Setting the Standard for Automation™

Ferramentas de auxílio ao Ciclo de Vida de Segurança

Standards

Certification

Education & Training

Publishing

Conferences & Exhibits

Monica Hochleitner, CFSE

- Safety Engineer da *exida* desde 2007
- Mais de 20 anos de experiência em Automação, Controle e Segurança
- Certificada pelo CFSE.org como *Certified Functional Safety Expert*
- Engenheira eletricista e mestre em engenharia de produção

Rede global de excelência

exida GmbH
Mr. Rainer Faller
Germany
+49 89 4900 0547

exida Asia Pacific PTE
Mr. Koen Leekens
Singapore
+65 9772 9547

Excel
Mr. Da
Singapore/M
+65 685

Pacific
eter Clark
ong Kong
222-5160

Ex
Jon I
United
+44 24 76

om LLC
am Goble
ellersville
453 1720

Exida C
David
+ 1 647 838 3377

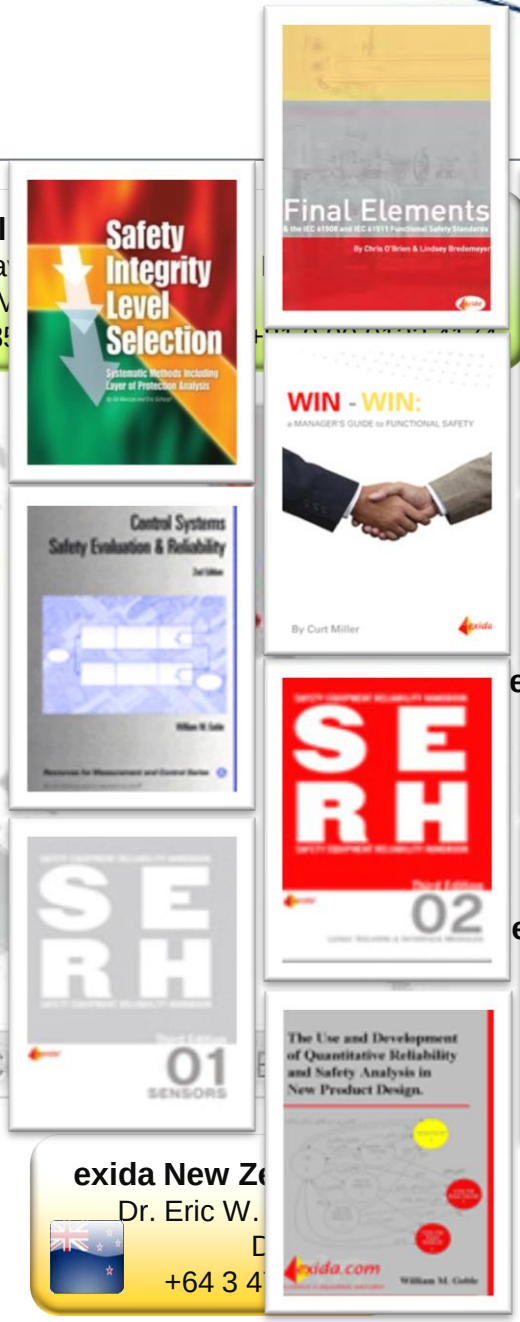
Region)
urt Miller
Houston
439 3793

exida
Certification S.A.

exida Netherlands
Mr. Rolf Spiker
Netherlands
+31 318 414 505

Mexico
Esparza
Mexico
611 9858

HEADQUARTERS SERVICE C



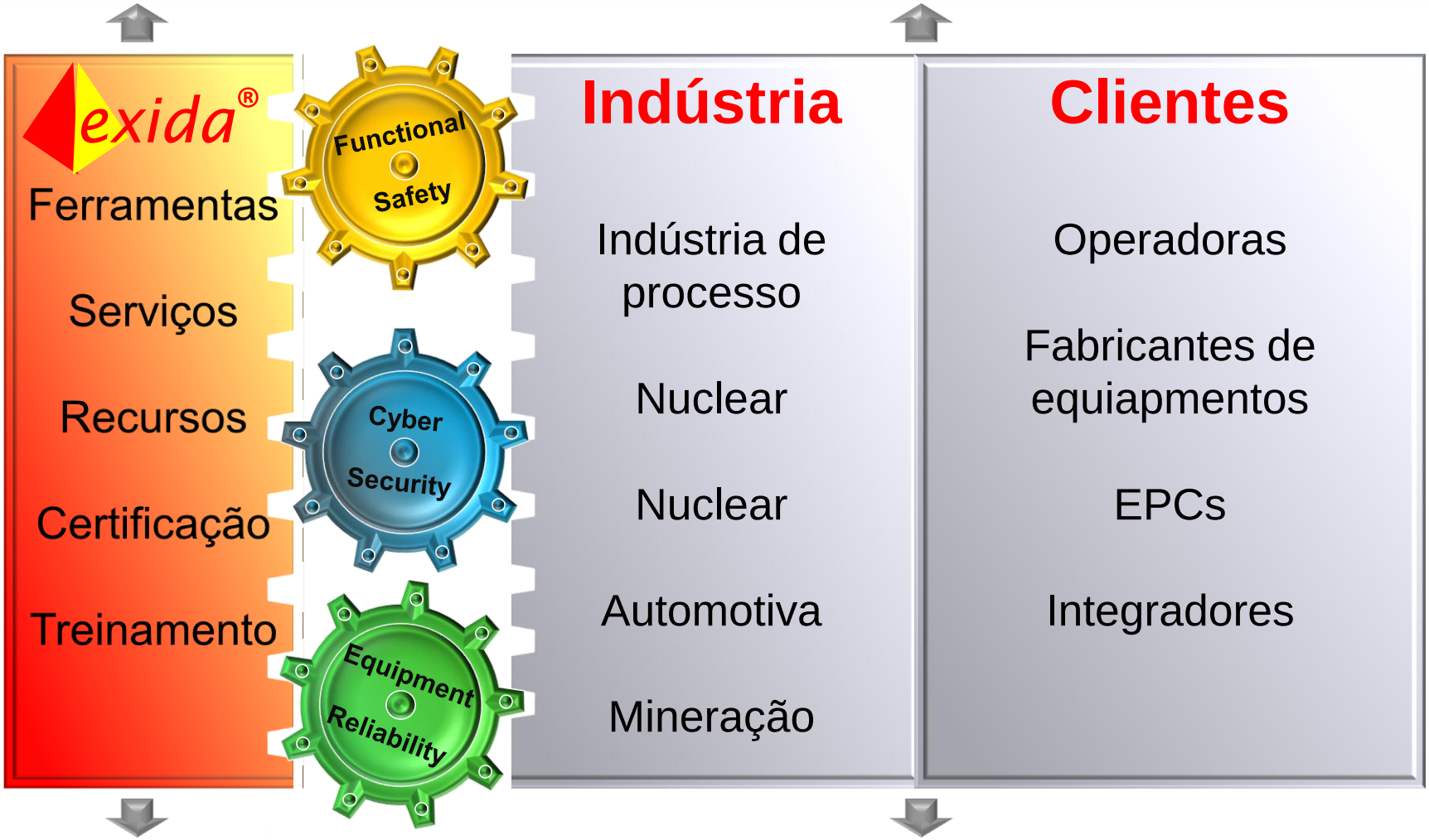
exida Certification SA
Mr. Peter Soderblom
Genolier
+41 22 364 14 34

exida South Africa
Mr. Owen Tavener-Smith
Westville
+27 31 267 1564

exida New Ze
Dr. Eric W.
D
+64 3 4

exida Consulting LLC
Mrs. Monica Hochleitner
Brazil
+55 21 8132-0736

Especialista em Segurança Funcional, *Cyber Security* & Gerenciamento de Alarmes



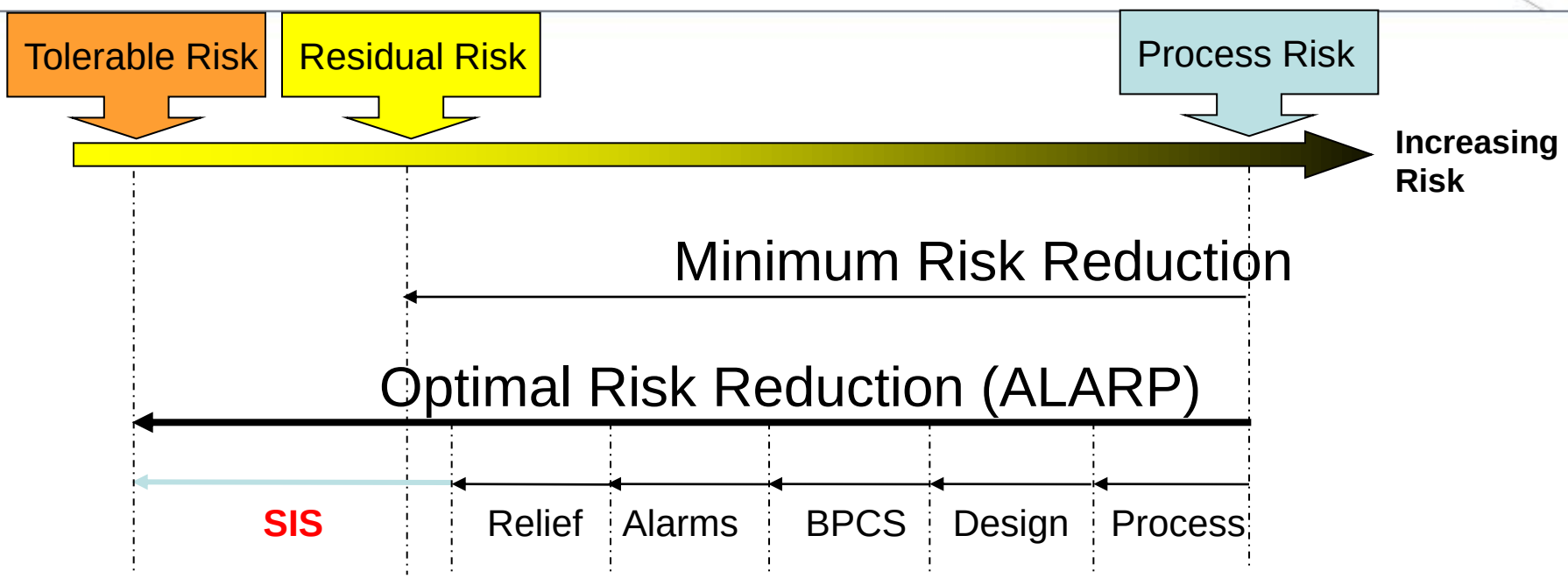
Sistema Instrumentado de Segurança

- Sistema que tem como objetivo levar o processo industrial para uma condição segura quando determinados limites são violados;

- Composto por Funções Instrumentadas de Segurança, responsáveis pela proteção/prevenção de cada situação de risco que o processo está exposto;

- Depende do correto funcionamento da instrumentação responsável pelas funções críticas, tanto na ação que deve desempenhar como na velocidade em que deve atuar.

Sistema Instrumentado de Segurança



Conceitos fundamentais

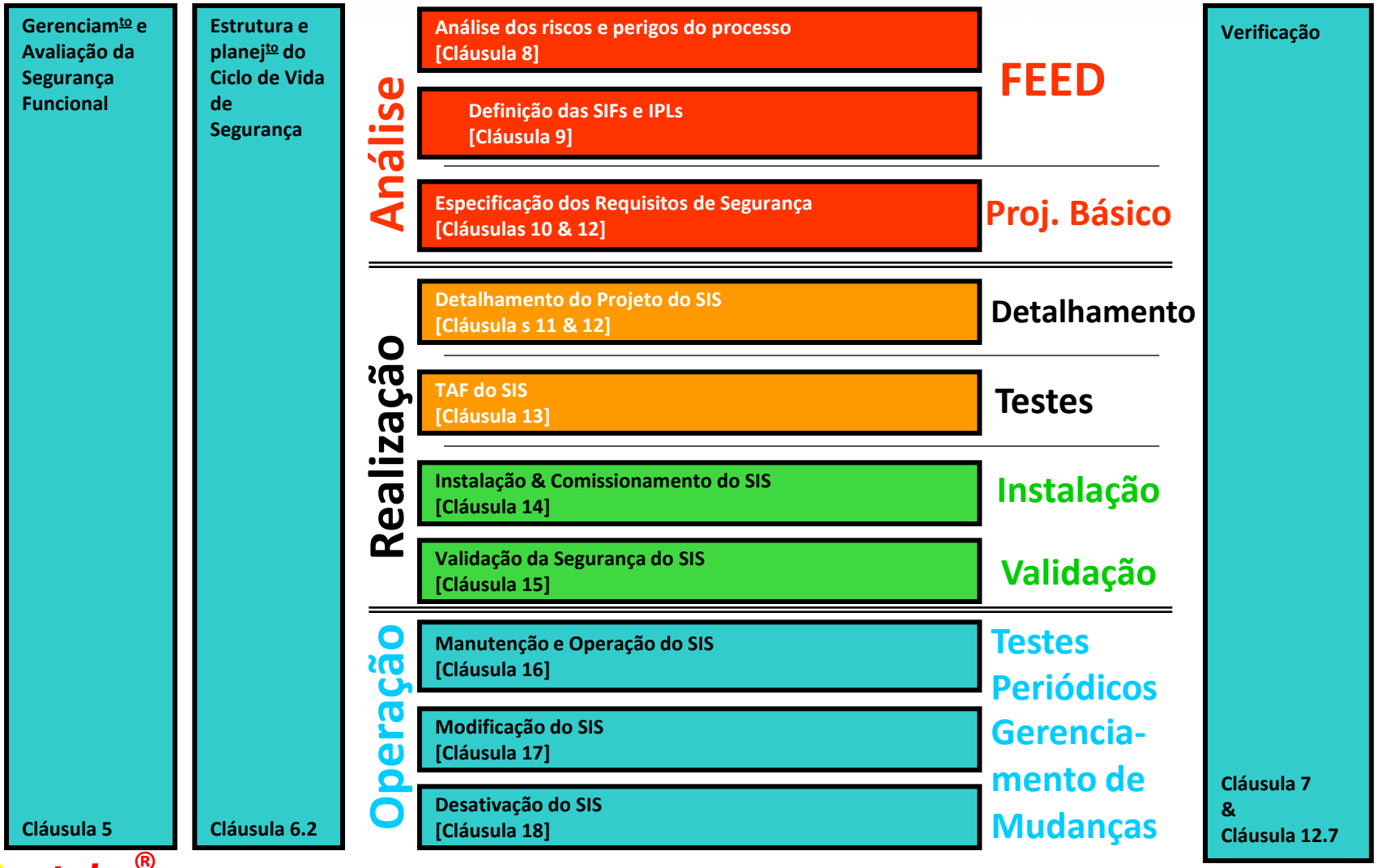
- Ciclo de Vida de Segurança (SLC); e
- Projeto baseado em desempenho (SIL).

Desempenho e Integridade de Segurança

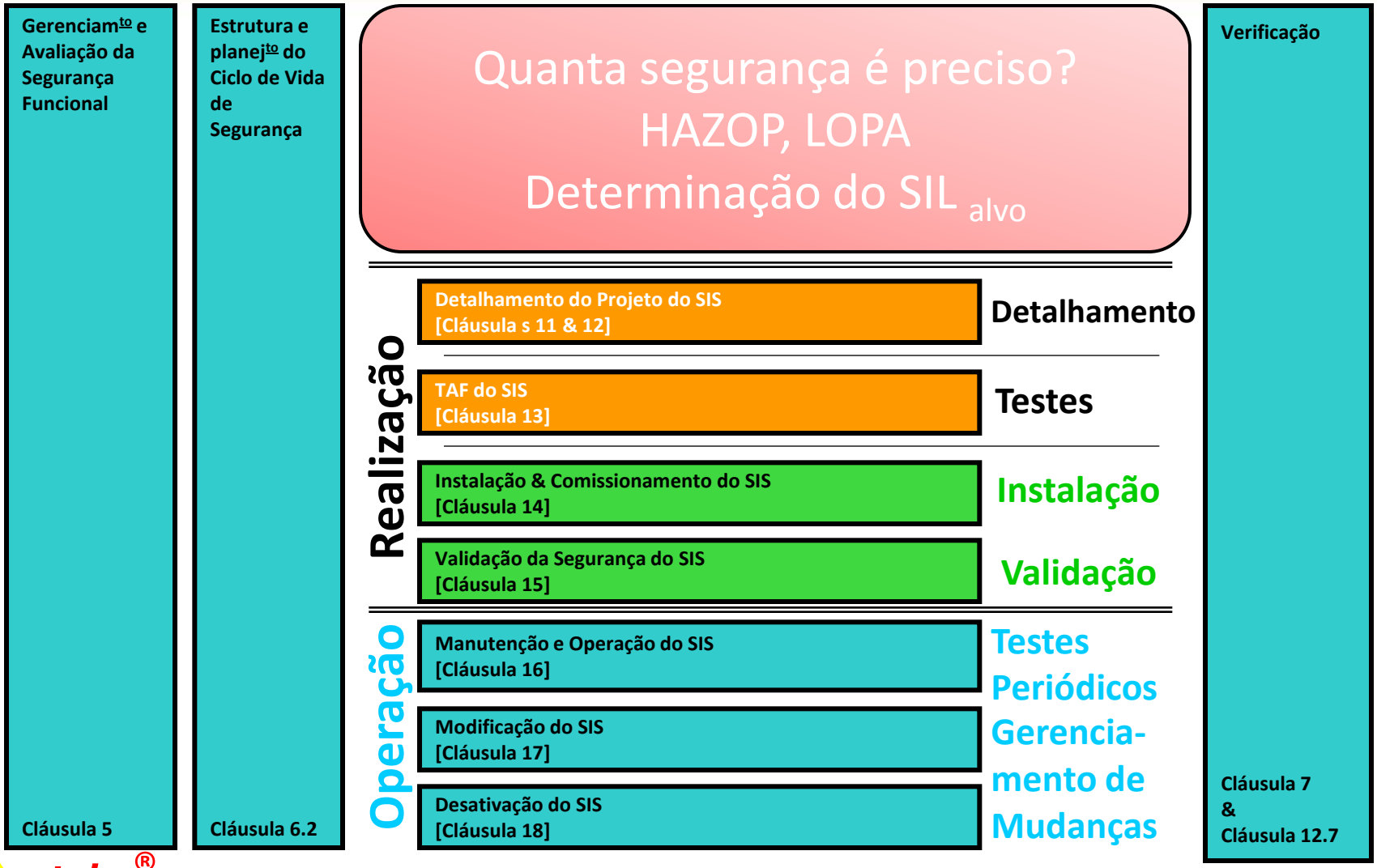
Nível de Integridade de Segurança SIL	Fator de Redução de Risco RRF	Probabilidade média de falha na demanda PFD_{avg}
SIL 4	100000 a 10000	$>=10^{-5}$ a $<10^{-4}$
SIL 3	10000 a 1000	$>=10^{-4}$ a $<10^{-3}$
SIL 2	1000 a 100	$>=10^{-3}$ a $<10^{-2}$
SIL 1	100 a 10	$>=10^{-2}$ a $<10^{-1}$

- Projeto do SIS baseado no risco do processo (específico para cada planta)

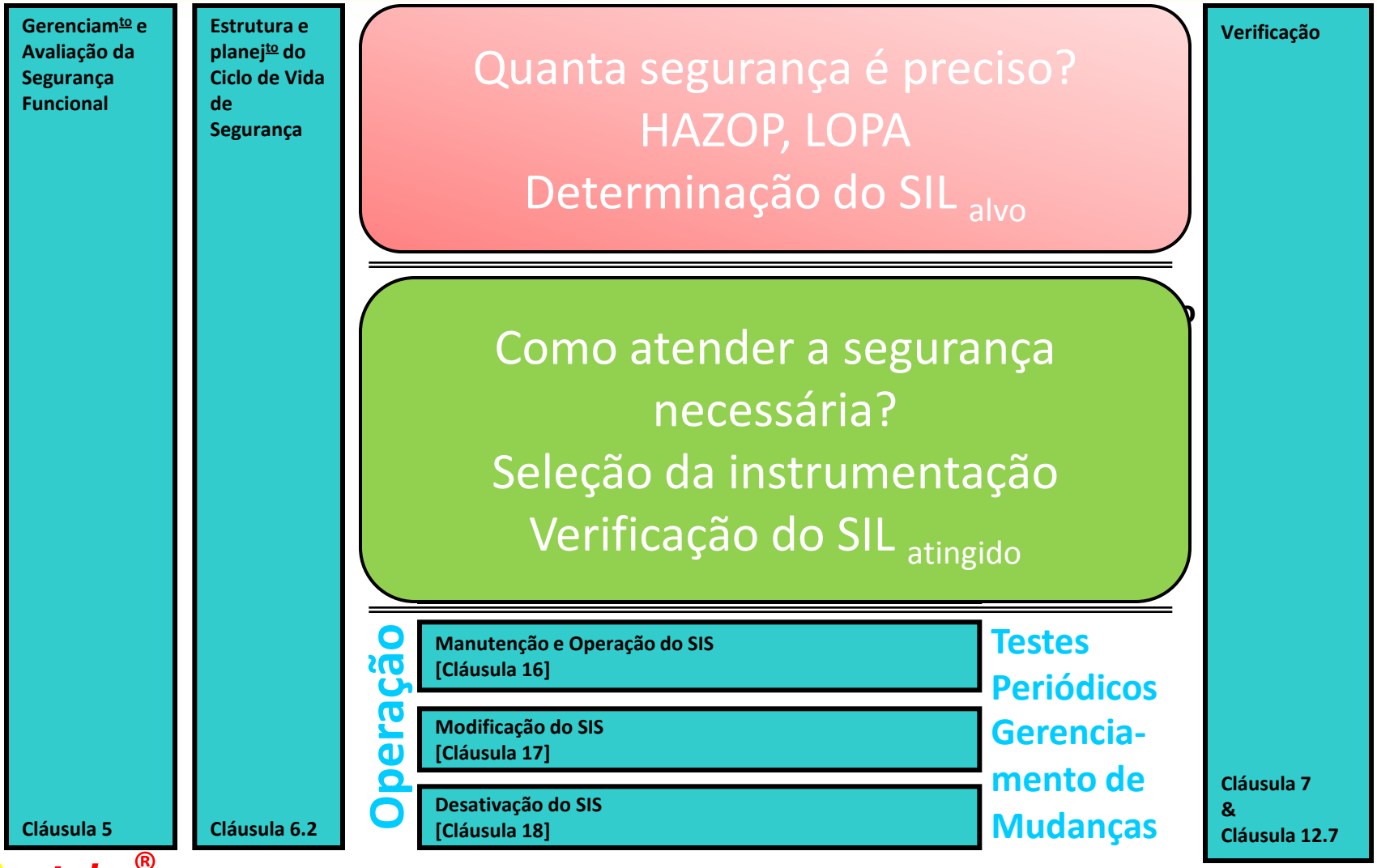
Ciclo de Vida de Segurança – IEC 61511



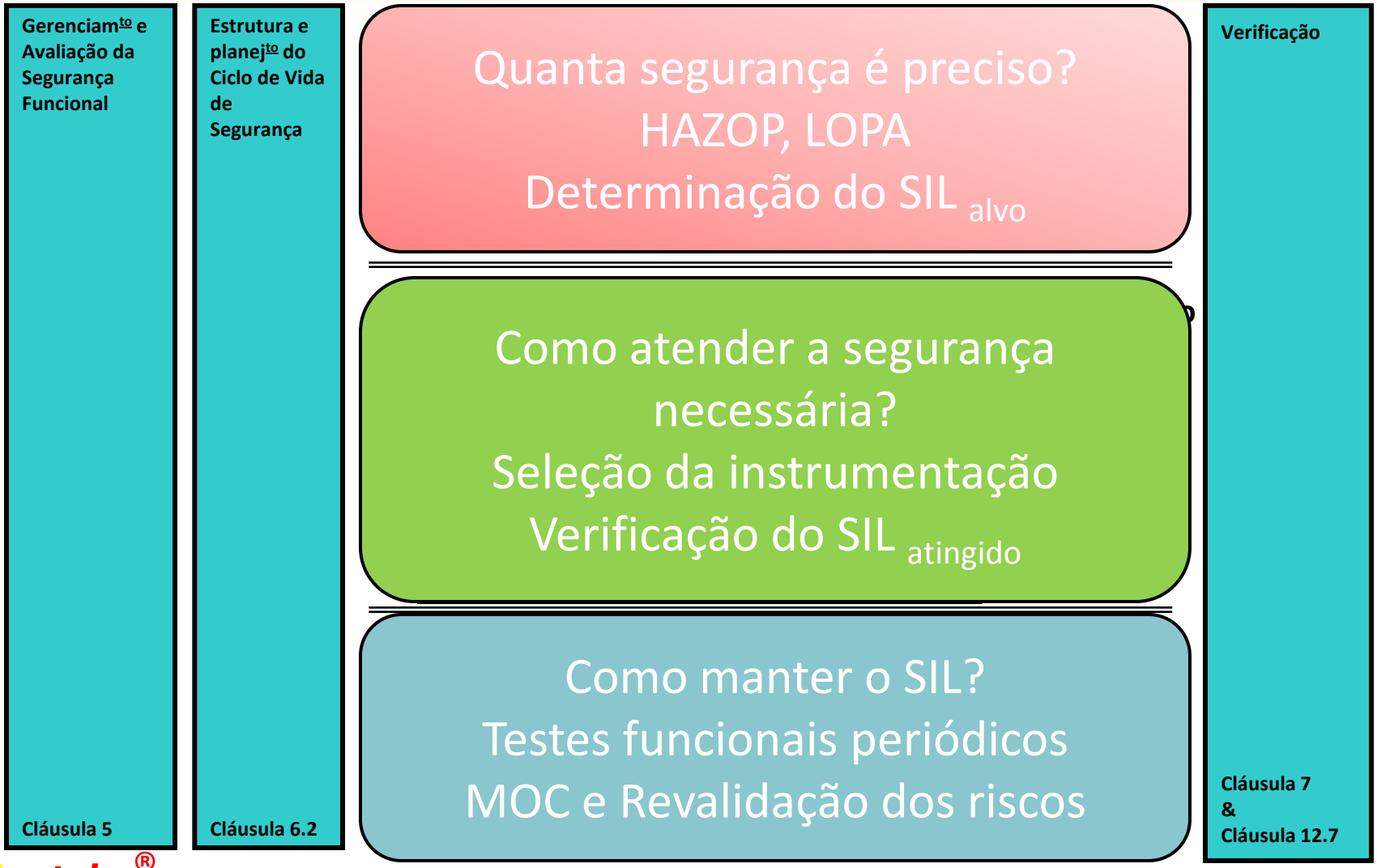
Ciclo de Vida de Segurança – IEC 61511



Ciclo de Vida de Segurança – IEC 61511



Ciclo de Vida de Segurança – IEC 61511



Ponto de partida

O que pode dar errado?
ex: **HAZOP**

O que precisa ser feito?
SRS

Como mantê-lo seguro?

Identificação do Risco

Análise do Risco & Seleção de SIL

Especificação dos Requisitos de Segurança

Verificação de SIL

SIL Sustain

Quão catastrófico pode ser?
ex: **LOPA**

Quão confiável é o sistema?

- Procedimentos Operacionais
- Procedimentos de Manutenção
- Procedimentos Testes Funcionais

SLC - CICLO DE VIDA DE SEGURANÇA PROPOSTO PELA IEC **61151 / 61508**

ANÁLISE

Análise de Risco:

- Freq. X Conseq. > HAZOP / LOPA
- Risco Tolerável/Red. Risco Necessário
- SRS → Definição das Especificação dos requisitos de segurança
- SIF → Definição das Funções de Integridade de Segurança.
- **SIL Selection** ..... → **SIL alvo**

EXECUÇÃO

Aplicação do sistema SIS:

- Definição de Tecnologias
- Redundância / Diversidades
- Aplicação das malhas
- Testes iniciais **(FAT, SAT & SIT)**
- **SIL Verification** ..... → **SIL Atingido**

OPERAÇÃO MANUTENÇÃO

Operação e Manutenção:

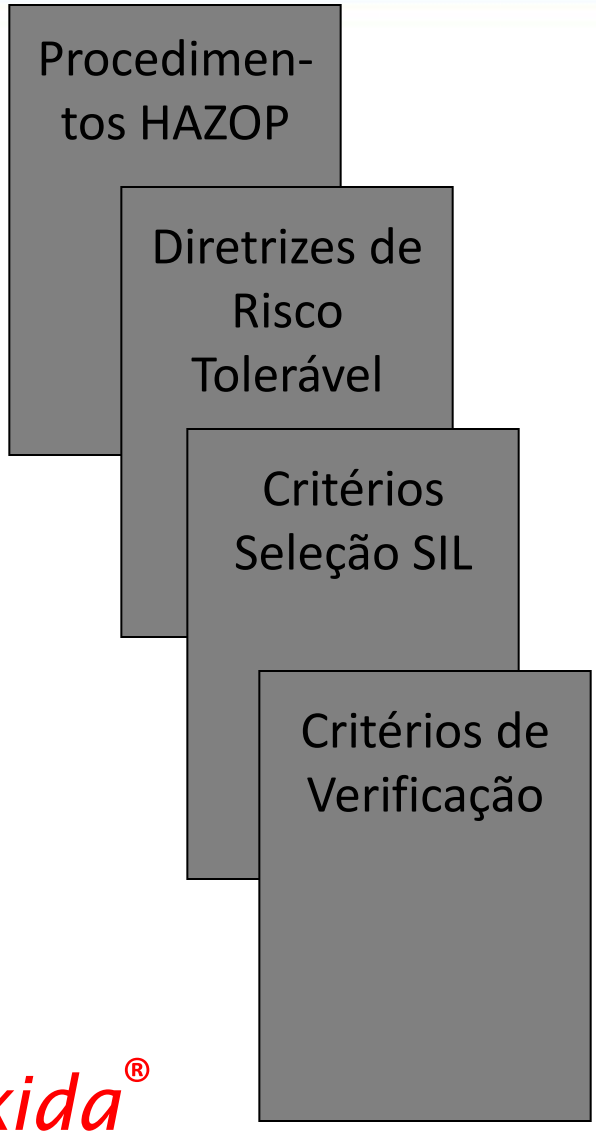
- Procedimentos operacionais e de Manutenção
- Rondas / Rotinas de checagem e testes
- Simulados
- **Gerenciamento das Mudanças do projeto**
- **Registro dos testes periódicos** ..... → **SIL Mantido**

VALIDAÇÃO DO PROJETO

GERENCIAMENTO DA SEGURANÇA FUNCIONAL

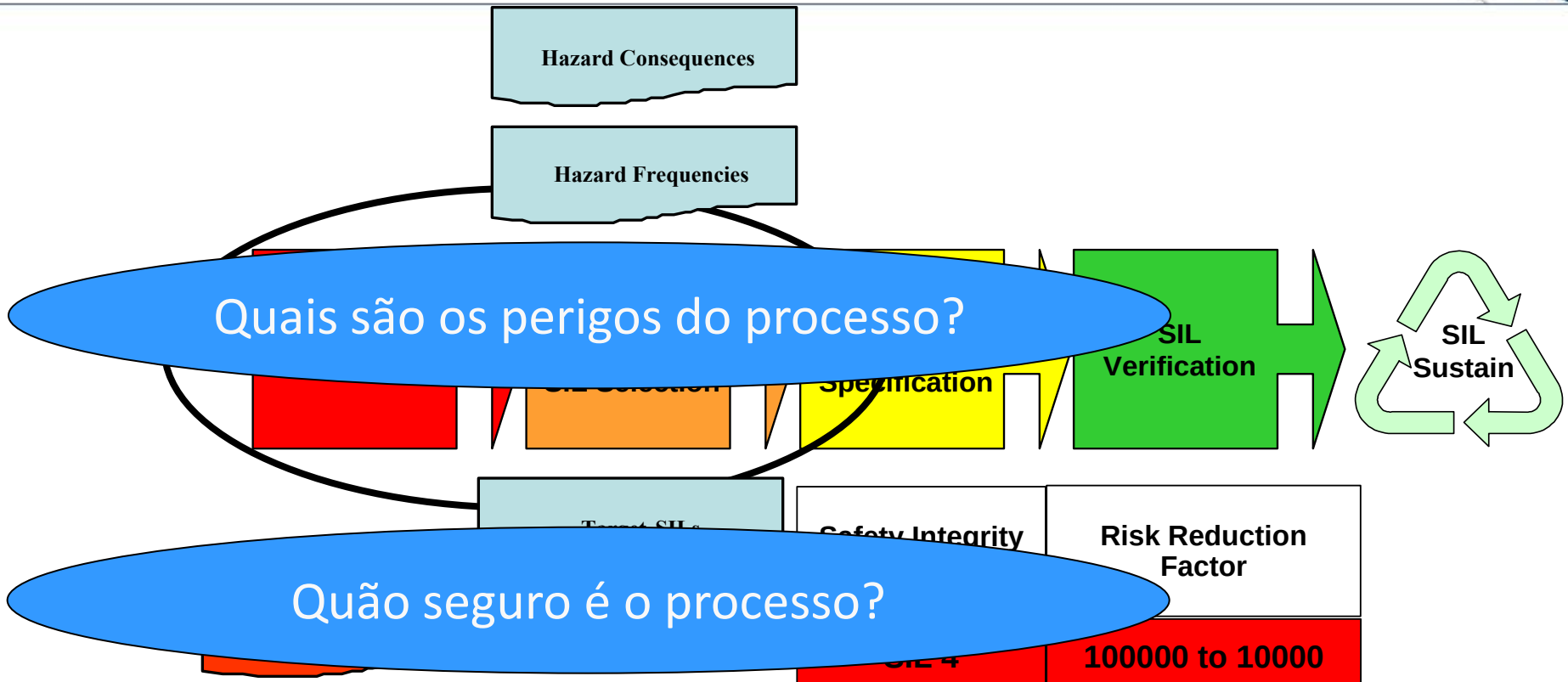
Fonte: Umicore, 2011

Implementação bem sucedida



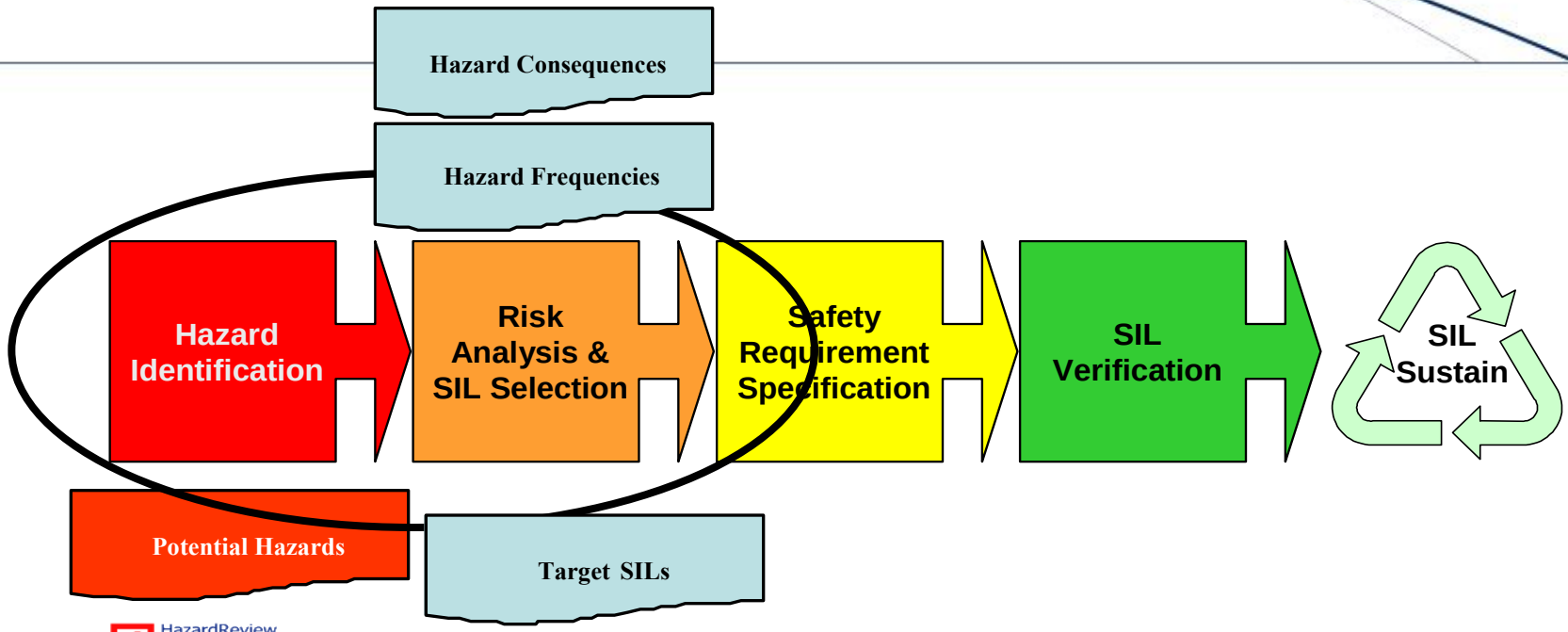
- Gerenciamento das Funções de Segurança:
- Procedimentos descrevendo e documentando as tarefas específicas de cada uma das etapas do SLC.

Análise de Risco



Safety Integrity	Risk Reduction Factor
SIL 4	100000 to 10000
SIL 3	10000 to 1000
SIL 2	1000 to 100
SIL 1	100 to 10

SLC – Ferramentas de Análise de Risco



HazardReview LEADER 2006

exSILentia

HAZID

exida

PHAWorks

DYADEM

PHA Pro

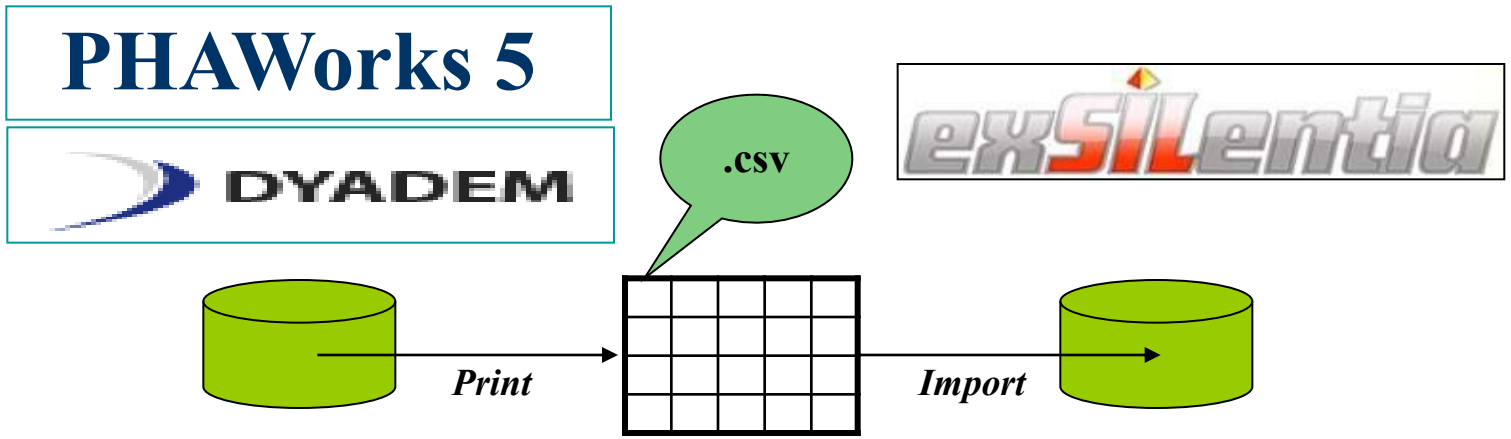
SILHazop

SILClass

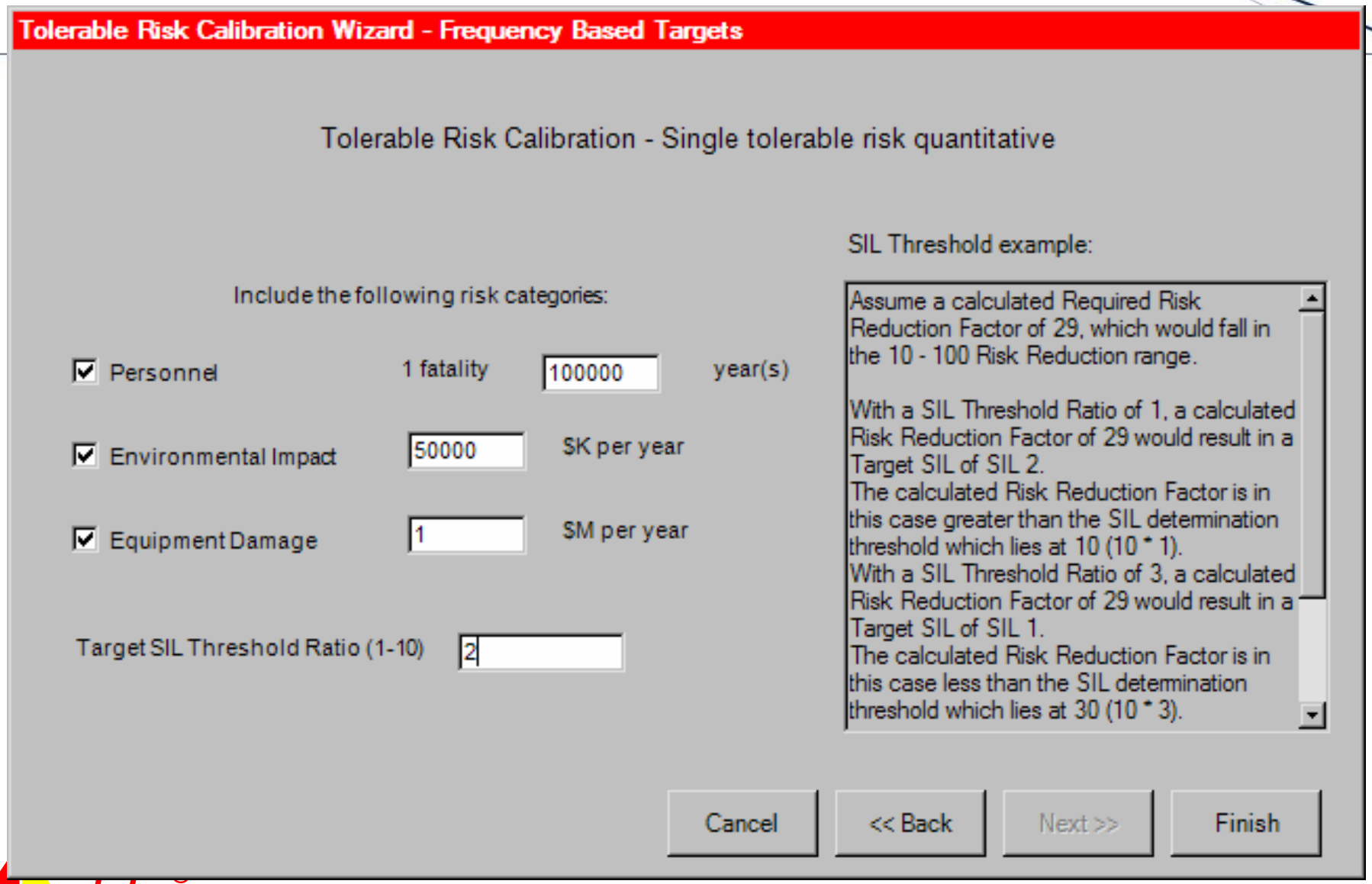
exida®

aim asset integrity management

Opções de Importação/Exportação de SIF



Critérios de Risco Tolerável



Análise de Camadas de Proteção

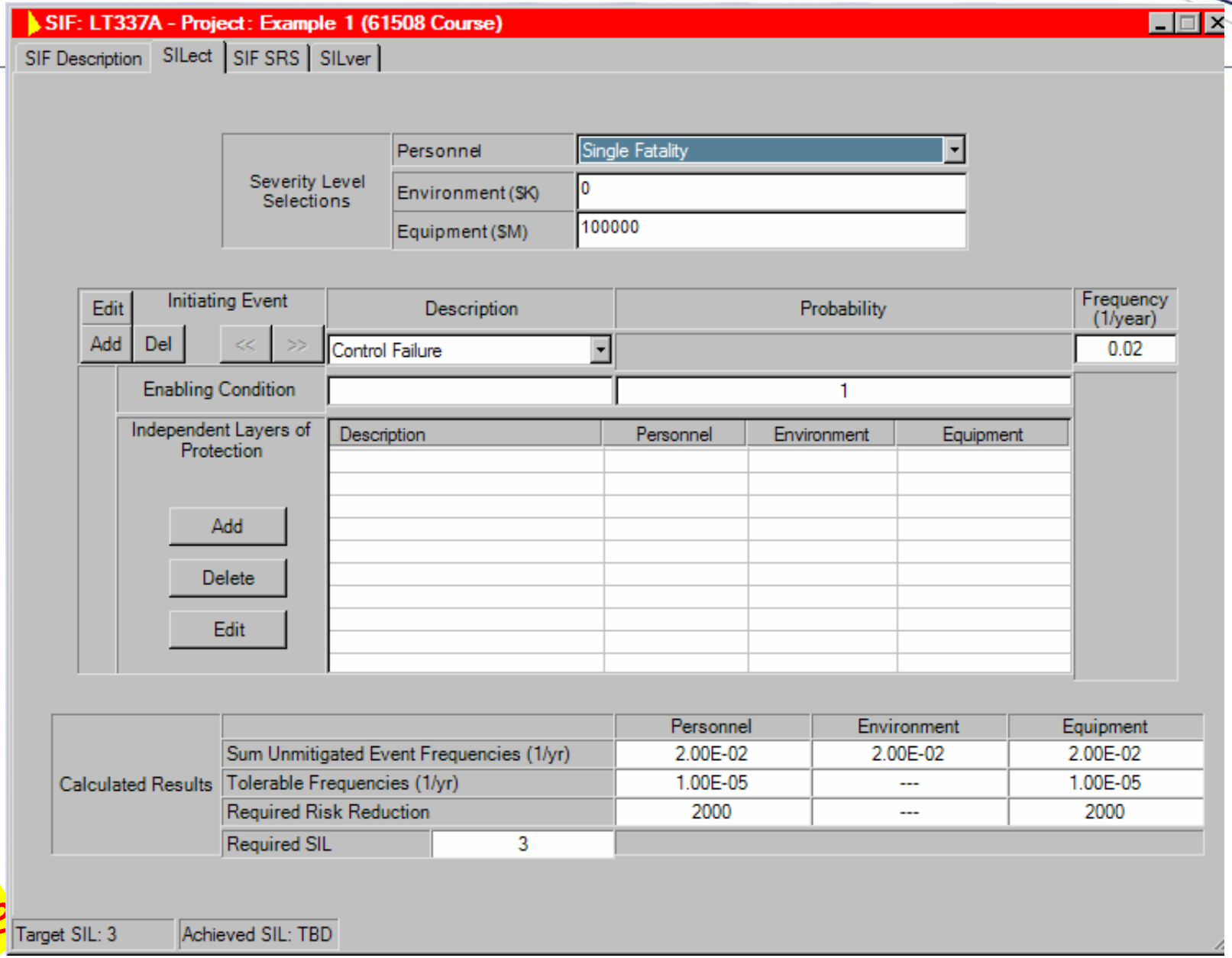
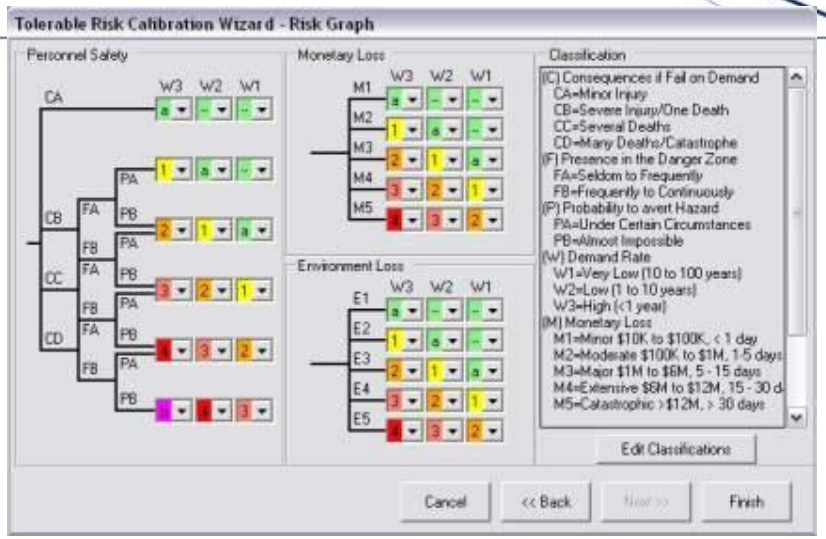
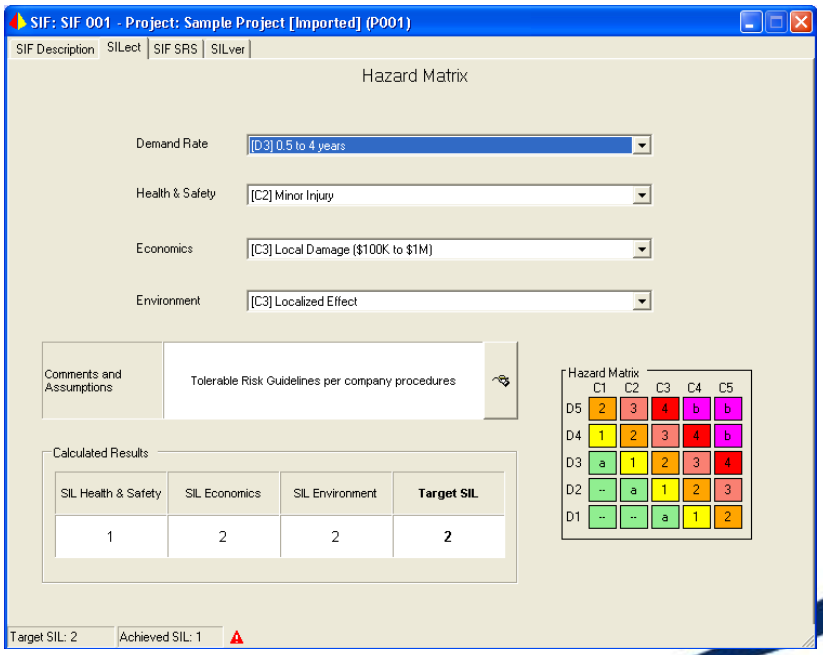


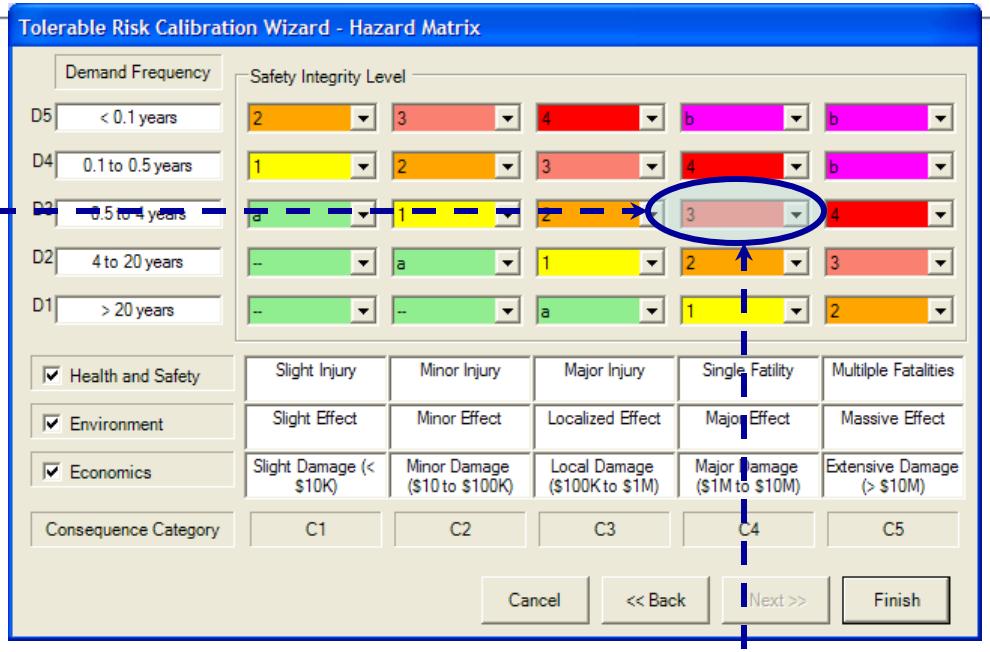
Gráfico de Risco – Matriz de Risco

Existem diversos métodos de determinação (seleção) de SIL – baseiam-se nos mesmos conceitos, mas possuem diferentes níveis de detalhes, bem como formas distintas de representação.





Seleção de SIL



Freqüência estimada da demanda:

- Pressão alta a cada 3 anos

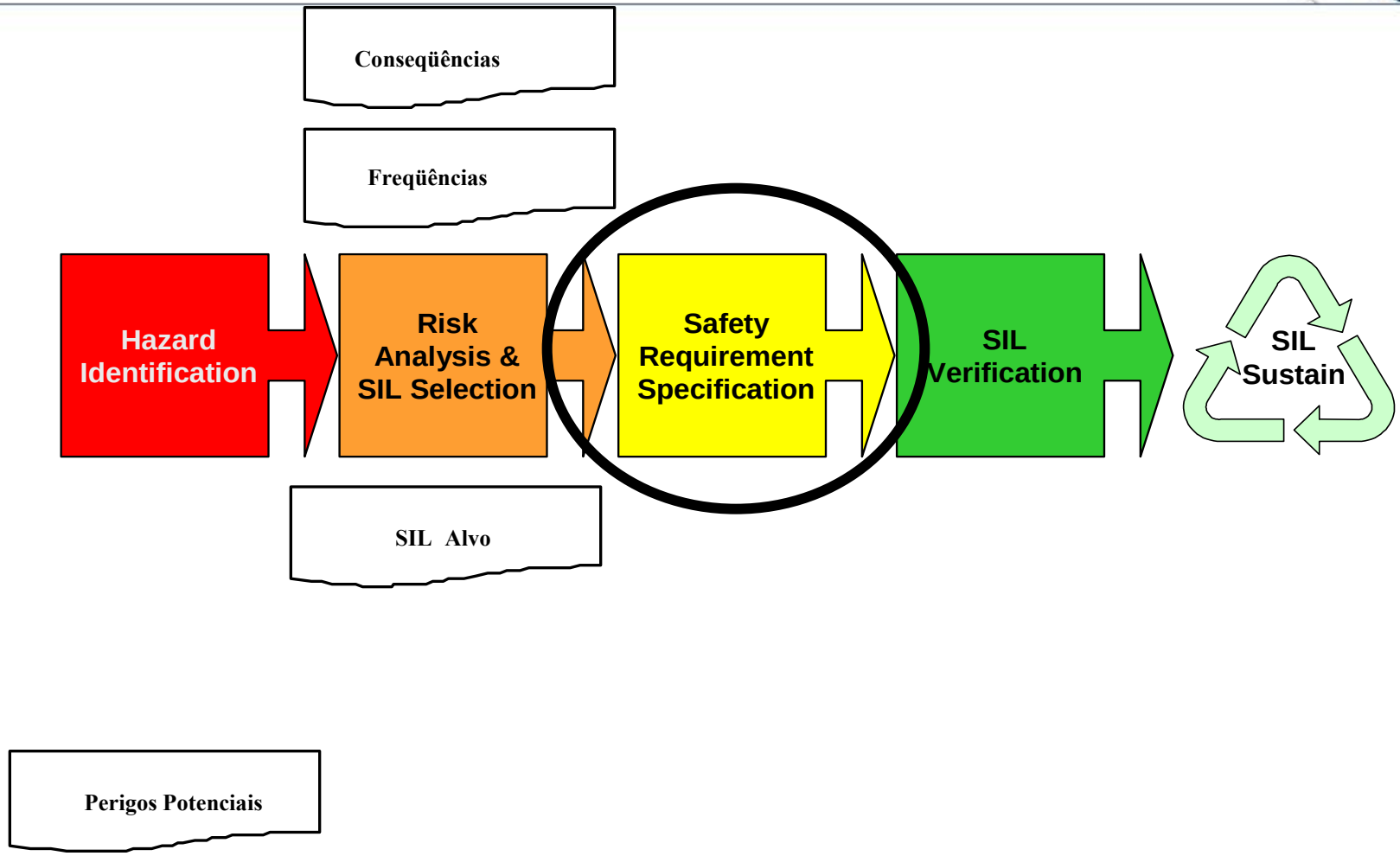
Conseqüência:

- Uma fatalidade
- Perda financeira de $4 Milhões

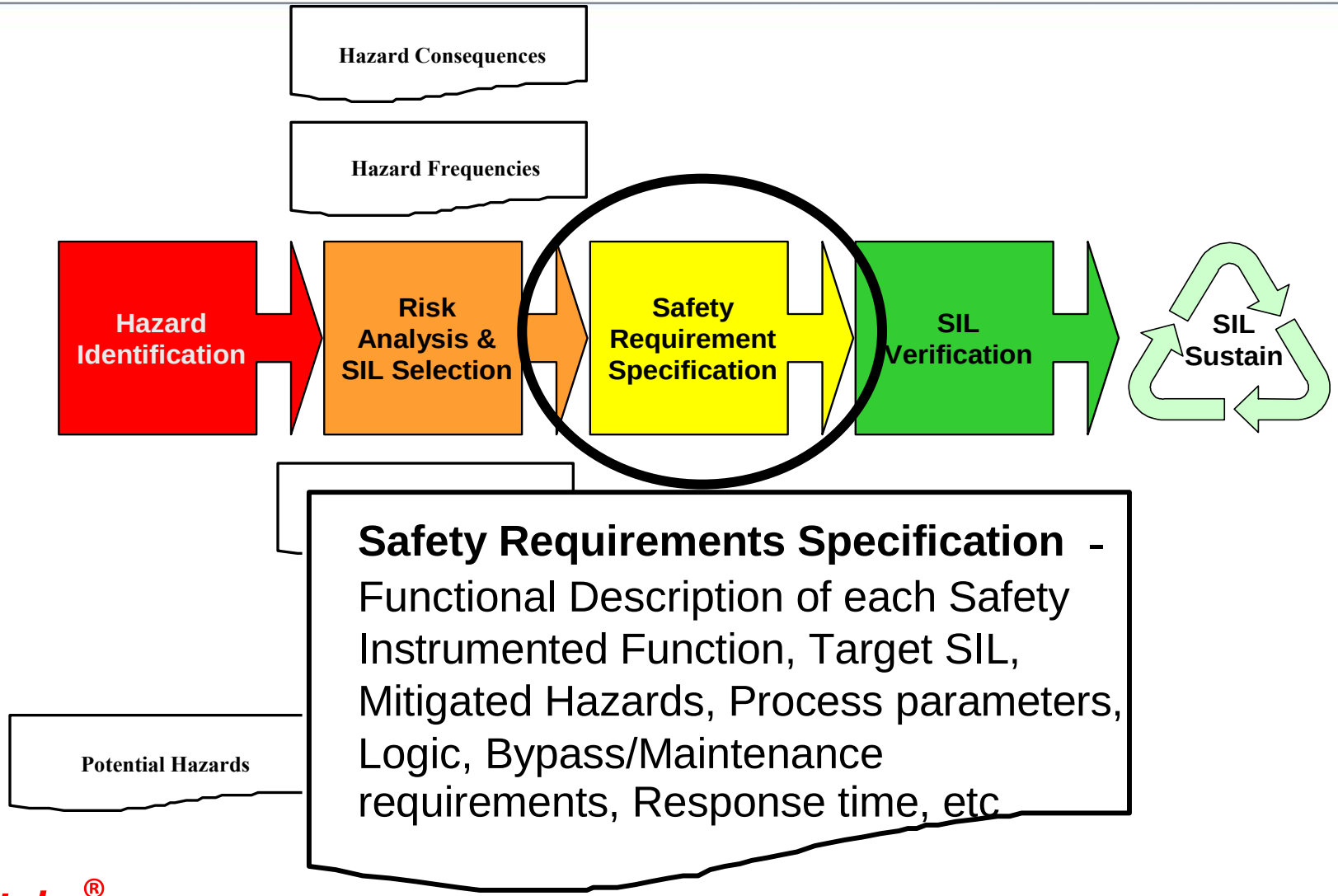
Item	Risco/Perigo	Descrição	Entradas	Saídas	SIL Alvo
SIF 1	Pressão alta na coluna C-51, com possível sobrecarga para o flare.	Pressão Alta na Coluna C-51 fecha as válvulas de vapor.	PT-51 PT-52 PT-53 (2oo3)	XV-51 Close XV-52 Close (1oo2)	3

Nota: O SIL Alvo e votação de entradas e saídas são apenas exemplos e não devem ser considerados recomendações ou sugestões.

SLC – Requisitos de Segurança



SRS – Requisitos de segurança



SLC - CICLO DE VIDA DE SEGURANÇA PROPOSTO PELA IEC **61151 / 61508**

ANÁLISE

Análise de Risco:

- Freq. X Conseq. > HAZOP / LOPA
- Risco Tolerável/Red. Risco Necessário
- **SRS → Definição das Especificação dos requisitos de segurança**
- SIF → Definição das Funções de Integridade de Segurança.
- **SIL Selection** ..... → **SIL alvo**

EXECUÇÃO

Aplicação do sistema SIS:

- Definição de Tecnologias
- Redundância / Diversidades
- Aplicação das malhas
- Testes iniciais **(FAT, SAT & SIT)**
- **SIL Verification** ..... → **SIL Atingido**

OPERAÇÃO MANUTENÇÃO

Operação e Manutenção:

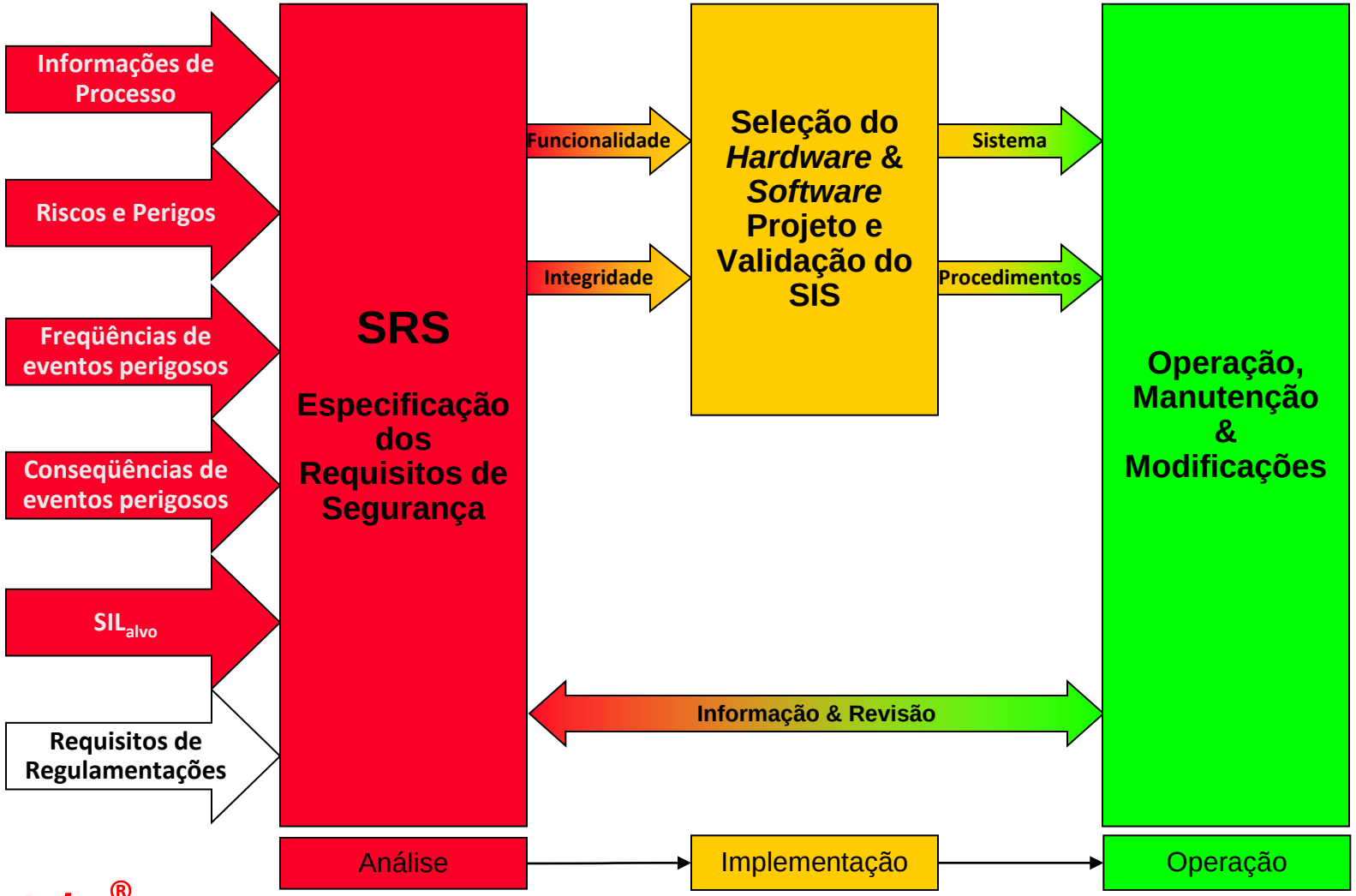
- Procedimentos operacionais e de Manutenção
- Rondas / Rotinas de checagem e testes
- Simulados
- **Gerenciamento das Mudanças do projeto**
- **Registro dos testes periódicos** ..... → **SIL Mantido**

VALIDAÇÃO DO PROJETO

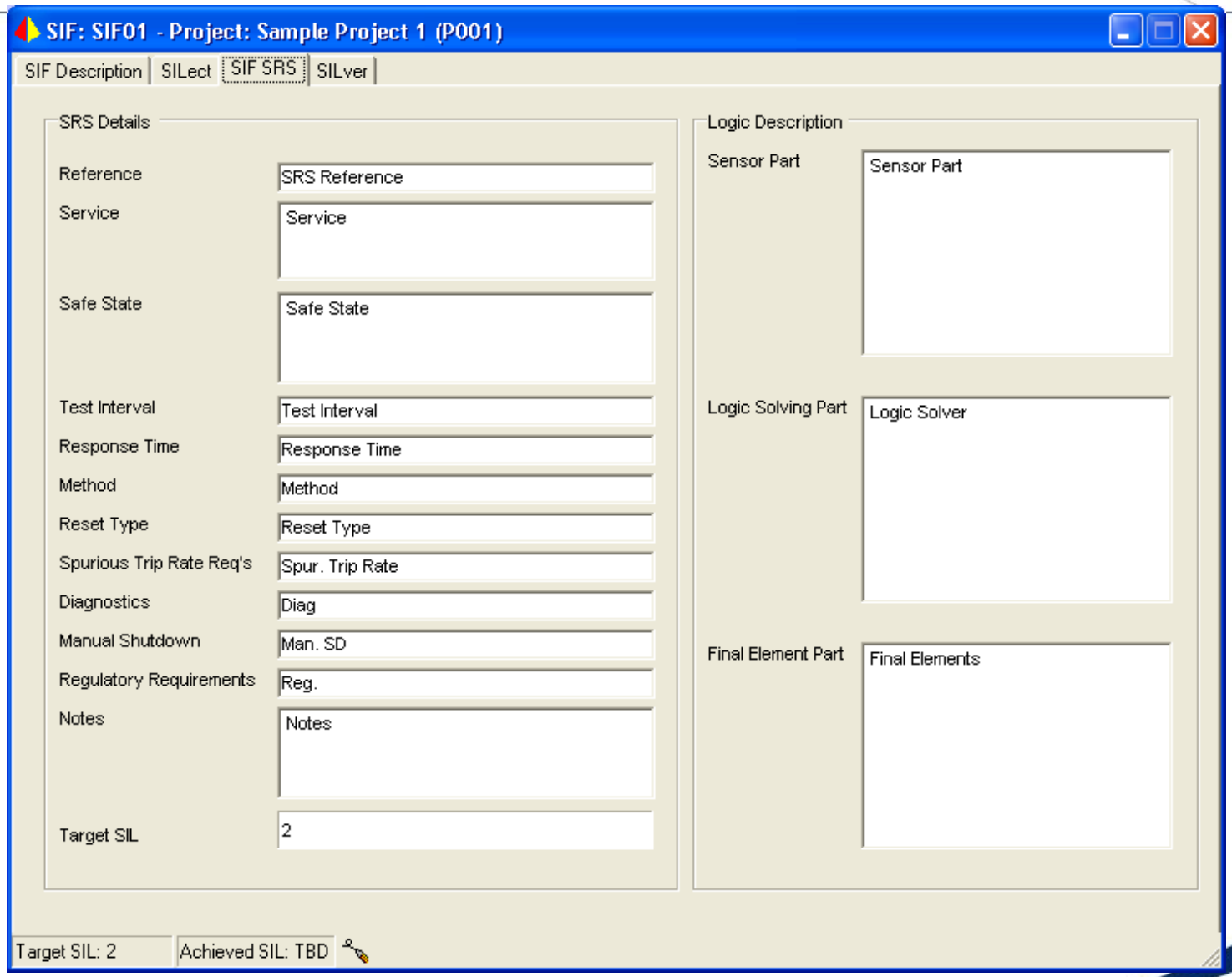
GERENCIAMENTO DA SEGURANÇA FUNCIONAL

Fonte: Umicore, 2011

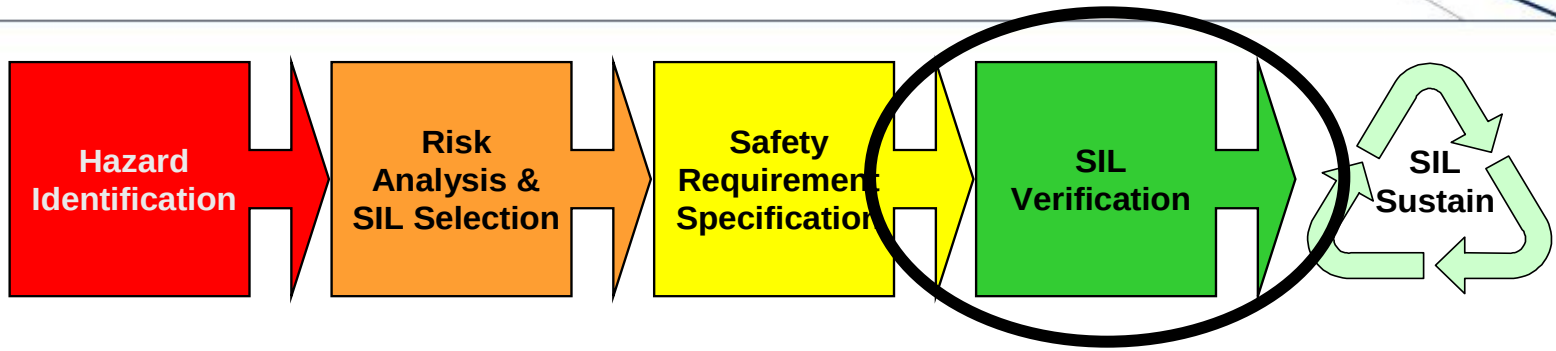
SRS: Base de Conhecimento



Ferramenta de SRS



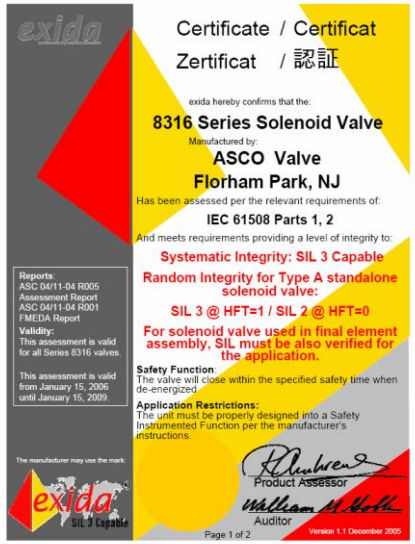
SLC – Projeto e Verificação



Dimensionar equipamentos conforme IEC 61511: Equipamentos utilizados em um SIS devem ser escolhidos com base na **certificação IEC 61508** para o SIL apropriado ou com base no critério de

"prior use" (uso anterior)

O equipamento certificado tem um "SIL Capability"


exida

Certificate / Certificat
Zertificat / 認証

exida hereby confirms that the:

8316 Series Solenoid Valve

Manufactured by:

ASCO Valve
Florham Park, NJ

Has been assessed per the relevant requirements of:

IEC 61508 Parts 1, 2

And meets requirements providing a level of integrity to:

Systematic Integrity: SIL 3 Capable

Random Integrity for Type A standalone solenoid valve:

SIL 3 @ HFT=1 / SIL 2 @ HFT=0

For solenoid valve used in final element assembly, SIL must be also verified for the application.

Reports:
ASC 04/11-04 R005 Assessment Report
ASC 04/11-04 R001 FMEDA Report

Validity:
This assessment is valid for all Series 8316 valves.

This assessment is valid from January 15, 2006 until January 15, 2009.

Safety Function:
The valve will close within the specified safety time when de-energized

Application Restrictions:
The unit must be properly designed into a Safety Instrumented Function per the manufacturer's instructions.

The manufacturer may use the mark:

exida SIL 3 Capable

Product Assessor

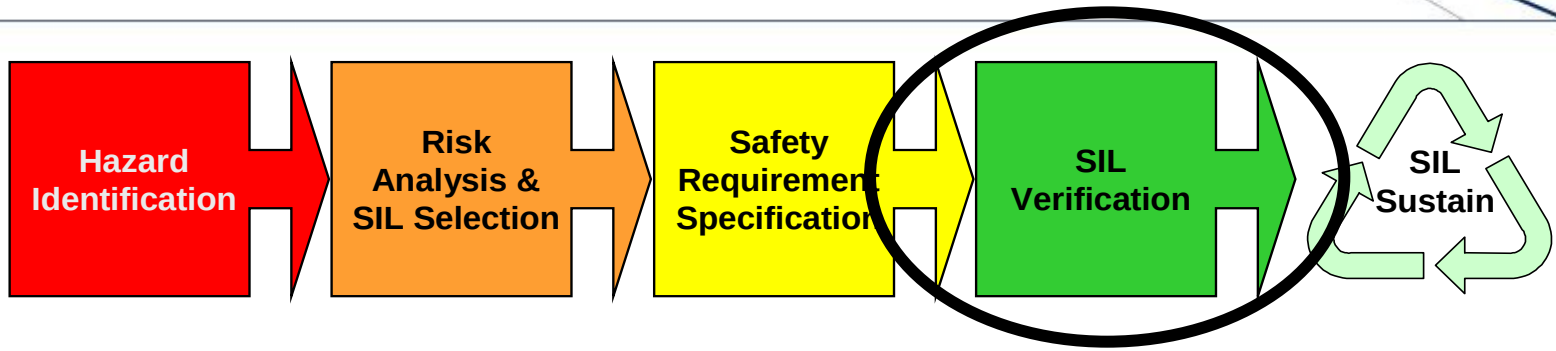
Auditor

Page 1 of 2

Version 1.1 December 2005

exida®

SLC – Verificação da Probabilidade



Método #1:

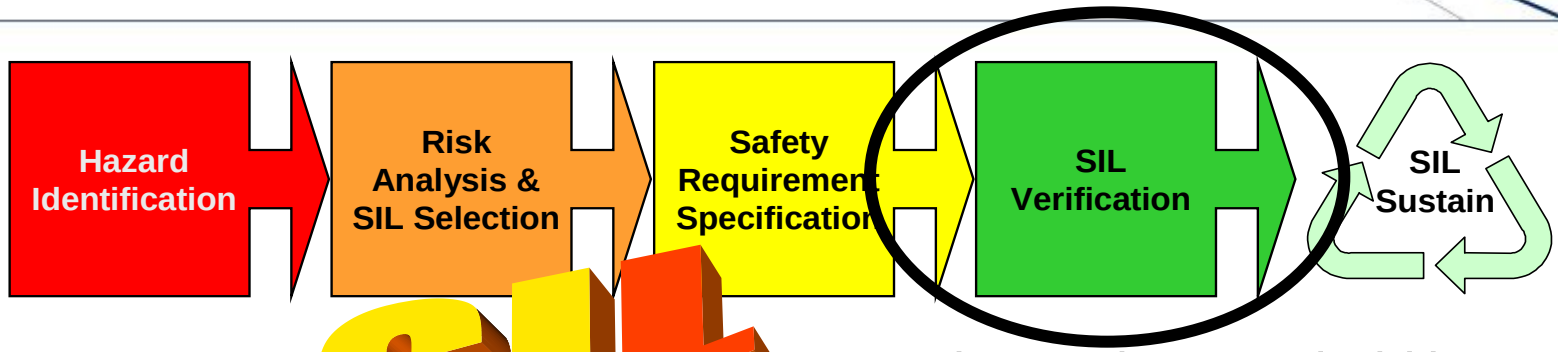
Modo Contínuo

O perigo está presente todo o tempo.

Random Failure Probability

Safety Integrity Level	Probability of dangerous failure per hour (Continuous mode of operation)
SIL 4	>=10^{-9} to <10^{-8}
SIL 3	>=10^{-8} to <10^{-7}
SIL 2	>=10^{-7} to <10^{-6}
SIL 1	>=10^{-6} to <10^{-5}

SLC – Verificação da Probabilidade



Random Failure Probability

Método #2:

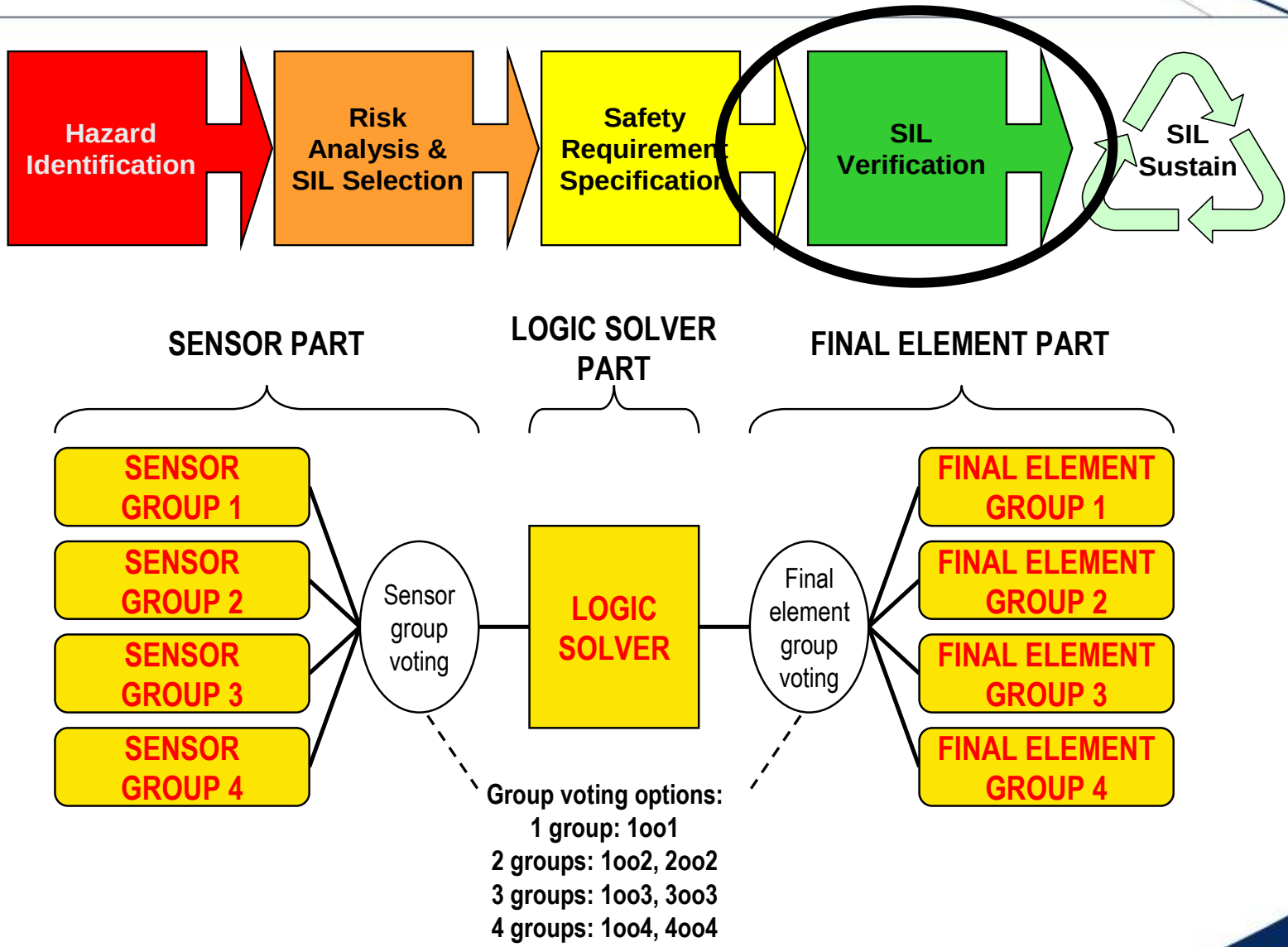
Modo na Demanda

O perigo raramente está presente

Safety Integrity Level	Probability of failure on demand (Demand mode of operation)
SIL 4	>=10^{-5} to <10^{-4}
SIL 3	>=10^{-4} to <10^{-3}
SIL 2	>=10^{-3} to <10^{-2}
SIL 1	>=10^{-2} to <10^{-1}

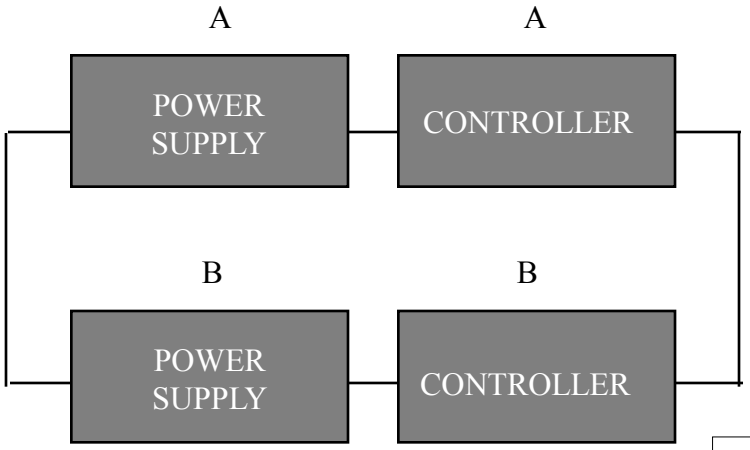
exida®

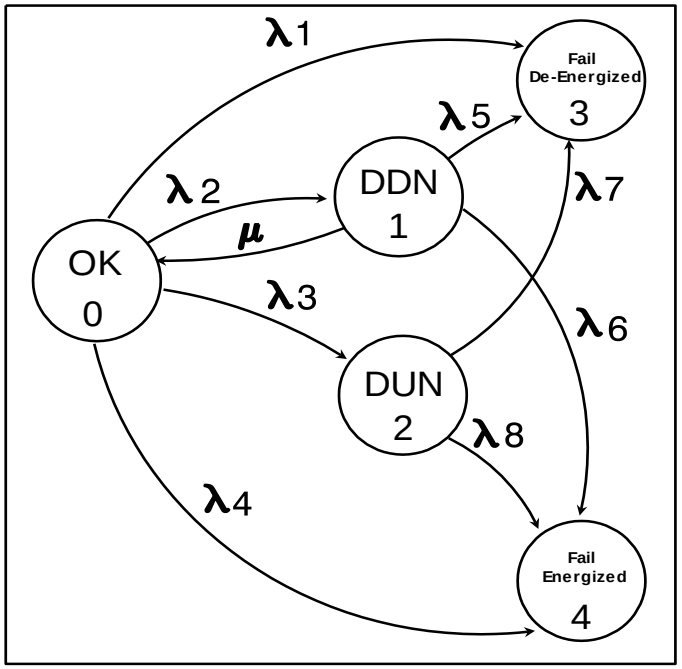
SLC – Projeto Conceitual

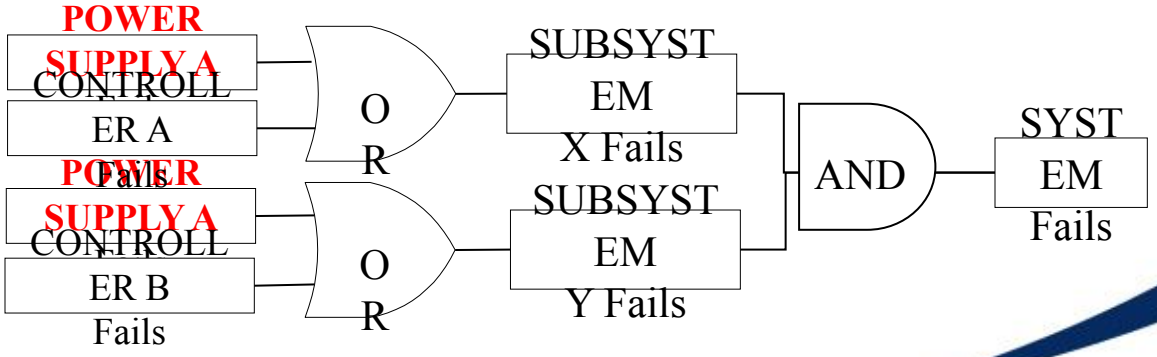


Técnicas de modelagem

- Diagrama de blocos
- Diagramas de árvore de falhas
- Modelos Markov
- Equações simplificadas



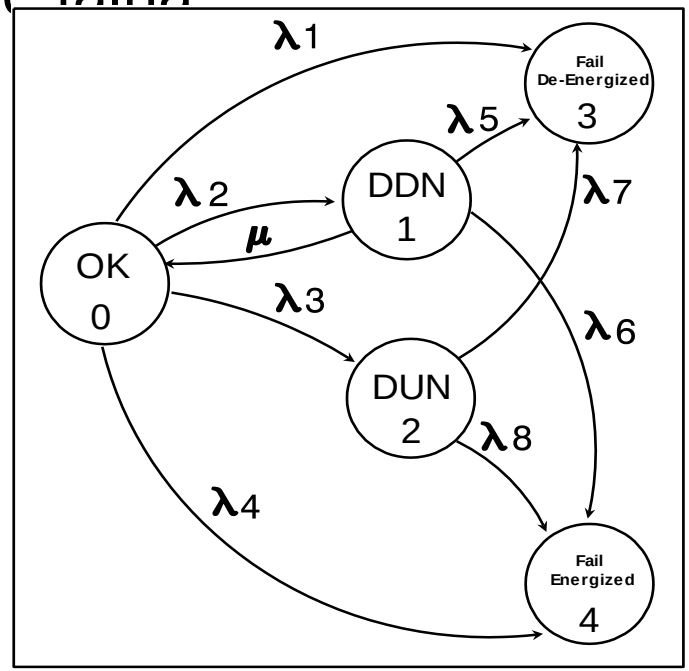




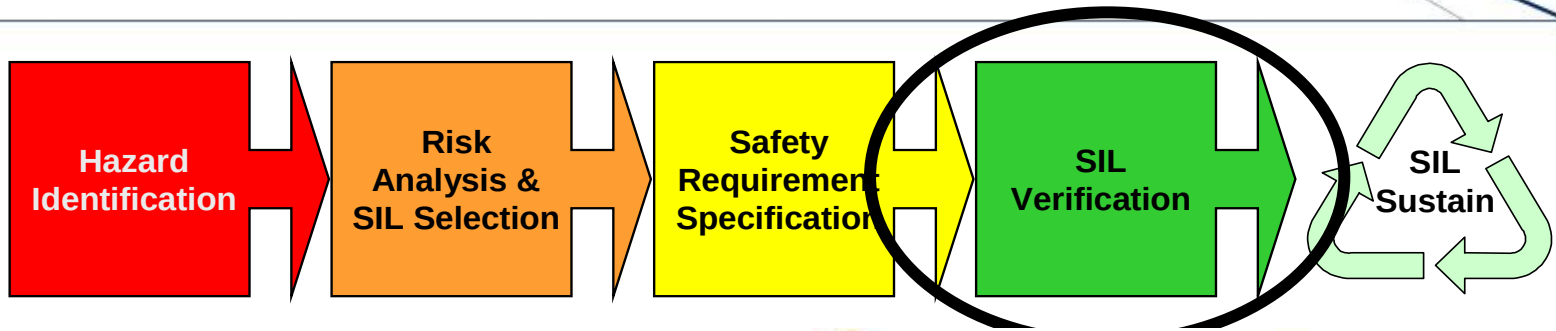
Problema das técnicas de modelagem

Representação e impacto de:

- Todos os elementos da SIF
- *Common Cause*
- Todos os modos de falha
- Todas as recuperações de falha
- Diagnósticos



SLC – Verificação das Probabilidades de Falha



SIL

Random Failure Probability

Safety Integrity Level	Probability of failure on demand (Demand mode of operation)
SIL 4	>=10^{-5} to <10^{-4}
SIL 3	>=10^{-4} to <10^{-3}
SIL 2	>=10^{-3} to <10^{-2}
SIL 1	>=10^{-2} to <10^{-1}

exSILentia

exida

SILCalc

aim asset integrity management

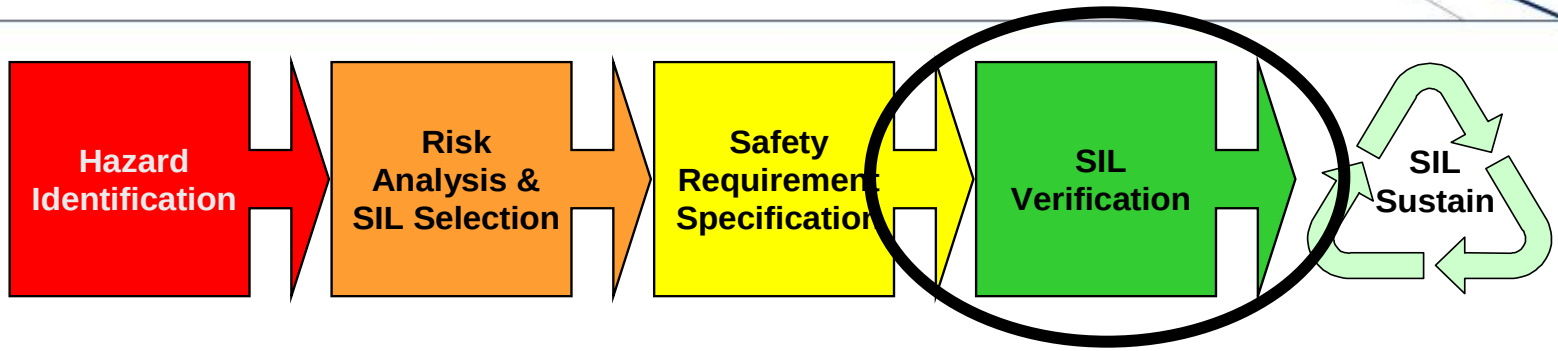
SIL Solver SIS-TECH

SafeCalc

SIL Core SilCore™

exida®

SLC – Detalhamento do Projeto



Detailed Design Documentation - Loop Diagrams, Wiring Diagrams, Logic Diagrams, Panel Layout, PLC Programming, Installation Requirements, Commissioning Requirements, etc.

Melhores Práticas

Considerações no cálculo do PFD_{avg}

Exemplo para a arquitetura 1oo2:

Contribuição de diagnósticos

Falhas só identificadas no PT

Falhas nunca identificadas

$$PFDavg = [2 * (\lambda_{DD})^2 * (MTTR + TI_A/2)^2] + [((\lambda_{DU})^2 * (TI_M)^2) / 3] + [((\lambda_{DN})^2 * Life^2) / 3]$$

$$+ [2 * TD * \lambda_{DU} * (((TI_M/2) + MTTR) / TI_M)] + [\lambda_{DU} * \beta * TI_M/2] + \text{outros…}$$

Degradação devido à bypass

Falhas devido à causa comum

Impactos não quantificáveis

Onde:

TI_A = Intervalo de teste automático
TI_M = Intervalo de teste manual
β = referente à causa comum
TD = Duração do teste

$_{DD}$ = Falha perigosa detectada
$_{DU}$ = Falha perigosa não detectada
$_{DN}$ = Falha perigosa nunca detectada
MTTR = Tempo médio para reparo

exida®

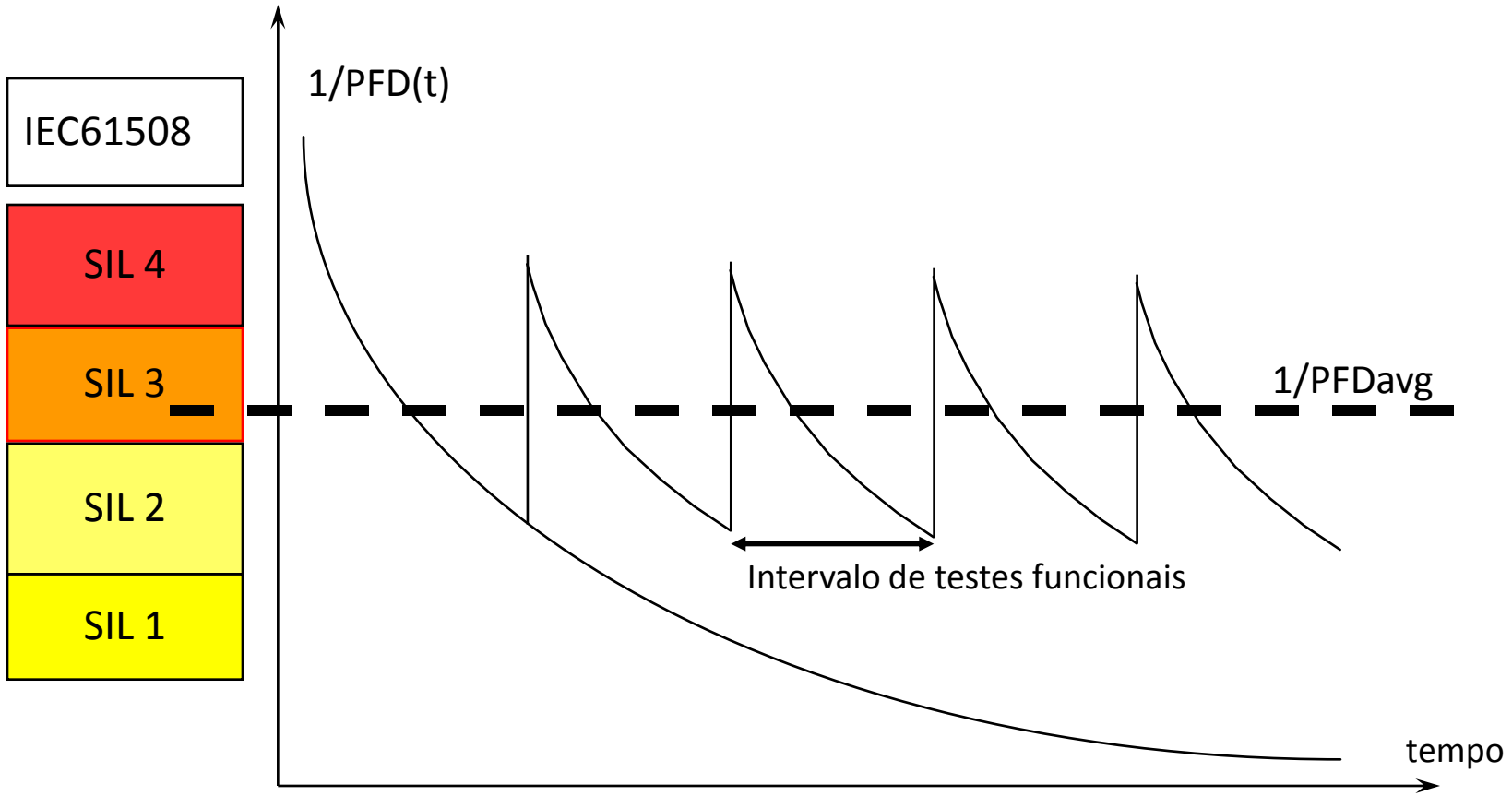
Obs: Fórmulas simplificadas válidas apenas para λ << TI (or MTTF >> TI)

Verificação de SIL

- Informações mínimas:
  - Tempo de campanha
  - Tempo de *start up*
  - MTTR
  - Intervalo de teste
  - Tipo de sensor
  - Tipo de unidade de processamento da lógica
  - Tipo de elemento final
  - Cobertura dos testes periódicos funcionais.

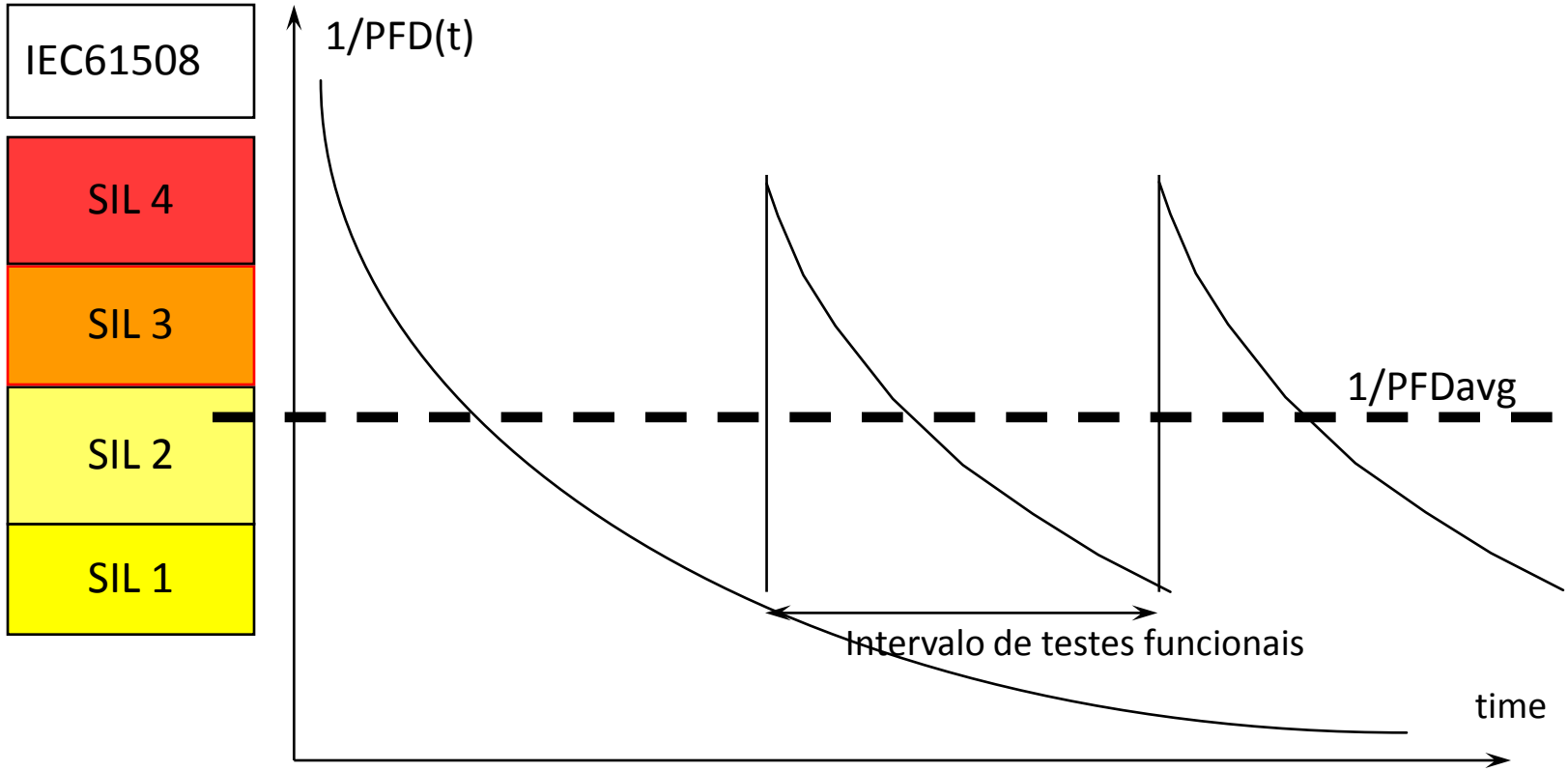
Intervalo de testes funcionais (1)

- Definido durante o detalhamento do projeto.



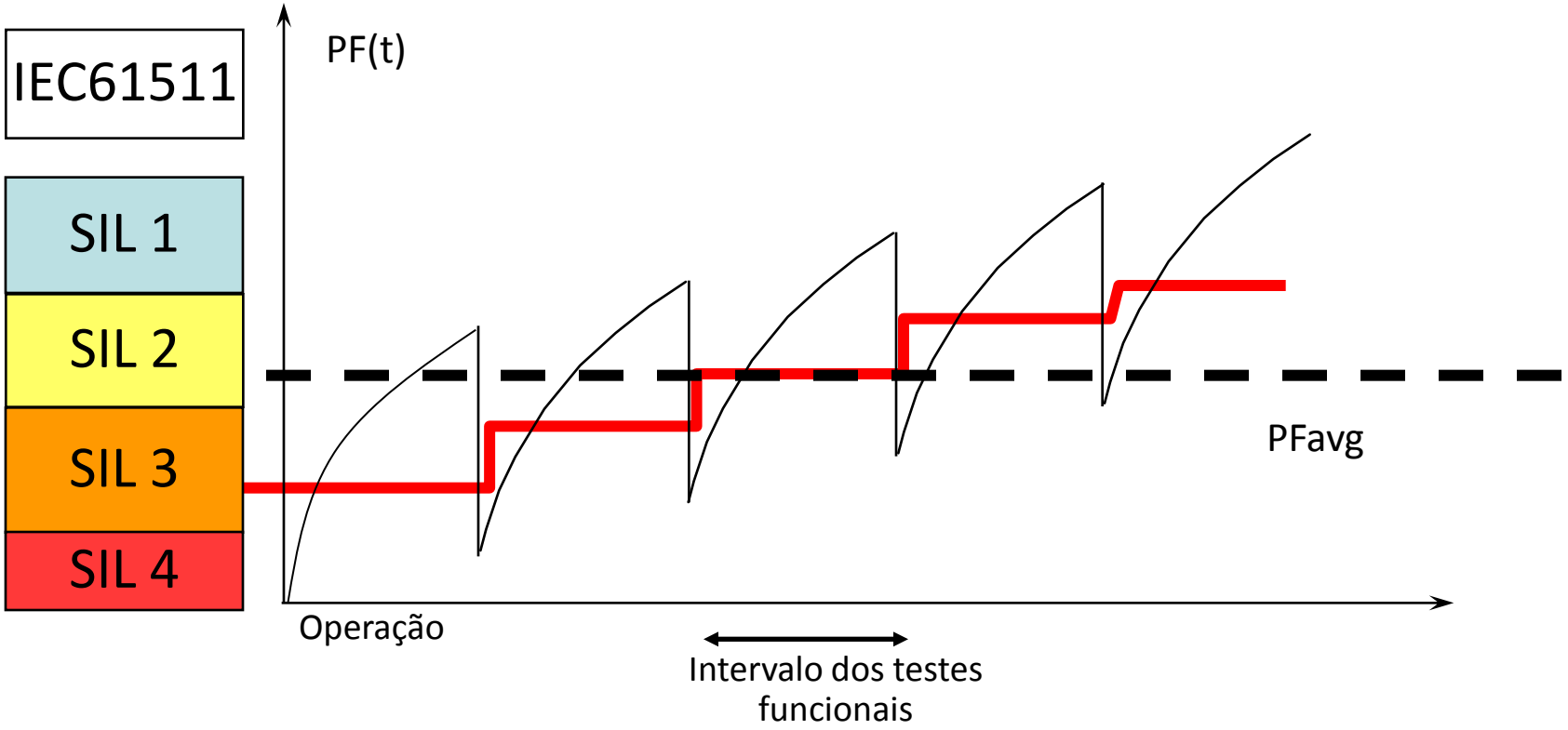
Intervalo de testes funcionais (2)

- Impacto da alteração da freqüência dos testes

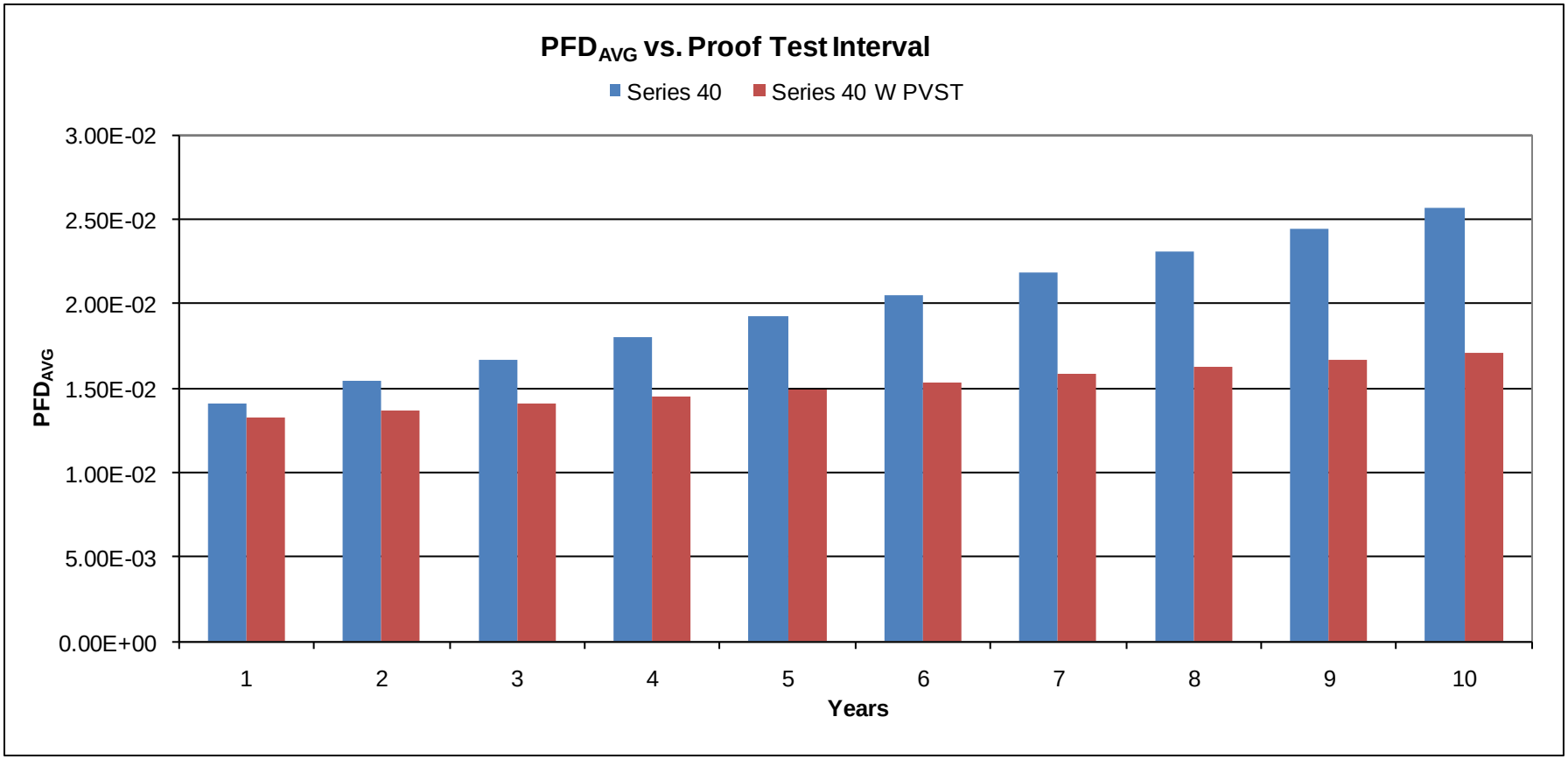


Efeito dos testes incompletos

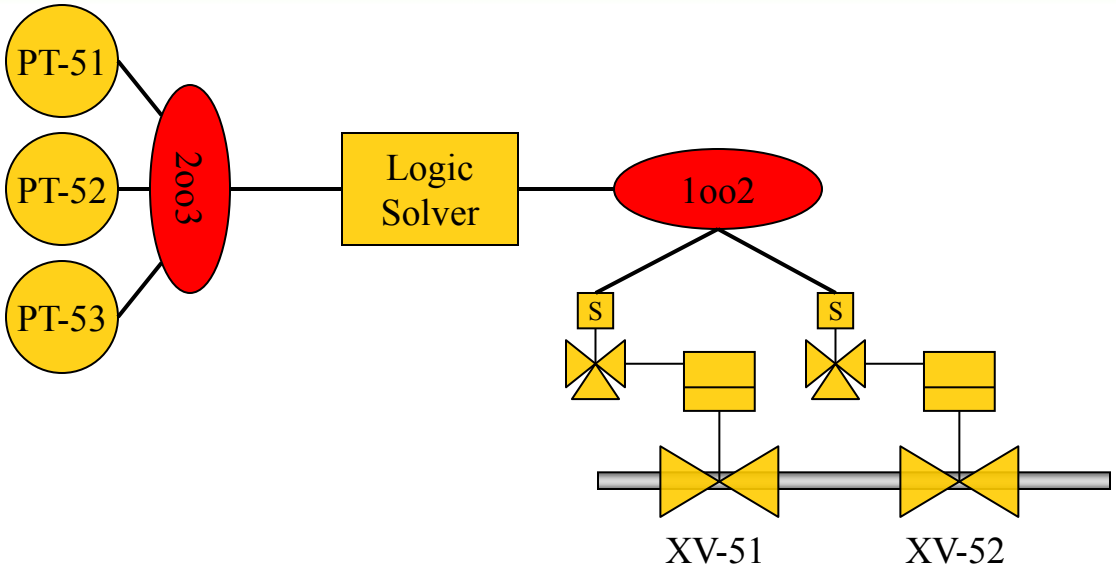
- Cobertura dos testes periódicos funcionais de 100% = todas as possíveis falhas do dispositivo são identificadas.



Diagnósticos *online*



Projeto Conceitual (I)



Item	Risco/Perigo	Descrição	Entradas	Saídas	SIL Alvo
SIF 1	Pressão alta na coluna C-51, com possível sobrecarga para o flare.	Pressão Alta na Coluna C-51 fecha as válvulas de vapor.	PT-51 PT-52 PT-53 (2oo3)	XV-51 Close XV-52 Close (1oo2)	3

Nota: O SIL Alvo e votação de entradas e saídas são apenas exemplos e não devem ser considerados recomendações ou sugestões.

Tolerância à falha do *hardware* - HFT

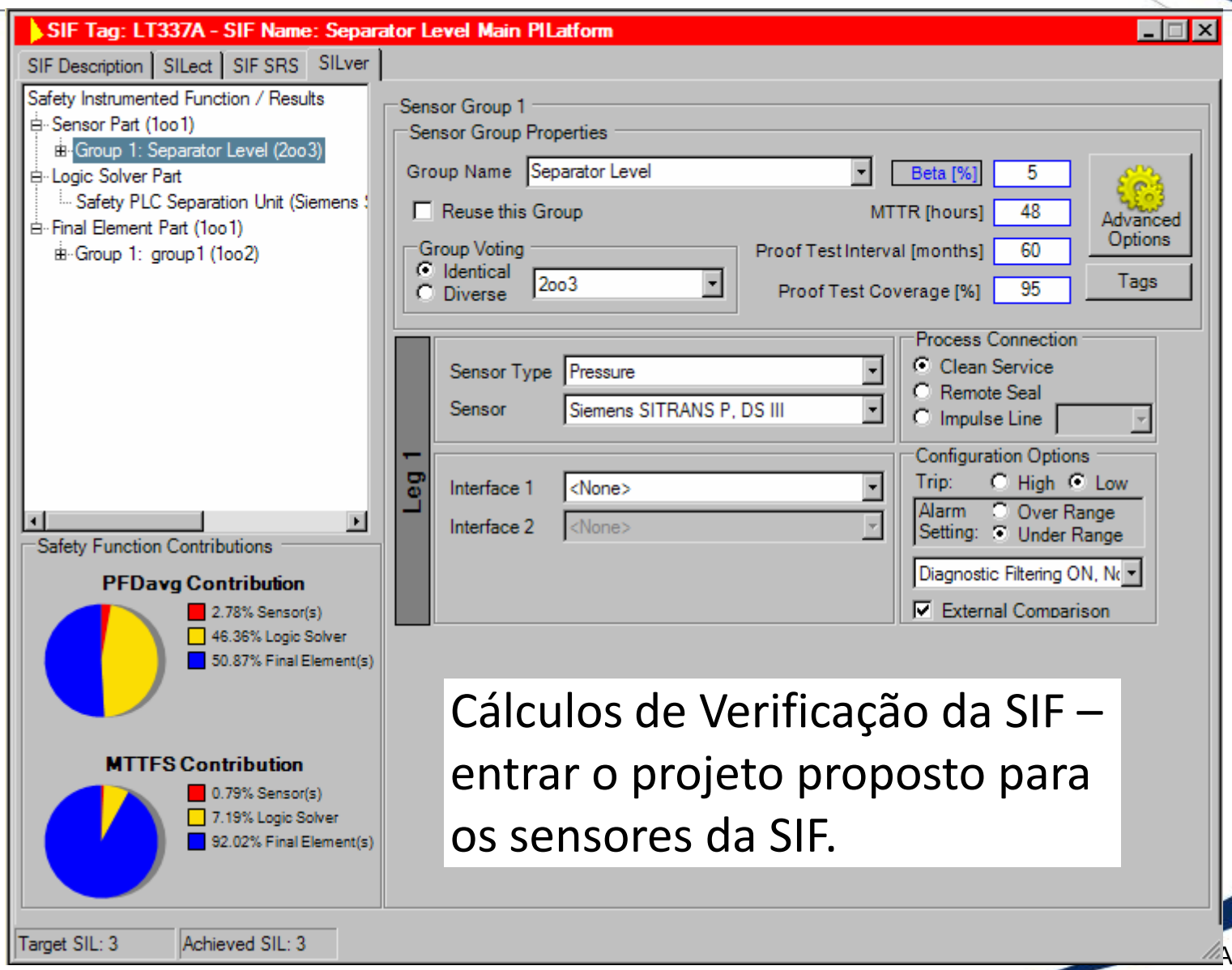
- IEC 61508:
  - Tipo A
  - Tipo B
- IEC 61511:
  - Unidade lógica
  - Elementos de campo

TYPE B

Safe Failure Fraction	Hardware Fault Tolerance		
	0	1	2
< 60 %	Not allowed	SIL 1	SIL 2
60 % - < 90 %	SIL 1	SIL 2	SIL 3
90 % - < 99 %	SIL 2	SIL 3	SIL 4
≥ 99 %	SIL 3	SIL 4	SIL 4

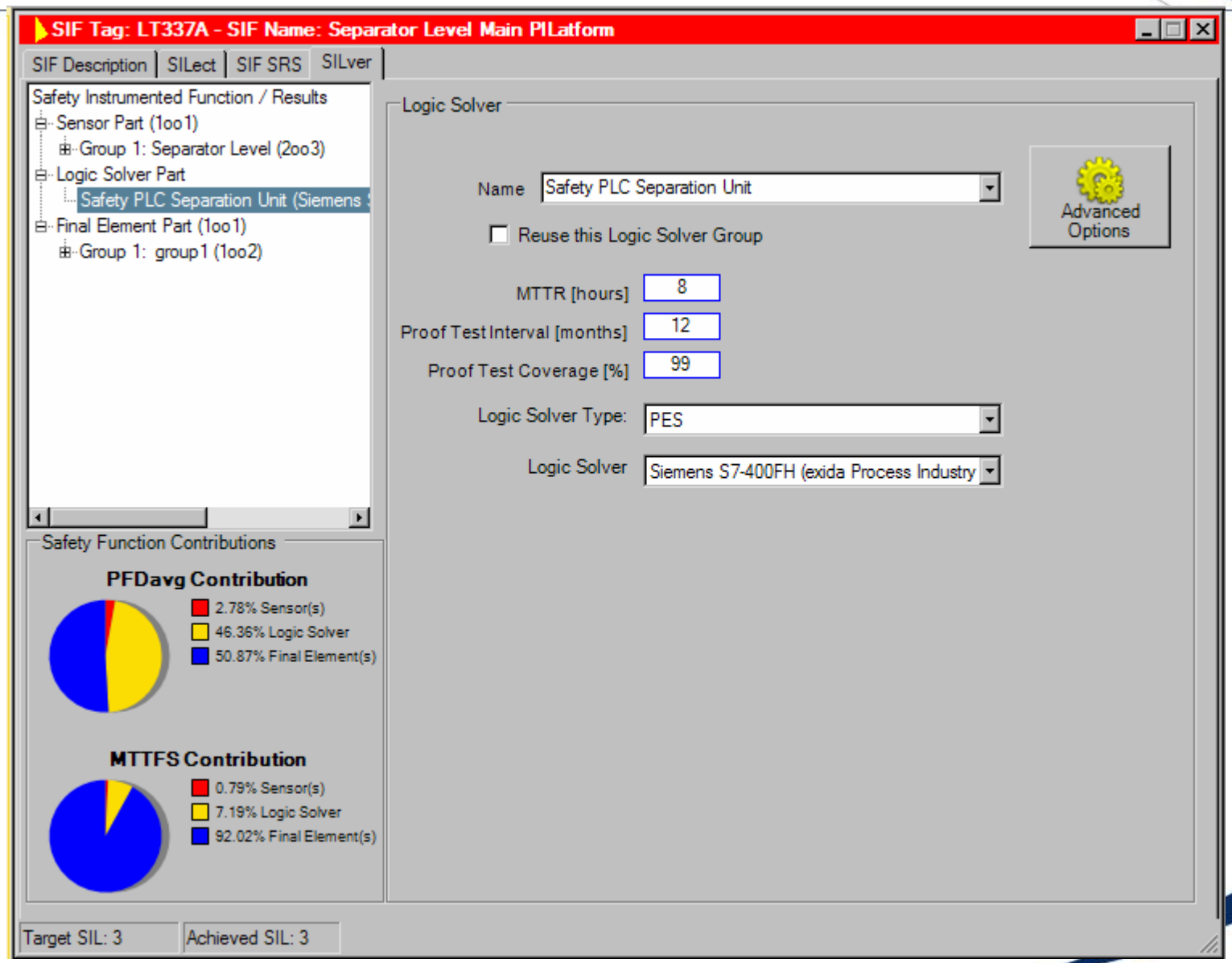
NOTE A hardware fault tolerance of N means that N+1 faults could cause a loss of the safety function

Projeto Conceitual (II) – Sensores

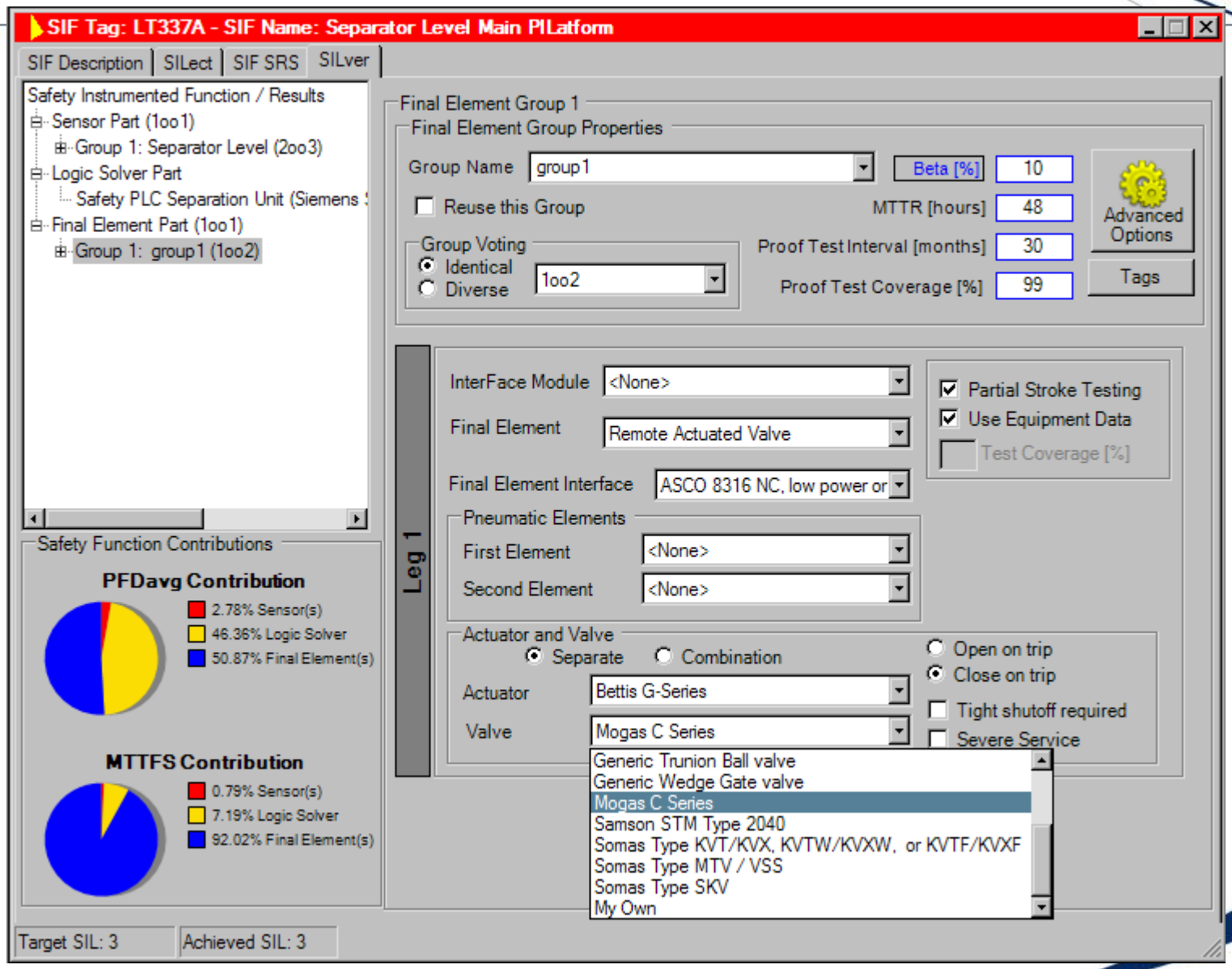


Cálculos de Verificação da SIF – entrar o projeto proposto para os sensores da SIF.

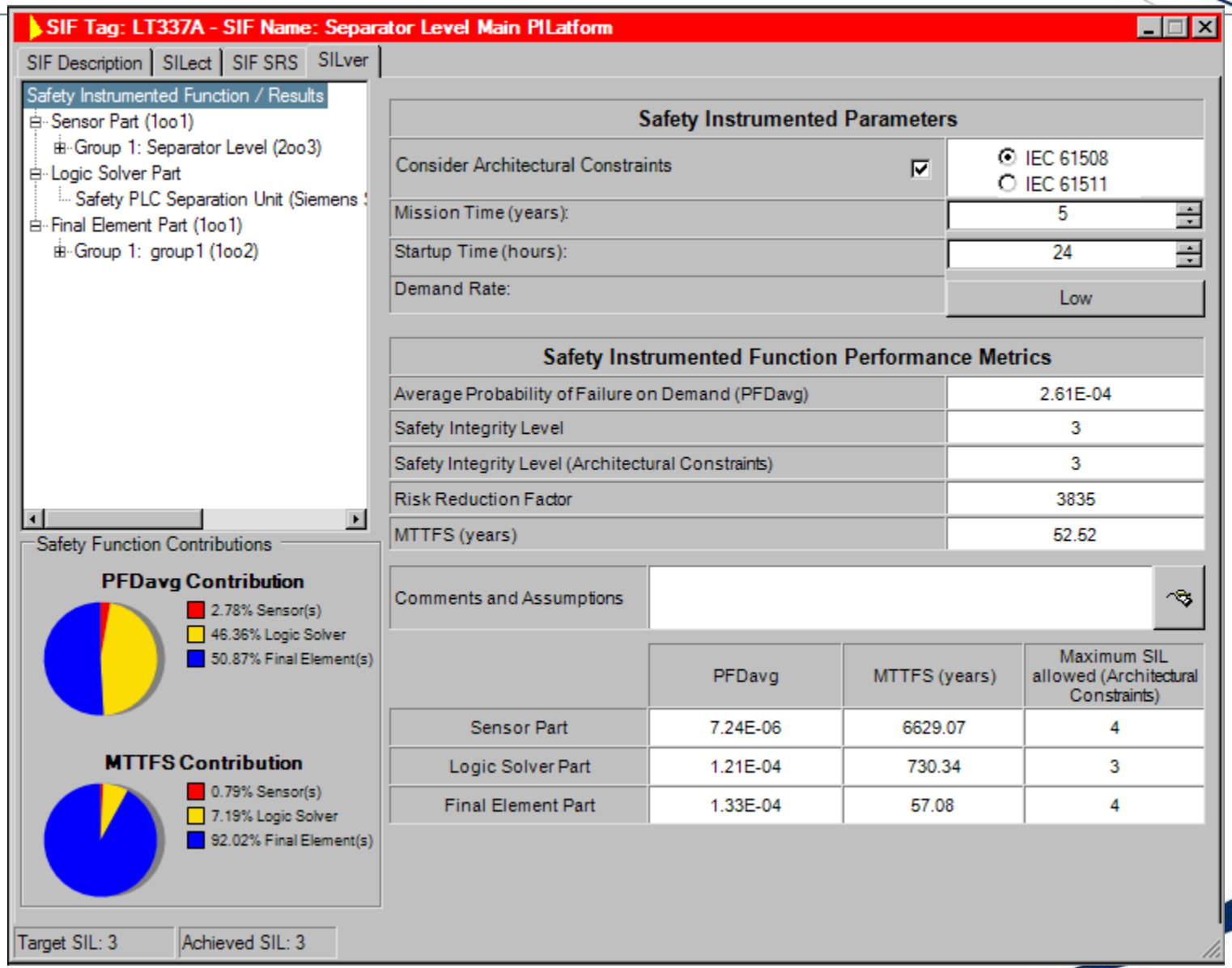
Projeto Conceitual (II) – Unidade Lógica



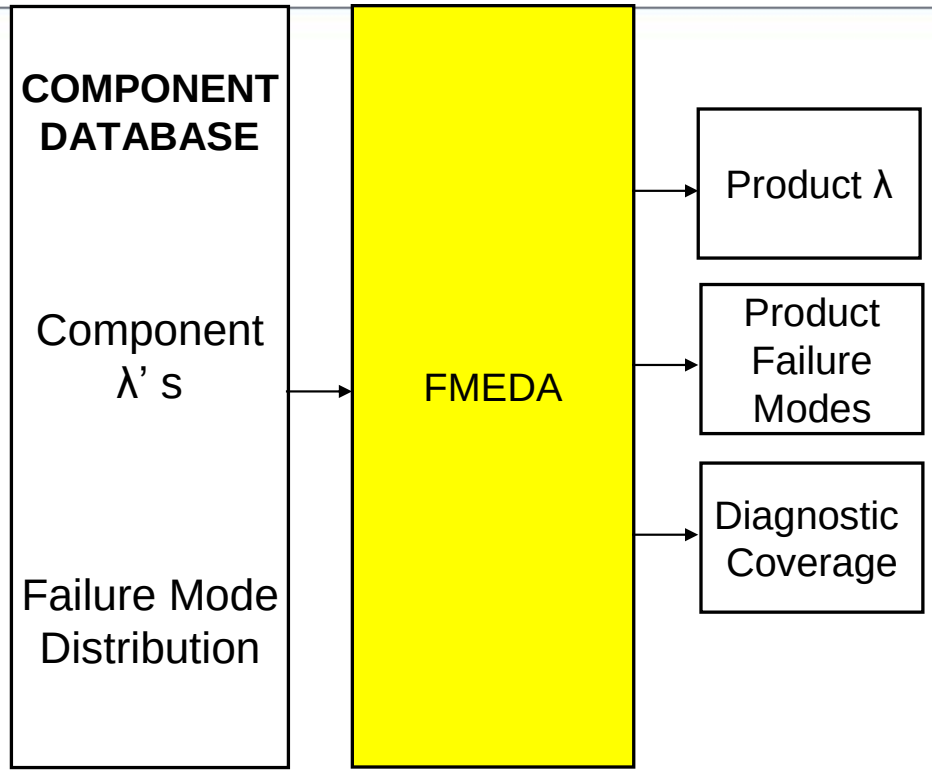
Projeto Conceitual (II) – Elementos Finais



Ciclo de Vida de Segurança



Base de dados de confiabilidade



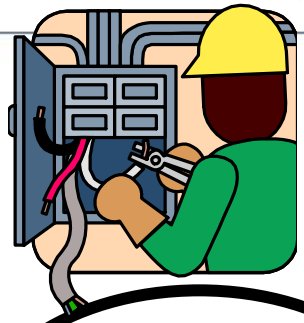
- Utilizando-se base de dados de componentes, taxas de falhas e modos de falhas de um produto (transmissor, módulo de E/S, solenoides, atuadores, válvulas) é possível determinar a confiabilidade do dispositivo do que simplesmente considerar os dados de falha de campo durante a garantia do produto.

Confiabilidade dos dados

	SN 29500	IEC 62380 telecom.	MIL-HDBK 217F
Equation for λ in [1/h]	$\lambda = \lambda_{ref} \cdot \pi_T$	$\lambda = 0.5 \cdot \left(\sum \pi_{T,i} \ldots + 1.4 \cdot 10^{-3} \cdot \sum \pi_{n,i} \ldots\right) \cdot 10^{-9}$	$\lambda = \lambda_b \cdot \pi_R \cdot \pi_Q \cdot \pi_E$
λ_{ref} [FIT]	**0.3**	Mission profile with cycles per year, here: perm. working	**1.2** with T = 40 °C and Stress = 0.5
π_T	**1** (at reference temp. = 55 °C)	$\pi_{T,avg=40\,°C}$ = **0.0014**	**---**
π_R (Resistance factor)	**---**	**---**	**1.0**
π_n (Variation factor per phase)	**---**	π_n = **0**, (da ΔT = 0)	**---**
π_Q (Quality factor)	**---**	**---**	**1.0**
π_E (Environment fac.)	**---**	**---**	**2.0** (ground fixed)
result [FIT]	**0.3**	**0.0007**	**2.4**

FIT: Failure in Time, 10^{-9} 1/h

SLC – Operação e Manutenção



Hazard Identification → Risk Analysis & SIL Selection → Safety Requirement Specification → SIL Verification → SIL Sustain

PERD

CCPS Center for Chemical Process Safety — An AIChE Industry Technology Alliance

- Operational Procedures
- Maintenance Procedures
- Proof Test Procedures

SIL Stat

SILLife

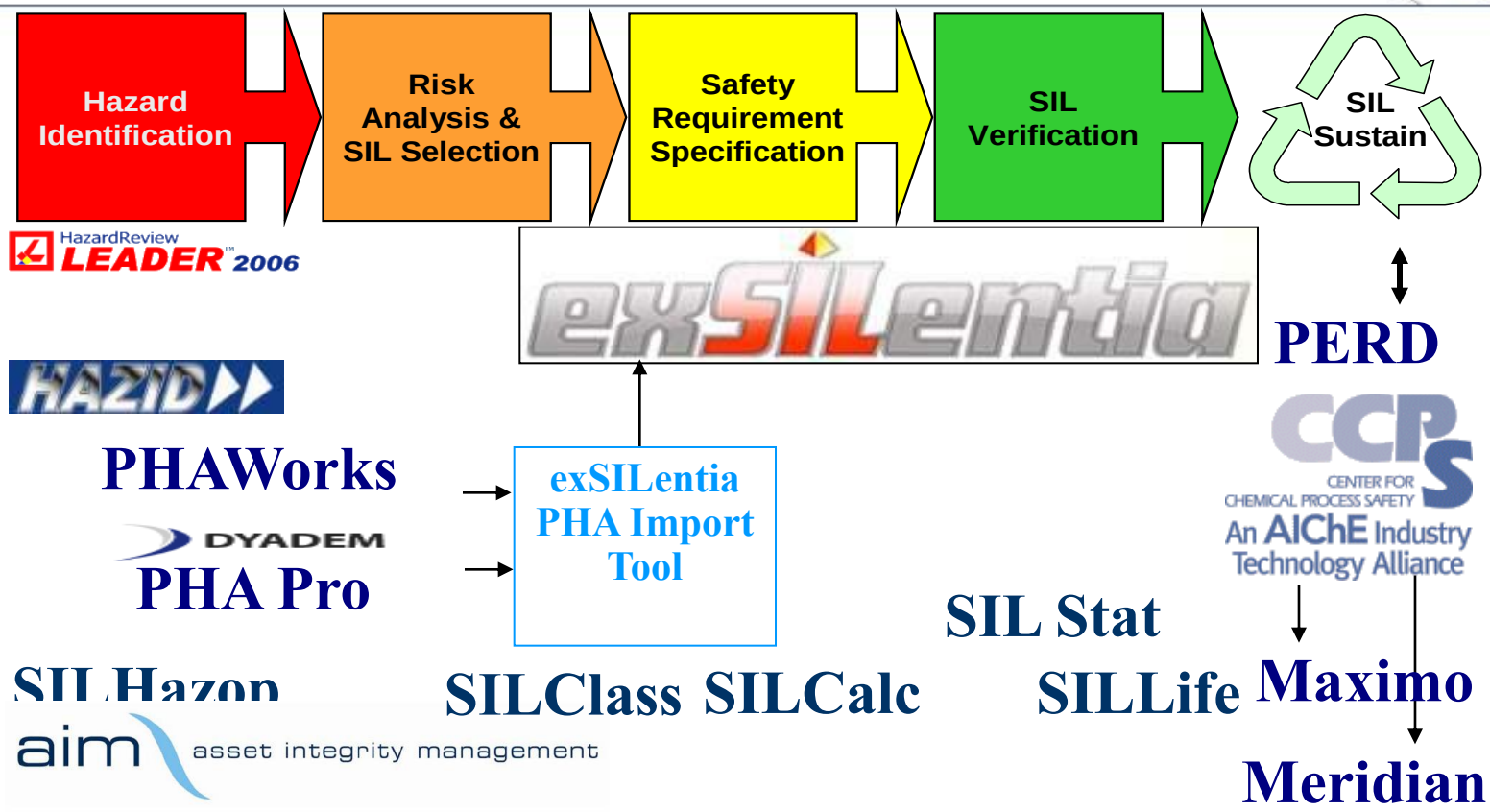
Maximo

aim asset integrity management

Meridian

exida®

Fatores de Sucesso (1) - Ferramentas de Apoio



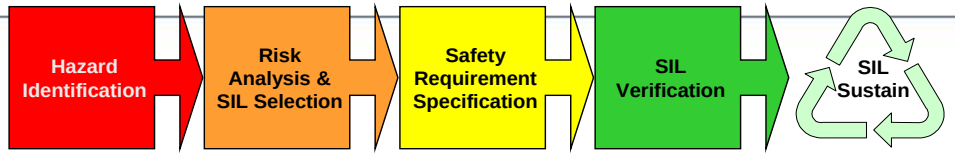
Diversas ferramentas de engenharia desenvolvidas por diferentes empresas para reduzir o número de horas de engenharia, melhorar a documentação e aumentar consistência dos projetos.

Futuro das Ferramentas de Apoio ao SLC

Operação Integrada:
Comissionamento e intervalo de testes da SIF

Fatores de Sucesso (2) - Competência de Profissionais

Diretrizes de Competência dos Profissionais envolvidos



Competência da Equipe

"…ensuring that applicable parties involved in any of the overall E/E/PE or software safety lifecycle activities are competent to carry out activities for which they are accountable."
-IEC 61508, Part 1, Paragraph 6.2.1 (h)

"Persons, departments, or organizations involved in safety lifecycle activities shall be competent to carry out the activities for which they are accountable."
-IEC 61511, Part 1, Paragraph 5.2.2.2

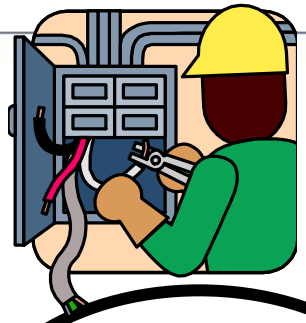
Requisitos do Programa de Competência

Exemplo da descrição de dois níveis de competência:

TABLE 2 Assessed Competencies

Area	Basic Requirements	Typical/Allowed Basic Tasks	Senior Requirements	Typical/Allowed Senior Tasks
User Hazard Identification / Process HAZOP	1) Hold a CFSP or CFSE Certificate. 2) Have read and understood the IEC 61508 and 61511 sections on process hazards analysis, the overall safety lifecycle and documentation. 3) Have read and understood relevant *exida* training, textbook and best practice material on Hazard identification and HAZOPs 4) Have read and understood at least 1 detailed Hazard Identification report.	Act as scribe or other basic participant in a hazard identification / HAZOP workshop. Prepare draft hazard identification documentation under the guidance of a Senior competent person in this area.	1) Hold a CFSE certificate. 2) Have read and understood relevant *exida* training, textbook and best practice material on Hazard identification and HAZOPs. 3) Have substantially participated in at least 2 hazard identification or Process HAZOP activities.	Coordinate and facilitate hazard identification workshops Independently prepare draft hazard identification documentation Review draft hazard identification documentation prepared by others prior to formal issue.

SLC – Operação e Manutenção



Hazard Identification → Risk Analysis & SIL Selection → Safety Requirement Specification → SIL Verification → SIL Sustain

- Operational Procedures
- Maintenance Procedures
- Proof Test Procedures

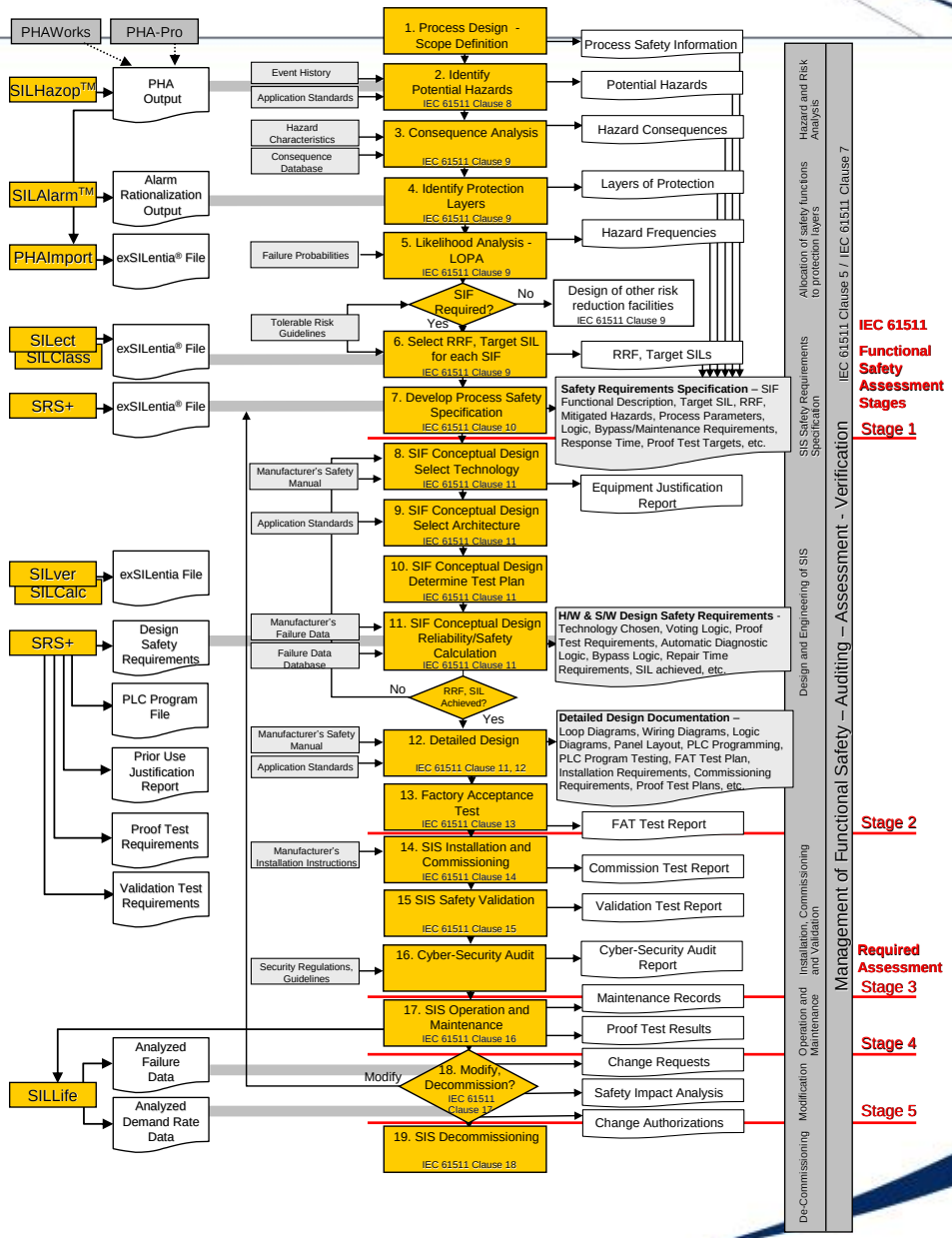
Operação & Manutenção

- Fase mais longa do SLC

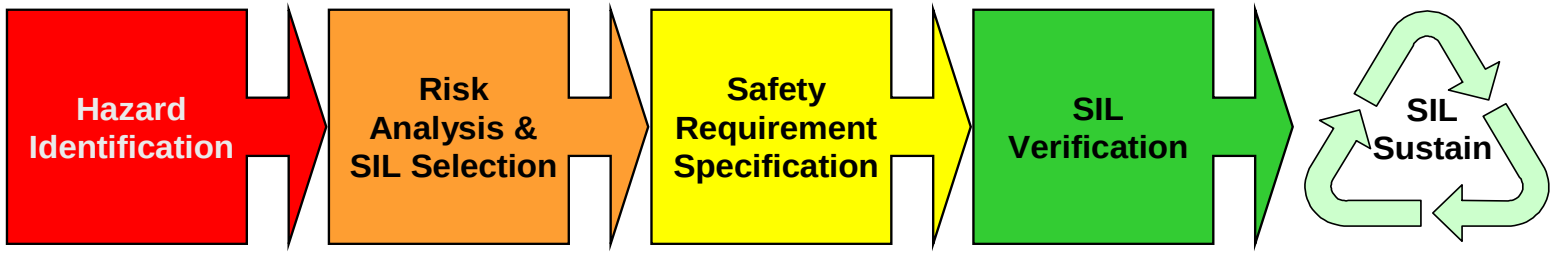
- Fatores críticos:
  - Plano de manutenção e registro das manutenções
  - Intervalo de testes funcionais
  - Cobertura dos testes periódicos
  - Gerenciamento das mudanças após partida
  - Procedimentos de bypass, reset
  - Considerações dos requisitos ambientais
  - Reavaliação periódica do projeto

Gerenciamento da Segurança e o SLC

- Define as atividades exigidas pela norma e melhores práticas;
- Define a documentação necessária para manter o SIS;
- Foco na comunicação entre as áreas e entre as fases do projeto;
- Trata a exposição do sistema, controle de acesso - *cybersecurity*;
- Auditorias periódicas para assegurar que o ciclo foi seguido.



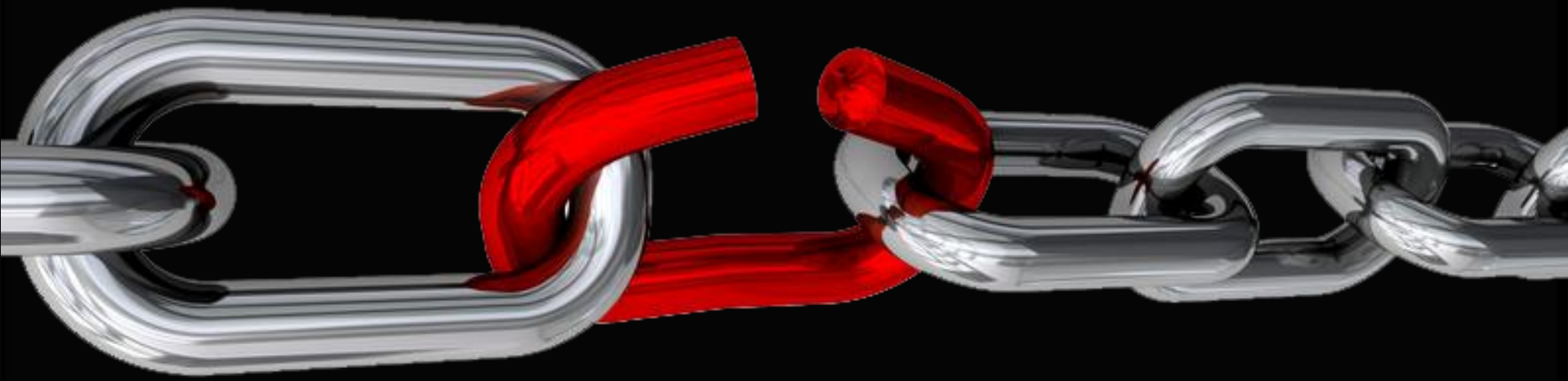
Conclusão



- O Ciclo de Vida de Segurança proposto pela ISA 84.01 / IEC 61511 pode resultar uma boa relação de custo x benefício. Os principais fatores de sucesso são:
  1. Gerenciamento das Funções de Segurança
     a. Procedimentos
     b. Ferramentas auxiliares
  2. Competência dos profissionais envolvidos

www.exida.com

Monica Hochleitner - monica@exida.com



A segurança de um sistema é tão forte quanto o seu elo mais fraco

exida