Falha

$f_i$ ..... taxa de falha

# INDÍCE

# 1. Introdução

Cada vez mais no mercado industrial e mais precisamente nas indústrias de transformação, o tema segurança tem sido amplamente discutido.

> Recentemente normas internacionas, como a IEC 61508 e ANSI/ISA 84.01 contemplam o projeto e a aplicação de Sistemas Instrumentados de Segurança - SIS. Essas normas têm suas bases desenvolvidas que implicam no estabelecimento de objetivos para redução de riscos através da confiabilidade e uma avaliação segura para verificar se esses objetivos foram atendidos pelo projeto. (GOBLE, WILLIAN M., *et al.*, Extending IEC 61508 Reliability Evaluation Techniques to Include Common Circuit Designs Used in Industrial Safety Systems, 2001)

Acidentes ambientais e que colocam a vida de seres humanos em risco, como o vazamento no reator nuclear na Usina de Chernobyl, na Ucrânia em 1986, o vazamento de petroleo no Golfo do México em 2010, ou ainda os riscos na usina nuclear de Fukushima I, provocados pelo tsunami em 2011, no Japão, são péssimos exemplos de acidentes que precisam ser evitados em novas instalações e motivam, cada vez mais, profissionais e empresas de projetos a pensarem em segurança de processos.

Confiabilidade nos processos de produção e transformação e a certeza de que em caso de falha ou de risco aparente de falha a planta será colocada em um estado seguro de operação são itens extremamente importantes no projeto e construção de um Sistema Instrumentado de Segurança - SIS.

Normas internacionais foram criadas para recomendar carateristícas de elaboração e excecução desses projetos que apresentam em sua arquitetura componentes Elétricos, Eletro-Eletrônicos ou Eletrônicos Programáveis (E/EE/EP), como por exemplo: sensores, cartões de aquisição de dados, válvulas de controle direcional atuadas por solenóide, controladores lógicos programáveis entre outros. Em particular a IEC 61508 e a ANSI 84.01 apresentam princípios e técnicas para se definir níveis de integridade de segurança, conhecida pela sigla SIL do inglês *Safety Integrity Level*.

A análise de falhas que podem ocorrer em uma planta, ocupa um importante espaço nos projetos SIS. O diagnóstico e análise de falhas dos componentes, e por consequência, de todo o Sistema, tem sido o grande desafio dos projetistas na definição dos níveis de confiabilidade e disponibilidade de uma determinada aplicação. Falhas que podem ser ou não detectadas e ainda aquelas consideradas como espúrias, podem ser mapeadas através de análises com

diagramas de Markov, lógicas Fuzzy e redes neurais. No entanto, a possibilidade de se obter diagnósticos que identifiquem os riscos e por consequência o tratamento dessas falhas em curto espaço de tempo de resposta recebe especial destaque por estar entre as técnicas de maior necessidade do mercado. Sua utilização, devido a aspectos de compatibilidade de comunicação entre componentes e dispositivos, lógicas e programas complexos de configuração, além de custos elevados, apresentam uma parcela significativa de dificuldade.

## 1.1. Objetivo Geral

Este trabalho apresenta um estudo sobre o uso de diagnósticos para os riscos de falhas. Apresenta, aspectos de segurança que as normas IEC e ANSI abordam. Demonstra, o uso de redes digitais de comunicação e sua contribuição para aplicações seguras conferindo níveis aceitáveis de confiabilidade e tempos de resposta adequados.

### 1.1.1. Objetivos Específicos

- Construir um protótipo de um sistema seguro de controle e através de simulação de sinais se possa identificar riscos de falhas e falhas;
- Utilizar um terminal inteligente de válvulas em operação local, sem a necessidade de estar conectado a uma rede de comunicação digital, onde se possa verificar diagnósticos;
- Contribuir com a apresentação de um dos modelos de cálculo disponível para obtenção SIL.

## 1.2. Estrutura do Trabalho

O método e o desenvolvimento deste trabalho teve como proposta uma apresentação direta e prática das recomendações de projeto de um SIS. Com a principal base de pesquisa na normalização disponível, apresenta alguns estudos que, quando avaliados sob a ótica da praticidade, sugerem conceitos mais acessíveis aos projetistas no tratamento de falhas. A dismistificação se inicia com a construção do protótipo, a demonstração da possibilidade de diagnóstico de falhas e conclui com uma sugestão de cálculo SIL.

Estrutura-se através de cinco capítulos principais e aborda os principais marcos e normas que compõe o tema e motivaram este estudo.

### 1.2.1. Revisão Bibliográfica

Com inumeras fontes de referências e conteúdo bibliográfico disponível para o estudo e projeto de SIS a Revisão Bibliográfica de que trata o Capítulo 2, apresenta o

embasamento teórico que irá permitir ao leitor se situar no contexto que será desenvolvido. Os metodos utilizados pelo mercado além da definição de termos, fórmulas e ensaios, completam esta fase.

### 1.2.2. Descrição e apresentação do Modelo de estudo

Definido o ambiente, será apresentado a construção do protótipo para estudo. Será construído um sistema de controle seguro para o controle de vazão de agua de um suposto circuito de refrigeração de um tanque. A figura 1, apresenta a válvula de controle proporcional atuada pneumaticamente que será utilizada.

**Figura 1 - Válvula de Controle Proporcional de Vazão**

A funcionalidade e confiabilidade do sistema serão validados através da análise do comportamento das entradas e saídas dos elementos de controle seguro da instalação ao longo de sua operação. A esse comportamento serão designados diagnósticos e, por consequência, o tratamento de falhas.

Considerando a afirmação do Dr. Luiz Carlos Felício, em seu livro Modelagem Dinâmica de Sistemas e Estudo da Resposta, que “é dentro do contexto de soluções aproximadas que encontramos o significado de Modelagem, pois Engenharia é um conjunto de modelos” (2010, p.2), o foco deste trabalho estará no modelo que representa a malha segura desse processo.

Portanto, na modelagem proposta, serão registrados os valores das entradas e saídas dos elementos seguros enquanto em operação e o monitoramento da alteração desses

valores irá indicar a probabilidade de falhas em que o SIS estaria sujeito e disparar as ações necessárias de intervenção e correção dos pontos críticos.

### 1.2.3. Avaliação e análise do Problema proposto

As duas áreas distintas que devem se interagir, para que a proposta de diagnóstico de falhas seja alcançada, serão detalhadas nesta etapa:

**Tratamento de Falhas -** onde a análise de riscos, confiabilidade e segurança serão objetivos estabelecidos para a excecução e projeto de um SIS, portanto, será apresentado uma abordagem sobre o estudo sobre falhas seguras (*fail safe*), falhas sob demanda (*failure on demand*) e circuitos redundantes responsáveis pela disponibilização do Sistema;

**Redes de Comunicação Digital -** essencial no sistema de controle proposto, será responsável pelos diagnósticos em tempo real e pela lógica de operação, no entanto, como também é vulnerável, merece uma atenção especial com relação aos meios fisícos utilizados, os mecânismos de proteção e a escolha do protocolo a ser utilizado, dentro das recomendações da norma IEC 61784-3 e suas referências.

### 1.2.4. Validação do Trabalho

Através da manipulação dos sinais monitorados no protótipo, serão apresentados os resultados da verificação dos diagnósticos percebidos. Apresenta-se um dos modelos de cálculo para verificação SIL de acordo com a IEC 61508-5.

### 1.2.5. Conclusão

Serão discutidos os resultados obtidos e as recomendações finais para a aplicação deste estudo.

Finalizando, comentários sobre as vantagens obtidas e algumas expectativas para trabalhos futuros.

# 2. Revisão Bibliográfica

Este conteúdo representa a base da pesquisa desenvolvida focando as definições de termos, aplicações, métodos e referências utilizadas, aborda os estudos das Dependências Funcionais de Falha (FDEP), a definição de uma Função de Segurança (SF), o que são Níveis de Integridade Segura (SIL), cálculos para a taxa de falhas, fatores de avaliação que são importantes na certificação de componentes, restrições de Arquitetura, uso de redundância em dispositivos, aplicações de redes Neurais na análise de sinais e finaliza com a proposta do uso de protocolos abertos em comunicação digital em aplicações da indústria em geral.

Os Sistemas Instrumentados Seguros (SIS) são tratados por normas internacionais, que recomendam os requisitos básicos para a excecução de um projeto, tendo como um dos principais objetivos garantir a Confiabilidade e Disponibilidade de um Processo Industrial.

As principais normas que fundamentalizam este trabalho são:

- ANSI/ISA 84.00.01 – 2004 - Sociedade de Instrumentação, Sistemas e Automação – ISA, fornecendo os requisitos minimos para a implementação de um SIS;
- IEC 61508 – 2010 - direcionada aos fabricantes de Equipamentos e Instrumentos; e
- IEC 61511 – 2003 - direcionada aos usuários, projetistas e integradores.

Sendo que essas duas últimas apresentam os aspectos que devem ser considerados nos Sistemas Elétricos/Eletrônicos/Eletrônicos prográmaveis (E/EE/EP) quando utilizados para excecutar funções de segurança.

Meshkat *et al* (2002) afirmam que os Sistemas Seguros e de Proteção podem experimentar duas fases distintas: em espera ou em operação. Alertam para a necessidade de combinar uma análise de dependência de falhas em ambas as fases. Um Sistema Seguro pode permanecer por um longo período de tempo em espera, sendo periodicamente testado e sob manutenção. Uma vez acionado, deve operar pelo tempo necessário da demanda. As características de falhas nessas duas fases são diferentes: falha quando o sistema está em espera e é acionado para entrar em operação - definido como falha sob demanda; ou, falha enquanto em operação - definido como falha segura, pois devem ser implementados rotinas para garantir a continuidade do processo.

A proposta dos autores, nesse trabalho, foi a de automaticamente combinar a análise da disponibilidade de um Sistema enquanto em espera, com a análise da confiabilidade enquanto

em operação utilizando-se de uma Estrutura de Falhas Dinâmicas – DFT (*Dinamic Fault Tree*). Essa estrutura de falhas captura a dependência dos componentes instalados que suportam o Sistema e que são utilizados para detectar ou iniciar o processo de demanda.

Eles apresentaram um sistema hipotético de combate a incêndio com o uso de dispositivos termo-sensíveis projetados para serem acionados em temperaturas pré-determinadas, lançando automaticamente água sob a forma de aspersão em uma determinada área, com vazão e pressão especificados, e comumente chamados de *Sprinklers* (chuveiros automáticos). Composto por três sensores de temperatura, duas bombas de alimentação de água e um controlador digital, desenharam sua respectiva arquitetura e apresentaram suas considerações sobre as relações de interdependência das possíveis falhas e a necessidade de redundância de componentes.

Cada uma das bombas de alimentação necessita que o seu suprimento de água, composto por válvulas e filtros, esteja dentro de níveis aceitáveis para entrar em operação. Quando a temperatura atinge valores acima do ponto de ajuste dos sensores, os mesmos enviam essa informação ao controlador para acionamento das bombas de alimentação. O sistema estará disponível sob demanda somente se dois sensores estiverem em condições de operação e no mínimo uma das bombas entrar em operação. O sistema continuará a atender a demanda enquanto uma das bombas e o controlador estiverem funcionais.

Ignorando-se as diferenças entre os estados, de operação ou em espera, que o sistema pode experimentar, as Dependências Funcionais (FDEP) podem ser modeladas utilizando-se a Estrutura de Falhas Dinâmicas (DFT) proposta na figura 2. A FDEP de cada bomba está relacionada com as válvulas e filtros no suprimento de água. A FDEP constitui um "gatilho" de uma ou mais entradas dependentes. Como em um circuito sequencial, quando ocorre o gatilho, as entradas em dependência serão forçadas a ocorrer. A relação entre o uso das bombas na operação é representado pela sigla CSP, reserva fria, (*cold-spare*). CSP é uma das portas dinâmicas disponíveis no circuito utilizadas para representar o uso de dispositivos reservas associados.

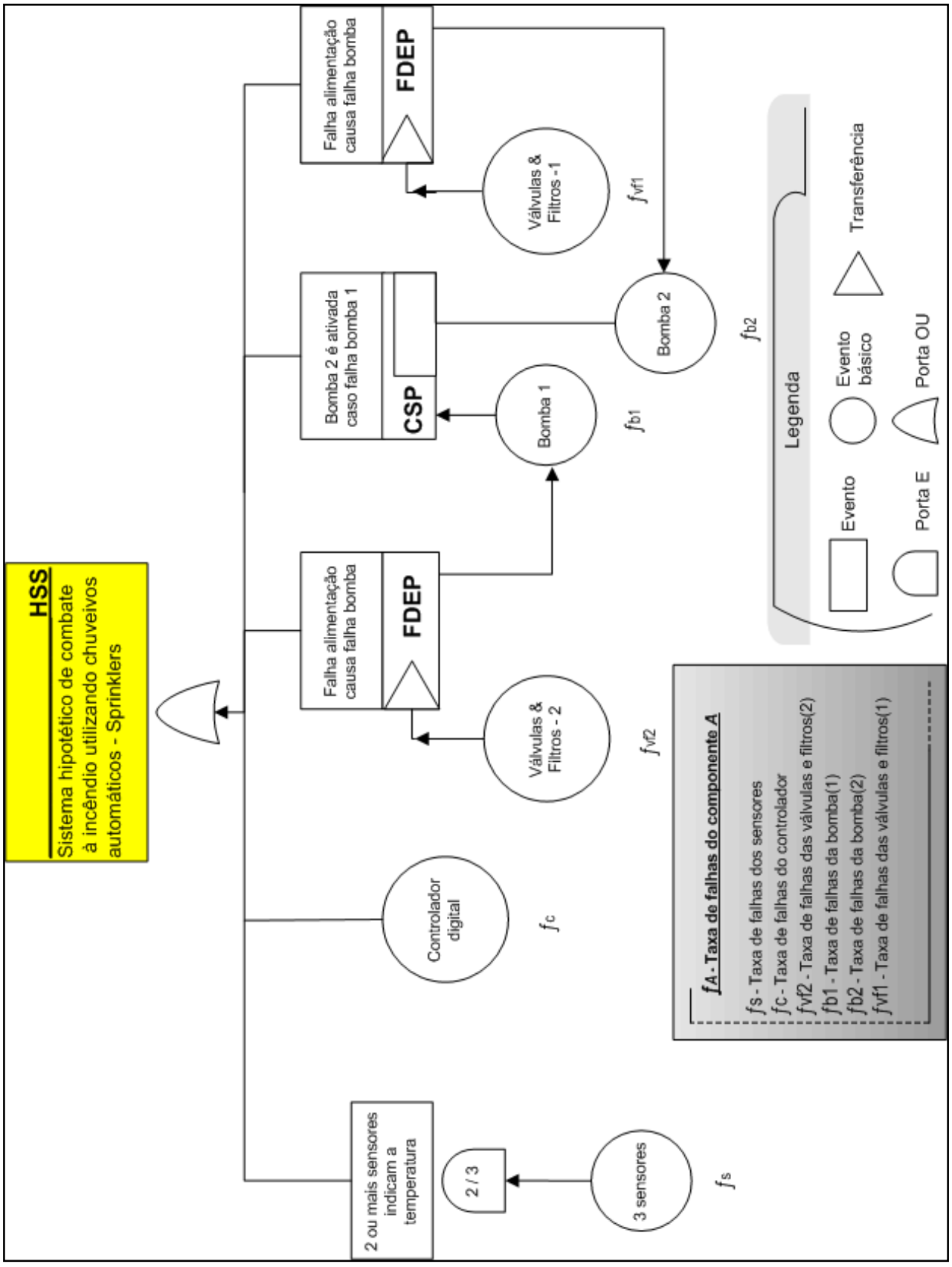



**Figura 2 - Estrutura de Falhas Dinâmicas - DFT**

**adaptado de:** ***Dependability Analysis of Systems with On-Demand and Active Failure Modes Using Dynamic Fault Trees. IEEE Transactions on Reliability. United States, Vol. 51, No.2, 2002.***

Os autores seguindo as recomendações da norma IEC 61508 parte 7, apresentaram através da utilização de cadeias Markov (MC), vide figura 3, a mesma análise de falhas e observam algumas dificuldades associadas ao seu uso:

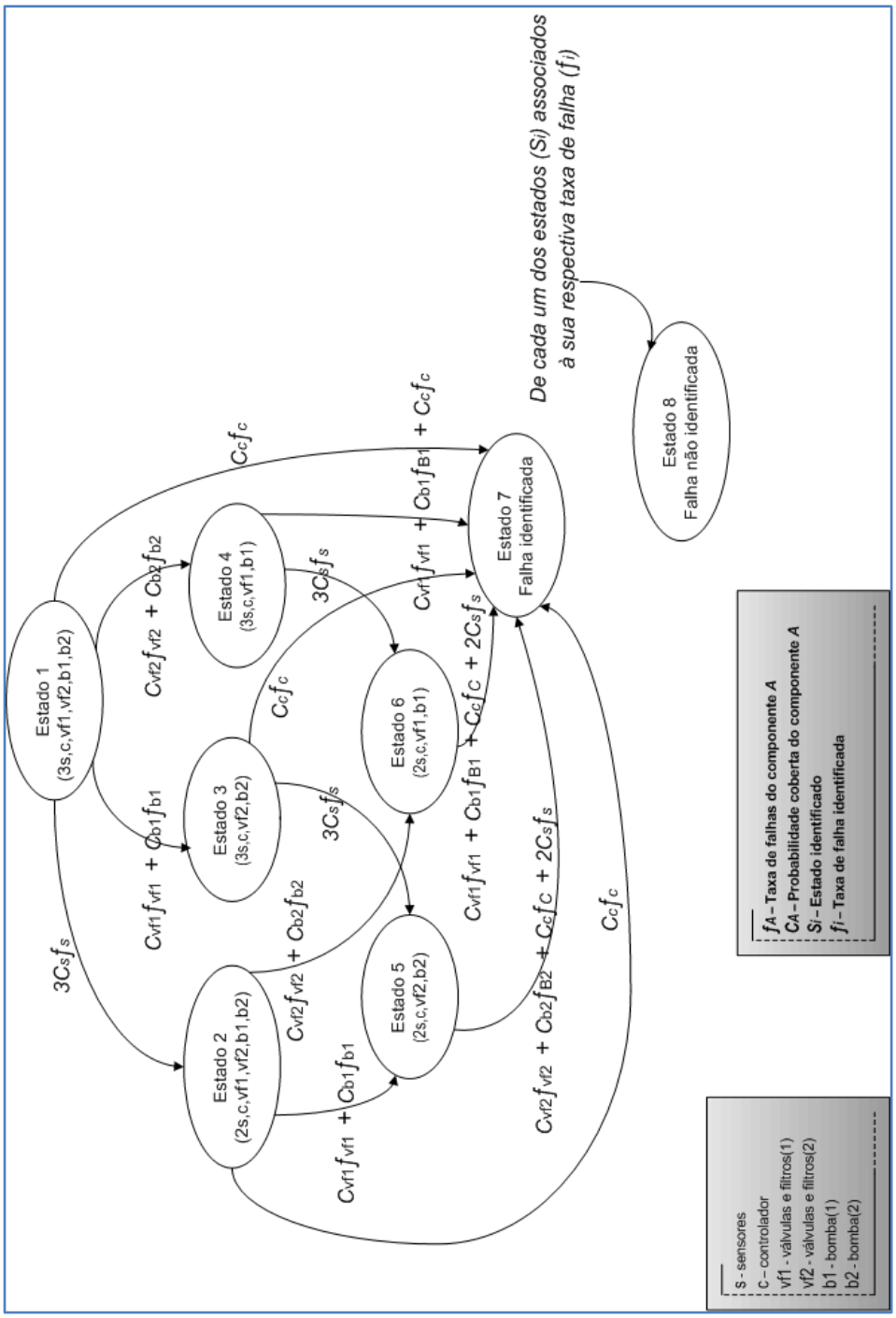



**Figura 3 - Cadeia Markov (MC)**

**fonte:** ***Dependability Analysis of Systems with On-Demand and Active Failure Modes Using Dynamic Fault Trees. IEEE Transactions on Reliability. United States, Vol. 51, No.2, 2002.***

1) Embora a bomba de alimentação e sensores fossem utilizados somente para a partida do sistema, a MC na figura 3 considera-os em toda a análise e cria estados correspondentes para cada fase da operação. Sistemas reais são bem mais complexos do que o aqui apresentado, sendo a explosão dos estados no espaço é um dos problemas encontrados;

2) Sob algumas circunstâncias, os componentes utilizados na partida de um sistema também estarão ativos durante a demanda, mas apresentando diferentes parâmetros de falha;

3) Os subsistemas de suporte podem ser motivo de reparo e manutenção enquanto o sistema principal encontrar-se em espera, mas não é possível que o mesmo sofra manutenção durante sua demanda.

Observa-se que a falha-coberta de um componente A é representado por "$C_A$". Falhas cobertas de componentes podem ou não conduzir a falha do sistema, dependendo das redundâncias remanescentes. Falhas não cobertas irão sempre conduzir a fallha do sistema. Para cada um dos estados ($S_i$) apresentados associa-se sua respectiva taxa de falhas ($f_i$). Goble e Bukowski (2001) abordam a necessidade de extensão dos métodos de avaliação da confiabilidade e segurança de Sistemas Instrumentados Seguros (SIS) quando se utilizam de componentes com diagnósticos incorporados ou circuitos analógicos. Um modo adicional de falha deve ser considerado – alarme, ou anúncio, do diagnóstico de falha. As definições de falha segura e falha sob demanda devem ser considerados nos circuitos analógicos.

A Função de Segurança (SF) de um SIS é de automaticamente interromper um processo industrial quando uma condição de risco for detectada. Apesar dos diferentes tipos de equipamentos utilizados, existe uma forte tendência para o uso daqueles que possuem lógicas programáveis embarcadas. Para todos esses equipamentos serem certificados para o uso em aplicações seguras eles necessitam atender as normas IEC61508 e a ANSI/ISA 84.01.

Essas normas são baseadas em perfomance e os passos a seguir, considerados:

i. No início do projeto, uma análise de riscos deve ser feita onde objetivos de confiabilidade e segurança são estabelecidos de acordo com o Nível de Integridade de Segurança (SIL), como apresentado na tabela 1;

**Tabela 1 - Nível de Integridade de Segurança (SIL)**

| Nível de Integridade de Segurança SIL | Probabilidade média de Falha sob Demanda $PFD_{avg}$ | Fator de Redução de Risco $\Delta R$ |
|---|---|---|
| **4** | $10^{-4} > PFD_{avg} \geq 10^{-5}$ | $10.000 \leq \Delta R < 100.000$ |
| **3** | $10^{-3} > PFD_{avg} \geq 10^{-4}$ | $1.000 \leq \Delta R < 10.000$ |
| **2** | $10^{-2} > PFD_{avg} \geq 10^{-3}$ | $100 \leq \Delta R < 1.000$ |
| **1** | $10^{-1} > PFD_{avg} \geq 10^{-2}$ | $10 \leq \Delta R < 100$ |

**fonte: IEC 61508 parte 1**

ii. Antes de sua implementação, uma análise de sua confiabilidade e segurança deve ser aplicada para verificar se a probabilidade de falhas do projeto atende aos objetivos estabelecidos durante a análise de riscos. A medida básica para a integridade segura é a Probabilidade média de Falha sob Demanda - $PFD_{avg}$.

Notas:

a) IEC61508 – parte 6 e ISA TR84.02 orientam como proceder com as análises de confiabilidade e risco;
b) Um SIS é projetado para operar por um período de tempo. Concluída sua Função de Segurança, é completamente testado e então colocado em espera até uma nova demanda;
c) A SF de um SIS consiste na capacidade em colocar um processo industrial em um estado em que todas suas saídas estejam desenergizadas.

Os métodos de análise descritos nas normas assumem dois modos de falhas, Falha Segura e Falha sob Demanda.

O cálculo para a Taxa Total de Falhas ($\gamma_{TOT}$) para os componentes de um SIS, pode ser definido como:

$$\gamma_{TOT} = \gamma^S + \gamma^D$$

onde: $\gamma^S$ – Taxa de Falha Segura e $\gamma^D$ – Taxa de Falha sob Demanda

Além disso deve-se considerar a capacidade do sistema em diagnosticar ou não a falha, caracterizando-as pelo fato de poderem ou não ser detectadas:

$$\gamma^{S} = \gamma^{SD} + \gamma^{SU}$$

e

$$\gamma^{D} = \gamma^{DD} + \gamma^{DU}$$

sendo que as taxas de falhas são representadas por:

$\gamma^{SD}$ – Taxa de Falha Segura detectada;

$\gamma^{SU}$ – Taxa de Falha Segura não detectada;

$\gamma^{DD}$ – Taxa de Falha sob Demanda detectada;

$\gamma^{DU}$ – Taxa de Falha sob Demanda não detectada.

Schwartz e Hochleitner (2010) apresentam três fatores importantes na avaliação de um dispositivo com certificação SIL. Os fabricantes de equipamentos e componentes industriais devem fornecer as taxas de falha e modos de falha de seus produto através de um relatório de Análise dos Modos de Falha, Efeitos e Diagnósticos (*Failure Modes Effects and Diagnostic Analysis - FMEDA*) onde devem ser detalhadas as restrições de arquitetura (*Architectural Constraints*) e a $\gamma_{DU}$ (taxa de falha perigosa não detectada) do dispositivo em questão.

Dispondo dessas informações e de acordo com os parâmetros de manutenção, tais como: intervalos de testes periódicos; cobertura e tempo de reparo; é possível determinar a probabilidade média de falha de um dispositivo sob demanda ($PFD_{avg}$), de forma que se possa estimar o período de uma possível situação de perigo de falha e definir quando a SF deverá executar sua proteção.

Complementam que, as restrições de arquitetura de um dispositivo determinam imediatamente qual nível de redundância (*HFT – Hardware Fault Tolerance*) deve ser usado para se atingir o SIL correspondente à redução de risco necessária de uma SF.

Alertam que a PFD de um dispositivo não determina o Nível de Integridade de Segurança (SIL) do produto, mas sim a contribuição dele na PFDavg da SF.

Outro ponto que se observa é a Restrição de Arquitetura (*Architectural Constraints*) que depende do tipo do dispositivo (A ou B, tabela 2) e da sua Fração de Falha Segura (SFF - *Safe Failure Fraction*).

**Tabela 2 - restrições de arquitetura para um dispositivo**

| Tolerância de Falha do Dispositivo (HFT) | | | | | | | |
|---|---|---|---|---|---|---|---|
| **Dispositivos Tipo A** | | | | **Dispositivos Tipo B** | | | |
| **Fração de Falha Segura** | **0** | **1** | **2** | **Fração de Falha Segura** | **0** | **1** | **2** |
| **< 60%** | SIL1 | SIL2 | SIL3 | **< 60%** | Não permitido | SIL1 | SIL2 |
| **60% < 90%** | SIL2 | SIL3 | SIL4 | **60% < 90%** | SIL1 | SIL2 | SIL3 |
| **90% < 99%** | SIL3 | SIL4 | SIL4 | **90% < 99%** | SIL2 | SIL3 | SIL4 |
| **≥ 99%** | SIL3 | SIL4 | SIL4 | **≥ 99%** | SIL3 | SIL4 | SIL4 |
| Nota: Um HFT (*Hardware Fault Tolerance*) de N, significa que N+1 falha pode causar a perda da Função de Segurança (SF) | | | | | | | |

**fonte: IEC 61508 parte 2**

Sendo, um dispositivo Tipo A um subsistema "não complexo" que utiliza elementos discretos e um dispositivo Tipo B um subsistema "complexo" que usa micro processadores ou lógica programável.

Com isso, demonstra-se que a restrição de arquitetura de um dispositivo estará associada a sua Fração de Falha Segura (SFF) e que por sua vez será calculada a partir dos dados publicados no FMEDA.

Finalizam com a recomendação de que, para se determinar se um dispositivo é adequado para uso em uma Função de Segurança, existem 3 aspectos críticos que devem ser considerados:

1. As Restrições de Arquitetura e a faixa de falhas perigosas não detectadas ($\gamma_{DU}$) do dispositivo;
2. A contribuição real e esperada do dispositivo ao PFDavg da SF;
3. Os processos de projeto e manufatura do fabricante avaliando se o dispositivo é certificado.

Parte dos conceitos com relação ao uso de redes de Comunicação Digital Fieldbus em Sistemas Instrumentados Seguros (SIS) são publicados por Franeková e Rátocný (2010), com uma modelagem e avaliação dos aspectos de segurança em circuitos fechados.

A grande utilização de redes industriais de comunicação e as modernas tecnologias de informação na medição e controle de processos fazem com que as redes de comunicação estejam cada vez mais presentes.

Atualmente a norma IEC61784-3 trata a função de Segurança nas redes industriais utilizadas na medição e controle de processos definindo perfís de segurança para Familias de Comunicação digital - CPF (Familia de Perfís de Comunicação), recomendados para uso em Sistemas Instrumentados Seguros com SIL 3.
Levando em consideração os quatro parâmetros básicos para monitorar o ciclo de vida de um Sistema: **Confiabilidade, Disponibilidade, Manutenção e Segurança s**ugerem a modelagem das propriedades de Segurança de um Sistema de Transmissão, através:

- das características funcionais da lógica de Segurança com sua respectiva Camadas de Segurança na Comunicação - SCL (*Safety Communication Layer*);
- dos efeitos de ruídos nos meios de transmissão;
- dos efeitos de falhas de equipamentos nos sistemas de transmissão.

Na tarefa de modelar os efeitos de falhas em Sistemas FieldBus de transmissão, observam que:

- Para Sistemas de Controle Seguros é necessário atender, em sua totalidade, todos, os requisitos de segurança e, consequentemente, conhecer todos os riscos que podem ser aceitáveis;
- O conhecimento de eventos atribuidos aos sistemas de transmissão formam a base para a verificação dos diagnósticos de falhas e não são utilizados somente na prevenção, mas também na detecção e no bloqueio dos efeitos dessas ocorrências.

Concluem com a recomendação de uma avaliação entre disponibilidade e nível de integridade (SIL) que se deseja de um SIS.

Gabor e Zmaranda (2009), apresentam um método, passo a passo, utilizado no projeto de Controle critíco para atender os requisitos de segurança e confiabilidade um Sistema Instrumentado de Segurança.

Definem Confiabilidade ou Disponibilidade como a capacidade de um sistema permanecer operando, tolerar falhas e de emitir sinais de alarme e controle, de forma que o processo seja colocado em modo de seguro de operação até que as mesmas sejam detectadas e reparadas.
Em análise da Estrutura de Falhas (FTA), demonstram que a falta do uso de Redundancia nos elementos básicos de um Sistema é a principal causa em não se atingir os objetivos de Confiabilidade e Segurança de um projeto.

Os tipos de arquiteturas redundantes são apresentados em conjunto com recomendações para as rotinas de teste de validação e manutenção de seus componentes, de forma que a Segurança e Confiabilidade de um processo sejam assegurados. Técnicas quantitativas também foram utilizadas para comparar essas arquiteturas tipícas de uso.

A notação utilizada nos circuitos redundantes representam a quantidade de elementos que precisam ser desernegizados do total disponíveis até que a planta se apresente em uma condição de operação insegura.

Uma notação 1oo1, lê se *one out of one* (um fora de um) significa que um elemento "fora" de um total de um elemento irá desernegizar o circuito.

Uma notação 2oo2, *two out of two*, representa dois elementos "fora" de um total de dois elementos do circuito.

Uma notação 2oo3, *two out of three*, representa dois elementos "fora" de um total de três elementos do circuito.

Na figura 4, apresenta-se as principais configugrações redundantes que podemos utilizar para projetos SIS. Como exemplo são utilizados bobinas de contatores ou de válvulas.

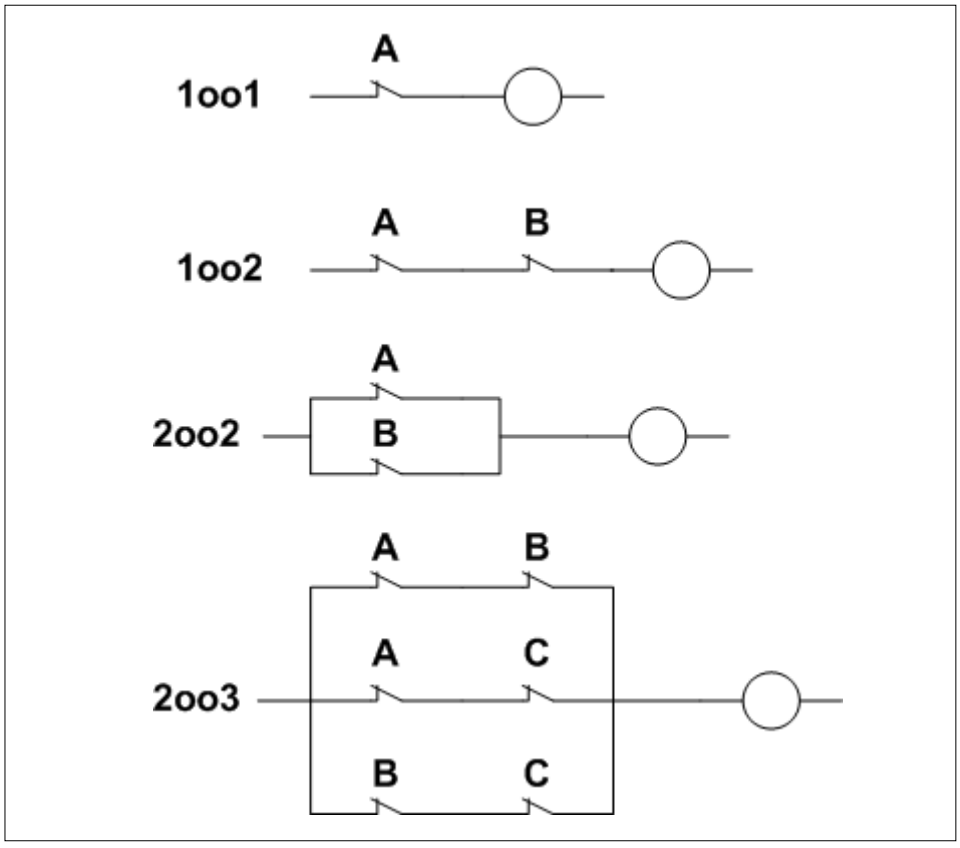



**Figura 4 - Tipos de arquitetura redundantes**

Babu e Shailesh (2002), utilizaram uma rede neural adaptável para o diagnóstico de falhas e controle de processo em um Trocador de Calor. Estabelecem relações diretas de sinais de entradas (alarmes e sensores) e saídas (falhas) para criar um algoritímo que permitisse o estudo de estado de um sistema.

Consideraram que as variações das condições físicas de um processo, dos sistemas de controle ou mesmo de fatores externos, poderiam ser monitoradas e armazenadas. Valores devido a desvios de condições fisícas de um determinado SIS, como por exemplo a variação de temperatura ou pressão fora de padrões previamente definidos poderiam ser determinantes para a detecção de falhas. A detecção e o diagnóstico em seu estágio inicial foi o prinicipal interesse nesse estudo.

A rede Neural poderia "armazenar conhecimento" através do histórico e suas características do processo ao longo da operação. Essa informação resultaria do conjunto de dados das variáveis que identificavam as condições de falha.

No modelo proposto foram gerados oito sinais de entradas para o sistema e oito saídas que identificavam as falhas a serem monitoradas. As combinações desses sinais puderam identificar a condição de risco.

Um detalhado estudo sobre a utilização da tecnologia "Fieldbus", termo sem tradução direta para o idioma português, em Automação Industrial é apresentada na 10ª. Conferência do IEEE (Thomesse, 2005). Relata as origens dessa tecnologia, incluindo análises técnicas e científicas, referente às redes industriais dos anos 70.

Dividido em duas partes, aborda, na primeira o conceito "Fieldbus" e os requisitos para seu uso, enquanto na segunda se dedica aos aspectos técnicos, serviços, protocolos, finalizando com algumas considerações sobre arquiteturas.

Com a possibilidade da comunicação entre sensores, dispositivos de campo, controladores e sistemas supervisórios, os protocolos "*Field Bus"* são utilizados nos processos contínuos de produção e assumem um papel importante na sua participação.

Especialmente nas indústrias de transformação, químicas, petroquímicas, papel e celulose e mineração, alguns outros aspectos são levados em consideração para difusão dessa tecnologia. Interferências eletromagnéticas, necessidades de redundância, interdependência e segurança de processos são algumas das caracteristícas das aplicações mais encontradas.

Apresenta, no final de seu trabalho, as duas normas de maior relevância para o uso e entendimento dessa tecnologia, com suas arquiteturas, perfis e familias de protocolos: a IEC 61158 e IEC 61784.

Dzung *et al* (2005) já comentam o aumento das "modernas" redes industriais de comunicação baseadas em protocolos abertos. Descrevem o estágio das especificações relevantes para um número de protocolos de automação normalizados e abordam os aspectos de segurança e vulnerabilidade que os caracterizam.

Apresentaram várias ferramentas e estudos de caso, descrevendo aspectos de segurança na configuração e operação de subestações e plantas industriais para acesso remoto. Recomendaram tecnologias de segurança e avaliaram as normas disponíveis, ressaltando os principais pontos que deveriam ser observados, como: Confidencialidade, Integridade, Disponibilidade, Autenticação e Autorização.

Concluem que a Segurança que deve ser levada em consideração na aplicação de protocolos industriais de comunicação, devem observar requisitos distintos daqueles quando utilizados nas Tecnologias de Informações Comerciais que tem uma maior preocupação com aspectos de Confiabilidade e Integridade dos Sistemas. O fator de maior importância na Indústria de transformação, sem dúvidas, deve ser a segurança operacional com a busca contínua da ausência de falhas catastróficas que possam colocar a vida de seres humanos em risco.

# 3. Descrição e Apresentação do Modelo de Estudo

Com o objetivo de demonstrar que a utilização de uma Estrutura de Falhas Dinâmicas (DFT), vista no capítulo anterior, pode ser facilmente implementada com suas respectivas funções de dependências e que o uso de redes digitais com tecnologia *Field Bus* possibilitam o diagnóstico de falhas em velocidades de até 500 Kbps garantindo os Níveis de Integridade Segura (SIL) com componentes certificados, foi construído um protótipo de um circuito de água para um suposto sistema de refrigeração de um tanque (TQ-1) no Centro de Treinamento da Ascoval, uma das unidades de negócio do grupo Emerson Eletric, situada na cidade de Barueri em São Paulo.

Para excecutar a Função de Segurança (SF), foram simulados, manualmente, sinais de sensores das variáveis de pressão, vazão e temperatura fora de padrões pré-estabelecidos.

O circuito, apresentado na figura 5, consiste no controle da vazão de água que é feito através de uma válvula principal (FCV-105) atuada pneumaticamente e com um posicionador digital, incorporado, de 4 a 20mA (FIC-104).

A atuação de Válvulas Solenóide utilizadas, a conexão e controle dos sinais de entradas e saídas provenientes dos elementos, a lógica de operação, os testes de rotina, os diagnósticos e a Função de Segurança (SF) são feitos através de um Terminal Inteligente de Válvulas (TIV).

A utilização do Terminal irá contemplar a aplicação de componentes discretos em um ambiente de rede digital, além de possuir a lógica de operação embarcada. As variáveis, temperatura do tanque, pressão e vazão da linha principal, são simuladas através de sinais analógicos utilizando geradores de 4 a 20mA de forma que:

(I) dois sinais de entrada, analógicos de temperatura, denominados IAT1 e IAT2, irão simular dois sensores (TSHL-300 e TSHL-301) distintos instalados em uma configuração em paralelo para a leitura da variável temperatura do Tanque (TQ-1). Seus valores serão considerados como responsáveis pelo aumento ou redução de vazão de água a ser controlada pela válvula principal de controle de vazão FCV-105. Alta temperatura, deverá demandar um aumento na vazão enquanto a baixa temperatura, uma redução;

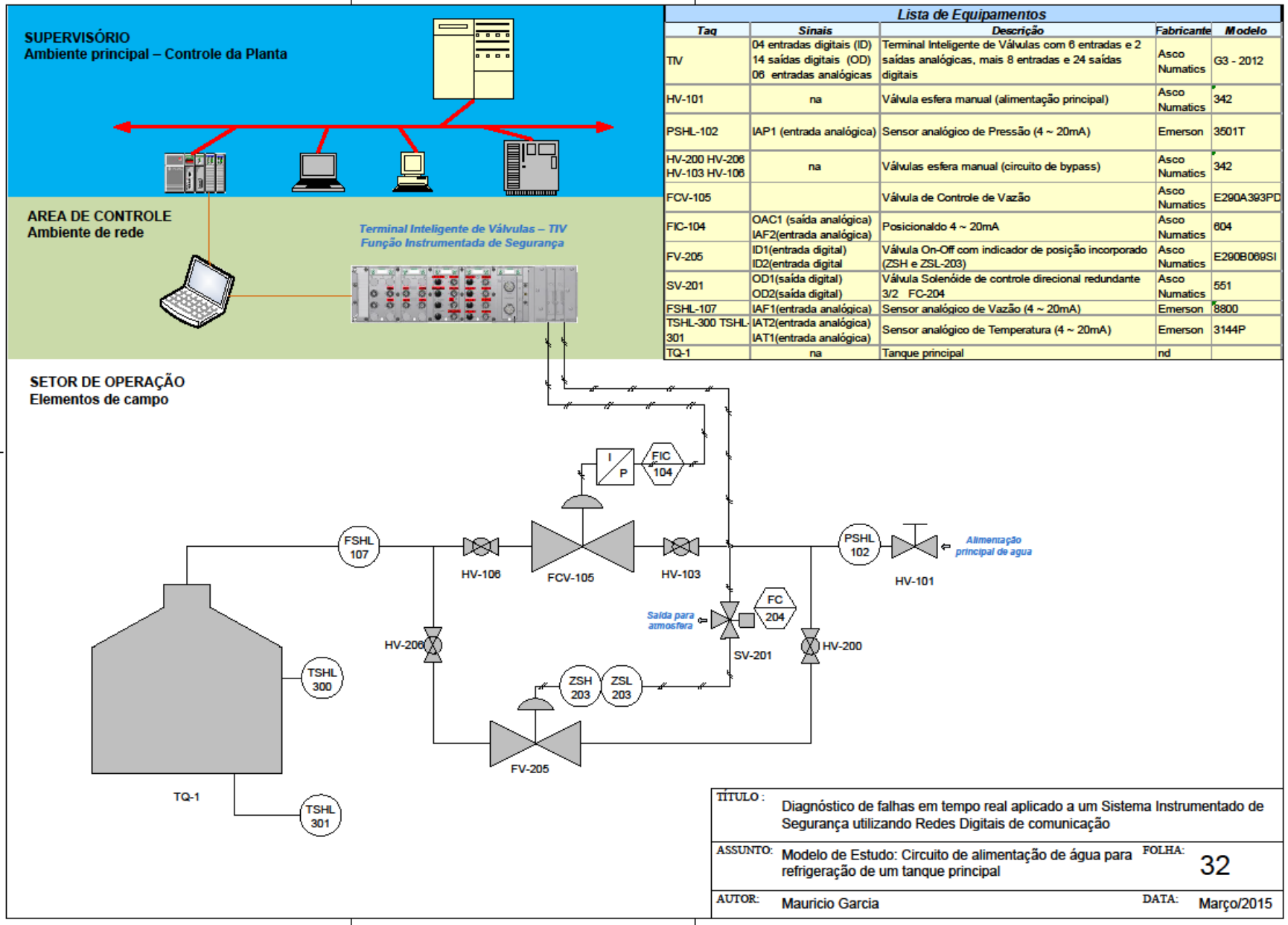
(II) um sinal de entrada, analógico de pressão, denominados IAP1, irá simular um sensor instalado na pressão montante (PSHL-102) da FCV-105. Seu valor será considerado como responsável pela leitura de pressão de água no circuito. Em operação normal IAP1 deverá ser maior que 0 (zero), para que exista vazão. O

diagnóstico de uma suposta falha no circuito de água será feito através do monitoramento do seu sinal de saída, indicando possíveis riscos ou falhas nos componentes responsáveis pela vazão de água;

(III) A variável vazão terá sua leitura simulada através de um sinal de entrada analógico, (IAF1), de 4 a 20mA e será comparado com um sinal de entrada analógico, também de 4 a 20mA, (IAF2), denominado de posição ou resposta e proveniente do posicionador digital (FIC-104) instalado em FCV-105. Qualquer diferença entre esses sinais irá identificar que a vazão requerida pelo controlador não está sendo atendida e portanto, uma indicação de possíveis riscos ou falhas no fluxo de água.

Uma Válvula Auxiliar, FV-205, será instalada, em paralelo (*by-pass*) a FCV-105, para que em caso de alarme devido ao risco ou falha do Controle de Vazão, a mesma alimente o circuito de água independentemente. A Função Instrumentada de Segurança (SIF) da planta, definida neste circuito será a desernegização de todos os elementos Elétricos, Eletrônicos e EletroEletrônicos Prográmaveis (E/EE/EEP) da malha de Controle Seguro e a linha principal deverá ser alimentada com a vazão máxima de água disponível.
Dois sensores magnéticos (ZSH/ZSL-203), pertencentes ao indicador de posição da sede da Válvula FV-205, irão gerar os sinais de entrada digitais ID1 e ID2 e uma Válvula Solenóide Redundante (FC-204) será responsável pela operação da FV-205.

O circuito é apresentado a seguir e, na sequência, serão apresentados os componentes individualmente com as principais caracteristícas de funcionamento, bem como os dados dos relatórios FMEDA relevantes para o cálculo teórico do Nível de Integridade de Segurança SIL.




**Lista de Equipamentos**

| Tag | Sinais | Descrição | Fabricante | Modelo |
|---|---|---|---|---|
| TIV | 04 entradas digitais (ID)<br>14 saídas digitais (OD)<br>06 entradas analógicas | Terminal Inteligente de Válvulas com 6 entradas e 2 saídas analógicas, mais 8 entradas e 24 saídas digitais | Asco Numatics | G3 - 2012 |
| HV-101 | na | Válvula esfera manual (alimentação principal) | Asco Numatics | 342 |
| PSHL-102 | IAP1 (entrada analógica) | Sensor analógico de Pressão (4 ~ 20mA) | Emerson | 3501T |
| HV-200 HV-206<br>HV-103 HV-106 | na | Válvulas esfera manual (circuito de bypass) | Asco Numatics | 342 |
| FCV-105 | | Válvula de Controle de Vazão | Asco Numatics | E290A393PD |
| FIC-104 | OAC1 (saída analógica)<br>IAF2(entrada analógica) | Posicionaldo 4 ~ 20mA | Asco Numatics | 604 |
| FV-205 | ID1(entrada digital)<br>ID2(entrada digital | Válvula On-Off com indicador de posição incorporado (ZSH e ZSL-203) | Asco Numatics | E290B069SI |
| SV-201 | OD1(saída digital)<br>OD2(saída digital) | Válvula Solenóide de controle direcional redundante 3/2 FC-204 | Asco Numatics | 551 |
| FSHL-107 | IAF1(entrada analógica) | Sensor analógico de Vazão (4 ~ 20mA) | Emerson | 8800 |
| TSHL-300 TSHL-301 | IAT2(entrada analógica)<br>IAT1(entrada analógica) | Sensor analógico de Temperatura (4 ~ 20mA) | Emerson | 3144P |
| TQ-1 | na | Tanque principal | nd | |

| | | | |
|---|---|---|---|
| TÍTULO : | Diagnóstico de falhas em tempo real aplicado a um Sistema Instrumentado de Segurança utilizando Redes Digitais de comunicação | | |
| ASSUNTO: | Modelo de Estudo: Circuito de alimentação de água para refrigeração de um tanque principal | FOLHA: | 32 |
| AUTOR: | Mauricio Garcia | DATA: | Março/2015 |

Figura 5 - Modelo proposto – Controle de Vazão

## 3.1. Válvula de Controle de Vazão (FCV-105)

A Válvula de Controle de Vazão selecionada (FCV-105), conexão roscada ao processo de ½", atende a uma vazão máxima de 82 l/min e suas principais caracteristicas estão descritas a seguir na Tabela 3. De fabricação Asco/Numatics é instalada com um Controlador digital de posição que, através de um sinal de 4 a 20 mA, habilita uma operação proporcional de sua sede de 0 a 100% de abertura. Possui uma função de falha segura que, na falta da tensão de alimentação, coloca a válvula na posição fechada e ainda, tem seu sinal de controle em malha dupla.

Portanto, a Válvula de Controle de Vazão, terá em seu posicionador os seguintes sinais:

- OAC1 - sinal entrada externo de 4 a 20mA simulando o controlador do processo;
- IAF2 - sinal de realimentação, gerado pelo posicionador para comprovação da posição da sede da válvula. Será comparado com o sinal de saída (IAF1) do Rotâmetro.

**Tabela 3 - Caracteristícas Técnicas da Válvula de Controle de Vazão (FCV-105)**

| | | | |
|---|---|---|---|
| **Posicionador Digital** | **Pressão de Pilotagem** | 500KPa (ar) |  |
| | **Tensão Nominal** | 24Vcc +/- 10% | |
| | **Sinal de ajuste** – OAC1 | 4 - 20mA | |
| | **Realimentação** – IAF2 | 4 - 20mA | |
| **Válvula 2 vias** | **Pressão Diferencial de Operação** | 700Kpa | |
| | **Temperatura ambiente** | 25ºC | |
| | **Conexão ao processo** | G 1/2" | |
| | **Código** | E290A393PD | |

## 3.2. Sensores de Pressão, Temperatura e Vazão

Os Sensores de Pressão, Temperatura e Vazão, serão simulados através de geradores de sinais analógicos de 4 a 20mA, tabela 4, de forma que manualmente possam ser criadas situações de falhas e distintas na operação.

**Tabela 4 - Características técnicas - Gerador de sinal 4 - 20mA**

| | | |
|---|---|---|
| alimentação | 15 a 24Vcc |  |
| saída | 4 a 20 mA | |

Apesar desses sinais serem simulados, foram utilizados dados e especificações de transmissores Emerson/Rosemont reais utilizados no mercado.

### 3.2.1. Transmissor de Pressão (PSHL-102)

O monitoramento da variável pressão, através do sinal simulado, será responsável pela leitura da linha principal de água. O circuito considera o uso de um transmissor de pressão em linha Rosemount 3501T, tabela 5, montado na pressão montante (PSHL-102). A ausência de sinal irá diagnosticar uma falha segura que será enviado para o TIV.

**Tabela 5 - Transmissores de Pressão (PSHL-102)**

| | | | | |
|---|---|---|---|---|
| **Escala de pressão** | | -100 a 1030 Kpa | |  |
| **Sinal de saída** (IAP1) | | hart 4 a 20mA | | |
| **Ponto de ajuste** | | 400 Kpa | | |
| **Tipo de leitura** | | Manométrica | | |
| **Modelo** | | 3051TG2A | | |
| **Conexão ao processo** | | ½" | | |
| $\gamma^{SD}$ | $\gamma^{SU}$ | $\gamma^{DD}$ | $\gamma^{DU}$ | SFF |
| 0 FIT | 188 FIT | 571 FIT | 126 FIT | 85,8% |

### 3.2.2. Transmissor de Temperatura (TSHL-300 e TSHL-301)

O monitoramento da variável temperatura, através dos sinais simulados "IAT1" e "IAT2", serão responsáveis pela leitura, em dois pontos distintos no tanque TQ-1. O circuito irá considerar o uso de dois transmissores de temperatura Rosemount 3144P, conforme tabela 6. Os dois pontos no tanque são denominados TSHL-300 e TSHL-301. Qualquer variação de 5% entre seus valores, irá diagnosticar uma falha segura. Esses sinais serão enviados para o TIV.

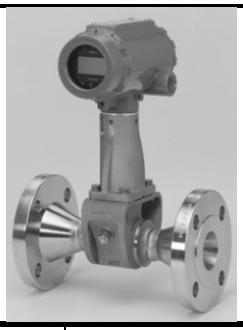
**Tabela 6 - Transmissores de Temperatura (TSHL-300 e TSHL-301)**

| | | | | |
|---|---|---|---|---|
| **Escala de temperatura** | | - 200 a 800 °C | |  |
| **Sinal de saída** (IAT1 e IAT2) | | hart 4 a 20mA | | |
| **Ponto de ajuste** | | 40 °C | | |
| **Tipo de sensor** | | RTDs de 2 de fios | | |
| **Modelo** | | 3144PA1 | | |
| **Precisão digital** | | ±0,10 °C | | |
| $\gamma^{SD}$ | $\gamma^{SU}$ | $\gamma^{DD}$ | $\gamma^{DU}$ | SFF |
| 0 FIT | 188 FIT | 571 FIT | 126 FIT | 85,8% |

### 3.2.3. Medidor de Vazão (FSHL-107)

Será simulado um Medidor de Vazão, da série 8800 da Emerson Process, vide tabela 7, com faixa de leitura de 6,6 a 90 l/min, instalado na saída da Válvula de Controle de Vazão (FCV-105). O sinal de saída de 4 a 20 mA (IAF1), será comparado ao sinal de retorno do Posicionar Digital da Válvula FVC-105 e através da lógica embarcada em TIV, as variações percebidas irão diagnosticar o risco de uma falha segura.

**Tabela 7 - Características técnicas - Medidor de Vazão**

| | | | | |
|---|---|---|---|---|
| **Faixa de leitura** | | 6,6 a 90 l/min | |  |
| **Sinal de saída (IAF1)** | | hart 4 a 20mA | | |
| **Ponto de ajuste** | | 40 l/min | | |
| **Modelo** | | 8800DF005 | | |
| $\gamma^{SD}$ | $\gamma^{SU}$ | $\gamma^{DD}$ | $\gamma^{DU}$ | SFF |
| 0 FIT | 188 FIT | 571 FIT | 126 FIT | 85,8% |

## 3.3. Válvula Atuador Pneumático (FV-205)

Como citado no inicio deste capítulo, a condição segura de operação do circuito será a alimentação do mesmo com a vazão máxima de água disponível. Para essa operação, será utilizada a Válvula Auxiliar (FV-205) atuador pneumático de 2 vias e 2 posições, Normalmente Aberta e conexão de ½", montada em paralelo (sistema de by-pass) com a Válvula de controle principal FVC-105.

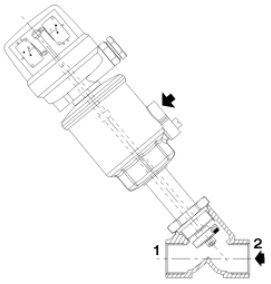
Será mantida na posição fechada através de uma Válvula Solenóide Redundante de Controle Direcional (FC-204), 3vias/2posições, responsável pela pressurização de seu atuador. Quando necessário os dois solenóides redundantes deverão ser desenergizados para que a mesma seja despressurizada e assuma sua posição de espera, totalmente aberta.

Como a Válvula Auxiliar, estará em espera até que o sistema demande sua operação ela deverá ser testada periodicamente, com o objetivo de atender os níveis de segurança SIL da planta.

Para essa função, será utilizado um indicador de posição, com dois sensores magnéticos (ZSH-203 e ZSL-203) em seu atuador pneumático, para que os testes possam ser realizados com a Planta em operação. Esse teste, denominado de "teste de curso parcial", consiste,

através de uma rotina escrita no TIV, em desenergizar ambos solenóides redundantes, de forma que no momento em que os dois sinais provenientes do indicador estiverem em “0”, a FV-205 estará operando. Caso, pelo menos um dos sinais mantenha-se em “1”, irá indicar que o atuador da FV-205, não está se movimentando, e portanto, falha na operação. A tabela 5, a seguir apresenta as características da FV-205.

**Tabela 8 - Características técnicas Válvula Auxiliar (FV-205)**

| | | | |
|---|---|---|---|
| **Indicador de Posição** | **Tipo de sensor** | Magneto-resistivo (MR) |   |
| | **Tensão de Operação** | 10 a 30 Vcc | |
| | **Sensibilidade** | Min. 2 mTesla (20 Gauss) | |
| | **Código** | PNP-QDS-M12 | |
| **Válvula 2 vias** | **Pressão Diferencial de Operação** | 700KPa | |
| | **Tipo de Operação** | Normalmente Aberta | |
| | **Conexão ao processo** | G 1/2" | |
| | **Código** | E290B069SI | |

## 3.4. Válvula Solenóide Redundante (FC-204)

Uma Válvula atuador Solenóide redundante de Controle Direcional (FC-204), consiste em uma válvula com duas bobinas, que podem operar simultâneamente. A principal característica de sua aplicação é a possibilidade de alimentar as duas com sinais distintos, de forma, que caso uma alimentação seja interrompida a outra irá permanecer operando. No modelo proposto, será utilizada na versão de 3 vias, 2 posições, já que está sendo utilizado um atuador simples ação, retorno por mola. No circuito, permanecerá com os dois solenóides energizados constantemente em 24Vcc, através de duas saídas (OD1 e OD2) distintas dos módulos de saída do TIV. Na falta de energia, alimentação de ar comprimido responsável pela atuação da FC-205, será interrompido fazendo com que o circuito seja alimentado com água, condição segura desejada. A tabela 6 apresenta as principais caracteristícas dessa válvula.

**Tabela 9 - Características Técnicas - Válvula Solenóide Redundante (FC-204)**

| | | | | |
|---|---|---|---|---|
| **Versão** | 3/2 vias simples redundante | |  | |
| **Conexão** | G ¼” | | | |
| **Pressão de trabalho** | 500Kpa | | | |
| **Solenóide** | 24Vcc – 1,4W | | | |
| $\gamma^{SD}$ | $\gamma^{SU}$ | $\gamma^{DD}$ | $\gamma^{DU}$ | SFF |
| 0 FIT | 188 FIT | 571 FIT | 126 FIT | 85,8% |

## 3.5. Terminal Inteligente de Válvulas - TIV

O Terminal Inteligente de Válvulas é uma plataforma que incorpora uma base múltipla de Válvulas de Controle Direcional pneumáticas, módulos de entradas e saídas digitais, analógicas e um módulo de comunicação para redes. Possui uma lógica de programação embarcada que possibilita escrever rotinas de operação e testes além de apresentar diagnósticos de estado para suas entradas e saídas. Como a proposta desse trabalho é a de apresentar a aplicação de um SIS utilizando Redes Digitais de Comunicação, o terminal será o elemento responsável pelo gerenciamento da Rede. Mesmo que não exista elementos de campo com comunicação *Field Bus*, o terminal irá receber os sinais discretos e irá se comunicar com a área de controle através do protocolo DeviceLogix®.

A configuração do terminal descrita, a seguir na Tabela 10, apresenta seus principais componentes.

**Tabela 10 - Configuração Terminal de Válvulas**

| Posição | Código | Descrição |
|---|---|---|
| 1 | 05HBA4Z6ML00061 | Válvula pneumática 3/2 vias - Série 2005 |
| 2 | 05HBA4Z6ML00061 | Válvula pneumática 3/2 vias - Série 2005 |
| 3 | G3DL106R0DRM | Módulo comunicação – protocolo Device Logix® |
| 4 | 240-207 | Módulo 16 saídas digitais PNP (M12 x 8) |
| 5 | 240-211 | Módulo 8 entradas / 8 saídas digitais PNP (M12 x 8) |
| 6 | 240-214 | Módulo 4 entradas analógicas 4-20 mA M12 |
| 7 | 240-215 | Módulo 2 entradas / 2 saídas analógicas 4-20 mA M12 |
|  | | |

# 4. Avaliação e análise do Problema Proposto

O cenário para o desenvolvimento dos testes aplicados no protótipo será apresentado de forma que o tratamento de falhas seja feito através de FDEP e seus diagnósticos verificados em velocidades de até 500 Kbps pelo TIV.

Será comprovado a possibilidade da utilização de redes *Field Bus*, mesmo sem sua disponibilidade fisíca na malha de controle, através da programação do TIV no protocolo de comunicação digital Device Logix®.

## 4.1. Tratamento de Falhas

Para a análise das FDEP do protótipo, apresentam-se 4 Sub-Sistemas com suas DFTs classificadas para avaliação SIL e respectivos pontos de monitoramento para verificação de diagnóstico e tratamento de falhas ou risco de falhas.

### 4.1.1. Subsistema principal – Controle de Vazão

Este subsistema refere-se ao controle da vazão de água na linha principal. Sua operação com o respectivo grupo de dispositivos é o primeiro bloco a sofrer a análise de tratamento de falhas.

Fazem parte a válvula FCV-105, o Medidor de Vazão FSHL-107, os sinais de entrada IAC1 proveniente do controlador e seu respectivo sinal de saída para a válvula de controle de vazão OAC1, de vazão IAF1 e de posição ou resposta IAF2.

A lógica de operação é que a vazão na FCV-105 deve ser mantida em 40 l/min, através de um sinal OAC1 de 12mA do controlador (sendo simulado através de IAC1). Satisfeita essa condição, o Posicionador de FCV-105 irá gerar o sinal IAF2 também no valor de 12mA. A vazão na linha principal estará sendo monitorada através do sinal IAF1.

Considerando que a vazão de água será responsável pelo controle de temperatura, serão utilizados dois sinais analógicos IAT1 e IAT2 simulados através de geradores de 4 a 20mA, como se, representassem dois transmissores de temperatura instalados em posições distintas no tanque.

Na DFT que trata a figura 6, pode-se identificar as condições possíveis de falhas.

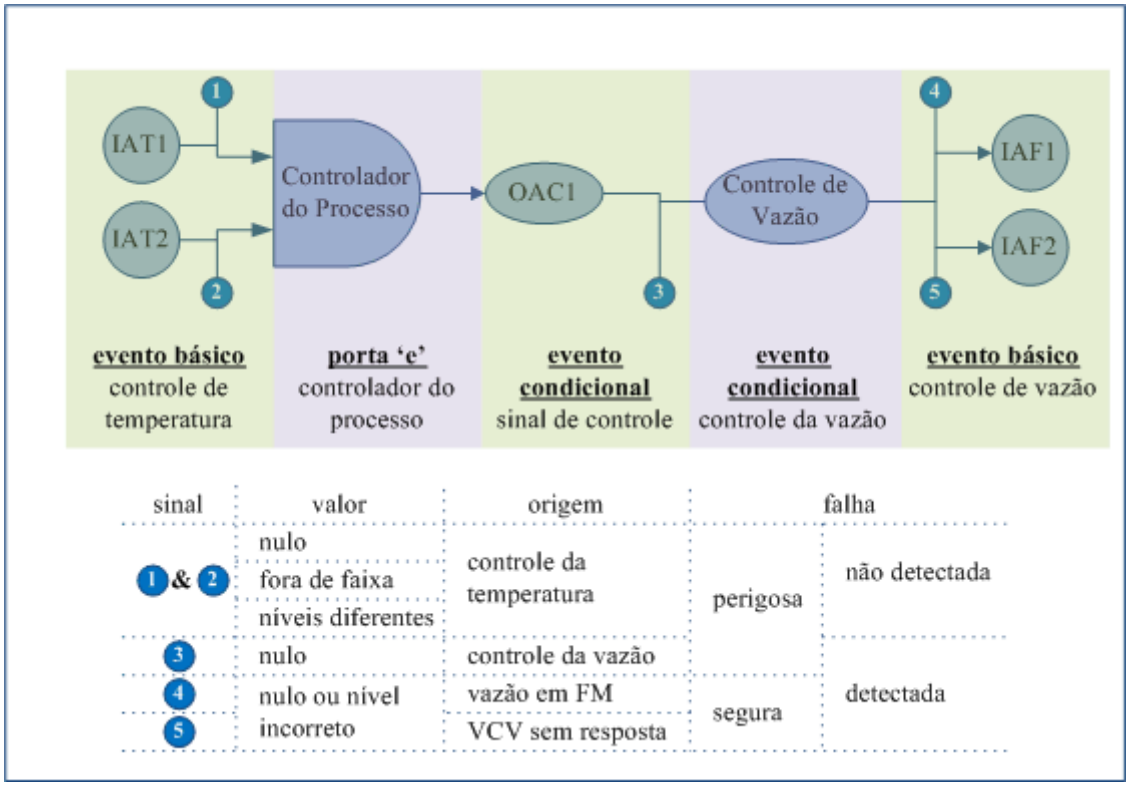



**Figura 6 - DFT Subsistema principal - Controle de Vazão**

Sendo monitorados

- Pontos 1 e 2 – Sinais IAT1 e IAT2 - perda, níveis diferentes ou fora da faixa aceitável do processo – falha não detectada no Processo (Controle da Temperatura);
- Ponto 3 – Sinal OAC1 - Perda ou nível incorreto - falha detectada no controlador;
- Ponto 4 – Sinal IAF1 - Perda ou nível incorreto – FSHL-107 não pode fazer a leitura da vazão;
- Ponto 5 – Sinal IAF2 - Perda ou nível incorreto – FCV-105 não responde ao sinal de controle.

### 4.1.2. Subsistema Pressão

A pressão de água na linha principal está diretamente ligada a vazão no circuito, e da mesma forma que os transmissores de temperatura vistos no item anterior, será simulado através de um gerador de sinal para que possa ser manipulado durante a operação.

Considera-se que para se existir fluxo no circuito, a pressão a montante de FCV-105 deve existir.

O sinal IAP1 será o responsável por esse monitoramento.

A figura 7 apresenta a DFT para o subsistema de Pressão.

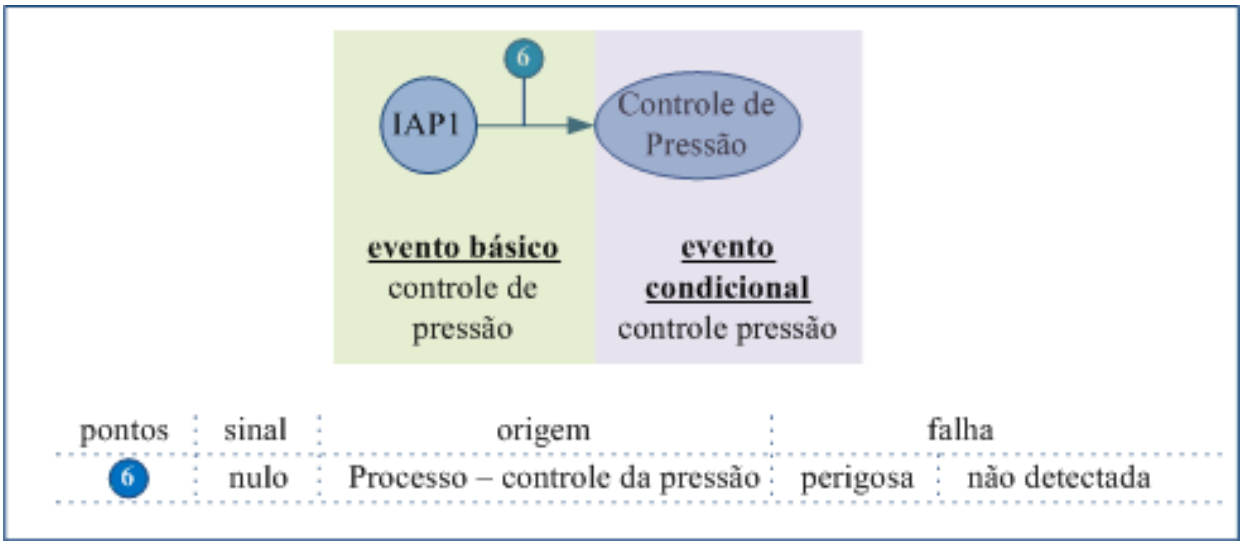



**Figura 7 - DFT Subsistema Controle de Pressão**

Sendo o ponto 6, monitorado de tal forma que:

- Perda do sinal IAP1 - falha detectada no transdutor de pressão a montante.

### 4.1.3. Subsistema – Função Instrumentada de Segurança (SIF)

O estado seguro de operação consiste em ter a Válvula Auxiliar (FV-205) atuada constantemente enquanto em espera através da Válvula Redundante (FC-204) com seus dois solenóides energizados pelos sinais digitais OD1 e OD2. Dois sensores de final de curso instalados no atuador de FV-205 serão responsáveis pelos sinais digitais de posição ID1 (aberto) e ID2 (fechado).

O corte dos sinais OD1 e OD2 irão desenergizar os solenóides de FC-204 resultando na despressurização do atuador de FV-205 e sua consequente abertura. A SIF do protótipo é estabelecida com o circuito alimentado com a vazão máxima disponível de água e todos seus componentes/dispositivos E/EE/EP desernegizado, resultando nulos os sinais de entrada ID1 e os sinais de saída OD1 e OD2.

A DFT do diagrama de blocos é apresentado na figura 8.

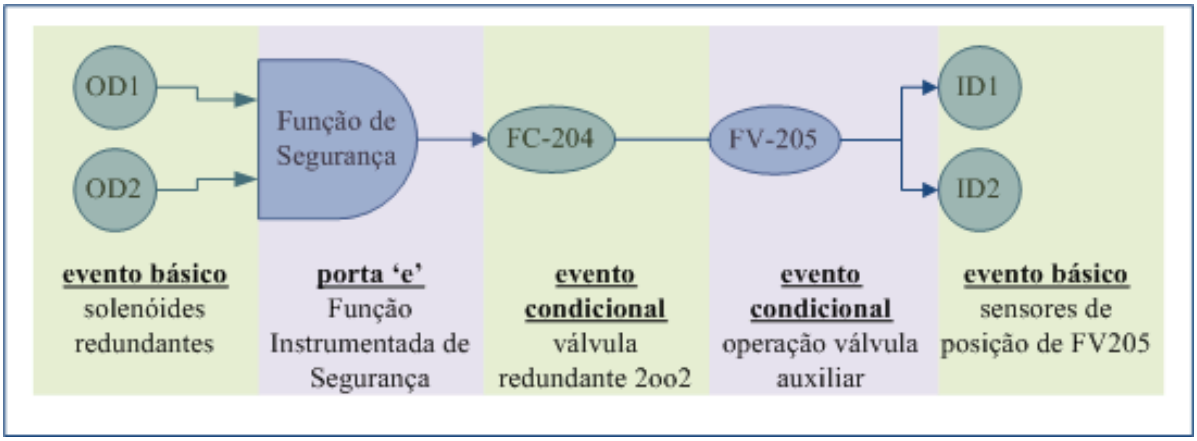



**Figura 8 – Diagrama de blocos para a Função Instrumentada de Segurança (SIF)**

### 4.1.4. Subsistema – Terminal Inteligente de Válvulas (TIV)

O TIV, elemento responsável pela lógica das Análises de Falhas e emissão dos sinais para os diagnósticos selecionados está composto por:

- Bloco Pneumático, responsável pela alimentação de ar comprimido aos elementos da malha segura do protótipo;
- Módulo de Comunicação Digital, protocolo Device Logix®, com a lógica de operação e diagnóstico embarcada;
- Módulos de entrada e saídas dos sinais utilizados na simulação.

Na figura 9, pode ser visto o terminal TIV com as indicações fisícas de entradas e saídas.

Na tabela 11, as descrições de cada um dos sinais monitorados.

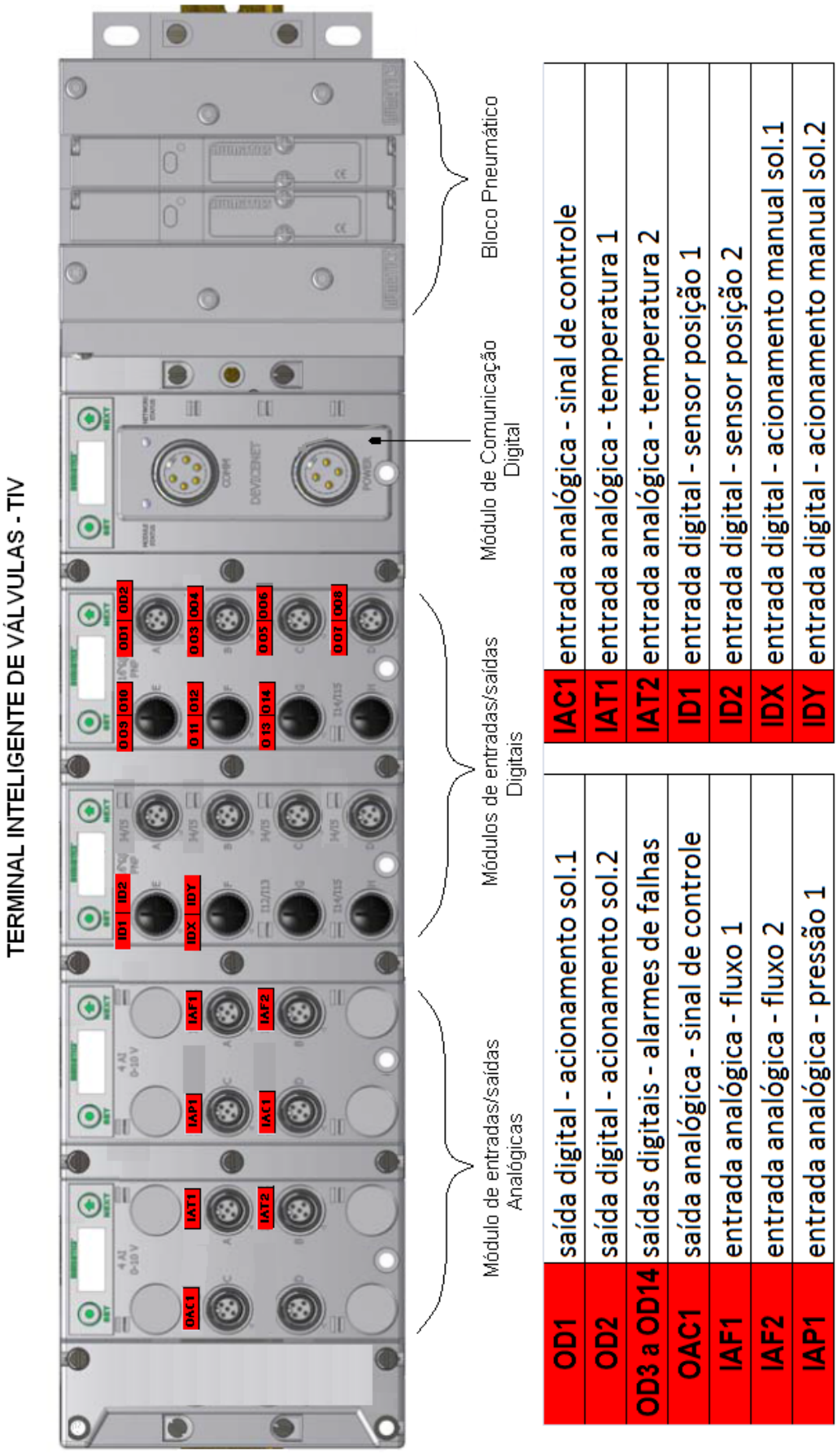



**Figura 9 - Representação fisica TIV com identificação de E/S**

**Tabela 11 - Descrição de Falhas - TIV**

| DFT | sinal | descrição | Origem | saída digital | estado | operação | Tipo de falha |
|---|---|---|---|---|---|---|---|
| Controle de Vazão | IAT1 | entrada analógica 4 ~ 20mA | Sensores de temperatura do tanque principal | **OD3** | ligada | falha do sensor de temperatura TSHL-301 | Segura detectada |
| | | | | | desligada | operação normal do sensor de temperatura TSHL-301 | |
| | IAT2 | entrada analógica 4 ~ 20mA | | **OD4** | ligada | falha do sensor de temperatura TSHL-302 | Segura detectada |
| | | | | | desligada | operação normal do sensor de temperatura TSHL-302 | |
| | OAC1 | saída analógica 4 ~ 20mA | Controlador do processo | **OD5** | ligada | ausência de sinal de controle - falha controlador | Perigosa detectada |
| | | | | | desligada | operação normal de controle | |
| | IAF1 | entrada analógica 4 ~ 20mA | Medidor de vazão | **OD6** | ligada | falha do sensor de vazão FSHL-107 ou circuito sem fluxo | Perigosa detectada |
| | | | | | desligada | operação normal do medidor de vazão | |
| | IAF2 | entrada analógica 4 ~ 20mA | retorno do posicionador na Válvula de Controle de Vazão | **OD7** | ligada | falha do sensor de vazão no posicionador FC-104 | Perigosa detectada |
| | | | | | desligada | operação normal do sensor de vazão de FC-104 | |
| Controle de Pressão | IAP1 | entrada analógica 4 ~ 20mA | Transdutor de pressão a montante | **OD8** | ligada | falha do sensor de pressão PSHL-102 ou circuito sem fluxo | Perigosa detectada |
| | | | | | desligada | operação normal - linha pressurizada | |
| Função Instrumentada de Segurança | OD1 | saída digital 24Vcc | solenóide 1 de SV-201 | **OD10** | ligada | solenóide 1 energizado operação normal | Segura não detectada |
| | | | | | desligada | falha solenóide 1 - substituir solenóide | |
| | OD2 | saída digital 24Vcc | solenóide 2 de SV-201 | **OD11** | ligada | solenóide 2 energizado operação normal | Segura não detectada |
| | | | | | desligada | falha solenóide 2 - substituir solenóide | |
| | ID1 | entrada digital 24Vcc | sensor de posição aberto de FV-205 | **OD12** | ligada | função "*by-pass*" acionada | Segura detectada |
| | | | | | desligada | válvula auxiliar fechada - operação normal | |
| | ID2 | entrada digital 24Vcc | sensor de posição fechado de FV-205 | **OD13** | ligada | válvula auxiliar fechada - operação normal | Segura detectada |
| | | | | | desligada | função "*by-pass*" acionada | |
| | | Lógica de operação | | **OD14** | ligada | operação normal | Perigosa não detectada |
| | | | | | desligada | Função de Segurança atuada - planta em risco | |

Além da lógica descrita para análise de falhas mencionadas, uma das principais características do TIV utilizado é o monitoramento e diagnóstico do módulo de comunicação e dos estados de entradas e saídas utilizadas conforme tabelas 12 e 13.

**Tabela 12 - Indicação de falhas módulo de comunicação**

| LED indicador | Cor | Estado | Descrição |
|---|---|---|---|
| **Estado da Rede** | Desligado | Desligado | Operação isolada – cabo não conectado ao nó. Operação normal.<br><br>Conectado à rede – Dispositivo não está ativo; Terminal não está sendo alimentado; Problemas físicos com a rede; Taxa de transferência incompatível. |
| | Verde | Ligado | Operação normal, dispositivo está ativo e a conexão estabelecida. |
| | | Piscando | Dispositivo está ativo – mas não estabelece conexão. |
| | Vermelho | Ligado | Dispositivo detectou um erro que causa a impossibilidade de se comunicar com a rede; Identificação da Mascára de rede duplicada; Problemas fisícos com a rede. |
| | | Piscando | Falha de comunicação – um ou mais módulos E/S não respondem. |
| **Estado do Módulo** | Desligado | Desligado | Falha critíca de equipamento. Microprocessador não está operando. |
| | Verde | Ligado | Operação normal. Dispositivo está operando corretamente. |
| | | Piscando | Falta de alimentação da linha. |
| | Verde / Vermelho | Piscando | Módulo em modo de auto teste. Ciclar alimentação para finalizar auto teste. |

**Fonte: Manual técnico AscoNumatics Série G3 –** Device Logix®

**Tabela 13 - Indicação de falhas módulos de Saída**

| Tipo de Saída | Estado | Condição de Falha | Bit |
|---|---|---|---|
| **Bobina da válvula solenóide montada no módulo pneumático** | Ligada | Sem falha | 0 |
| | | Falha – curto circuito, temperatura ou corrente acima do limite. | 1 |
| | Desligada | Sem falha | 0 |
| | | Falha – carga em aberto | 1 |
| **Saídas discretas** | Ligadas | Sem falha | 0 |
| | | Falha – curto circuito, temperatura ou corrente acima do limite. | 1 |

**Fonte: Manual técnico AscoNumatics Série G3 –** Device Logix®

## 4.2. Comunicação Digital

A lógica apresentada para as combinações de entradas e saídas com seus respectivos diagnósticos podem ser encontradas atualmente no desenvolvimento de programas específicos em Sistemas Digitais de Controles Distribuidos (SDCDs) através de Controladores Lógicos Programáveis, Supervisórios e computadores industriais, no entanto, os valores para as licenças de uso, hora-homem de programação, além de equipamentos para aplicações em grande escala podem resultar em custos na ordem de centenas de milhares de Reais que acabam inviabilizando ou tornando extremamente complexas aplicações localizadas e de pequeno porte.

O objetivo aqui proposto é poder fazer o uso dos benefícios e confiabilidade das redes digitais de forma dedicada resultando em um projeto acessível.

### 4.2.1. Device Net

*Device Net* é um protocolo aberto de comunicação serial utilizado em aplicações industriais para a interligação de dispositivos e equipamentos, baseado no protocolo CAN (*Controller Area Network*) originalmente foi desenvolvido pela Allen Bradley e atualmente vários fabricantes utilizam essa tecnologia.

A ODVA (*Open DeviceNet Vendor Association*) é uma organização independente que regulamenta as principais especificações do protocolo DeviceNet, além de supervisionar os testes de conformidade dos produtos que serão utilizados nestes sistemas.

Uma rede DeviceNet pode ter até 64 pontos de utilização com a capacidade de trafego de até 8 bytes de dados por ponto em até 3 taxas de transferência (*baud rates*) configuráveis de 125Kbps, 250Kbps ou 500Kbps. Durante os ensaios aplicados ao protótipo, essas taxas definem os tempos de resposta para o anúncio e diagnóstico de falhas implementadas.

### 4.2.2. Módulo de Comunicação Device Logix®

Device Logix® é uma tecnologia da Rockwell Automation que permite que um ponto Device Net seja programado localmente para excecutar uma sequência ou rotina de operação independente do controlador ou do sistema supervisório principal de uma planta. O RS Linx Classic Lite, utilizado para escrever a lógica é disponibilizado gratuitamente em: http://compatibility.rockwellautomation.com/Pages/MultiProductDownload.aspx?Keyword=Free&crumb=112 e necessita somente do cabo de comunicação para a programação no

módulo de comunicação do TIV. Concluída essa etapa, o TIV podrá operar sem a necessidade de estar conectado à uma rede, excecutando as rotinas pré-estabelecidas.

A lógica de programação utilizada neste estudo consiste em comparar sinais analógicos gerados pelos elementos de campo com padrões pré-estabelecidos (referências). Valores fora das faixas aceitáveis estariam relacionados a possiveís falhas ou perigo de falhas no circuito. Esse diagnóstico de risco irá gerar sinais digitais de forma que, a Função Instrumentada de Segurança, seja implementada. O diagrama em bloco dessa programação pode ser encontrado no Anexo 1 deste trabalho.

Importante destacar que a rede de comunicação, ambientes de supervisão (supervisórios) e o controlador da planta, não estão dentro dos objetivos de avaliação, neste trabalho.

A análise de diagnóstico e falhas está sendo aplicada aos elementos de campo que constituem um SIS e estão amparados pelas diretrizes de projeto recomendados pela IEC 61508.

# 5. Validação do Trabalho

Vários métodos disponíveis podem ser utilizados para a determinação dos níveis de integridade segura (anexo 2) de uma aplicação pois, devido aos inúmeros trabalhos de pesquisa e desenvolvimento que são publicados, existe a necessidade de que mais de uma forma de avaliação seja utilizada.

A norma IEC 61508 parte 5 – anexo B, lista seis deles e cita os fatores que devem ser levados em consideração durante essa tarefa:

- Critérios aceitáveis para riscos que precisam ser atendidos. Técnicas não deverão ser aplicáveis, caso se evidencie que o nível recomendado de risco tenha sido reduzido para valores convenientes e que possam ser praticáveis;
- Modo de operação da Função de Segurança. Alguns métodos somente são aplicados para modos de baixa demanda de operação. Definidos através da IEC 61508 parte 4, modos de baixa demanda são aqueles onde a frequência da demanda de operação em um sistema seguro não é superior a uma vez ao ano ou duas vezes no intervalo de testes de verificação, enquanto alta demanda ou demanda contínua é superior a uma vez ao ano ou duas vezes no intervalo de testes;
- Conhecimento e experiência dos profissionais envolvidos na determinação SIL e quais são as técnicas utilizadas pelo segmento de mercado a que pertence;
- Nível de confiabilidade. Necessário e resultante dos riscos residuais definidos por critérios de organismos ou entidades setorizadas dos usuários;
- Utilização de mais de um método de avaliação. Um método pode ser utilizado para propósitos de monitoramento seguido por outro com proposta mais rigorosa, caso se identifique a necessidade de atender níveis mais elevados de SIL;
- Avaliaçãos dos possíveis acidentes. Métodos mais rigorosos podem ser aplicados para acidentes que possam causar danos de maior impacto a operação, meio ambiente ou seres humanos;
- Origem das causas de falhas. Comuns ou provenientes de demanda que ocorrem nos sistemas de segurança E/EE/EEP.

## 5.1. Determinação SIL

Métodos Quantitativos e Qualitativos para a determinação SIL são empregados de acordo com as aplicações simples ou complexas. Ilustra-se aqui os princípios gerais para sua utilização, mas não fornecem uma fórmula de cálculo específica. O uso, aqui empregado, de estrutura dinâmica de falhas apresenta uma aplicação simples de controle de processo.

As tabelas 14 e 15, extraidas da IEC 61508 parte 7, apresentam respectivamente a classificação e interpretação das classes de risco:

**Tabela 14 - Exemplo de Classificação de Risco de Acidentes**

| Frequência | Consequência | | | |
|---|---|---|---|---|
| | Catástrofe | Critíca | Marginal | Desprezível |
| **Frequente** | I | I | I | II |
| **Provável** | I | I | II | III |
| **Ocasional** | I | II | III | III |
| **Remota** | II | III | III | IV |
| **Improvável** | III | III | IV | IV |
| **Inconcebível** | IV | IV | IV | IV |
| Nota 1: A classificação acima com as classes de risco I, II, III e IV dependem do setor e também de acordo com a frequência das ocorrências registradas. Portanto, esta tabela deve ser vista como um exemplo de como se deve construir uma tabela de acordo com a aplicação desejada;<br>Nota 2: A determinação SIL de acordo com as frequências nesta tabela é apresentada no item 5.2. Exemplo de Cálculo. | | | | |

**Fonte: IEC 61508** – parte 7

**Tabela 15 - Interpretação para as Classes de Risco**

| Classe de Risco | Interpretação |
|---|---|
| **Classe I** | Risco intolerável |
| **Classe II** | Risco indesejável e tolerável caso a redução do risco for impráticavel ou os custos para a redução extremamente disproporcionais em relação a melhoria obtida |
| **Classe III** | Risco tolerável caso o custo para a redução exceder a melhoria obtida |
| **Classe IV** | Risco insignificante |

**Fonte: IEC 61508** – parte 7

A aplicação do método Quantitativo necessita particular atenção nas situações em que:

- o risco tolerável for expresso de forma numérica. Por exemplo: a consequência de uma falha específica não pode ocorrer com uma frequência maior que um em $10^3$ anos;
- níveis SIL definidos de acordo com a Tabela 1 - Nível de Integridade de Segurança (SIL), apresentada no capítulo 2, pagina 21 ou tabelas 2 e 3 da IEC 61508 - parte 1, anexo 1 deste trabalho.

Os principais pontos a seguir também devem ser observados para cada SF a ser implementada:

- determinação do risco tolerável conforme tabela 14;
- determinação do risco do Equipamento sob Controle (EUC);
- determinação da redução de risco para atender os níveis toleráveis;
- alocação da redução dos riscos necessários no sistema E/EE/EP, outras tecnologias de sistemas seguros e outras medidas de redução de riscos.

Extraida da norma IEC 61508 parte 5 anexo D, a figura 10, aloca a estrutura do cálculo para a situação em que:

$$PFD_{avg} = \frac{F_t}{F_{np}}$$

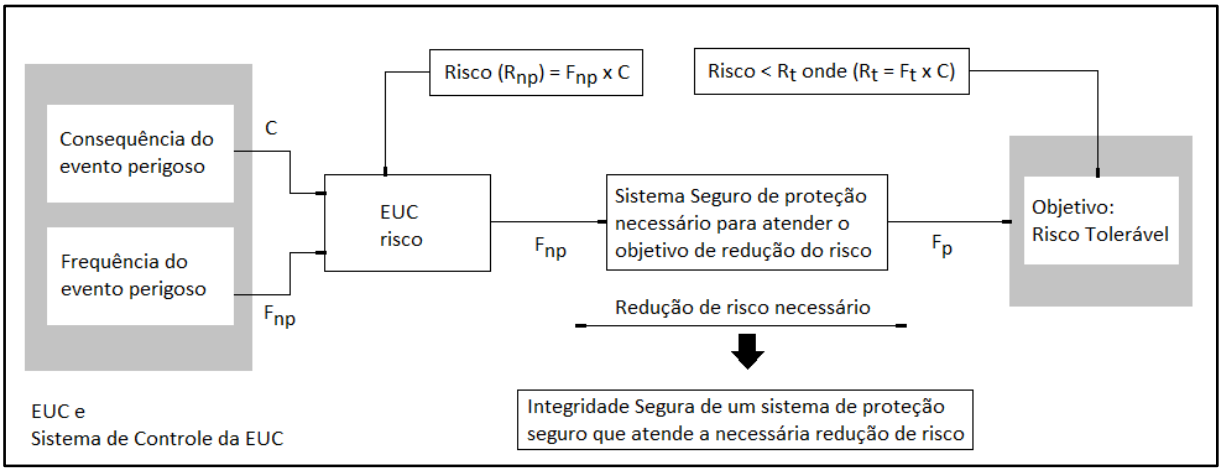



**Figura 10 - Integridade Segura - exemplo para um sistema seguro de proteção**
**fonte: IEC 61508 parte 5, anexo D**

Onde:

$PFD_{avg}$ – é a probabilidade média de falha sob demanda para um sistema seguro de proteção, cujo objetivo de risco de falha é a medida desse sistema operando em modo de baixa demanda;

$F_t$ – é a frequência tolerável de perigo de falha;

$F_{np}$ – é a taxa de demanda de um sistema seguro de proteção;

C – é a taxa de consequência da falha perigosa;

$F_p$ – é a frequência do risco com as medidas de proteção implementadas.

## 5.2. Verificação de diagnósticos

Os diagnósticos de falhas foram validados através da simulação da programação do TIV apresentada no anexo 1 deste trabalho. A lógica em blocos, descreveu o comportamento dos sinais analógicos e digitais no circuito monitorado e representou o comportamento de cada uma das DFTs dos subsistemas discutidos no capítulo 4.

Após a validação de cada um dos blocos a seguir, foram avaliados os tempos de resposta entre os sinais simulados de falhas e a indicação nas saídas monitoradas.

### 5.2.1. Controle de Vazão

Dividiu-se em duas verificações: sinais de Temperatur e sinais de Vazão. A temperatura do tanque principal monitorada por dois sensores de temperatura; a vazão do circuito, pelo posicionador da válvula de controle FCV-105 e o medidor de vazão FSHL-107. Destaca-se que o sinais de temperatura e de vazão foram simulados através de geradores de 4 a 20mA.

#### 5.2.1.1. Sinais de controle da Temperatura

A simulação dos sinais IAT1 e IAT2 referem-se ao controle de temperatura do tanque, que está diretamente ligado à vazão de agua para a refrigeração. No protótipo, a diferença entre seus valores é desprezível, no entanto, é possível que em ambientes industriais essa diferença, devido a dimensões e volumes maiores, precise ser considerada e corrigida pelos controladores.

A figura 11, apresenta o bloco lógico que identifica ou não a presença do sinal de resposta dos sensores de temperatua. A ausência de sinal nas entradas IAT1 ou IAT2 acusa através da mudança de estado das saídas OD3 ou OD4 de 0 para 1.

O uso do bloco lógico com a função “NOT”, foi o mais indicado para a identificação de ausência de todos os sinais dos sensores utilizados. Foi utilizado, com os sensores de Temperatura, Vazão e Pressão.

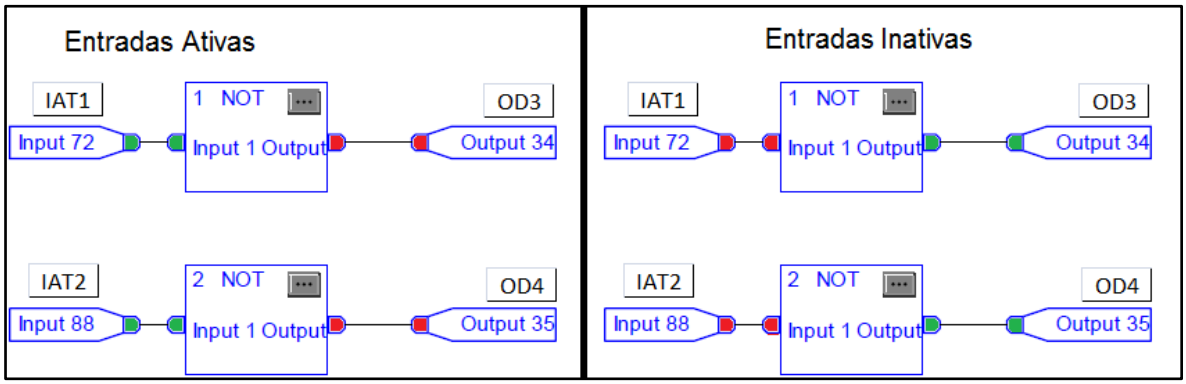



**Figura 11 – simulação de saídas - váriavel temperatura**

### 5.2.1.2. Sinais de Controle da Vazão

Os sinais IAF1 e IAF2 referem-se ao controle de vazão de agua no circuito. Mantido o sinal de controle para a válvula FCV-105, o sinal de retorno IAF2 proveniente do posicionador deve indicar o mesmo nível aplicado, confirmando a vazão de saída correta, enquanto um sinal redundante IAF1 é gerado pelo medidor de vazão FSHL-107. Da mesma forma que no monitoramento anterior dos sensores de temperatura, os sinais da vazão também foram avaliados pela lógica que na ausência de seus níveis de entrada, as saídas OD6 e OD7 indicaram a falha dos instrumentos.

A figura 12, apresenta a simulação desse bloco.

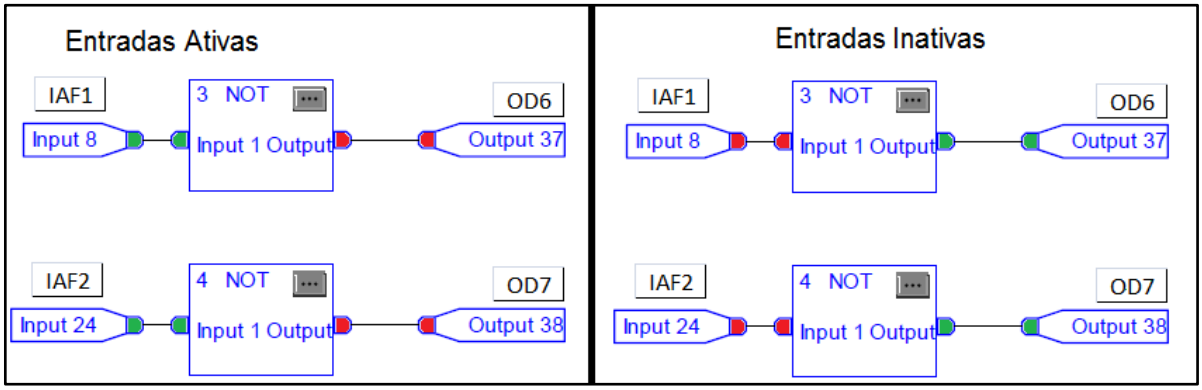



**Figura 12 – simulação de saídas - váriavel vazão**

### 5.2.2. Controle de Pressão

O sinal IAP1 refere-se ao monitoramento da pressão de agua no circuito. O leitor deve observar que o monitoramento dessa grandeza, aqui apresentado, apesar de prático necessita

algumas considerações em aplicações reais. Os testes aplicados, são feitos sem considerar a vazão do circuito e simula o valor da pressão na entrada da válvula de controle FCV-105.

Pressão e Vazão em um circuito qualquer estarão sempre relacionados, cabe ao projetista definir qual das duas grandezas deverá ser monitorada e nas situações onde as duas forem objeto de análise, a lógica de programação deverá considerar sua interação.

A figura 13, apresenta a linha de monitoramento com a mesma lógica anterior e da mesma forma foi validada na simulação. Quando percebido a falta de sinal de entrada IAP1 a saída OD8 idenficou a falha.

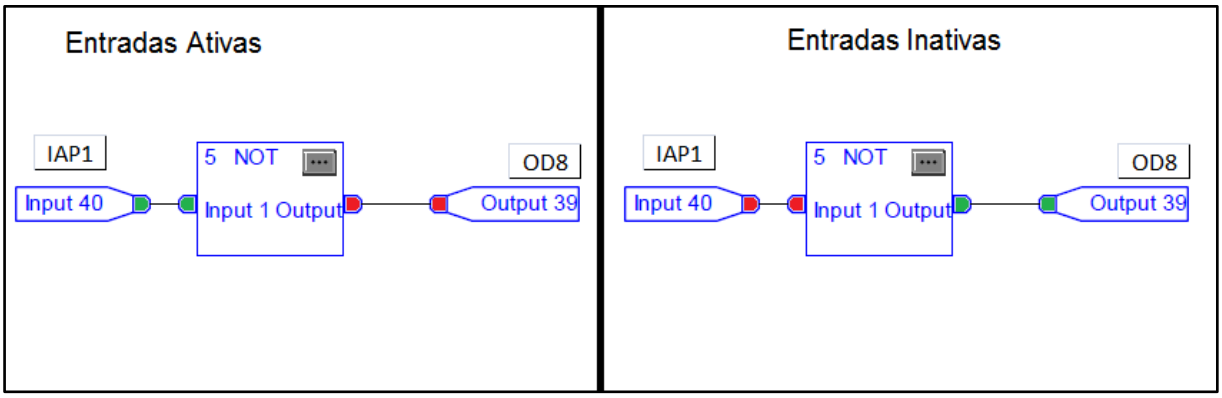



**Figura 13 – simulação de saídas – váriavel pressão**

### 5.2.3. Função Instrumentada de Segurança (SIF)

A simulação da SIF do protótipo foi verificada através das saída digital OD14. As saídas digitais OD1 e OD2 responsáveis pela energização dos solenóides da válvula direcional redundante FC-204. Quando desenergizadas, a vazão máxima do circuito é obtida através da válvula auxiliar FV-205. A figura 14, a seguir, apresenta as simulações feitas com os sinais de entradas digitais IDX e IDY.

Utilizando um bloco lógco “NOR”, pôde-se diagnosticar a ausência dos sinais de entrada dos solenóides e portanto ativar a saída OD14. Ao mesmo tempo, pôde-se identificar a falha dos solenóides através das saídas digitais OD10 e OD11.

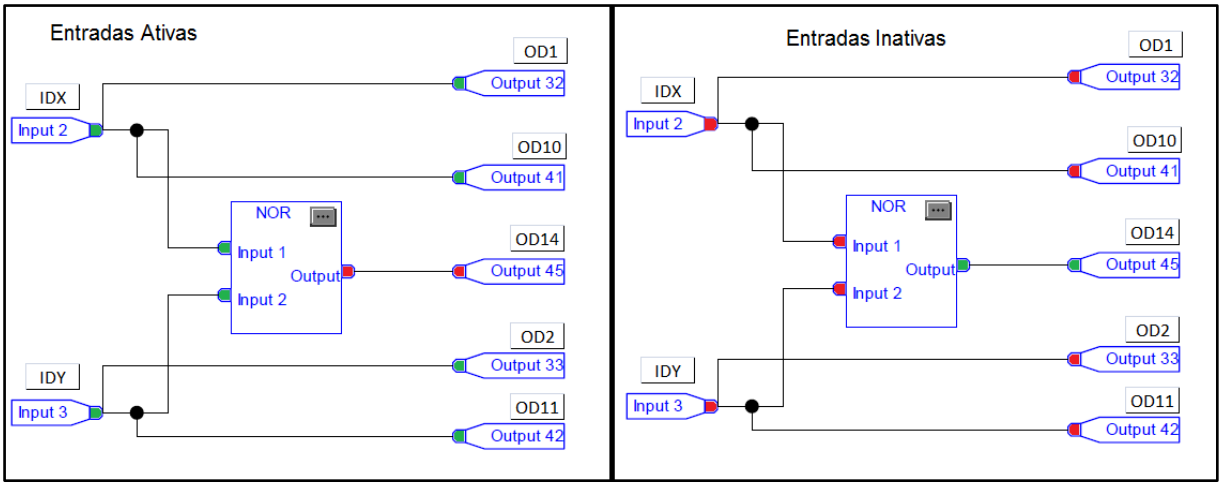



**Figura 14 – simulação de entradas - Função de Segurança**

### 5.2.4. Sinal de Controle

Apesar da malha de controle não ser objeto dos testes realizados, foi simulado a ausência do sinal de controle na entrada IAC1. Conforme simulação apresentada na figura 15 abaixo, a falta de sinal em IAC1 resulta a falta de sinal na saída de controle OAC1 e por consequência um diagnóstico de falha na saída digital OD5.

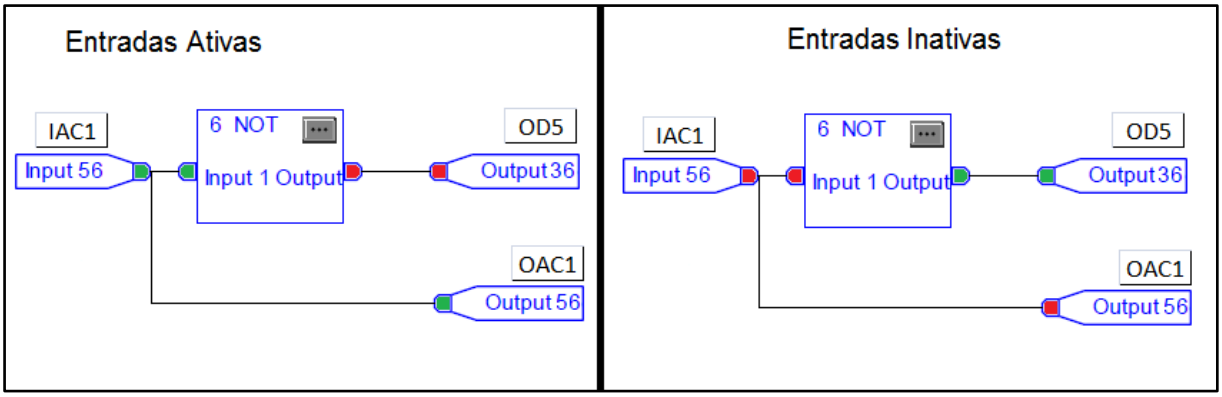



**Figura 15 – simulação de entrada – lógica de controle**

## 5.3. Tempos de resposta

Os ensaios realizados avaliaram os tempos de resposta entre as falhas provocadas no sistema e os diagnósticos apresentados no TIV. Com o auxilio de um ociloscópio e um programa de aquisição de dados, foi possível mensurar os tempos entre um sinal de corrente proveniente

de cada uma das entradas analógicas simuladas e seus respectivos sinais de saída digital de diagnóstico.

Com a lógica de programação gravada no TIV e em operação local, ou seja, sem estar conectado à rede de comunicação, estabelece-se uma sequência de simulações levando as entradas de um estado ativo (20mA) para um estado inativo (0mA), verifica-se o estado da saída digital nas duas situações distintas e o tempo de resposta entre as mudanças.

A figura 16, apresenta a média de 20 medições realizadas durante os ensaios realizados na fase dos testes de validação. Foram tomados entre o instante de corte do sinal de entrada A e a mudança de estado do sinal de saída B do nível 0Vcc para 24Vcc. O eixo de tempo foi ajustado para melhor avaliação de leitura gráfica. A transição apurada entre sinais se completa no tempo máximo de 100ms.

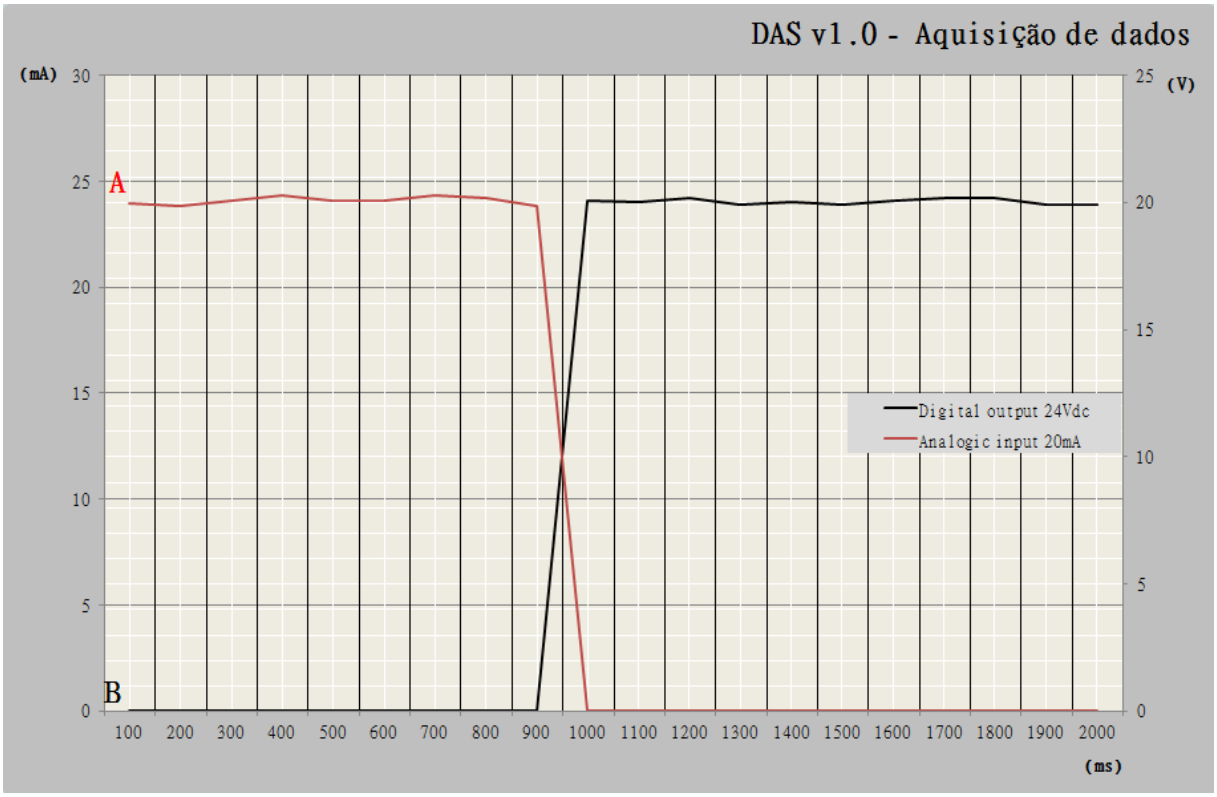



**Figura 16 - Análise gráfica dos sinais de entradas e saídas**

# 6. Conclusão

Demonstra-se através do protótipo de estudo, a possibilidade de monitoramento de falhas com o uso de técnicas de comunicação digital. Os intervalos de tempo máximo de 100ms, apurados entre os sinais simulados e seus respectivos diagnósticos nos módulos de entradas e saídas do TIV, comprovam a viabilidade desta proposta em uso industrial. Essa característica confere aos usuários a confiabilidade de que ações corretivas possam ser implementadas de acordo com a demanda que cada processo exige.

Apesar da apresentação dos métodos de cálculo e avaliação do nível SIL deve-se, antes da aplicação de todas, ou mesmo parte das técnicas aqui apresentadas, seja feita uma análise detalhada da Revisão Bibliográfica de que trata o capítulo 2, bem como, as recomendações das normas vigentes, IEC61508, 61511, 61784 e ANSI/ASI 84.01. Também deve-se considerar o ambiente digital que estará sendo utilizado e sua respectiva topologia.

As expectativas com relação aos dados obtidos foram atendidos quando da validação dos testes efetuados.

Pôde-se observar que durante a simulação dos sinais de temperatura, vazão e pressão, em todas as situações onde o valor de referência não foi atendido ou o sinal aplicado possuia valor 0 (zero) a saída de diagnóstico de falha apresentou valor “ligado” diagnosticando falha ou risco de falha.

A SF, também simulada, foi detectada através da saída 19 no TIV.

O módulo de comunicação foi avaliado e evidenciado através dos indicadores luminosos, o estado de operação tanto da rede como do próprio módulo.

Considerando-se que:

- os métodos de cálculo para classificação SIL, podem ser aplicados, quando o circuito sugerido for utilizado;
- os elementos de campo utilizados possuem certificação SIL;
- foi utilizado um TIV com o protocolo de comunicação DeviceLogix;
- todos os testes apresentados, com resultados satisfatórios, foram aplicados sem a necessidade do TIV estar conectado a rede de comunicação digital.

Apresenta-se como resultado final que:

- O diagnóstico e o tratamento de falhas puderam ser obtidos através do uso de terminais inteligentes de válvulas em ambiente de comunicação digital, com velocidades no tempo de resposta em até 100ms e sem a necessidade de conectividade constante à rede;
- Esses resultados conferem aos projetistas e usuários de SIS uma proposta prática, simples e com custos reduzidos de instalação, seja pelo reduzido numero de componentes, seja pela facilidade de programação, comissionamento e monitoramento dos Sistemas Seguros;
- Ressalta-se que a aplicabilidade desta proposta deve sempre considerar a utilização de equipamentos e componentes com certificação SIL.

## 6.1. Proposta para trabalhos futuros

A utilização da comunicação digital é uma realidade na indústria de processos e tem se mostrado cada vez mais presente nos sistemas de supervisão e controle. Complementando a análise, diagnóstico e tratamento de falhas aqui apresentados poderiam ser consideradas como propostas de trabalhos futuros:

- a utilização desse modelo em uma aplicação de controle de processo utilizando uma malha de controle real, onde além dos sinais digitais, seriam monitoradas as faixas de operação dos sinais analógicos;

- ou ainda, a construção e avaliação deste mesma proposta para diagnóstico e tratamento de falhas utilizando-se de elementos de campo e comunicação em redes sem meio fisíco (*wireless*).

# 7. Referências

AMERICAN NATIONAL STANDARD INSTITUTE/INTERNATIONAL SOCIETY OF AUTOMATION. **ANSI84.00.01: Functional Safety: Safety Instrumented Systems for the Process Industry Sector**: United State of America, 2004. ISBN: 1-55617-919-7

BABU, B.V.; SHAILESH, M.. **Adaptive Networks for Fault Diagnosis and Process Control**. India: Department of Chemical Enginnering – Birla Institute of Technology and Science Pilani, 2002.

DZUNG, Dacfey. et al. **Security for Industrial Communication Systems.** Proceedings of the IEEE. England, Vol. 93, Nº 6, 2005.

FELÍCIO, Luiz Carlos. **Modelagem da dinâmica de sistemas e estudo da resposta.** Segunda Edição. São Paulo: RiMa, 2010.

FRANEKOVÁ, Mária; RÁSTOCNY, Karol. **Safety Model of Safety-Related Fieldbus Transmission Systems.** Slovakia: Department of Control and Information Systems, Faculty of Electrical Engineering - Unversity of Zilina, Univerzitná, 2010.

GABOR, Gianina; ZMARANDA, Doina. **Techniques used to design safe and reliable critical control or shutdown systems.** Romania: Department of Computer Science, University of Oradea, Faculty of Electrical Engineering and Information Technology, 2009.

GOBLE, William M.; BUKOWSKI, Julia V. - **Extending IEC61508 Reliability Evaluation Techniques to Include Common Circuit Designs Used in Industrial Safety Systems.** Proceedings Annual Reliability and Maintainability Symposium. England, 2001.

INTERNATIONAL ELECTROTECNICAL COMMISSION. **IEC61158: Digital data communications for measurement and control – Fieldbus for use in industrial control systems**: Switzerland, 2002.

INTERNATIONAL ELECTROTECNICAL COMMISSION. **IEC61508: Functional safety of electrical/electronic/programmable electronic safety-related systems**: Switzerland, 2003.

INTERNATIONAL ELECTROTECNICAL COMMISSION. **IEC61511: Functional safety: Safety instrumented systems for the process industry sector**: Switzerland, 2003.

INTERNATIONAL ELECTROTECNICAL COMMISSION. **IEC61784: Digital data communications for measurement and control**: Switzerland, 2003.

INSTRUMENTATION SYSTEM AND AUTOMATION SOCIETY (ISA). **TR84.00.02: Safety Instrumented Functions (SIF) - Safety Integrity Level (SIL) Evaluation Techniques Part 2: Determining the SIL of a SIF via Simplified Equations - Techinical Report**: United States, 2002. ISBN: 1-5617-803-4.

JUNIOR, Reinaldo Siquilante. **Diagnóstico e Tratamento de Falhas Críticas em Sistemas Instrumentados de Segurança.** São Paulo: Escola Politécnica da Universidade de São Paulo, 2011.

MESHKAT, Leila; DUGAN, J.Bechta; ANDREWS, John D.. **Dependability Analysis of Systems with On-Demand and Active Failure Modes Using Dynamic Fault Trees.** IEEE Transactions on Reliability. United States, Vol. 51, No.2, 2002.

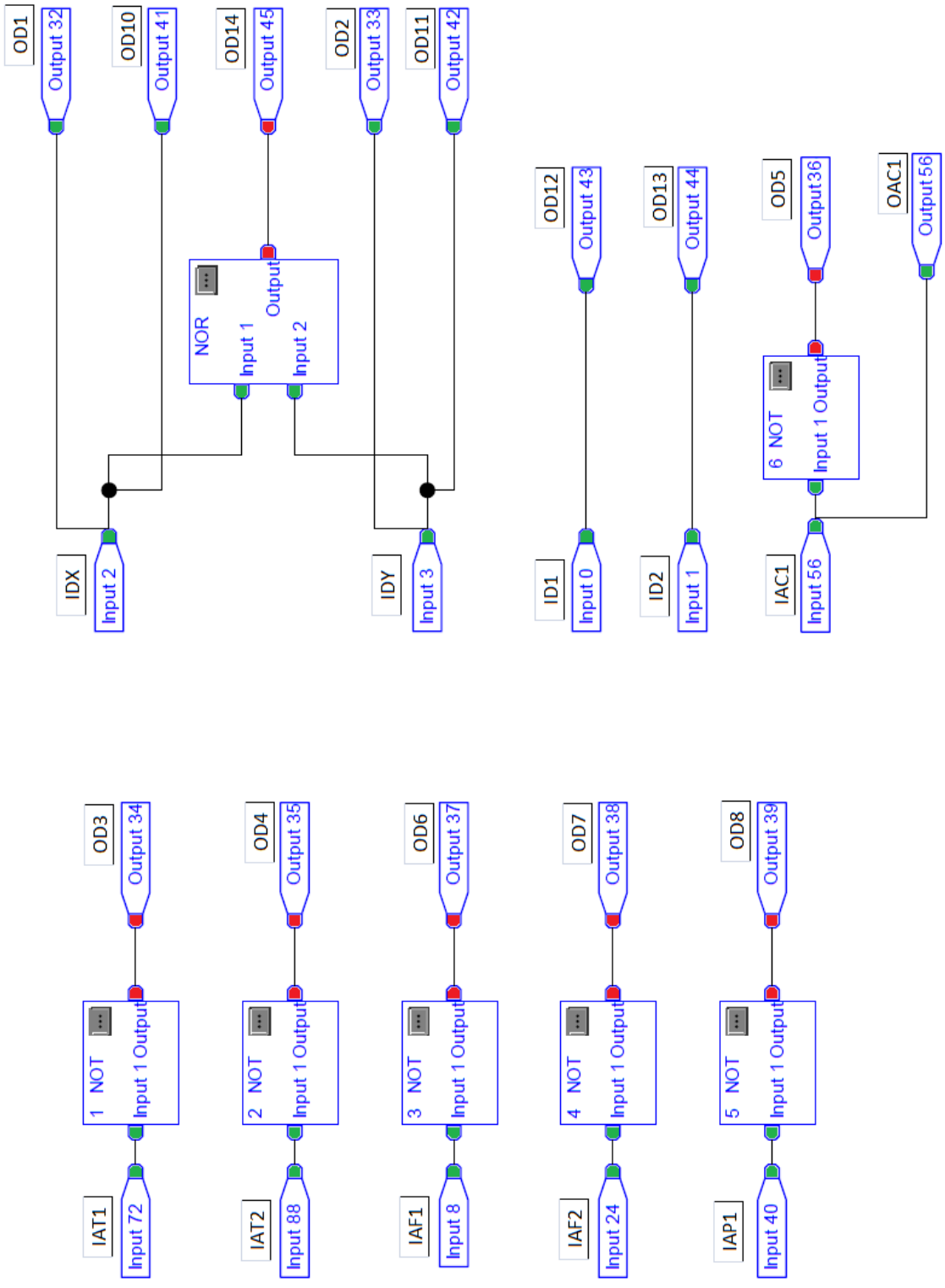
SCHWARTZ, William A.; HOCHLEITNER, Monica L.. **3 Fatores Importantes na Avaliação de um dispositivo Certificado SIL (A B C é tão importante quanto 1 2 3)**. Disponível em <http://www.exida.com/Resources/Whitepapers#679>, acesso em 10/Março/2013.

THOMESSE, Jean Pierre. **Fieldbus Technology in Industrial Automation. Emerging Technologies and Factory Automation.** 10th IEEE Conference 19 a 22/Setembro. United States, Vol.1, 2005.

TREYTTL, Albert; SAUTER, Thilo; SCHWAIGER, Thilo. **Security Measures for Industrial Fieldbus Systems – State of the Art and Solutions for IP-based Approaches.** Proceedings of International Workshop on Factory Communication Systems - Vienna University of Thechnology. Austria, 2004.

ZHANG, J.; MORRIS A.J. - **On line process fault diagnosis using fuzzy neural networks.** Proceedings of Intelligent Systems Engineering – IEEE. England, Spring of 1994.

# Anexo 1 – Diagrama de blocos/programação - TIV



# Anexo 2 – tabelas 2 e 3 – Nível Integridade de Segurança (SIL)

**Tabela 2 - Nível de Integridade de Segurança (SIL): valores objetivos de falhas para uma função segura, definido para um sistema seguro E/EE/EP operanndo em modo de baixa demanda**

| Nível de Integridade de Segurança - SIL | Probabilidade média de Falha sob Demanda $PFD_{avg}$ |
|---|---|
| **4** | $10^{-4} > PFD_{avg} \geq 10^{-5}$ |
| **3** | $10^{-3} > PFD_{avg} \geq 10^{-4}$ |
| **2** | $10^{-2} > PFD_{avg} \geq 10^{-3}$ |
| **1** | $10^{-1} > PFD_{avg} \geq 10^{-2}$ |
| Ver notas de 1 a 7 para interpretação desta tabela | |

**Tabela 3 - Nível de Integridade de Segurança (SIL): valores objetivos de falhas para uma função segura, definido para um sistema seguro E/EE/EP operanndo em modo de alta ou contínua demanda**

| Nível de Integridade de Segurança - SIL | Probabilidade média de Falha sob Demanda $PFD_{avg}$ |
|---|---|
| **4** | $10^{-8} > PFD_{avg} \geq 10^{-9}$ |
| **3** | $10^{-7} > PFD_{avg} \geq 10^{-8}$ |
| **2** | $10^{-6} > PFD_{avg} \geq 10^{-7}$ |
| **1** | $10^{-5} > PFD_{avg} \geq 10^{-6}$ |
| Ver notas de 1 a 7 para interpretação desta tabela | |

Nota 1 – Ver 3.5.12 da IEC 61508-4 para definição dos termos de baixa demanda e alta ou contínua;

Nota 2 – O parâmetro na tabela 3 para o modo de operação em alta ou contínua demanda, probabilidade de falha perigosa por hora, em algumas vezes é denominada como frequência de falha perigosa ou taxa de falha perigosa, em números de falha perigosa por hora;

Nota 3 – Para um sistema seguro E/EE/EP operando em alta ou contínua demanda que tem a função de operar por um tempo definido sem a possibilidade de manutenção, o nível de integridade segura para uma função segura pode ser encontrada da seguinte maneira: Determine a probabilidade de falha para a função de segurança durante o tempo de operação e divida pelo tempo de operação, para obter a probabilidade de falha por hora, em seguida utilize a tabela 3 para determinar o nível de integridade seguro necessário.

Nota 4 – A norma define limite mínimos como valores objetivos de falhas. São especificados como o menor limite para o nível de integridade seguro 4 (por exemplo uma probabilidade

média para falha de $10^{-5}$ para excecutar sua função sob demanda, ou a probabilidade de falha perigosa por hora). Pode ser possível atender projetos de sistemas seguros com valores menores para aplicações não complexas, mas os valores apresentados nas tabelas são relativos a aplicações complexas;

Nota 5 – Valores objetivos de falhas que podem ser atendidos quando dois ou mais sistemas seguros E/EE/EP são utilizados, podem ser melhores dos apresentados nas tabelas acima, possibilitando que níveis adequados de independência sejam atingidos;

Nota 6 – É importante notar que as medidas dos níveis de integridade segura 1, 2, 3 e 4 são valores objetivos. É aceitável que a integridade segura do equipamento (ver 3.5.5 da IEC 61508-4) seja possível quantificar e aplicar técnicas confiáveis de avaliação de diagnósticos para que valores objetivos sejam atendidos. Análises qualitativas tem sido feitas com respeito as medidas necessárias para atender a sistematica de integridade segura (ver 3.5.4 da IEC 61508-4);

Nota 9 – Os requisitos de integridade segura para cada função segura deve ser qualificada para indicar qual parâmetro objetivo, entre:

- a probabilidade média de falha para excecutar sua função de projeto sob demanda (para o modo de baixa demanda de operação), ou
- a probabilidade de falha perigosa por hora (para o modo de alta ou contínua demanda de operação).