



Setting the Standard for Automation™

Ferramentas de auxílio ao Ciclo de Vida de Segurança

Standards

Certification

Education & Training

Publishing

Conferences & Exhibits

- ◆ 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 Fallner
Germany
+49 89 4900 0547

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

Excel
Mr. Da...
Singapore/M...
+65 68...

Ex
Jon I...
United I...
+44 24 76...

Exida C
David I...
+ 1 647 838 3377

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

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...
+64 3 4...

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

Pacific
eter Clark
ong Kong
222-5160

om LLC
am Goble
ellersville
453 1720

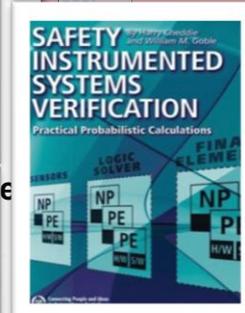
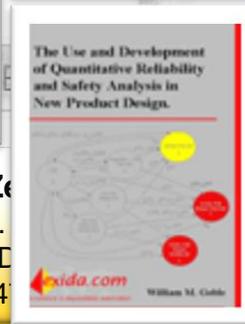
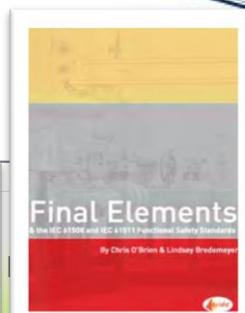
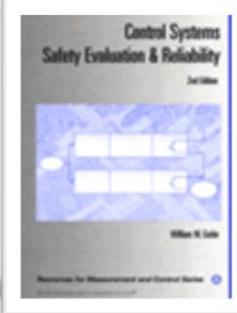
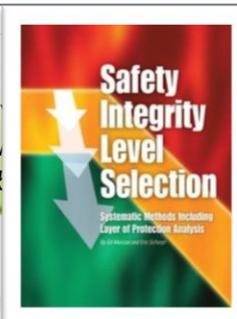
Region)
urt Miller
Houston
439 3793

Mexico
Esparza
Mexico
611 9858

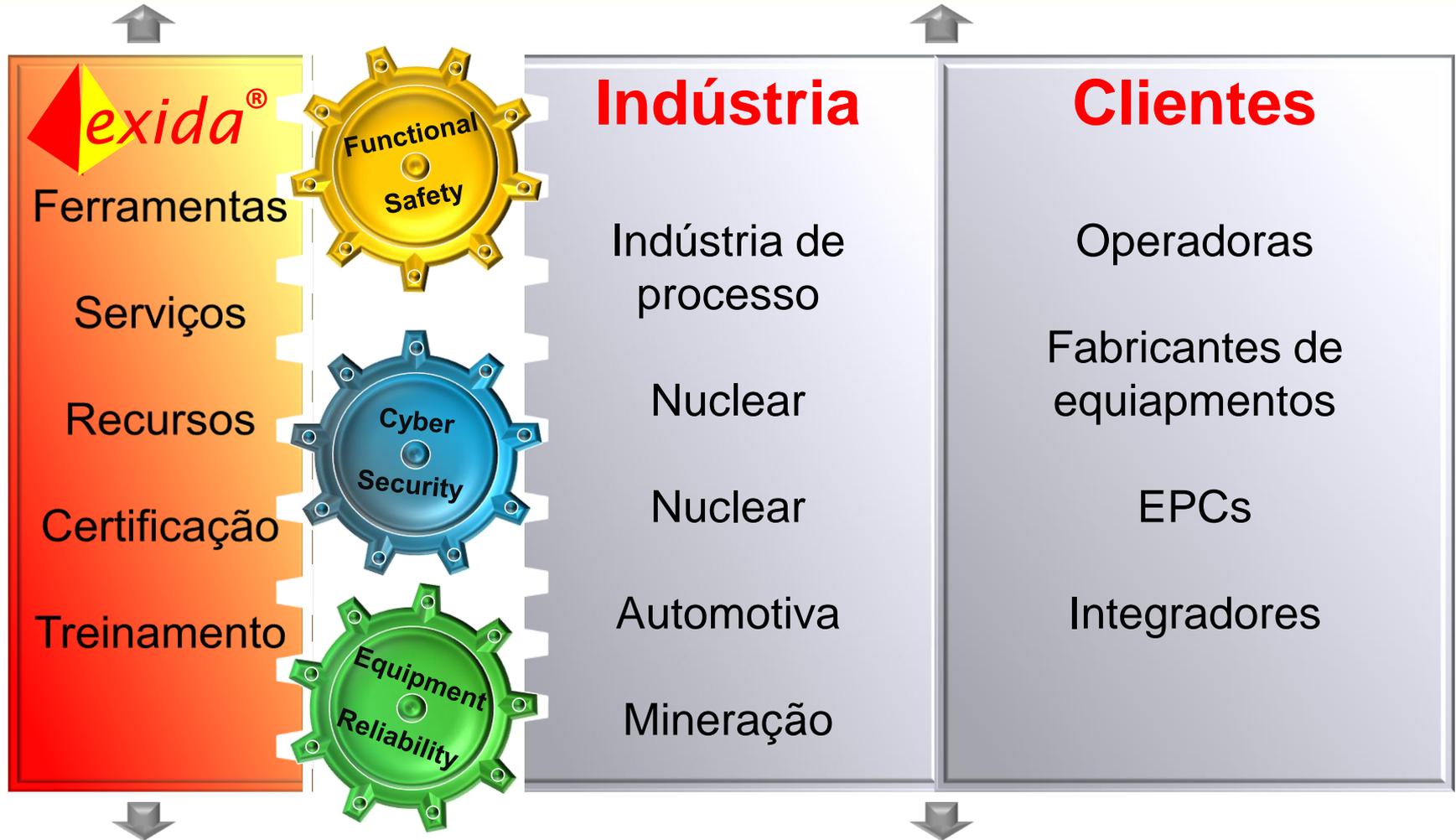


exida
Certification S.A.

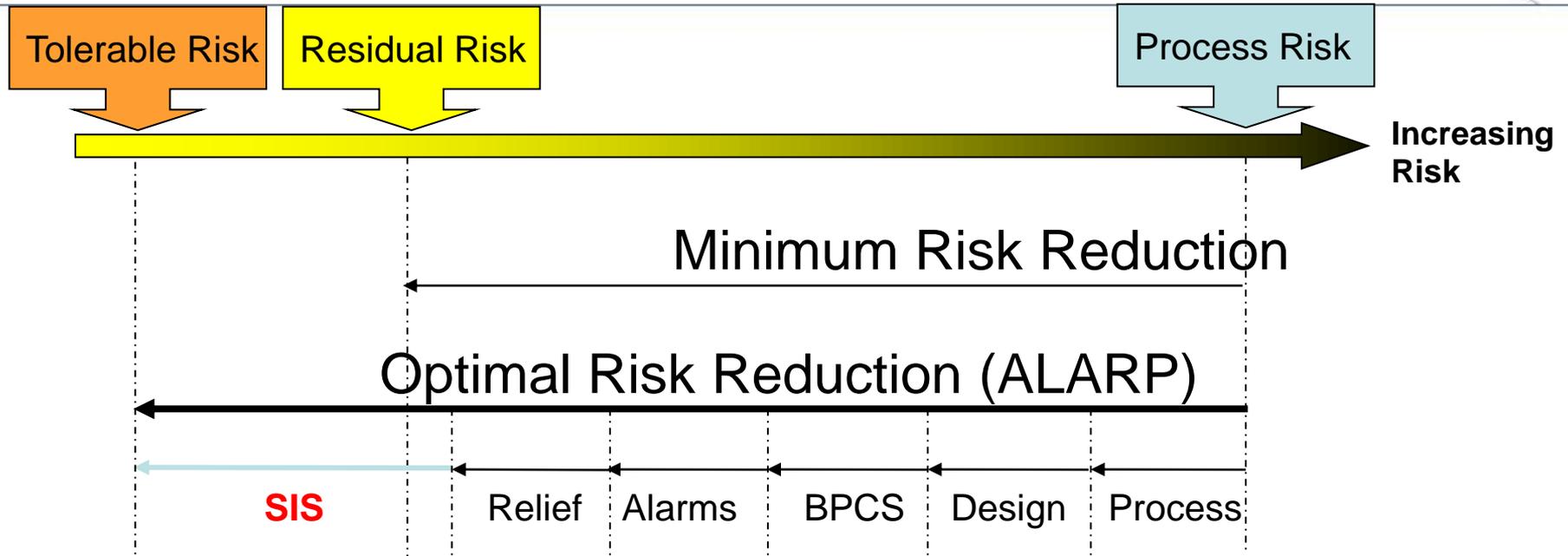
HEADQUARTERS SERVICE C



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



- ◆ 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.

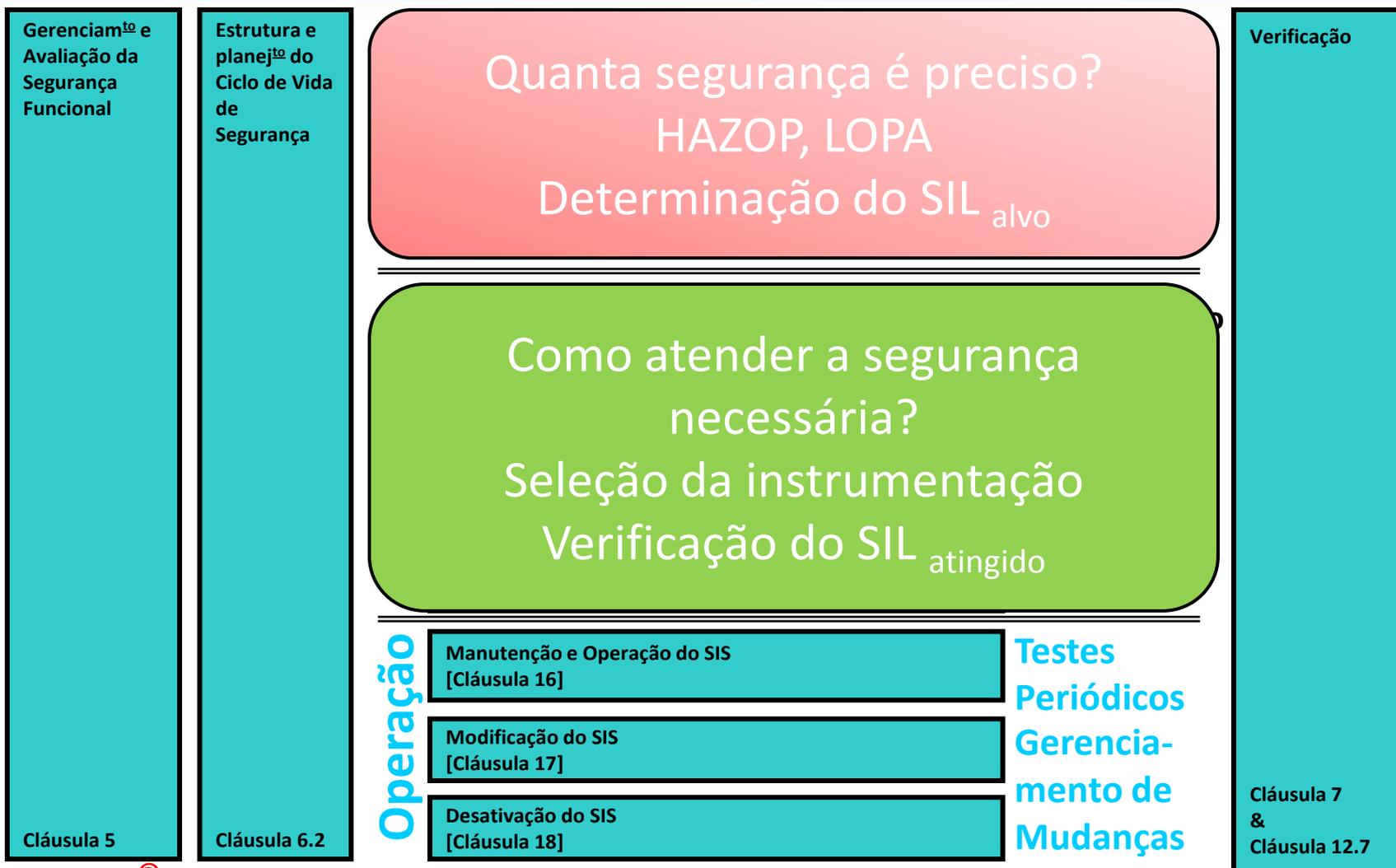


- ◆ Ciclo de Vida de Segurança (SLC); e
- ◆ Projeto baseado em desempenho (SIL).

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	$\geq 10^{-5}$ a $< 10^{-4}$
SIL 3	10000 a 1000	$\geq 10^{-4}$ a $< 10^{-3}$
SIL 2	1000 a 100	$\geq 10^{-3}$ a $< 10^{-2}$
SIL 1	100 a 10	$\geq 10^{-2}$ a $< 10^{-1}$

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





Gerenciamento e
Avaliação da
Segurança
Funcional

Estrutura e
planejamento do
Ciclo de Vida
de
Segurança

Quanta segurança é preciso?
HAZOP, LOPA
Determinação do SIL_{alvo}

Como atender a segurança
necessária?
Seleção da instrumentação
Verificação do SIL_{atingido}

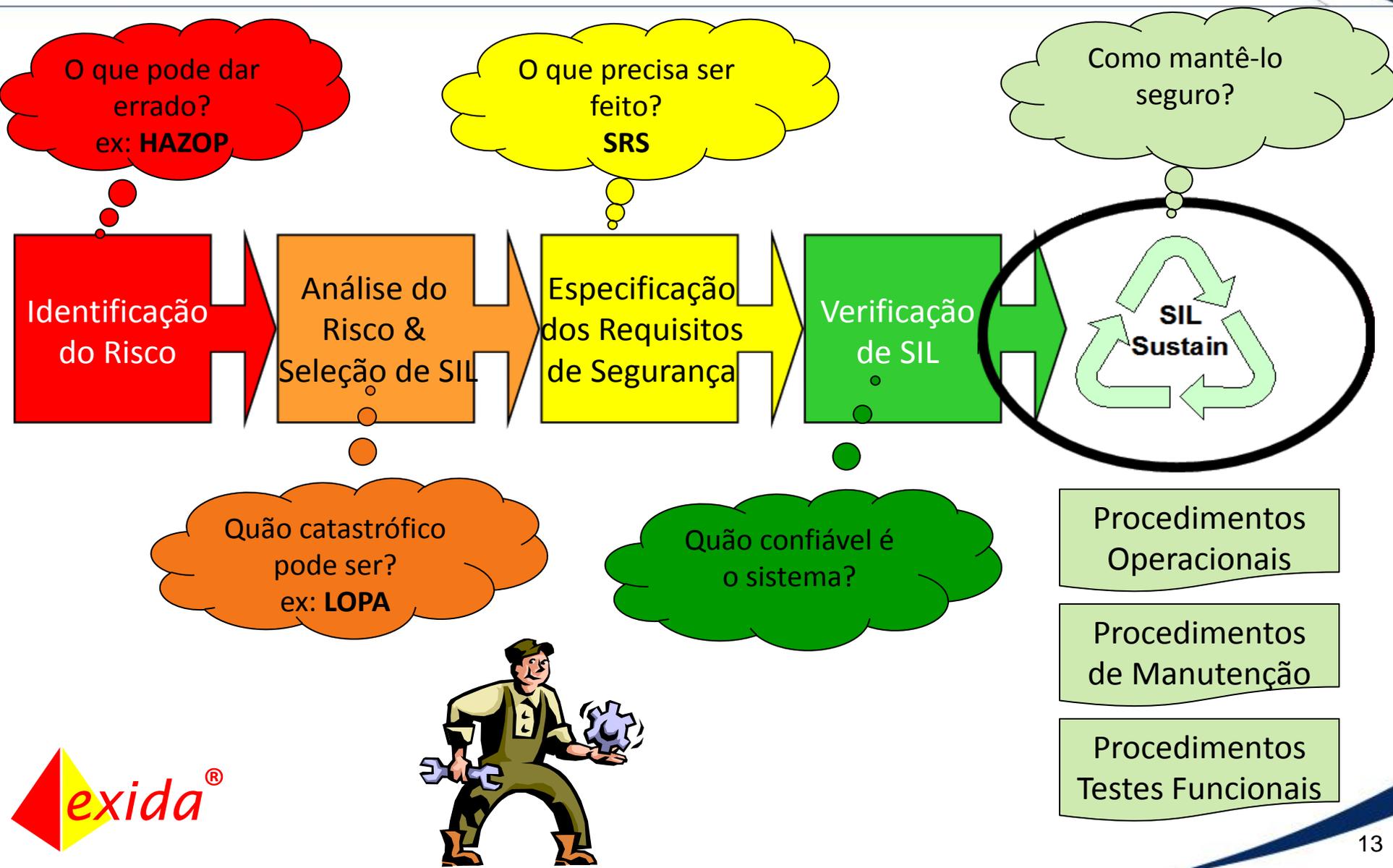
Como manter o SIL?
Testes funcionais periódicos
MOC e Revalidação dos riscos

Verificação

Cláusula 5

Cláusula 6.2

Cláusula 7
&
Cláusula 12.7



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**

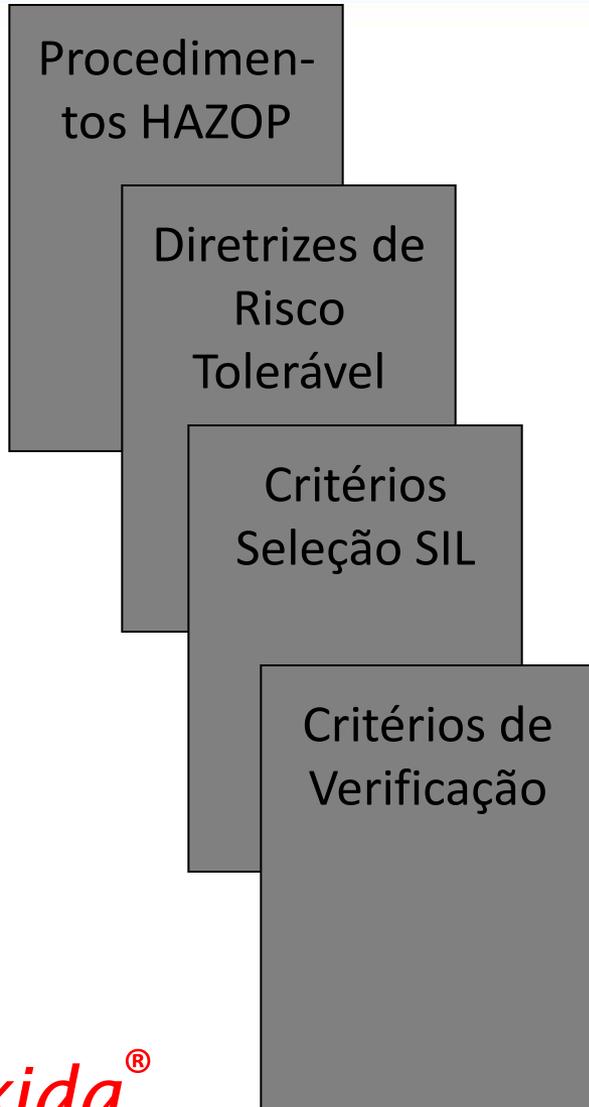
OPERAÇÃO MANUTENÇÃO

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



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



Hazard Consequences

Hazard Frequencies

Quais são os perigos do processo?

SIL Verification

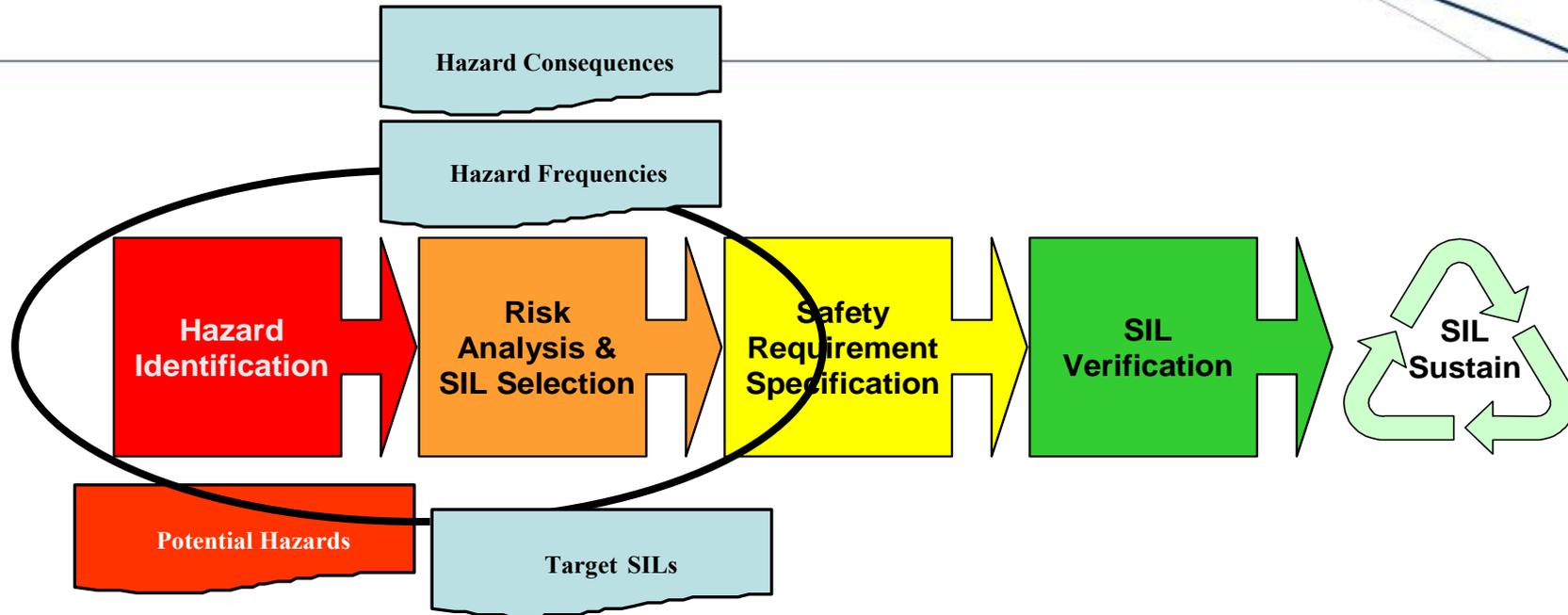
SIL Sustain

Quão seguro é o processo?

SIL

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



PHAWorks

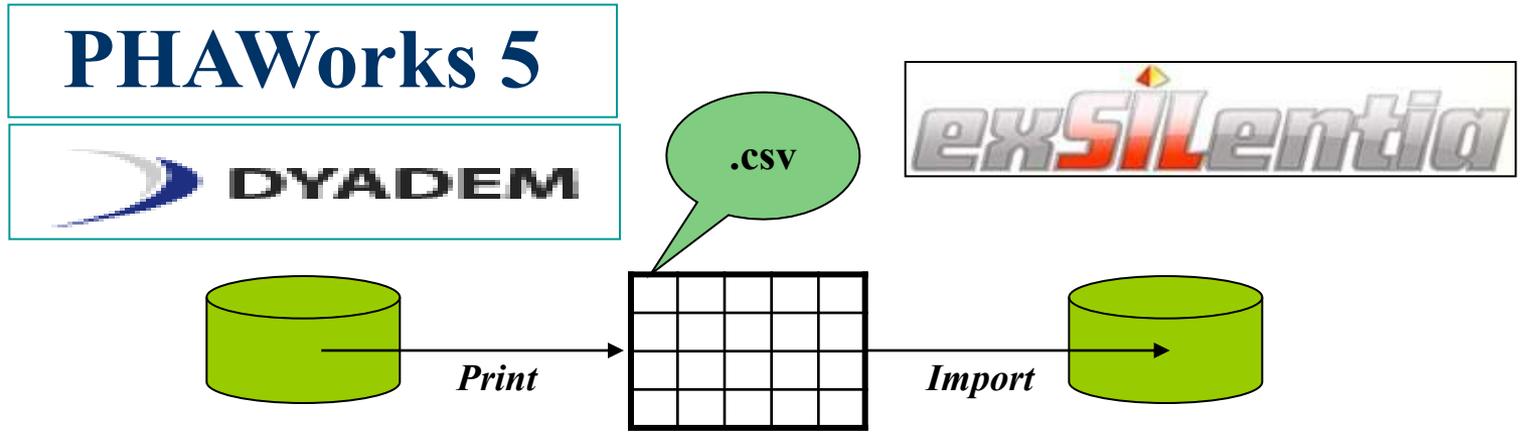


SILHazop

SILClass



Opções de Importação/Exportação de SIF



Critérios de Risco Tolerável



Tolerable Risk Calibration Wizard - Frequency Based Targets

Tolerable Risk Calibration - Single tolerable risk quantitative

Include the following risk categories:

- | | | | |
|--|------------|-------------------------------------|-------------|
| <input checked="" type="checkbox"/> Personnel | 1 fatality | <input type="text" value="100000"/> | year(s) |
| <input checked="" type="checkbox"/> Environmental Impact | | <input type="text" value="50000"/> | SK per year |
| <input checked="" type="checkbox"/> Equipment Damage | | <input type="text" value="1"/> | SM per year |

Target SIL Threshold Ratio (1-10)

SIL Threshold example:

Assume a calculated Required Risk Reduction Factor of 29, which would fall in the 10 - 100 Risk Reduction range.

With a SIL Threshold Ratio of 1, a calculated Risk Reduction Factor of 29 would result in a Target SIL of SIL 2.

The calculated Risk Reduction Factor is in this case greater than the SIL determination threshold which lies at 10 ($10 * 1$).

With a SIL Threshold Ratio of 3, a calculated Risk Reduction Factor of 29 would result in a Target SIL of SIL 1.

The calculated Risk Reduction Factor is in this case less than the SIL determination threshold which lies at 30 ($10 * 3$).

Cancel

<< Back

Next >>

Finish

Análise de Camadas de Proteção



SIF: LT337A - Project: Example 1 (61508 Course)

SIF Description | SILEct | SIF SRS | SILver

Severity Level Selections

Personnel	Single Fatality
Environment (\$K)	0
Equipment (\$M)	100000

Edit	Initiating Event		Description	Probability			Frequency (1/year)
Add	Del	<< >>	Control Failure	1			0.02
Enabling Condition							
Independent Layers of Protection			Description	Personnel	Environment	Equipment	
Add							
Delete							
Edit							

Calculated Results		Personnel	Environment	Equipment
Sum Unmitigated Event Frequencies (1/yr)		2.00E-02	2.00E-02	2.00E-02
Tolerable Frequencies (1/yr)		1.00E-05	---	1.00E-05
Required Risk Reduction		2000	---	2000
Required SIL		3		

Target SIL: 3 | Achieved SIL: TBD



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.

Tolerable Risk Calibration Wizard - Risk Graph

Personnel Safety

- CA: W3=a, W2=a, W1=a
- CB: FA=1, PB=a, FB=2, PA=1, FA=2, PB=a
- CC: FA=3, PB=2, FB=3, PA=2, FA=3, PB=2
- CD: FA=3, PB=3, FB=3, PA=3

Monetary Loss

- M1: W3=a, W2=a, W1=a
- M2: W3=1, W2=a, W1=a
- M3: W3=2, W2=1, W1=a
- M4: W3=3, W2=2, W1=1
- M5: W3=3, W2=3, W1=2

Environment Loss

- E1: W3=a, W2=a, W1=a
- E2: W3=1, W2=a, W1=a
- E3: W3=2, W2=1, W1=a
- E4: W3=3, W2=2, W1=1
- E5: W3=3, W2=3, W1=2

Classification

- (C) Consequences if Fail on Demand
- CA=Minor Injury
- CB=Severe Injury/One Death
- CC=Several Deaths
- CD=Many Deaths/Catastrophe
- (F) Presence in the Danger Zone
- FA=Seldom to Frequently
- FB=Frequently to Continuously
- (P) Probability to avert Hazard
- PA=Under Certain Circumstances
- PB=Almost Impossible
- (W) Demand Rate
- W1=Very Low (10 to 100 years)
- W2=Low (1 to 10 years)
- W3=High (<1 year)
- (M) Monetary Loss
- M1=Minor \$10K to \$100K, < 1 day
- M2=Moderate \$100K to \$1M, 1-5 days
- M3=Major \$1M to \$6M, 5 - 15 days
- M4=Extensive \$6M to \$12M, 15 - 30 d
- M5=Catastrophic > \$12M, > 30 days

Buttons: Cancel, << Back, Next >>, Finish

SIF: SIF 001 - Project: Sample Project [Imported] (P001)

SIF Description | SILect | SIF SRS | SILver

Hazard Matrix

Demand Rate: [D3] 0.5 to 4 years

Health & Safety: [C2] Minor Injury

Economics: [C3] Local Damage (\$100K to \$1M)

Environment: [C3] Localized Effect

Comments and Assumptions: Tolerable Risk Guidelines per company procedures

Calculated Results

SIL Health & Safety	SIL Economics	SIL Environment	Target SIL
1	2	2	2

Target SIL: 2 | Achieved SIL: 1

Hazard Matrix

	C1	C2	C3	C4	C5
D5	2	3	4	b	b
D4	1	2	3	4	b
D3	a	1	2	3	4
D2	--	a	1	2	3
D1	--	--	a	1	2



Seleção de SIL



Tolerable Risk Calibration Wizard - Hazard Matrix

Demand Frequency: D5 (< 0.1 years), D4 (0.1 to 0.5 years), **D3 (0.5 to 4 years)**, D2 (4 to 20 years), D1 (> 20 years)

Safety Integrity Level Matrix:

2	3	4	b	b
1	2	3	4	b
a	1	2	3	4
-	a	1	2	3
-	-	a	1	2

Consequence Category: C1, C2, C3, **C4**, C5

Buttons: Cancel, << Back, Next >>, Finish

Frequência estimada da demanda:

- Pressão alta a cada 3 anos

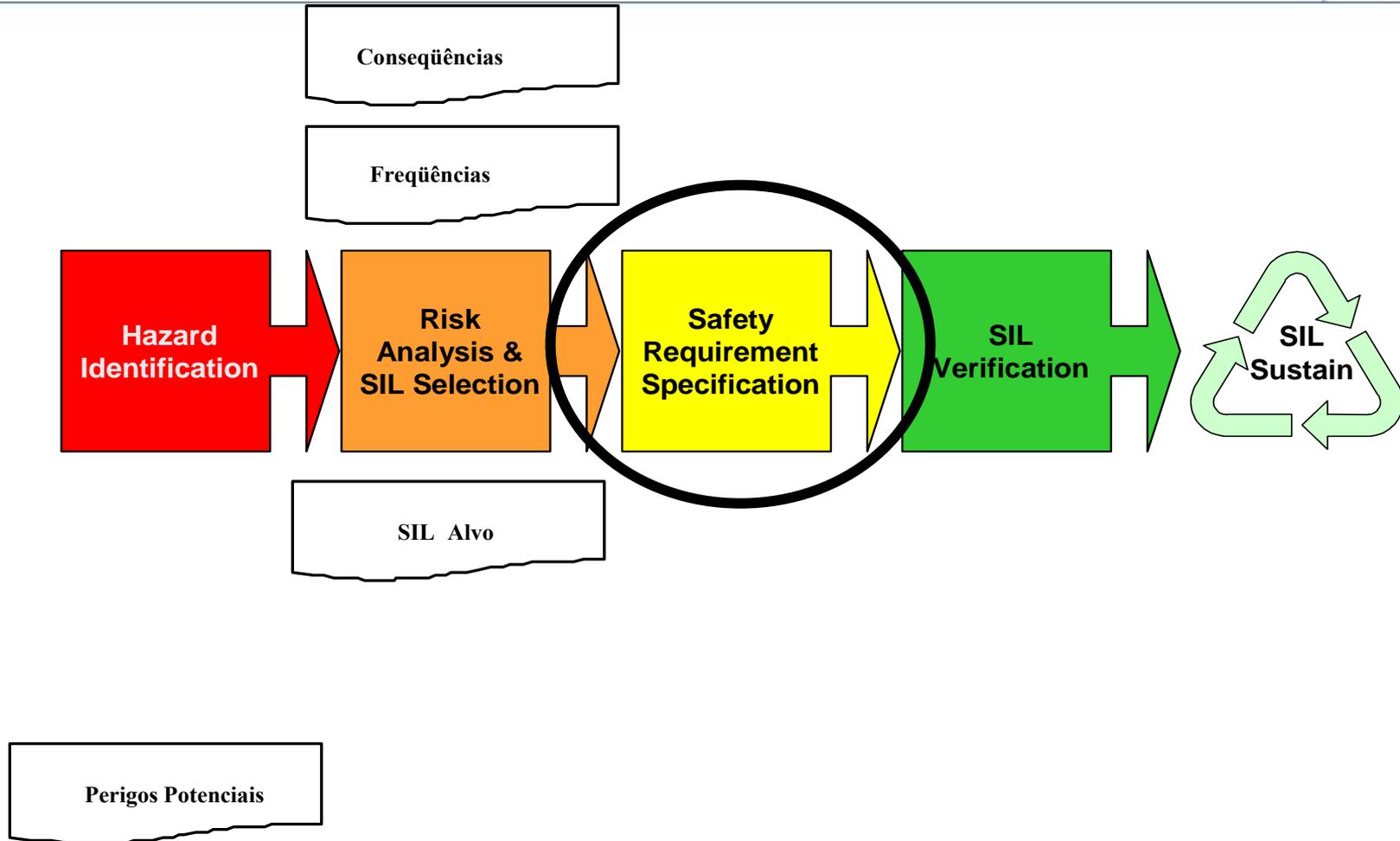
Consequência:

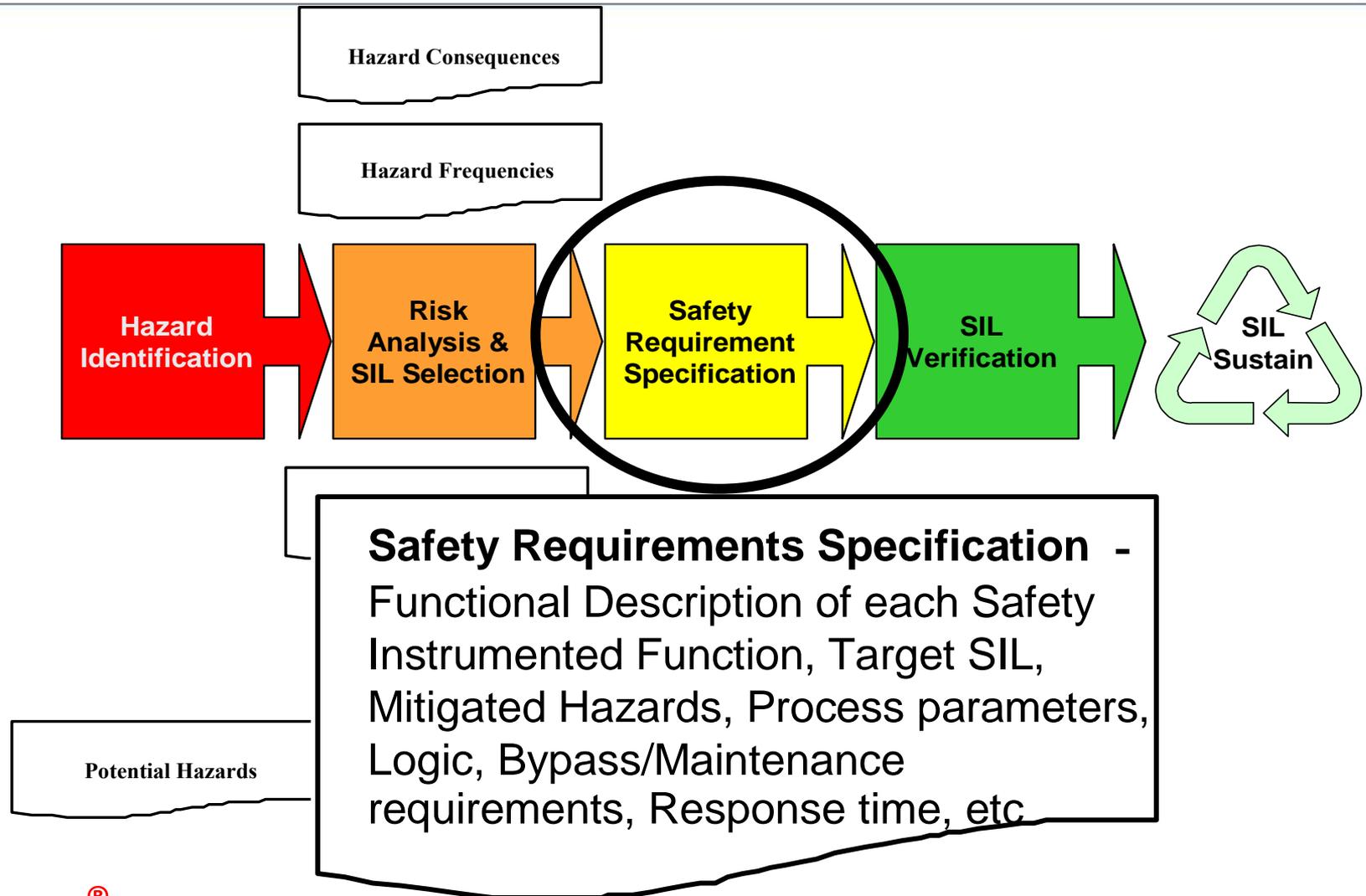
- Uma fatalidade
- Perda financeira de \$4 Milhões

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





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**

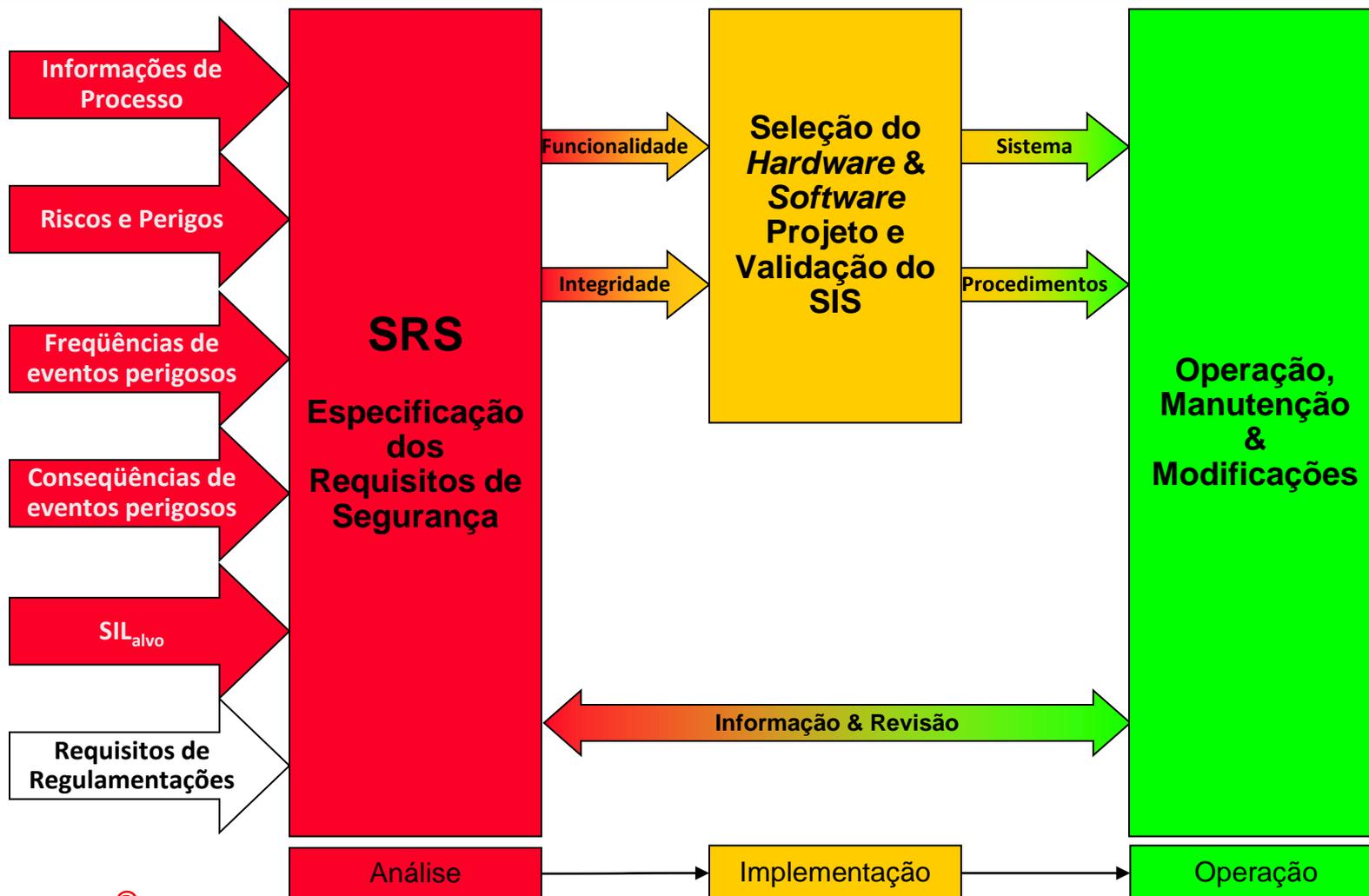
OPERAÇÃO MANUTENÇÃO

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



Ferramenta de SRS



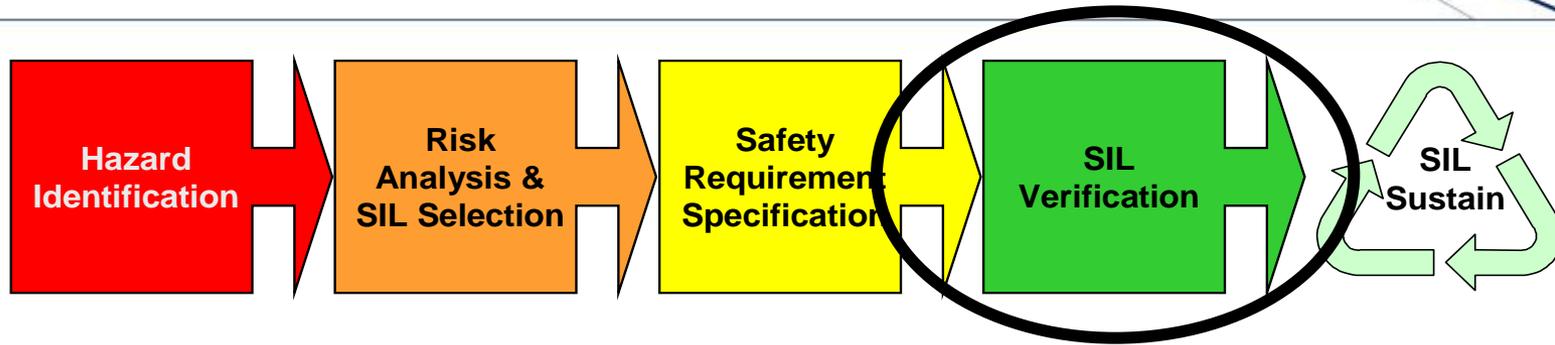
SIF: SIF01 - Project: Sample Project 1 (P001)

SIF Description | SILect | **SIF SRS** | SILver

SRS Details		Logic Description	
Reference	SRS Reference	Sensor Part	Sensor Part
Service	Service		
Safe State	Safe State		
Test Interval	Test Interval	Logic Solving Part	Logic Solver
Response Time	Response Time		
Method	Method		
Reset Type	Reset Type		
Spurious Trip Rate Req's	Spur. Trip Rate		
Diagnostics	Diag		
Manual Shutdown	Man. SD		
Regulatory Requirements	Reg.	Final Element Part	Final Elements
Notes	Notes		
Target SIL	2		

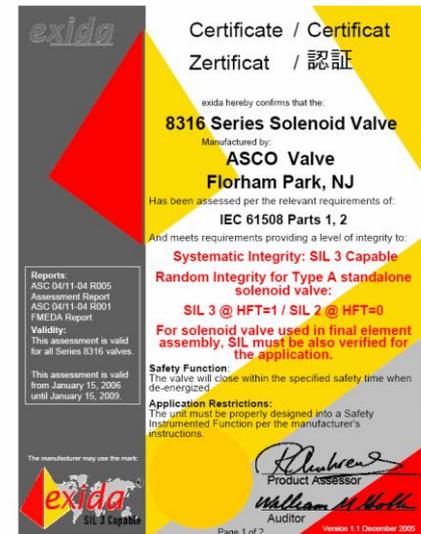
Target SIL: 2 Achieved SIL: TBD

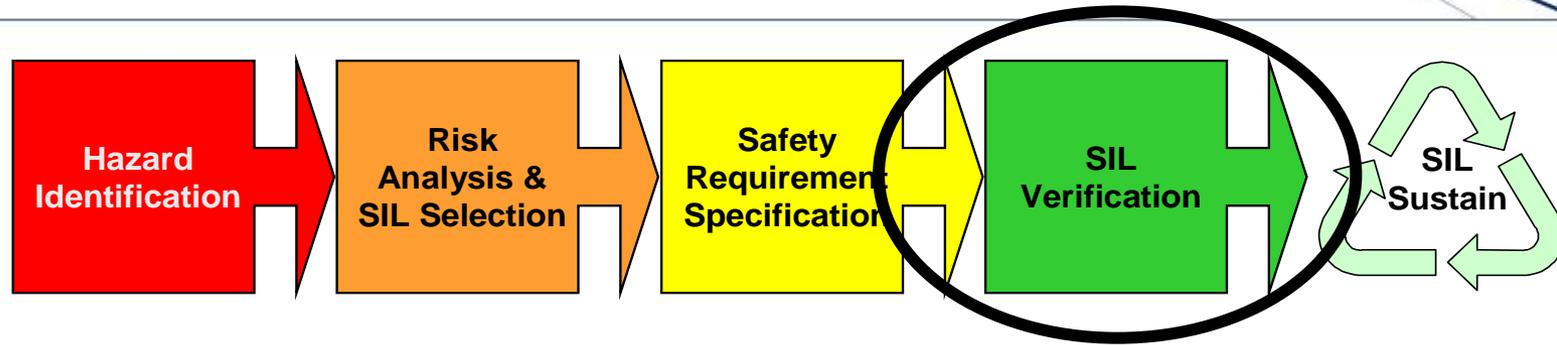




Dimensionar equipamentos conforme IEC 61511: Equipamentos utilizados em um SIS devem ser escolhidos com base na **certificação IEC 61508** para o SIL apropriado ou com base no critério de **“prior use”** (uso anterior)

O equipamento certificado tem um **“SIL Capability”**





Random Failure Probability

Método #1:

Modo Contínuo

O perigo está presente todo o tempo.

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

SIL



SIL

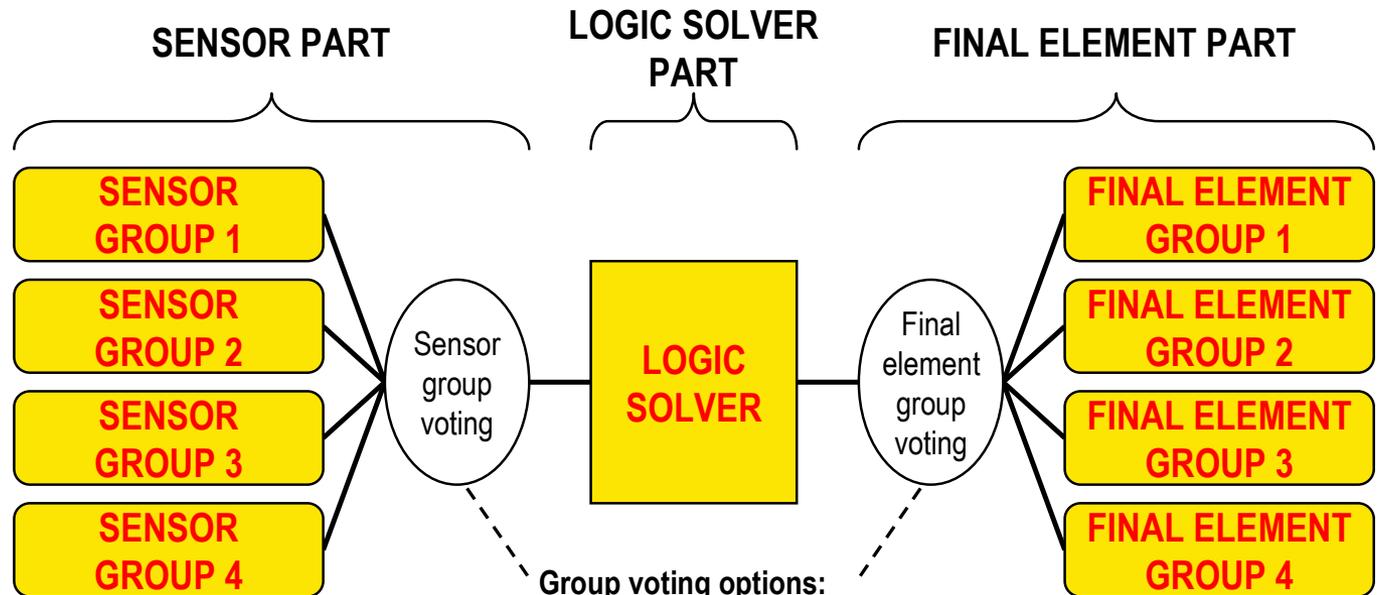
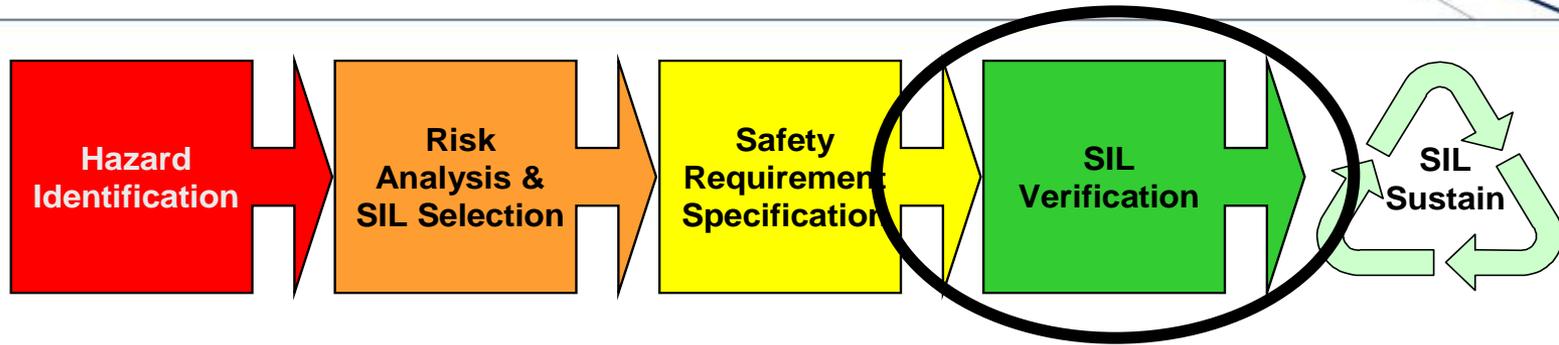
Método #2:

Modo na
Demanda

O perigo
raramente está
presente

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

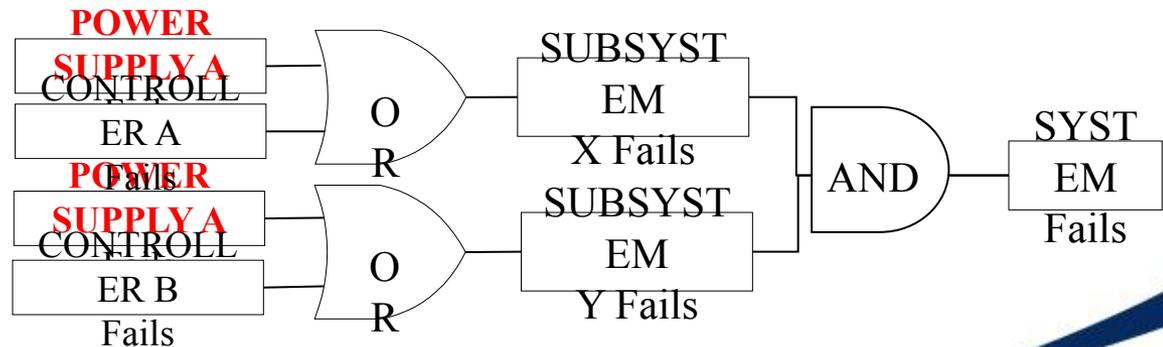
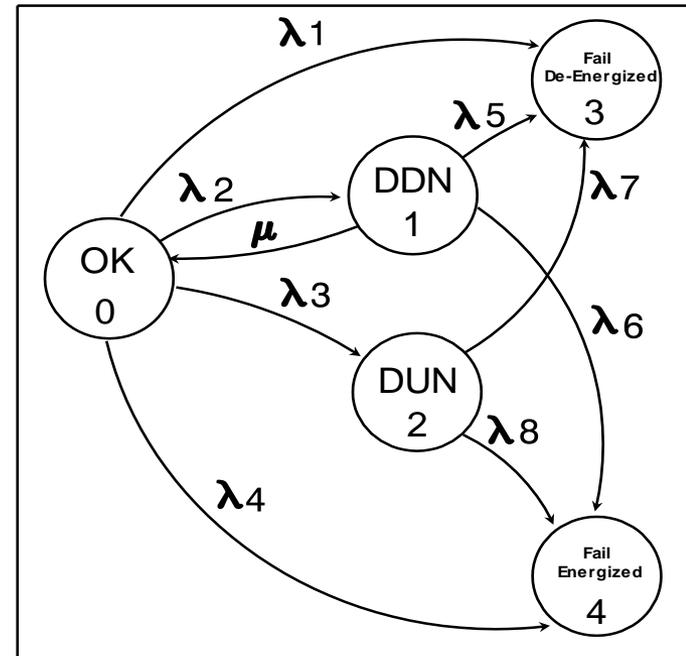
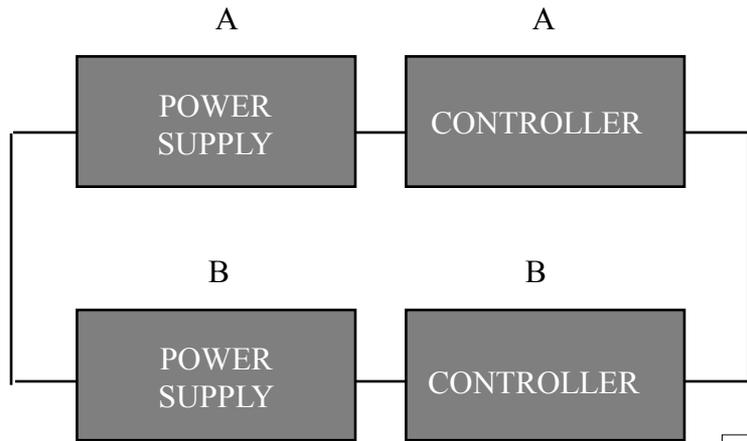
SLC – Projeto Conceitual



Group voting options:
1 group: 1oo1
2 groups: 1oo2, 2oo2
3 groups: 1oo3, 3oo3
4 groups: 1oo4, 4oo4

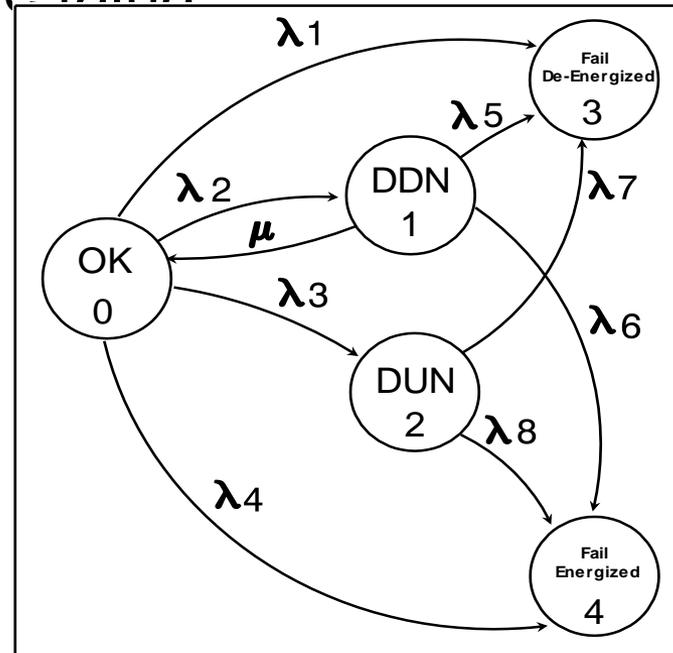


- ◆ Diagrama de blocos
- ◆ Diagramas de árvore de falhas
- ◆ Modelos Markov
- ◆ Equações simplificadas

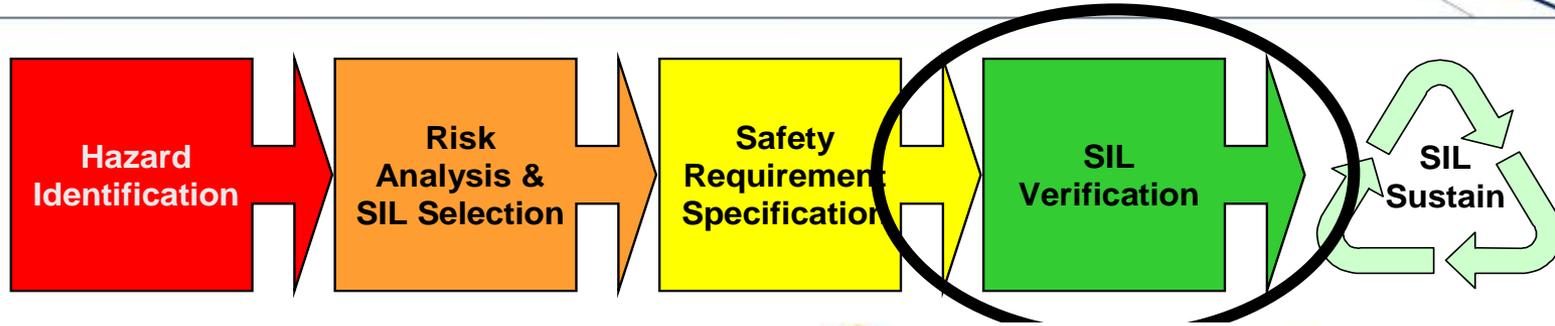


Representação e impacto de:

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



SLC – Verificação das Probabilidades de Falha



Random Failure Probability

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



SILCalc



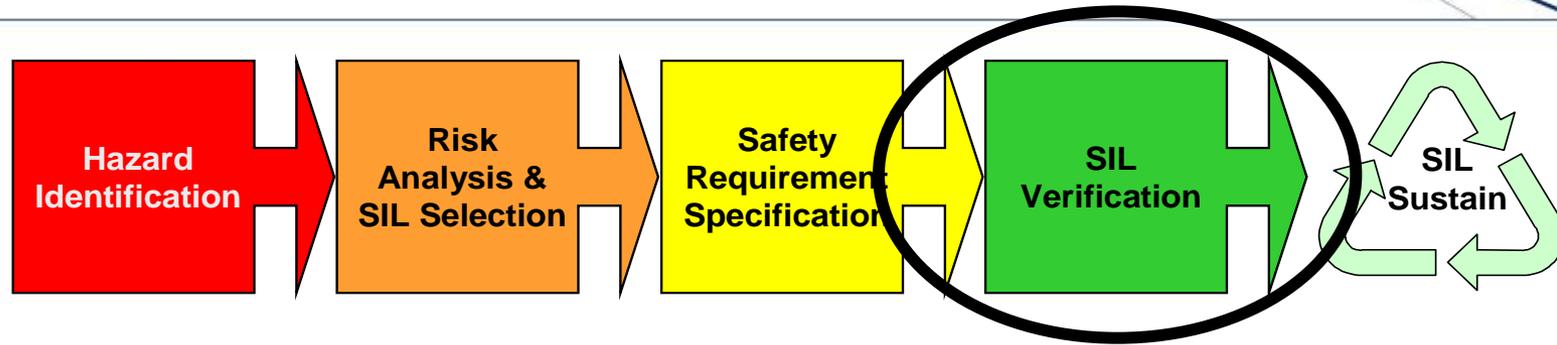
SIL Solver SIS-TECH

SafeCalc

SIL Core



SLC – Detalhamento do Projeto



**Melhores
Práticas**

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

Exemplo para a arquitetura 1oo2:

Contribuição de diagnósticos

Falhas só identificadas no PT

Falhas nunca identificadas

$$PFD_{avg} = [2 * (\lambda_{DD})^2 * (MTTR + TI_A/2)^2] + [((\lambda_{DU})^2 * (TI_M)^2) / 3] + [((\lambda_{DN})^2 * Life^2) / 3] \\ + [2 * TD * \lambda_{DU} * ((TI_M/2) + MTTR) / TI_M] + [\lambda_{DU} * \beta * TI_M/2] + \text{outros...}$$

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

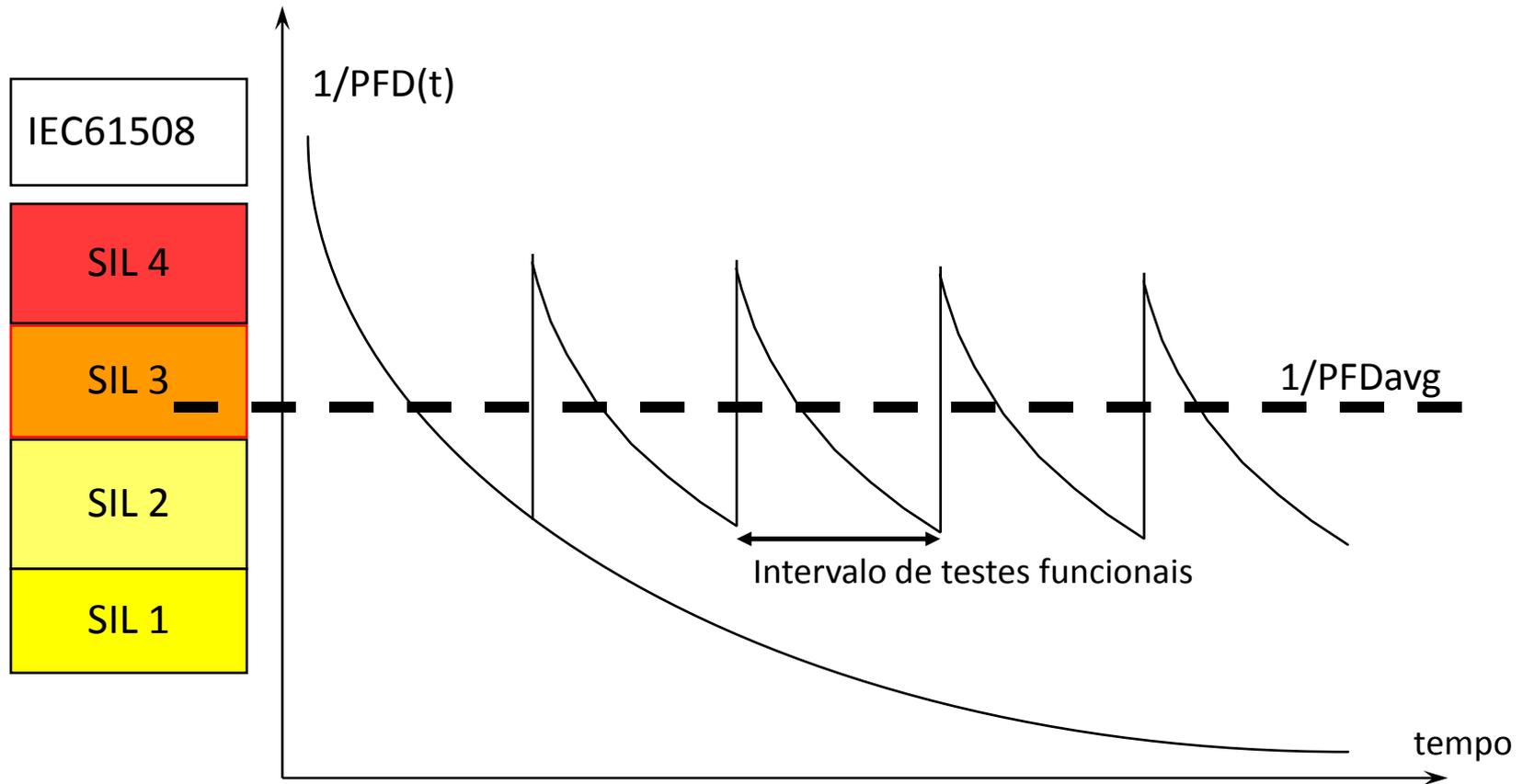
DN = Falha perigosa nunca detectada

$MTTR$ = Tempo médio para reparo

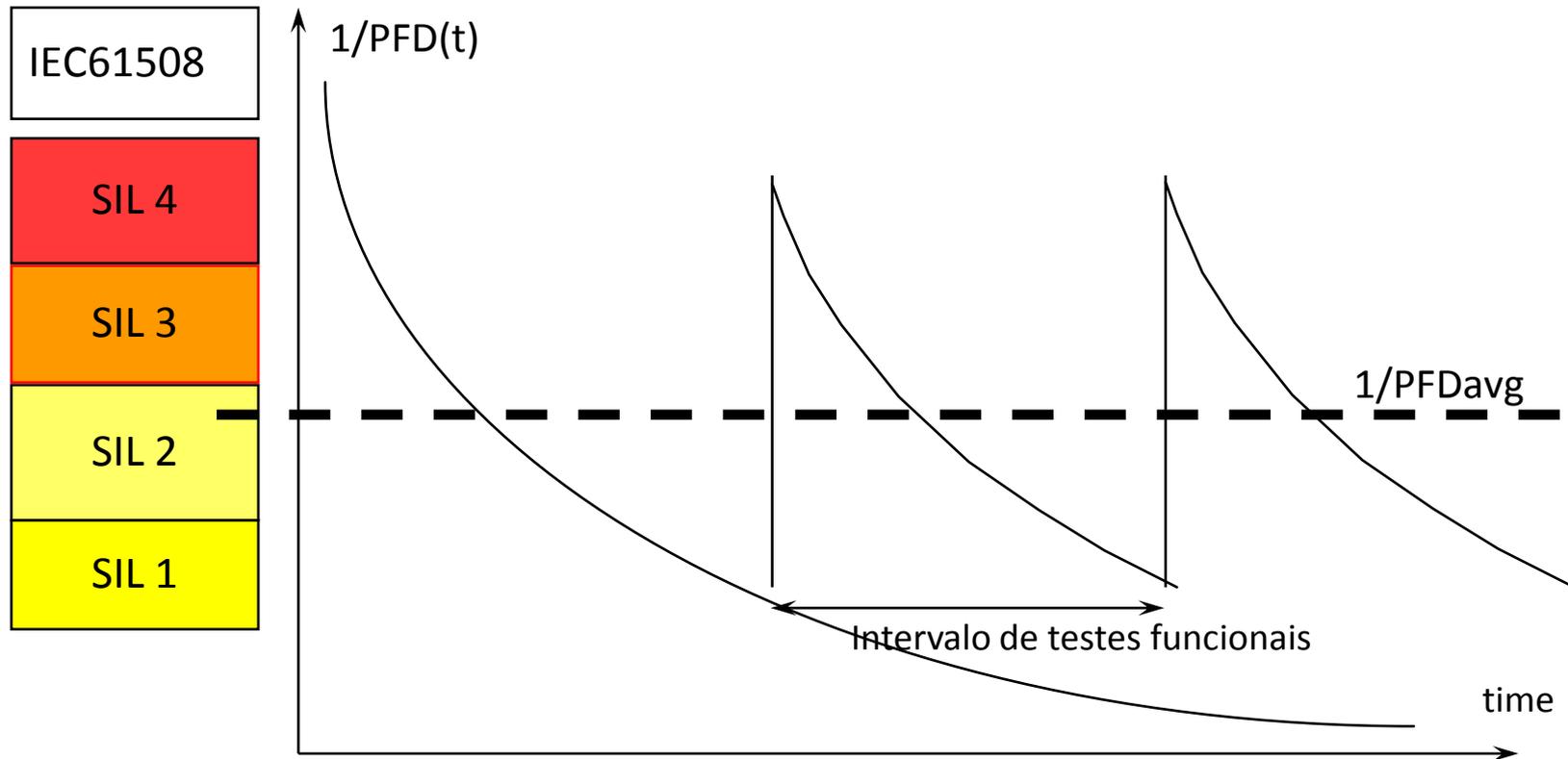
◆ Informações mínimas:

- ◆ 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.

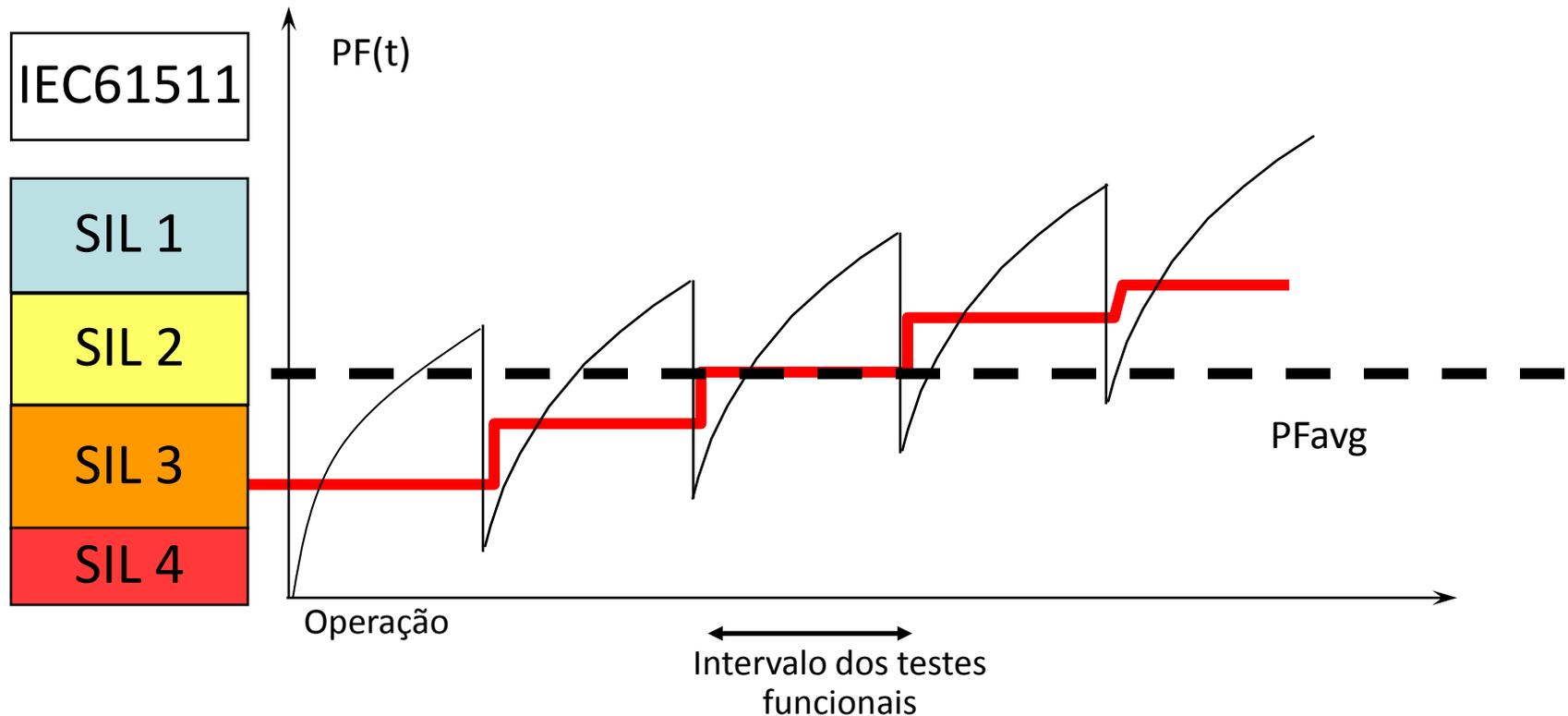
- ◆ Definido durante o detalhamento do projeto.

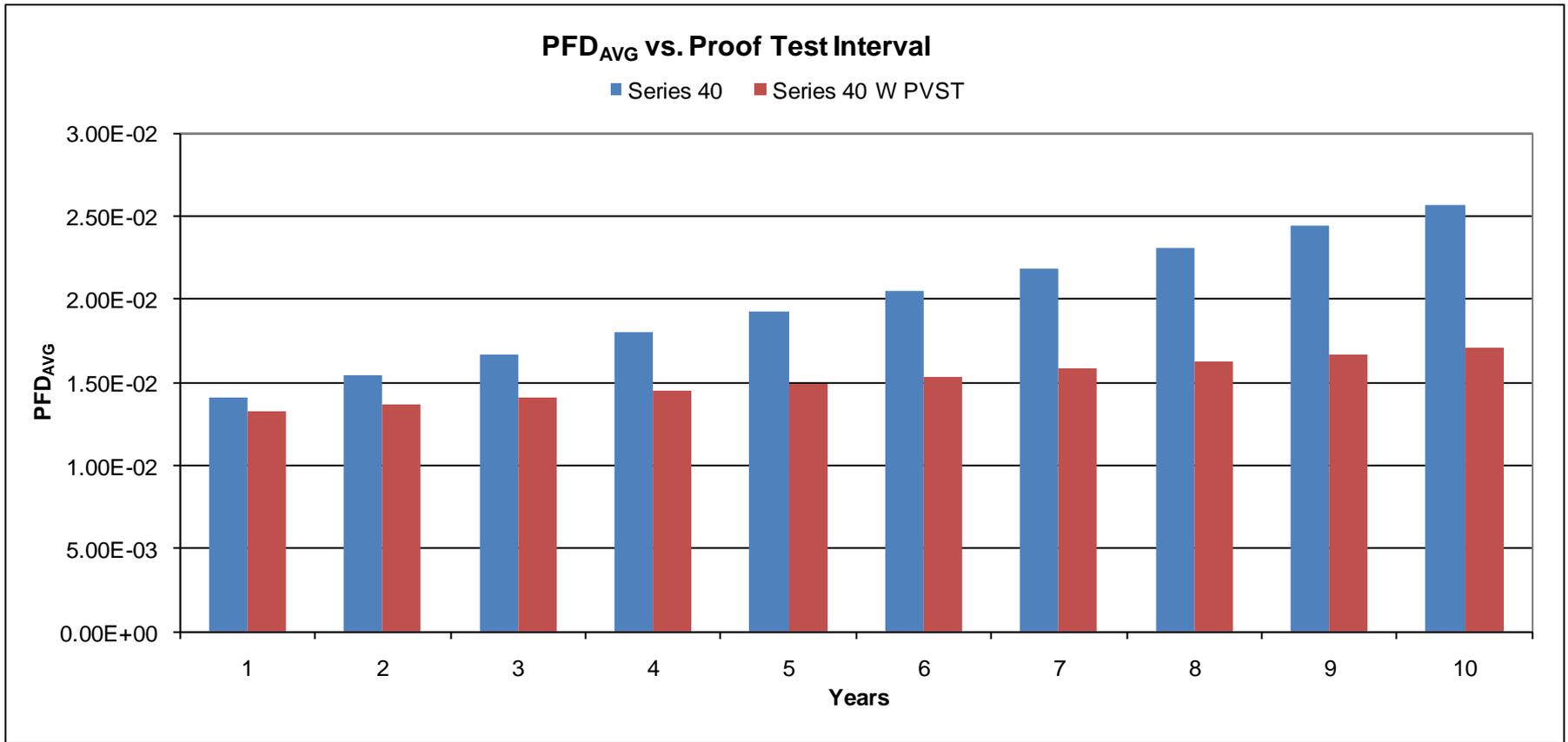


◆ Impacto da alteração da freqüência dos testes

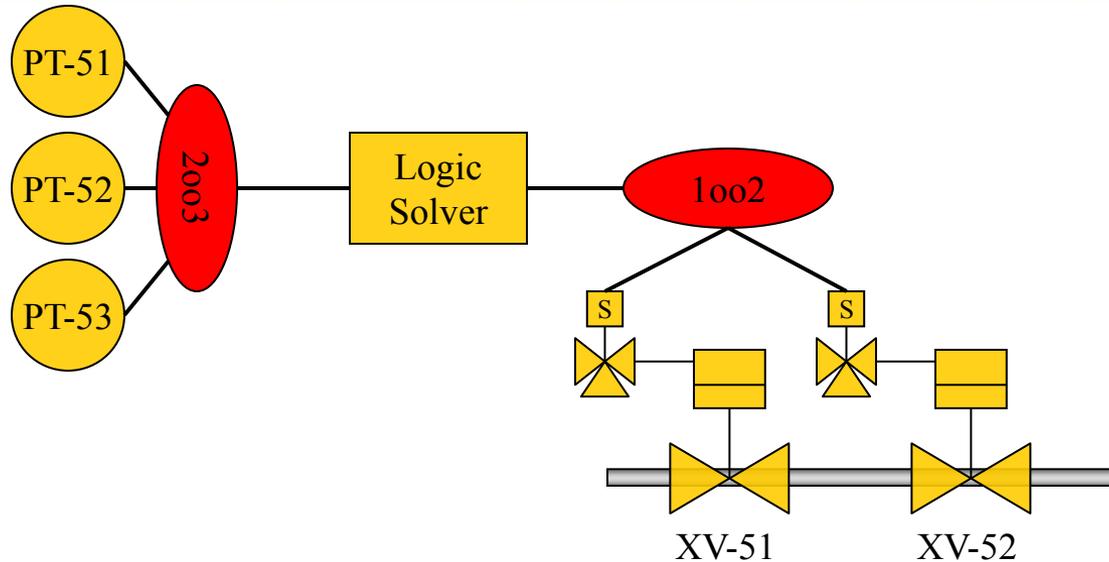


- ◆ Cobertura dos testes periódicos funcionais de 100% = todas as possíveis falhas do dispositivo são identificadas.





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 (2003)	XV-51 Close XV-52 Close (1002)	3

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

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

◆ IEC 61508:

◆ Tipo A

◆ Tipo B

◆ IEC 61511:

◆ Unidade lógica

◆ Elementos de campo

Projeto Conceitual (II) – Sensores



SIF Tag: LT337A - SIF Name: Separator Level Main PILatform

SIF Description | SILect | SIF SRS | SILver

Safety Instrumented Function / Results

- Sensor Part (1001)
 - Group 1: Separator Level (2003)**
- Logic Solver Part
 - Safety PLC Separation Unit (Siemens ...)
- Final Element Part (1001)
 - Group 1: group1 (1002)

Sensor Group 1

Sensor Group Properties

Group Name: Separator Level

Beta [%]: 5

Reuse this Group

MTTR [hours]: 48

Group Voting: Identical, Diverse

Proof Test Interval [months]: 60

Proof Test Coverage [%]: 95

Advanced Options

Tags

Sensor Type: Pressure

Sensor: Siemens SITRANS P, DS III

Process Connection: Clean Service, Remote Seal, Impulse Line

Configuration Options

Interface 1: <None>

Interface 2: <None>

Trip: High, Low

Alarm Setting: Over Range, Under Range

Diagnostic Filtering ON, No

External Comparison

Leg 1

Safety Function Contributions

PFDavg Contribution

- 2.78% Sensor(s)
- 46.36% Logic Solver
- 50.87% Final Element(s)

MTTFS Contribution

- 0.79% Sensor(s)
- 7.19% Logic Solver
- 92.02% Final Element(s)

Target SIL: 3 | Achieved SIL: 3

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

Projeto Conceitual (II) – Unidade Lógica



SIF Tag: LT337A - SIF Name: Separator Level Main PIatform

SIF Description | SILect | SIF SRS | SILver

Safety Instrumented Function / Results

- Sensor Part (1001)
 - Group 1: Separator Level (2003)
- Logic Solver Part
 - Safety PLC Separation Unit (Siemens)
- Final Element Part (1001)
 - Group 1: group1 (1002)

Logic Solver

Name: Safety PLC Separation Unit

Reuse this Logic Solver Group

Advanced Options

MTR [hours]: 8

Proof Test Interval [months]: 12

Proof Test Coverage [%]: 99

Logic Solver Type: PES

Logic Solver: Siemens S7-400FH (exida Process Industry)

Safety Function Contributions

PFDavg Contribution

- 2.78% Sensor(s)
- 46.36% Logic Solver
- 50.87% Final Element(s)

MTTFS Contribution

- 0.79% Sensor(s)
- 7.19% Logic Solver
- 92.02% Final Element(s)

Target SIL: 3 Achieved SIL: 3

Projeto Conceitual (II) – Elementos Finais



SIF Tag: LT337A - SIF Name: Separator Level Main PIlatform

SIF Description | SILect | SIF SRS | SILver

Safety Instrumented Function / Results

- Sensor Part (1oo1)
- Group 1: Separator Level (2oo3)
- Logic Solver Part
 - Safety PLC Separation Unit (Siemens)
- Final Element Part (1oo1)
 - Group 1: group1 (1oo2)

Final Element Group 1

Final Element Group Properties

Group Name: group1 Beta [%]: 10 MTTR [hours]: 48 Advanced Options

Reuse this Group

Group Voting: Identical Diverse 1oo2 Proof Test Interval [months]: 30 Proof Test Coverage [%]: 99 Tags

InterFace Module: <None> Partial Stroke Testing Use Equipment Data Test Coverage [%]

Final Element: Remote Actuated Valve

Final Element Interface: ASCO 8316 NC, low power or

Pneumatic Elements

First Element: <None>

Second Element: <None>

Actuator and Valve

Separate Combination Open on trip Close on trip Tight shutoff required Severe Service

Actuator: Bettis G-Series

Valve: Mogas C Series

- Generic Trunion Ball valve
- Generic Wedge Gate valve
- Mogas C Series
- Samson STM Type 2040
- Somas Type KVT/KVX, KVTW/KVXW, or KVTF/KVXF
- Somas Type MTV / VSS
- Somas Type SKV
- My Own

Safety Function Contributions

PFDavg Contribution

- 2.78% Sensor(s)
- 46.36% Logic Solver
- 50.87% Final Element(s)

MTTFS Contribution

- 0.79% Sensor(s)
- 7.19% Logic Solver
- 92.02% Final Element(s)

Target SIL: 3 | Achieved SIL: 3

Ciclo de Vida de Segurança



SIF Tag: LT337A - SIF Name: Separator Level Main PILatform

SIF Description | SILect | SIF SRS | SILver

Safety Instrumented Function / Results

- Sensor Part (1oo1)
 - Group 1: Separator Level (2oo3)
- Logic Solver Part
 - Safety PLC Separation Unit (Siemens : ...)
- Final Element Part (1oo1)
 - Group 1: group1 (1oo2)

Safety Instrumented Parameters

Consider Architectural Constraints IEC 61508 IEC 61511

Mission Time (years): 5

Startup Time (hours): 24

Demand Rate: Low

Safety Instrumented Function Performance Metrics

Average Probability of Failure on Demand (PFDavg)	2.61E-04
Safety Integrity Level	3
Safety Integrity Level (Architectural Constraints)	3
Risk Reduction Factor	3835
MTTFS (years)	52.52

Comments and Assumptions

	PFDavg	MTTFS (years)	Maximum SIL allowed (Architectural Constraints)
Sensor Part	7.24E-06	6629.07	4
Logic Solver Part	1.21E-04	730.34	3
Final Element Part	1.33E-04	57.08	4

Safety Function Contributions

PFDavg Contribution

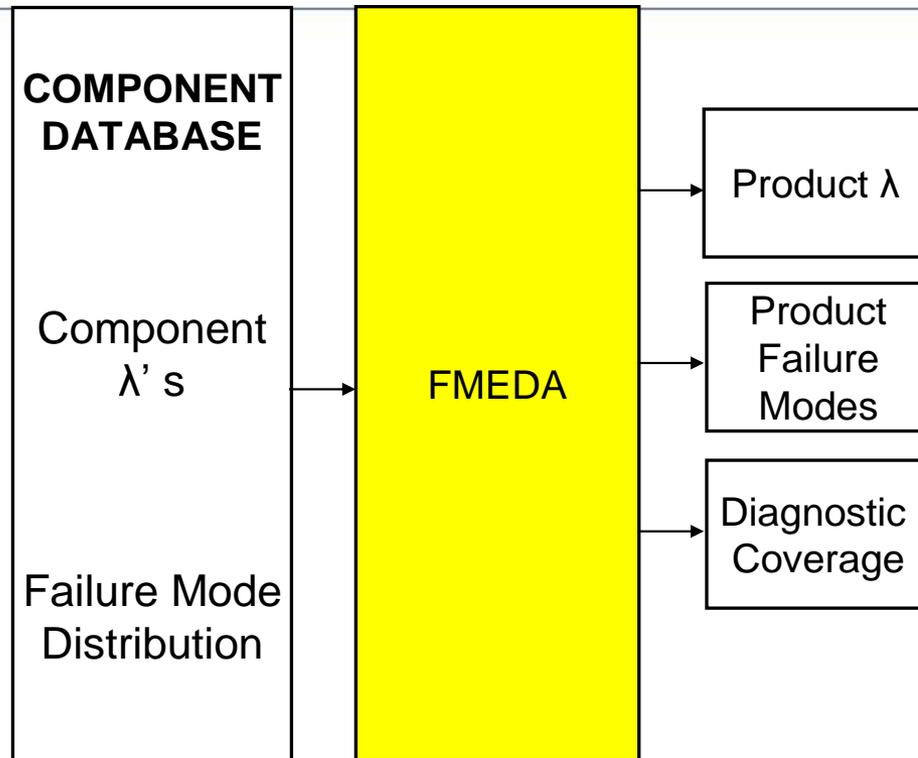
- 2.78% Sensor(s)
- 46.36% Logic Solver
- 50.87% Final Element(s)

MTTFS Contribution

- 0.79% Sensor(s)
- 7.19% Logic Solver
- 92.02% Final Element(s)

Target SIL: 3 Achieved SIL: 3





- 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.

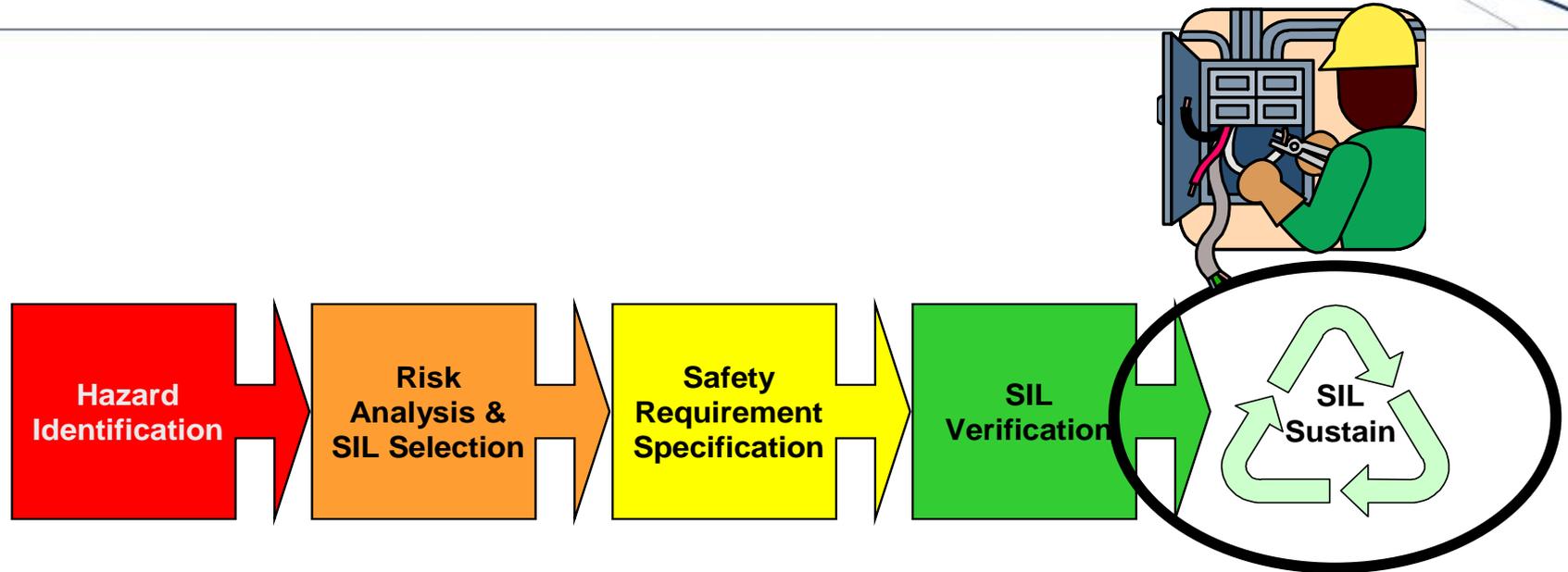
Confiabilidade dos dados



	SN 29500	IEC 62380 telecom.	MIL-HDBK 217F
Equation for λ in [1/h]	$\lambda = \lambda_{ref} \cdot \pi_T$	$\lambda = 0.5 \cdot \left(\sum \pi_{T,i} \dots + 1.4 \cdot 10^{-3} \cdot \sum \pi_{n,i} \dots \right) \cdot 10^{-9}$	$\lambda = \lambda_b \cdot \pi_R \cdot \pi_Q \cdot \pi_E$
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)	$\pi_{T,avg=40\text{ °C}} = \mathbf{0.0014}$	---
π_R (Resistance factor)	---	---	1.0
π_n (Variation factor per phase)	---	$\pi_n = \mathbf{0}$, (da $\Delta T = 0$)	---
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



PERD

CCPS
CENTER FOR
CHEMICAL PROCESS SAFETY
An AIChE Industry
Technology Alliance

Operational Procedures

Maintenance Procedures

Proof Test Procedures

SIL Stat

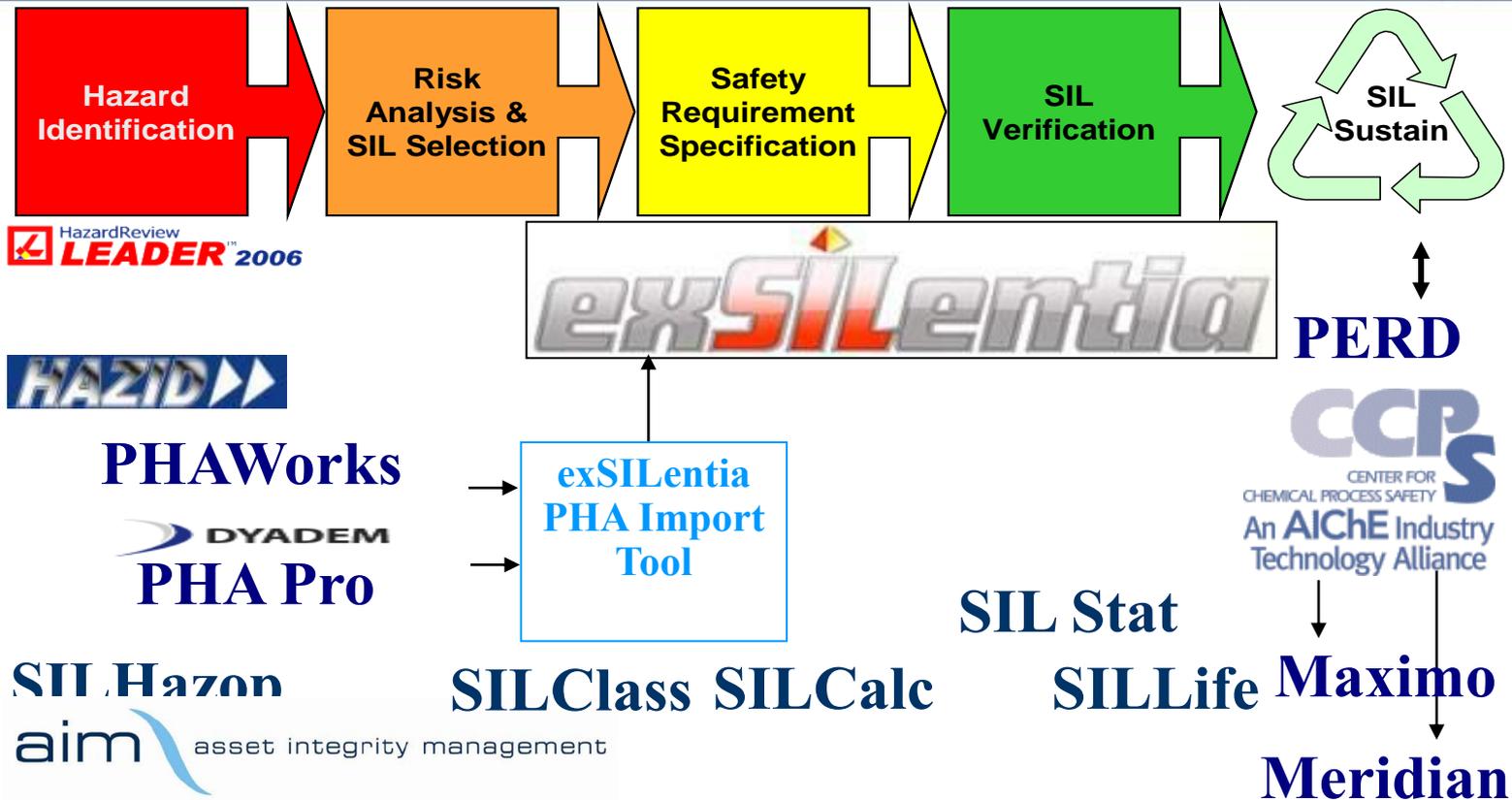
SILLife Maximo

Meridian

aim asset integrity management



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



HazardReview
LEADER™ 2006

SILHazop



PHAWorks

DYADEM

PHA Pro

SILHazop



exSILentia
Import
Function

SILCommision

SILProof

SILLife

SIL Stat

PERD

Maximo

Meridian



Operação Integrada:
Comissionamento e intervalo de testes
da SIF



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

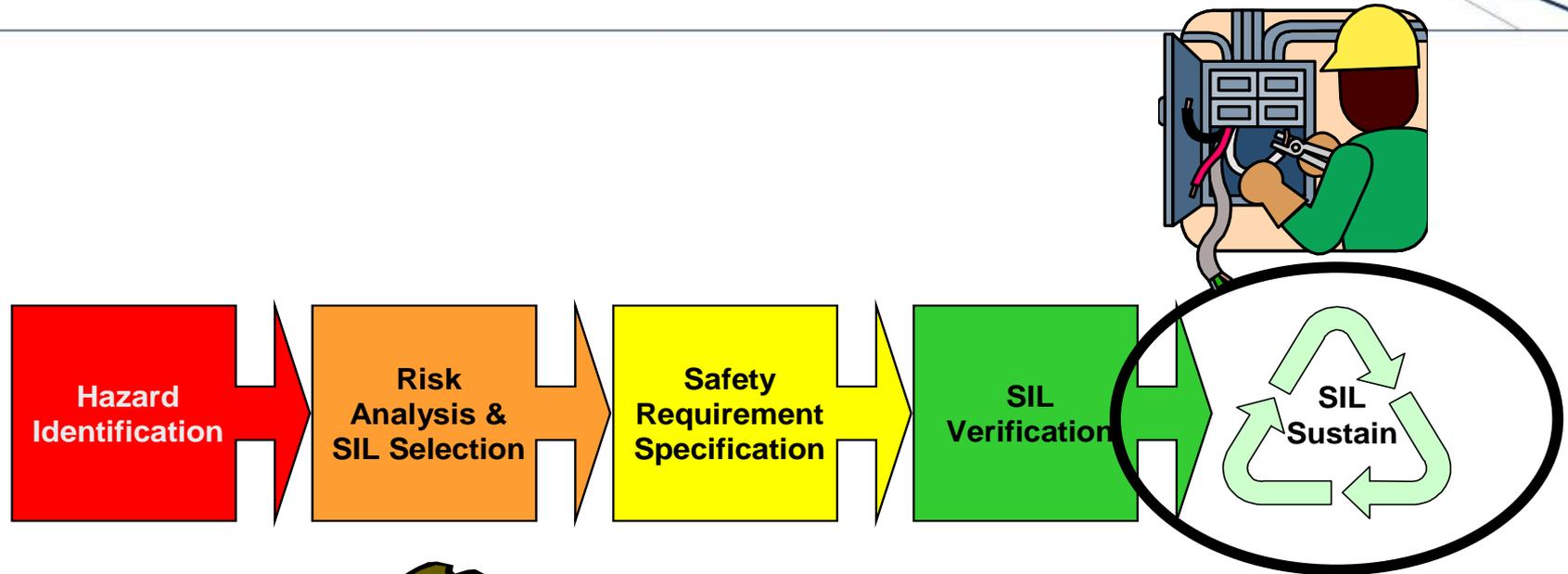
Exemplo da descrição de dois níveis de competência:

TABLE 2 Assessed Competencies

Area	Basic Requirements	Typical/Allowed Basic Tasks	Senior Requirements	Typical/Allowed Senior Tasks
User Hazard Identification / Process HAZOP	<ol style="list-style-type: none"> 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 <i>exida</i> training, textbook and best practice material on Hazard identification and <u>HAZOPs</u> 4) Have read and understood at least 1 detailed Hazard Identification report. 	<p>Act as scribe or other basic participant in a hazard identification / HAZOP workshop.</p> <p>Prepare draft hazard identification documentation under the guidance of a Senior competent person in this area.</p>	<ol style="list-style-type: none"> 1) Hold a CFSE certificate. 2) Have read and understood relevant <i>exida</i> training, textbook and best practice material on Hazard identification and <u>HAZOPs</u>. 3) Have substantially participated in <u>at least 2 hazard identification</u> or Process HAZOP activities. 	<p>Coordinate and facilitate hazard identification workshops</p> <p>Independently prepare draft hazard identification documentation</p> <p>Review draft hazard identification documentation prepared by others prior to formal issue.</p>



SLC – Operação e Manutenção



Operational Procedures

Maintenance Procedures

Proof Test Procedures

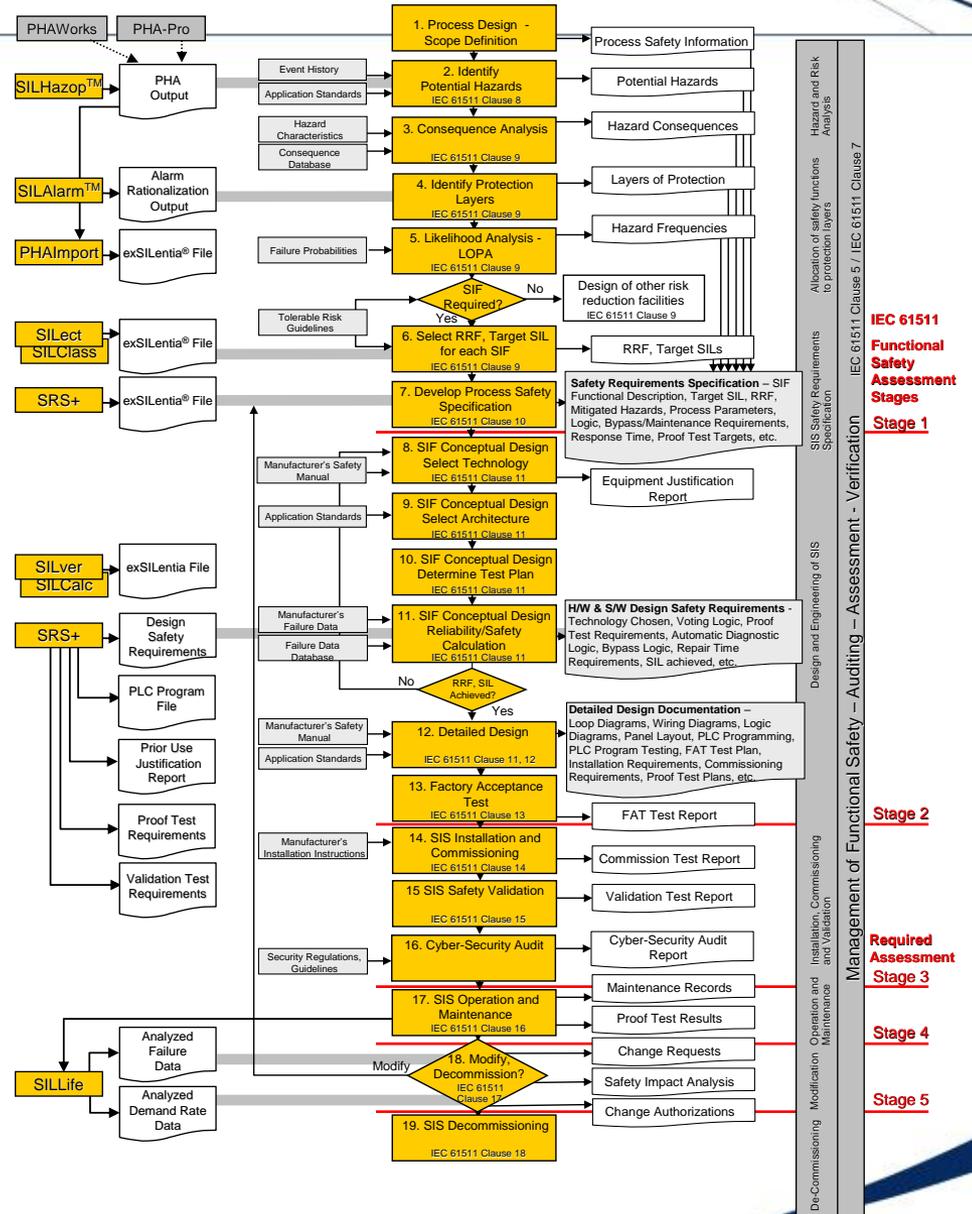
- ◆ Fase mais longa do SLC

- ◆ 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.

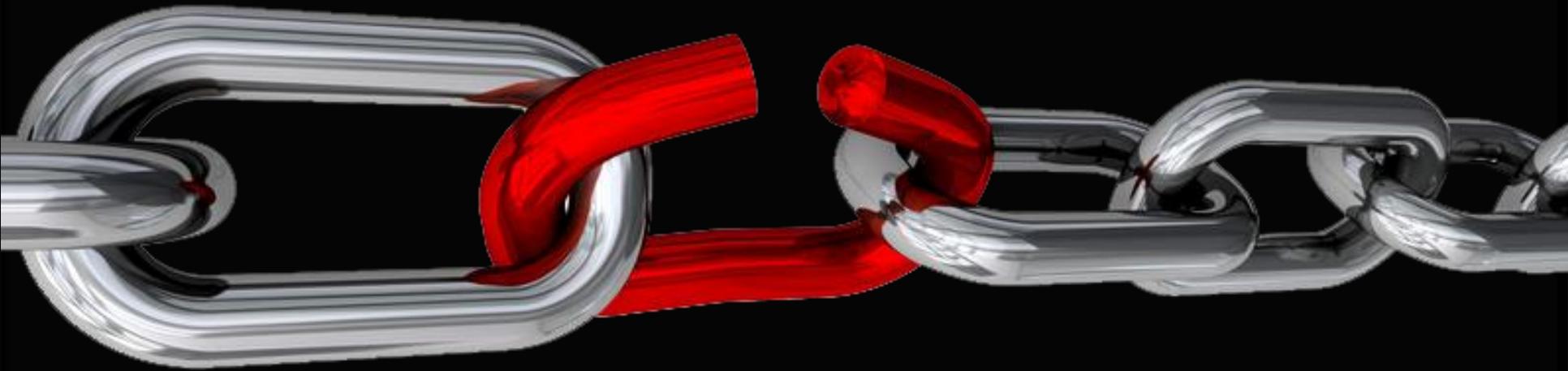




- ◆ O Ciclo de Vida de Segurança proposto pela ISA 84.01 / IEC 61511 pode resultar uma boa relação de custo x benefício. Os principais fatores de sucesso são:
 1. Gerenciamento das Funções de Segurança
 - a. Procedimentos
 - b. Ferramentas auxiliares
 2. Competência dos profissionais envolvidos

www.exida.com

Monica Hochleitner - monica@exida.com



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

