THE REYNOLDS COMPANY
ELECTRICAL SUPPLY

Machine Safety vs Process Safety - SIL vs PLe

May 19, 2021

Our Guest Panelists

Justin Ryan
ISA Certified Automation Professional
ISA84 SIS Expert
TÜV Cyber Security Specialist
Rockwell Automation

Eric Bombere
Functional Safety Engineer – Machinery (TÜV Rheinland)
Rockwell Automation

2021 Online Events

Register to receive a calendar invite

THE REYNOLDS COMPANY
ELECTRICAL SUPPLY

- **Tech Talks**
  - **PowerFlex Integration with Fisher ROC**
    Wed, May 26, 2021 @ 10am
  - **Stratix 5800 / Networks update**
    Wed, June 9, 2021 @ 10am
  - **Rockwell Automation Integrated Services Agreements**
    Wed, June 23, 2021 @ 10am

- **User Groups**
  - **System Redundancy Best Practices**
    Wed, June 19, 2021 @ 10am

reynoldsonline.com

Intro to Safety – Machinery and Process

Improving Productivity and Safety Compliance

May 2021

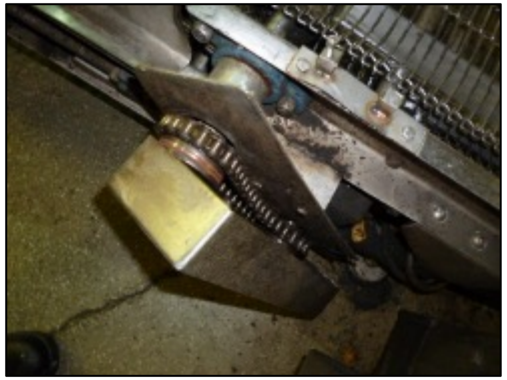
Eric Bombere
ecbombere@rockwellautomaiton.com
804-922-9836

Justin Ryan
jjryan1@ra.rockwell.com
713-385-4275

Machine Safety

www.rockwellautomation.com

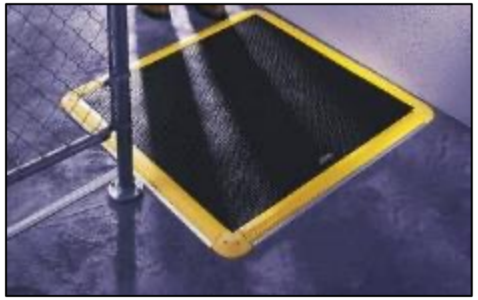
Machinery Safe Guarding & E-Stop



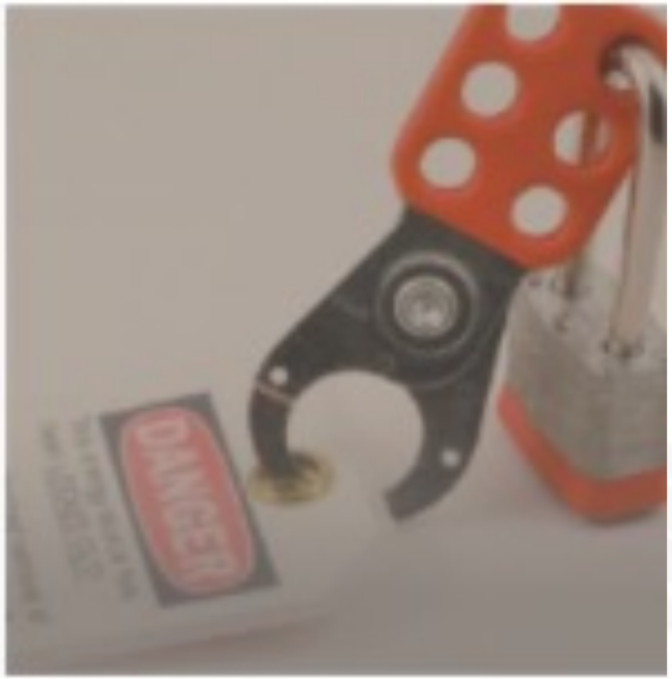








Controls & Safety Measures



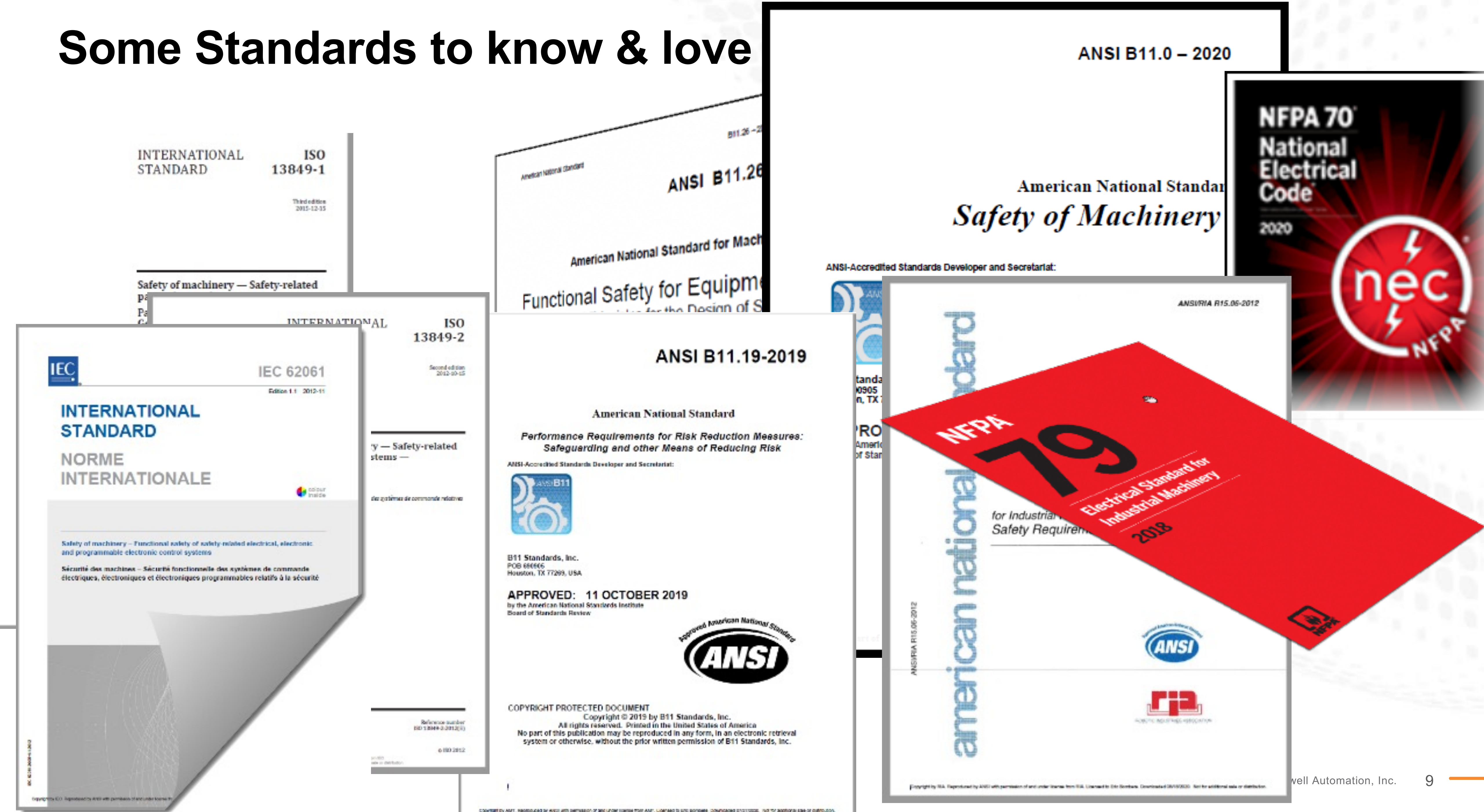
https://www.osha.gov/dts/osta/lototraining/hottopics/ht-relche-1-2.html

What Is "Functional Safety?"

Formal Definition: "part of the overall safety relating to the EUC and EUC control system that depends on the correct functioning of E/E/PE safety related systems and other risk reduction measures" (IEC 61508-4 2010)

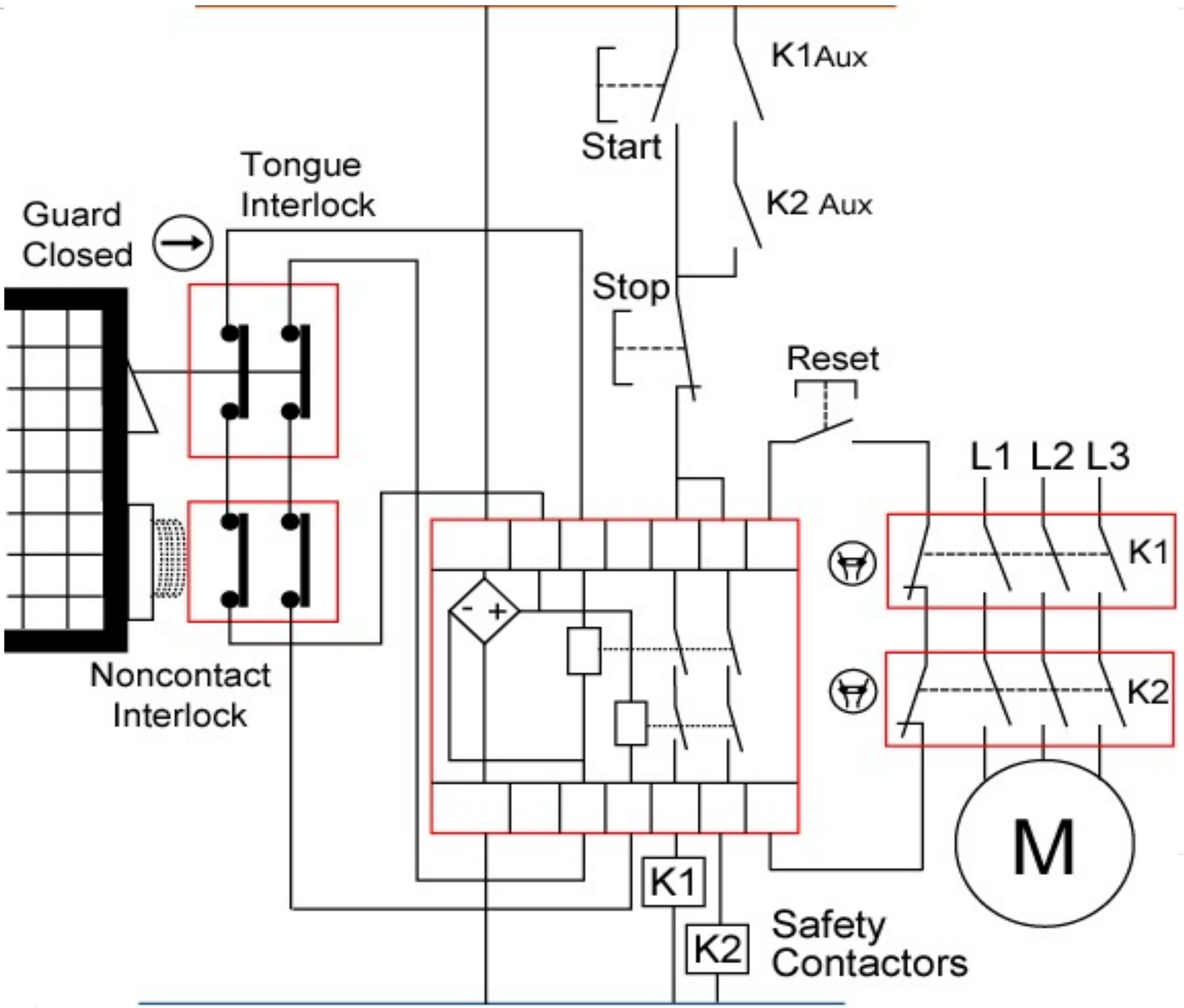
Practical Definition: Use of an automation system to guarantee safety of people

Some Standards to know & love



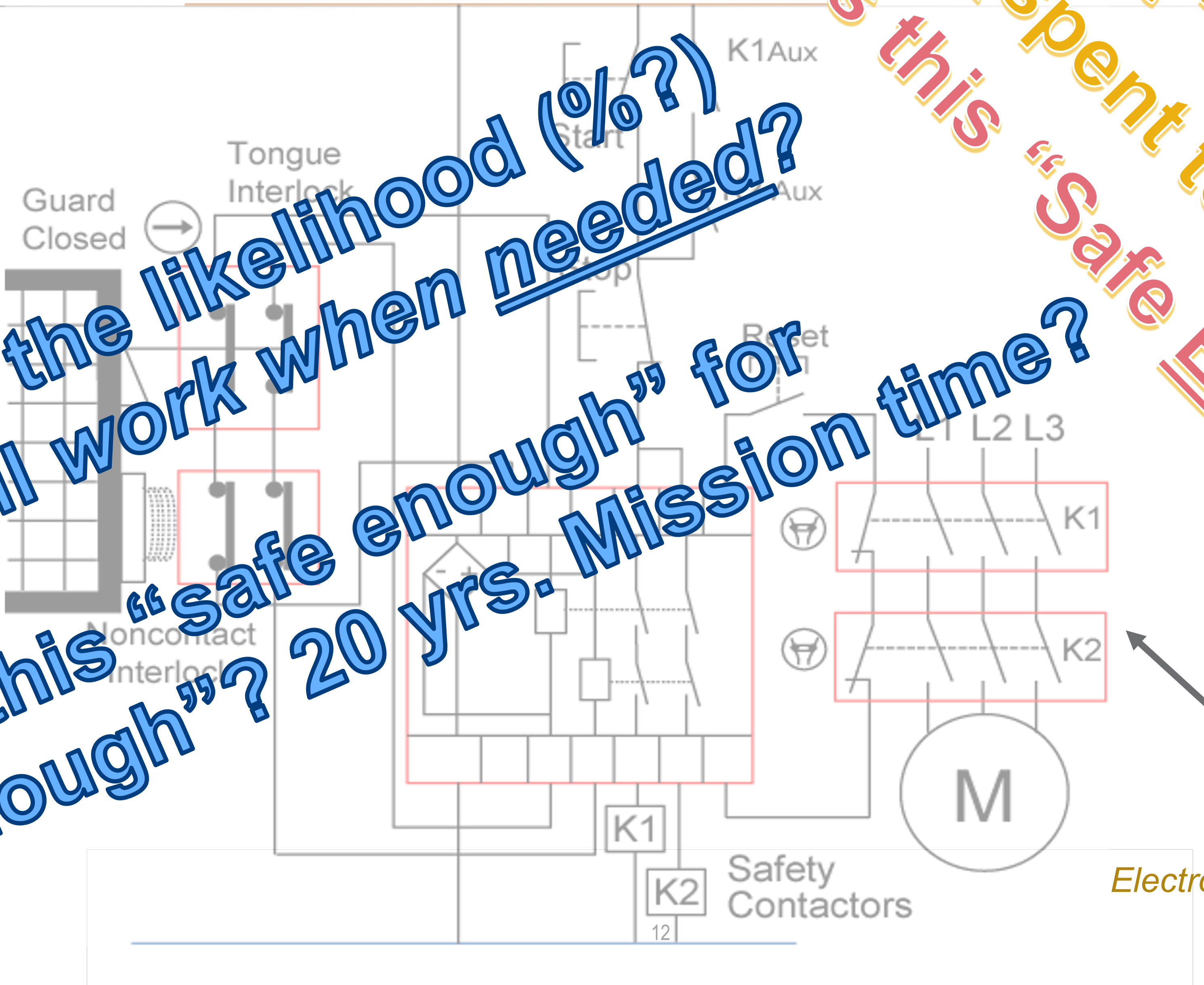
Example "Functional Safety" Control System

Example "Functional Safety" Control System



11

Example "Functional Safety" Control System



What's the likelihood (%?)
This will work when needed?

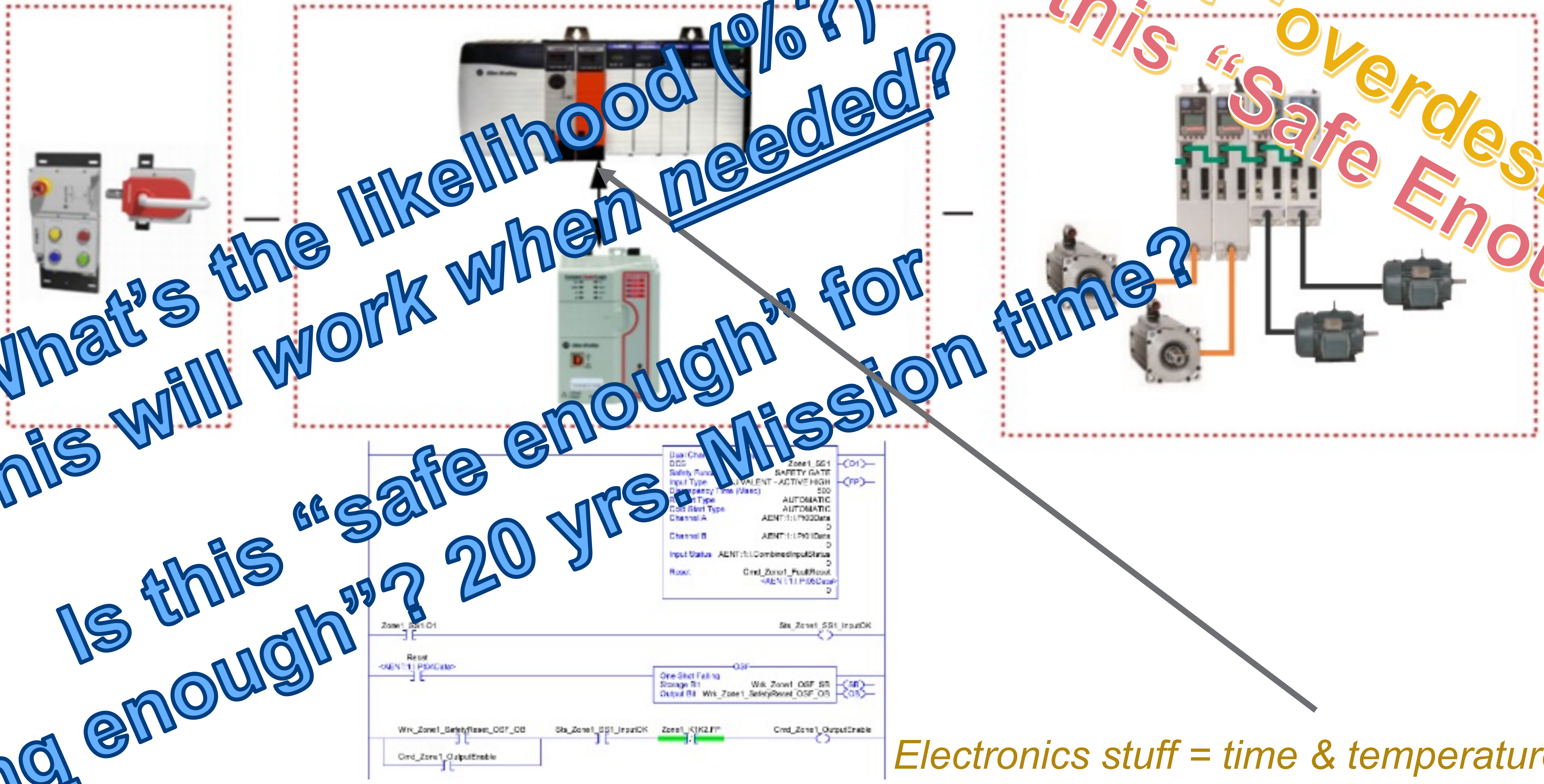
Is this "safe enough" for
"long enough"? 20 yrs. Mission time?

Is this "Safe Enough"?

Is it "overdesigned"
(spent too much $?)

Electromechanical stuff = wear & tear

Example "Functional Safety" Control System



What's the likelihood (%?)
This will work when needed?

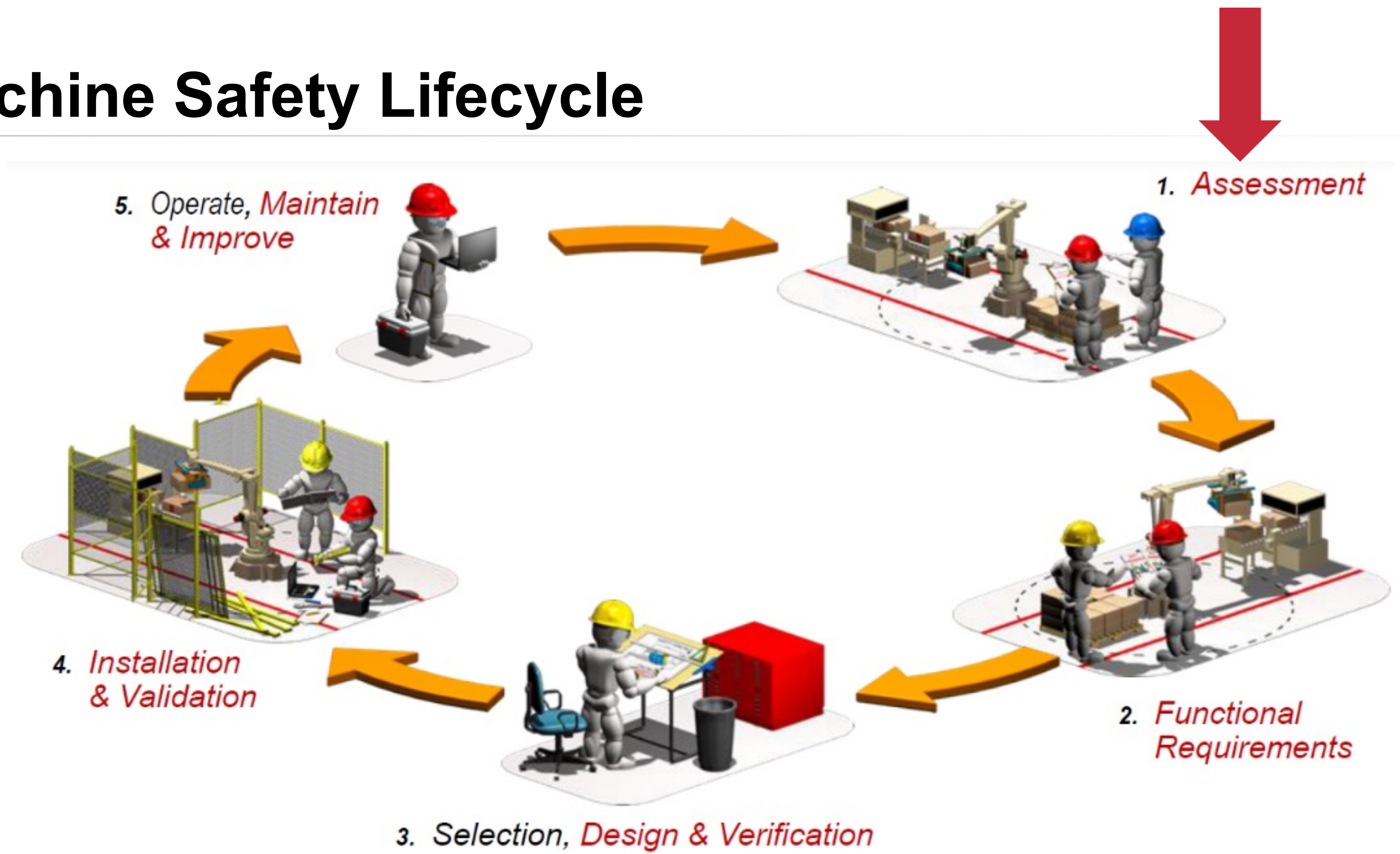
Is this "safe enough" for
"long enough"? 20 yrs. Mission time?

Is it "overdesigned"
Is this "Safe Enough"?

Electronics stuff = time & temperature failures

Rockwell Automation

Machine Safety Lifecycle



Risk Assessment "Scoring Systems" – Elements of Risk

6.4 Assess initial risk

The risks associated with each hazard shall be assessed using the following steps:

1) Select a risk scoring system (6.4.1);
2) Assess risk using the risk factors of the risk scoring system (6.4.2);
3) Derive a risk level (6.4.3).

Continuous exposure?
Once an hour?
Once a month?

Risk *related to the considered hazard*	is a function of	**Severity of harm** *that can result from the considered hazard*	and	**Probability of occurrence** *of that harm*

Bruise?
Cut?
Break?
Loss of limb?

Easy to avoid?
Slow moving machine?
Not possible to avoid?
Can't see see it coming?

From ANSI B11.0

Risk Estimation / Scoring Systems & Models

HRN – "Hazard Rating Number"

- The likelihood of occurrence (LO)
- The frequency of exposure (FE)
- The degree of possible harm (OPH)
- The number of persons at risk (NP)

LO FE DPH NP=H.R.N.
0.1 X 0.1 X 4 X 1=0.04
Degree of risk: = Negligible

LO FE DPH NP=H.R.N.
2 X 5 X 4 X 1=40
Degree of risk: = Significant

Nº Persons	Factor
1-2 Persons	1.00
3 -7 Persons	2.00
8 -15 Persons	4.00
16 - 50 Persons	8.00
More than 50	12.00

Frequency	Factor
Annual	0.50
Monthly	1.00
Weekly	1.50
Daily	2.50
Hourly	4.00
Constant	5.00

Probability	Factor
Little/low possibility, under extreme circumstances	0.03
Highly improbable, but still likely	1.00
Improbable, but still possible	1.50
Possible, but unusual	2.00
Although improbable, it may occur	5.00
Probable , Not surprising	8.00
Probable , Can be expected	10.00
Certain , No doubt	15.00

Max. Loss	Factor
Scratch, bruise	0.10
Burn, cut, short illness	0.50
Minor bone fracture or minor temporary illness	2.00
Major bone fracture or major temporary illness	4.00
Loss of a limb, eye or hearing, permanent	6.00
Loss of two limbs, eyes or hearing, permanent	10.00
Fatality	15.00

HRN Result	Min.	Max	Colour
Negligible	0	5	
Low but relevant	5	50	
High	50	500	
Unacceptable	500	10000000000	

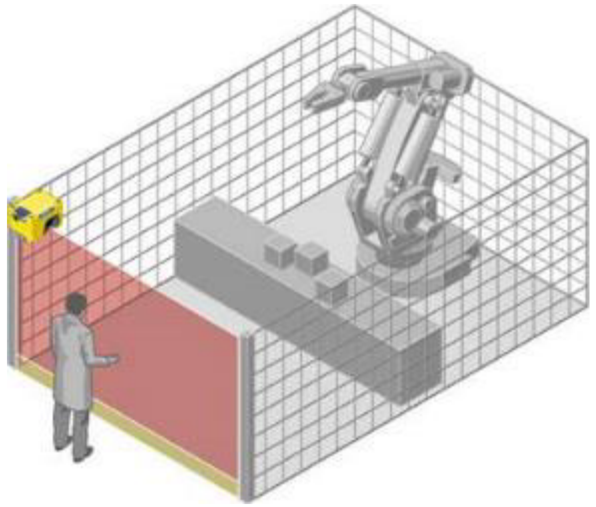
Rockwell Automation

Functional Safety Design

- IF *we're going to use Electrical/Electronic/Programmable Electronics/Pneumatics/Hydraulics as part of the Safety System to be implemented,*

- THEN *we need to <u>design</u>, <u>verify</u> & <u>validate</u> that system is adequate for the requirements*

  - HOW *do we do that???*



Design Requirements Commensurate with Risk Assessment

Ref: ANSI/RIA TR R15.306

Table 2 – Risk level decision matrix

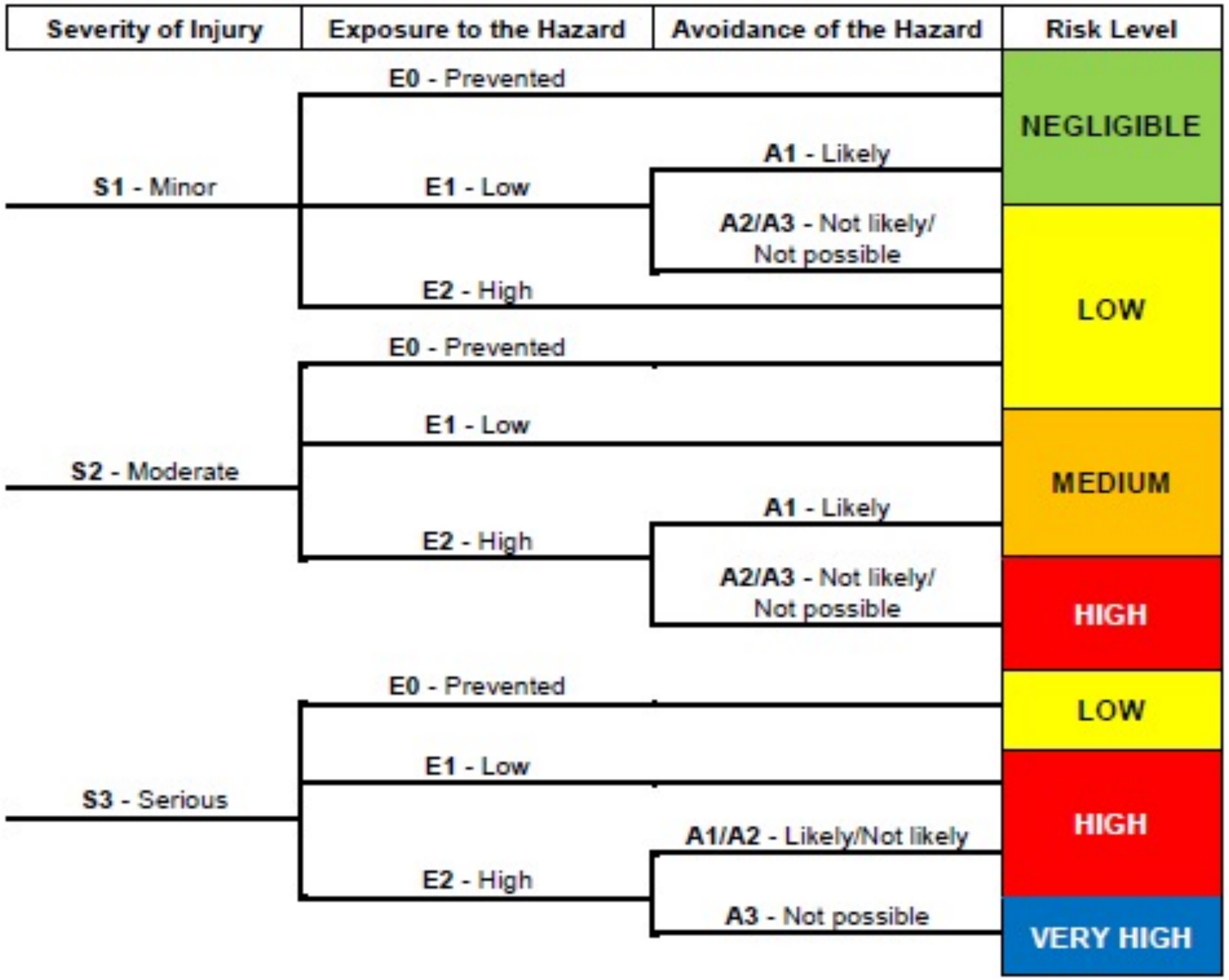


Table 5 – Minimum functional safety performance

Risk Level	PL_r	Structure Category
NEGLIGIBLE (see 6.5.3.1)	b	-
LOW	c	2
MEDIUM	d	2
HIGH	d	3
VERY HIGH (see 6.5.3.2)	e	4

Note: PLe not typical with robotics

Functional Safety Design

Decide & Design appropriate levels of

- Redundancy?
- Diagnostics & Monitoring?
- Component & System Reliability?
- Other System Design criteria?

Door / Gate Interlock Switch

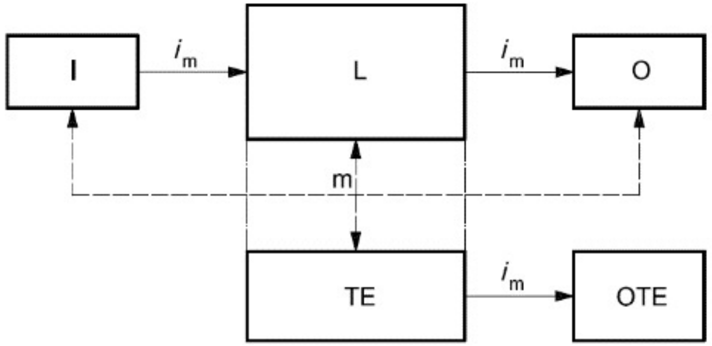
Safety Monitoring Relay

Safety-Rated Motor Control

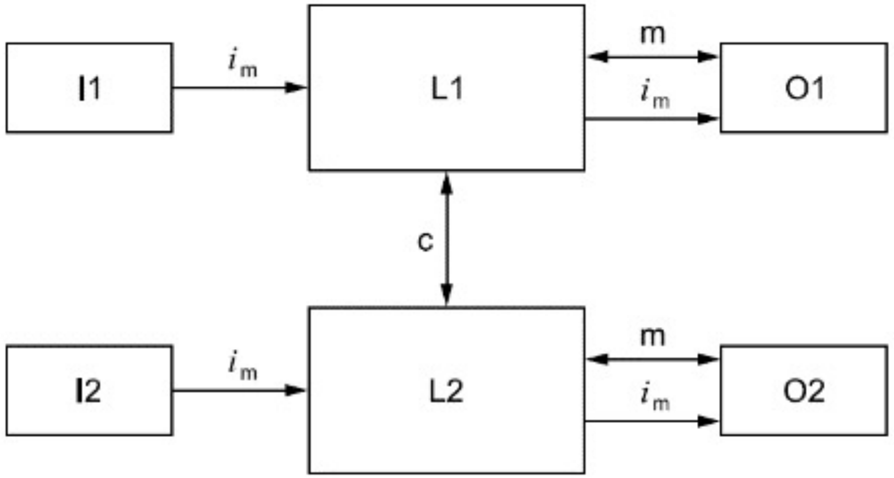
Categories / Architecture / Structure

- **Category B** (“Basic” – nothing special)

- **1** (“Safety Rated” devices)
- **2** (Testing/Monitoring/Diagnostics)

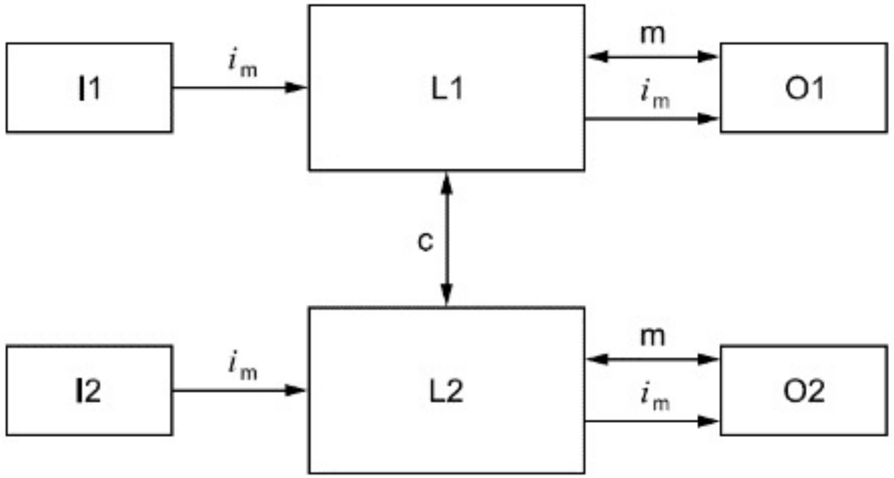


- **3** (Redundancy + Testing)
- **4** (Highest level of testing)



Calculate Performance Level of the Safety Function

- **PL** is based on combination of
  - Category (Architecture)
  - MTTFd (years)
  - Diagnostic Coverage %
  - Common Cause Failures #

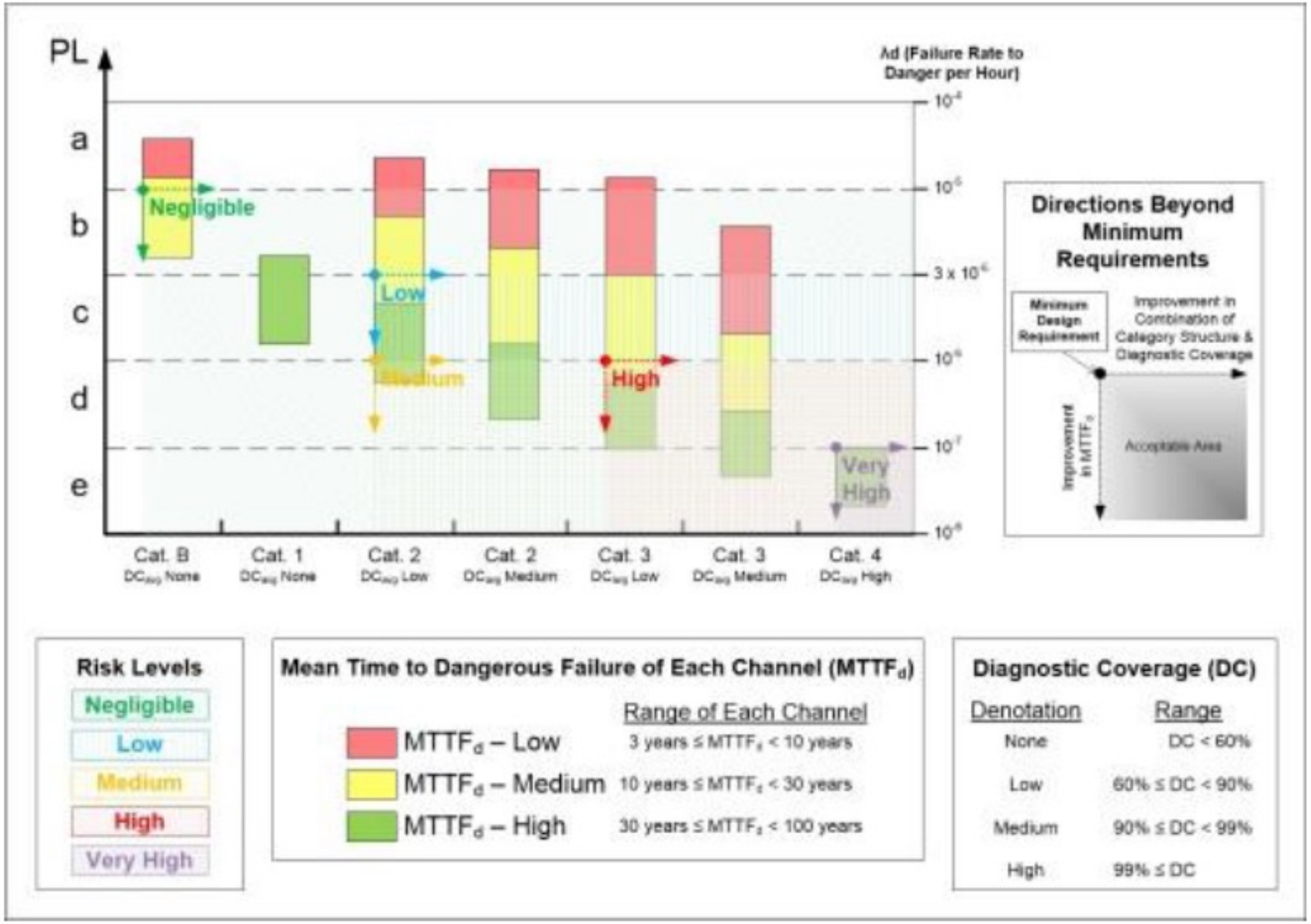


$$MTTF_D = 2/3\left[MTTF_D(ch1) + MTTF_D(ch2) - \frac{1}{\frac{1}{MTTF_D(ch1)} + \frac{1}{MTTF_D(ch2)}}\right]$$

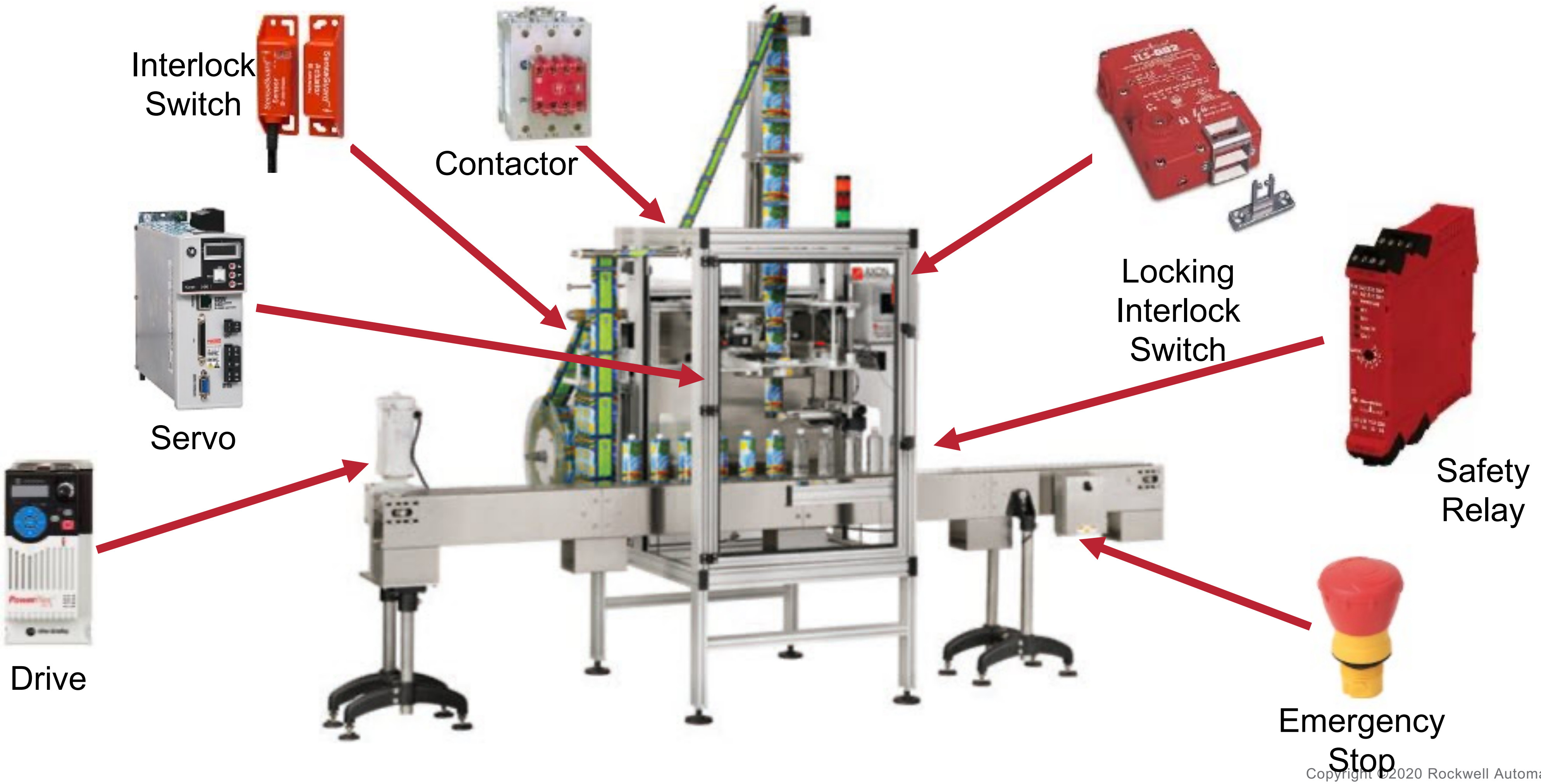
$$DCavg = \frac{\frac{DC1}{MTTFd1} + \frac{DC2}{MTTFd2} + \cdots + \frac{DCN}{MTTFdN}}{\frac{1}{MTTFd1} + \frac{1}{MTTFd2} + \cdots + \frac{1}{MTTFdN}}$$

Design to, and verify, Performance Level (PL)

- **PL** is based on combination of
  - Category (Architecture)
  - MTTFd (years)
  - Diagnostic Coverage %
  - Common Cause Failures #



Do this for Each Safety Function on the Machine



What about Safety Integrity Levels?

ISO 13849-1: Performance Levels (PL)

IEC 62061: Safety Integrity Levels (SIL)

Table 3 — Relationship between performance level (PL) and safety integrity level (SIL)

PL	SIL (IEC 61508–1, for information) high/continuous mode of operation
a	No correspondence
b	1
c	1
d	2
e	3

When a safety-related control function is designed using one or more SRP/CS, each SRP/CS shall be designed either according to this part of ISO 13849 or according to IEC 62061/IEC 61508 (see also ISO/TR 23849) — although there is correspondence between the PLs of this part of ISO 13849 and the SILs of IEC 61508 and IEC 62061. SRP/CSs are to be combined according to 6.3.

What about Safety Integrity Levels?

ISO 13849-1: Performance Levels (PL)

IEC 62061: Safety Integrity Levels (SIL)

Standard:	ISO 13849-1	IEC 62061
“Ratings”:	**PL** (a … e)	**SIL** (1,2,3)
Redundancy:	Structure (category: B,1,2,3,4)	Architecture (A,B,C,D)
Reliability:	$MTTF_d$	PFH_D
Diagnostic/Monitoring (%)	DC	SFF
Common Cause Failures:	CCF Score 65 / 100	CCF, ß factor (%)
Notes:	Readily applied to electromechanical devices	Readily applied to electronic systems

IEC 62061 Ed. 2.0 b:2021

This second edition cancels and replaces the first edition, published in 2005, Amendment 1:2012 and Amendment 2:2015. This edition constitutes a technical revision.

NEW Edition

<u>This edition includes the following significant technical changes with respect to the previous edition:</u>

1. – structure has been changed and contents have been updated to reflect the design process of the safety function,
2. – standard extended to non-electrical technologies,
3. – definitions updated to be aligned with IEC 61508-4,
4. – functional safety plan introduced and configuration management updated (Clause 4),
5. – requirements on parametrization expanded (Clause 6),
6. – reference to requirements on security added (Subclause 6.8),
7. – requirements on periodic testing added (Subclause 6.9),
8. – various improvements and clarification on architectures and reliability calculations (Clause 6 and Clause 7),
9. – shift from "SILCL" to "maximum SIL" of a subsystem (Clause 7),
10. – use cases for software described including requirements (Clause 8),
11. – requirements on independence for software verification (Clause 8) and validation activities (Clause 9) added,
12. – new informative annex with examples (Annex G),
13. – new informative annexes on typical MTTFD values, diagnostics and calculation methods for the architectures (Annex C, Annex D and Annex H).

IEC62061 “2nd Edition” (2021)

extended to non-electrical technologies

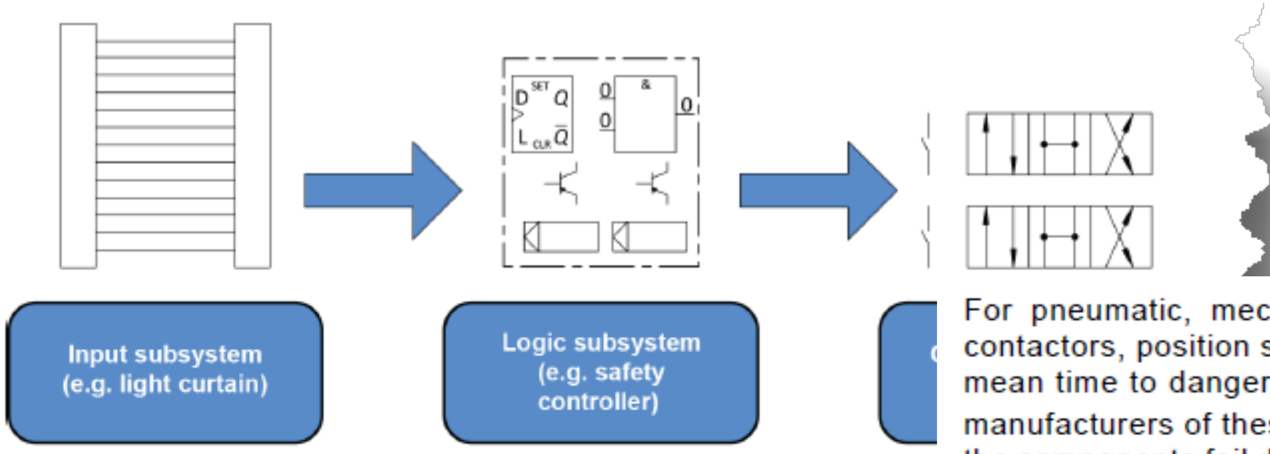


Figure 4 – Example of a combination of subsystems a

For pneumatic, mechanical and electromechanical components (pneumatic valves, relays, contactors, position switches, cams of position switches, etc.) it can be difficult to calculate the mean time to dangerous failure ($MTTF_D$ for components), which is given in years. Usually the manufacturers of these kinds of components only give the mean number of cycles until 10 % of the components fail dangerously (B_{10D}). This Clause 7 gives a method for calculating an $MTTF_D$ for components by using B_{10D} given by the manufacturer related closely to the application dependent cycles.

NOTE 3 Hydraulic components are mostly characterized with $MTTF_D$.

If the appropriate basic and well-tried safety principles are met, the $MTTF_D$ value for a single pneumatic, electromechanical or mechanical component can be estimated.

The mean number of cycles until 10 % of the components fail dangerously (B_{10D}) should be

IEC62061 “2nd Edition” (2021)

6.8 Security aspects

Security covers intentional attacks on the hardware, application programs and related software, as well as unintended events resulting from human error.

NOTE 1 Security aspects are considered in the security lifecycle of the machine (or higher system level) and throughout the life cycle of the machine.

NOTE 2 Since this document does not provide specific requirements on security aspects, guidance is provided in IEC TR 63074, ISA TR84.00.09, ISO/IEC 27001:2013, ISO TR 22100-4 and IEC 62443 (all parts).

Process Safety

www.rockwellautomation.com

Safety Moment

Safety Complacency

15-year anniversary of Texas City explosion

- 15 people killed; 180 people injured
- $1.5B in financial loss
- Operational procedures were not followed
- Personnel training was inadequate
- Instrumentation failed or provided false information
- HMI did not provide adequate process information
- Blowdown drum was citing by OSHA in 1992
- “In the years prior to the incident, **eight** serious releases of flammable material from the ISOM blowdown stack had occurred”
- Contractors were attending a lunch celebrating a month without a worktime injury

Remember

1. A safety incident does not have to be a violation of the daily routine, it can be a product of it.
2. Good safety performance can lead to a false sense of safety
3. Always question any deviations from defined risk levels
4. Study near-misses from the viewpoint of ***normalization of deviation***
5. Utilize outside & independent evaluations

KEY ISSUES:
SAFETY CULTURE
REGULATORY OVERSIGHT
PROCESS SAFETY METRICS
HUMAN FACTORS

BP
TEXAS CITY, TEXAS
MARCH 23, 2005

Source: https://www.csb.gov/bp-america-refinery-explosion/

Process Safety Overview

Process Safety means different things to different people, so the first thing to do is to define what Process Safety is NOT, then to explain what it actually IS (and what standards cover it).

Process Safety ***IS NOT*** about choosing a certified logic solver and calling it "Done".

Process Safety ***IS ACHIEVED*** by following series of well defined activities starting with identifying and quantifying ***RISK***, then implementing and managing safeguards to ***Reduce and Maintain*** that risk to an acceptable (tolerable) level, throughout the life of the Process.

Risk is defined by how often (frequency) and how bad (consequence) a hazardous event may be should it occur.

Risk Reduction is the SIL (Safety Integrity Level) required to reduce the risk to an acceptable level.

IEC Standards Structure

Basic Safety Standard (BSS)

Defines “Functional Safety”
Defines the “Rules”
for achieving Functional Safety
(regardless of application, technology or industry)

IEC 61508
International Performance Based Standard for all Industries

This standard is also used to asses/certify the suitability of Technology for use in Safety Applications.

Sector Standards

IEC 61511 is now published as
ANSI/ISA61511 – 1:2018

IEC 61511 - Process Industry **IEC 61513 - Nuclear Sector** **IEC 62061 - Machinery**

Legal Requirement for Process Safety

OSHA Process Safety Management

In 1991 OSHA published 29CFR1910.119, Process Safety Management (PSM) of highly hazardous chemicals.

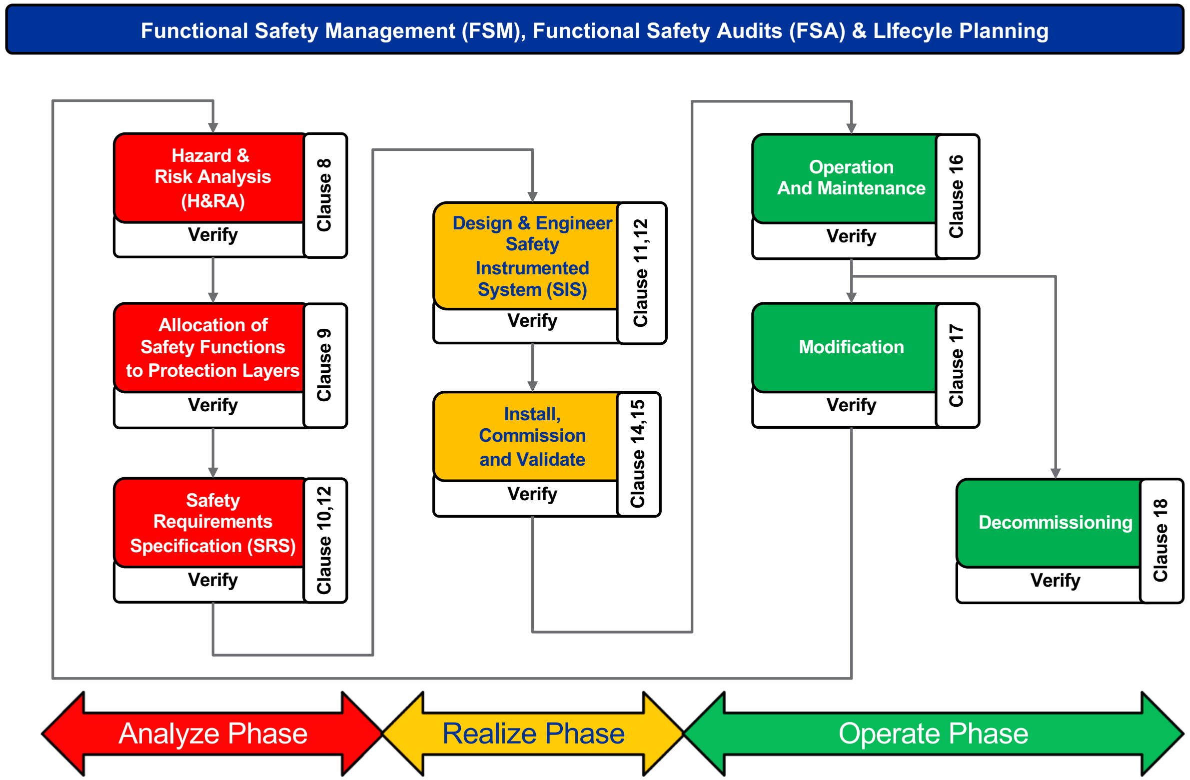
- Where it applies
  - “A process which involves a chemical at or above the specified threshold quantities...”
    - **10,000lbs of Anhydrous Ammonia**
    - **1,500lbs of Hydrogen Sulfide**
    - **10,000lbs of Flammable Liquid (flashpoint <100^{o}F) or Gas (Category 1)**
  - “ This OSHA standard is required by the Clean Air Act Amendments as is the EPA’s Risk Management Plan.”
- Even in industries that aren’t required to follow PSM, they often look to PSM as a best practices (RAGAGEP)

OSHA PSM Problem Statement

Unexpected releases of toxic, reactive, or flammable liquids and gases in processes involving highly hazardous chemicals have been reported for many years. Incidents continue to occur in various industries that use highly hazardous chemicals which may be toxic, reactive, flammable, or explosive, or may exhibit a combination of these properties. **Regardless of the industry that uses these highly hazardous chemicals, there is a potential for an accidental release any time they are not properly controlled.** This, in turn, creates the possibility of disaster.

IEC61511 – What is it ?

It is THE sector standard for the Process Sector, a sector defined as:
"a wide variety of industries within the process sector for example, chemicals, oil and gas, pulp and paper, pharmaceuticals, food and beverage, and non-nuclear power generation".



- This standard takes the relevant parts of IEC61508 then applies 'Process Sector' language making it understandable to "Process Users".
- e.g.
  EUC risk (IEC61508)
  risk arising from the EUC or its interaction with the EUC control system
  process risk (IEC61511)
  risk arising from the process conditions caused by abnormal events (including BPCS malfunction).

IEC61511 = how to apply IEC61508 in the Process Sector

Other Important Standards (Application Standards)

IEC/ISA61511 is a standard that simply addresses how to mitigate identified hazards, specifically those in the Process Sector. It does not attempt to be specific about whether the hazard is related to Burner Management, Toxic exposure due to leaks, etc. It simply says that whatever the Hazard is (or what equipment is involved), here is a method you can use to quantify how much risk reduction is required to prevent the consequences.

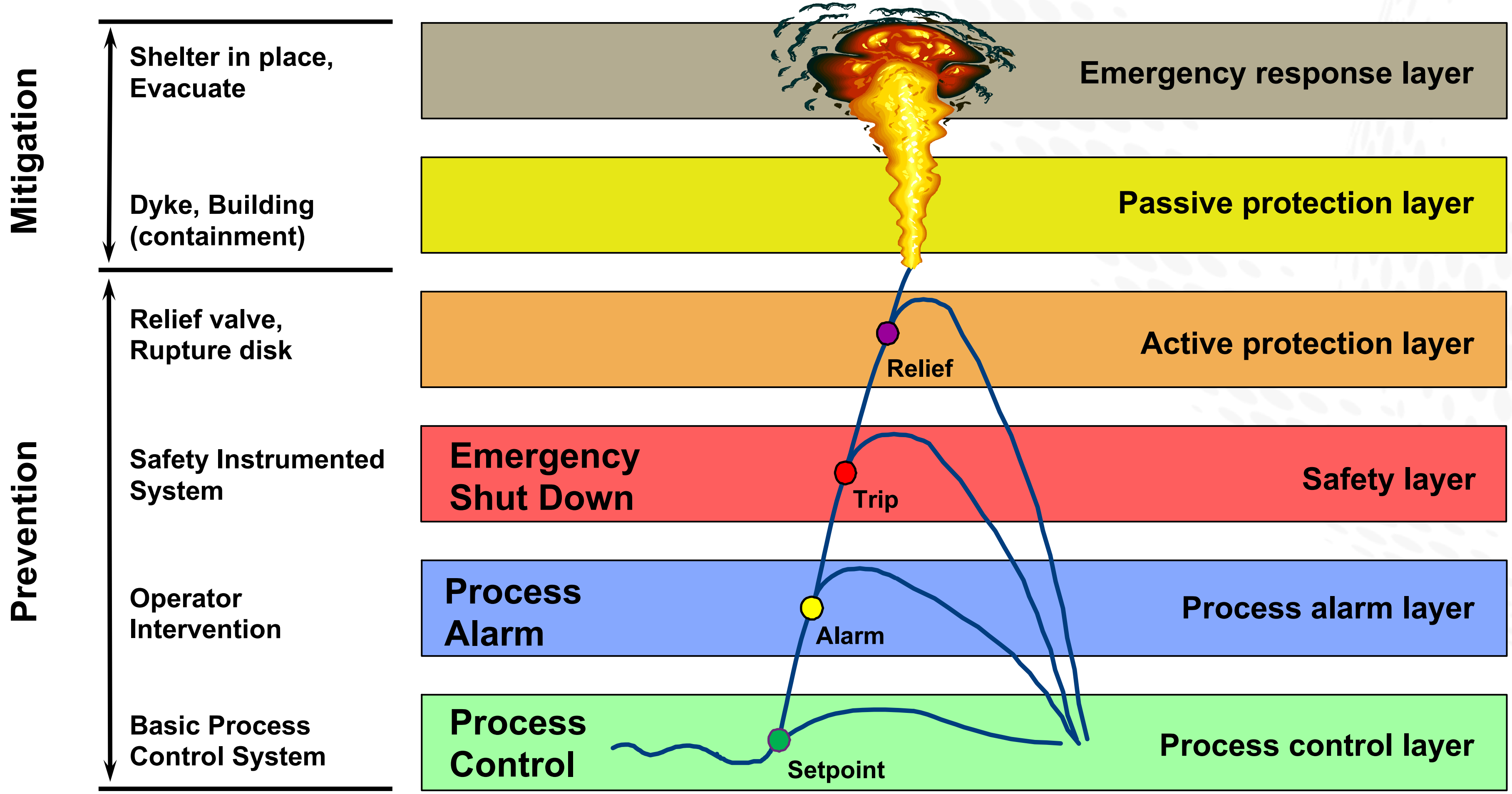
NFPA – National Fire Protection Association

- NFPA85 – specific guidelines for Boilers
- NFPA86 – specific guidelines for Ovens and Furnaces
- NFPA87 – specific guidelines for Heaters
- NFPA72 – specific guidelines for Fire Alarm systems (not Gas and not Protection systems)

API – American Petroleum Institute

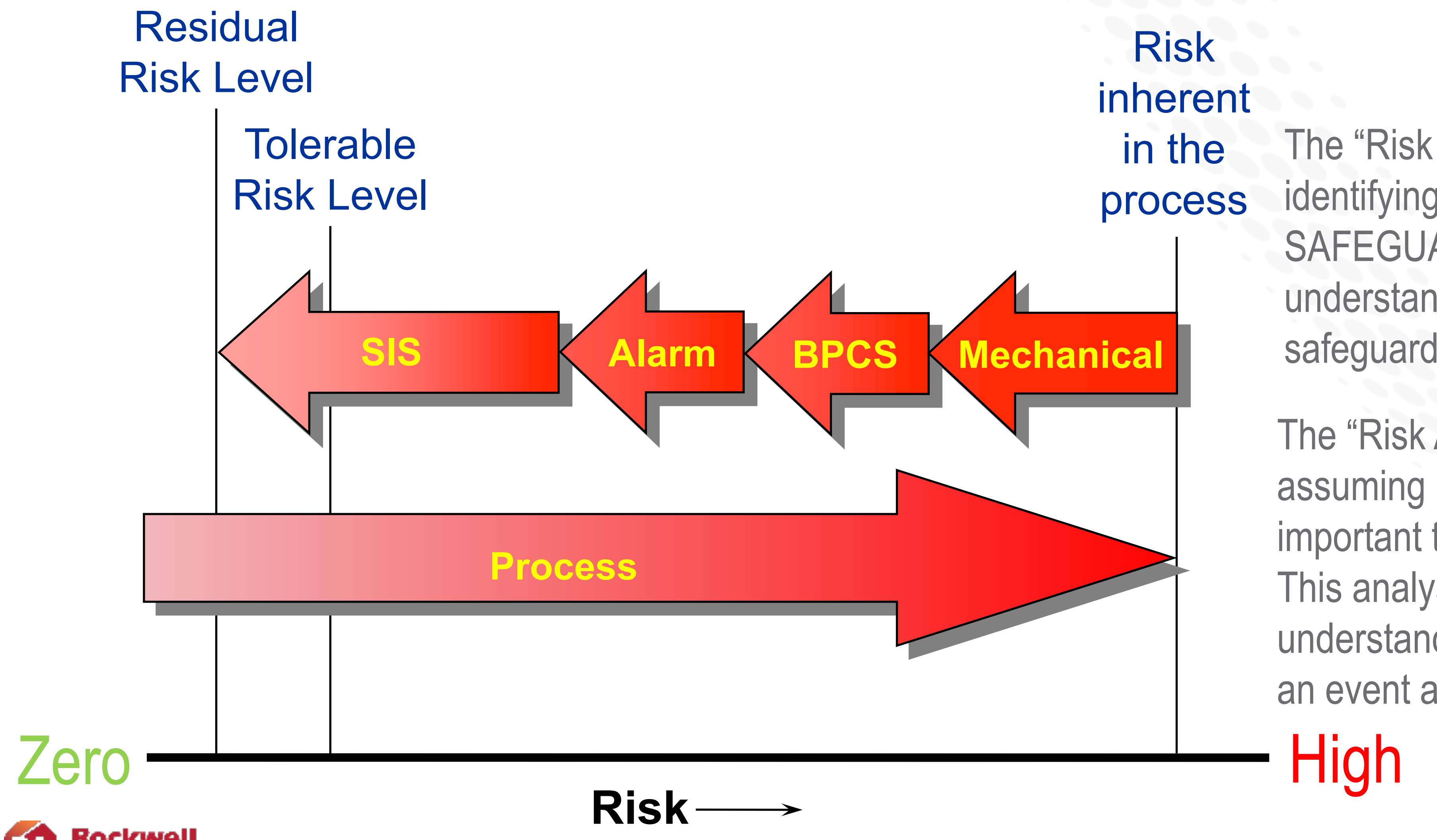
- API14C – specific guidelines for safety in offshore platforms (legal requirement in GoM)
- API17F – specific guidelines for Subsea Production systems
- API556 – specific guidelines for Heaters (Production, Refining and Chemicals)

Layers of Protection



Process Safety Lifecycle

Analysis Phase – Assessing Risk

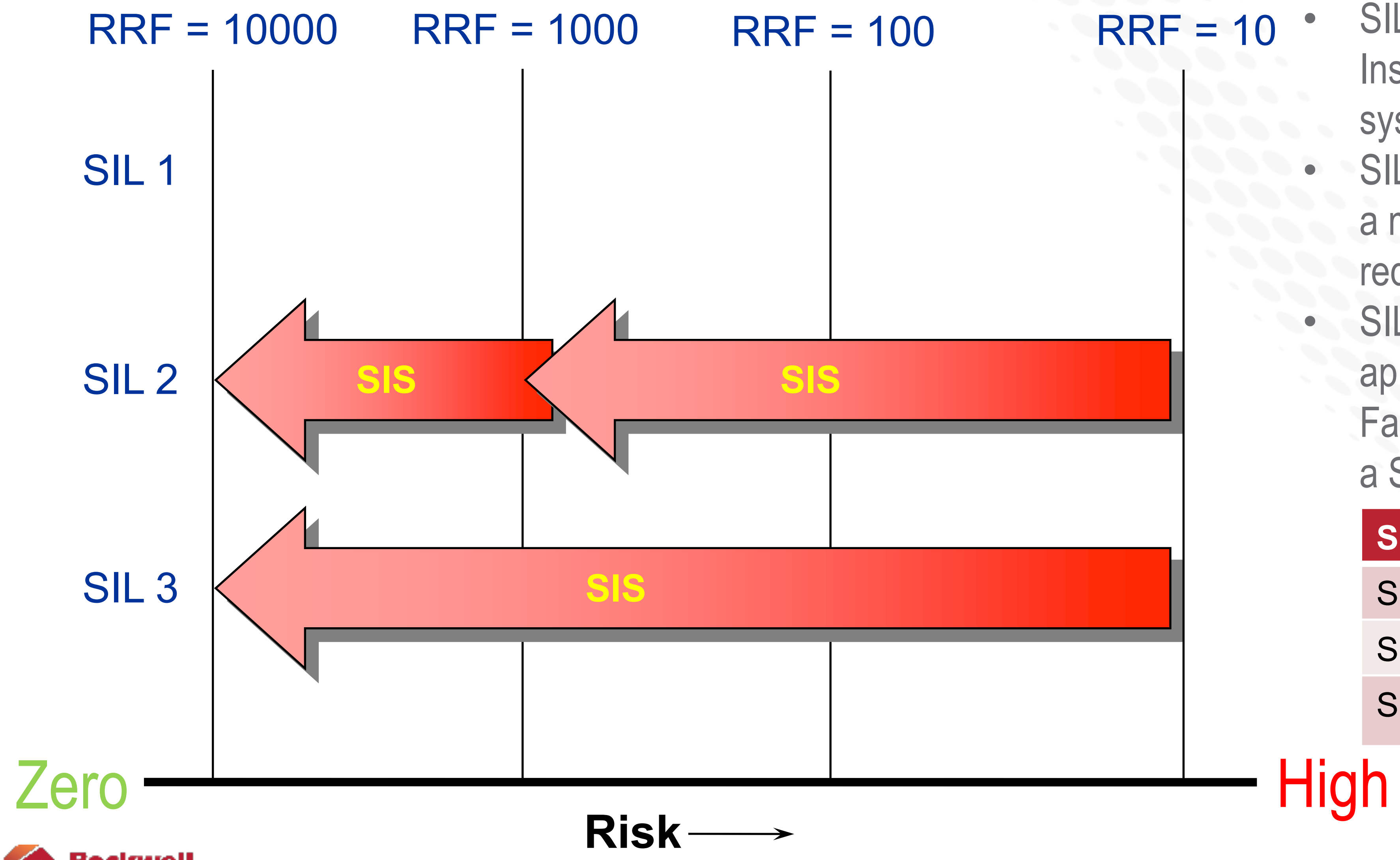


The "Risk Reduction" is performed by identifying and quantifying the SAFEGUARDS, this is important to understand the effectiveness of the safeguards.

The "Risk Assessment" is performed assuming NO SAFEGUARDS, this is important to the next step.
This analysis is done on the basis of understanding both the CONSEQUENCE of an event and the FREQUENCY of an event.

Safety Integrity Levels

Risk Reduction Factors



- SIL targets are assigned to each Safety Instrument Functions(SIF) NOT to the system.
- SIL is NOT a measure of reliability, it is a measure of the degree of risk reduction needed to meet a target
- SIL covers a range of risk reduction, appropriate Risk Reduction Factors(RRF) should be determined for a SIF.

SIL	RRF
SIL 1	10 ≤ RRF < 100
SIL 2	100 ≤ RRF < 1000
SIL 3	1000 ≤ RRF < 10000

SIS Controller Portfolio

Small Applications
Compact GuardLogix®

Large Applications
GuardLogix®

- Multiple control disciplines
- Flexible and scalable
- Real-time information-enabled
- Standard, unmodified Ethernet
- One common integrated design environment
- Local and distributed I/O options

Process Safety Configured
ControlLogix w/1715 I/O

- Common platform with BPCS
- Fault Tolerant logic solver and I/O
- Online edit capability for safety logic
- Common programming environment

Process safety
AADvance® /Trusted®

- Scalable redundancy for fault tolerance
- Provides safety and availability requirements
- Diverse SIS offering
- Distributed processing power

Rockwell Automation

Safety Functions Documents – Example Application Techniques

- Well over 100 examples
- BOM, Wiring, Configuration/Programming
- Verification & Validation
- Some now have.DXF, .ACD, other files attached

Click or Scan:

Link here: www.machinesafetysolutions.com

Application Technique

Allen-Bradley

Emergency Stop Products: Integrated Safety Controller Connected to a Series of Dual-channel E-stop Buttons Safety Function

Products: GuardLogix 5570 or Compact GuardLogix 5370 Controller, POINT Guard I/O Safety Module, Dual-channel E-stop Button

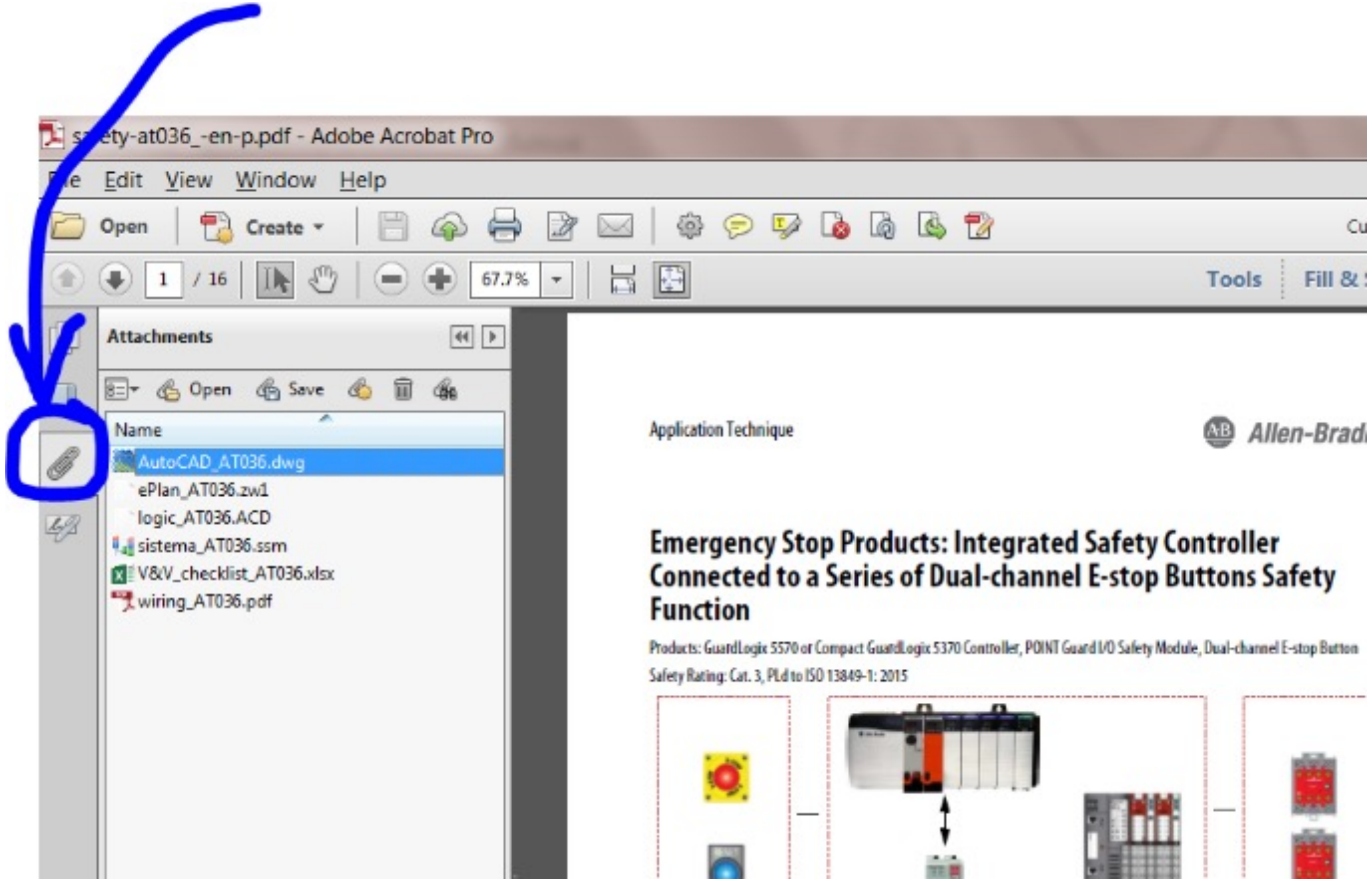
Safety Rating: Cat. 3, PLd to ISO 13849-1: 2015

LISTEN. THINK. SOLVE.

Allen-Bradley · Rockwell Software

Rockwell Automation

Safety Functions Documents – Example Application Techniques



- Many now have attachments
- In Adobe, click the *paperclip icon*
  - AutoCad & ePlan files
  - .ACD file for Logix
  - SISTEMA File
  - Verification & Validation checklists

Click or Scan:

Link here: www.machinesafetysolutions.com

Rockwell Automation

www.machinesafetysolutions.com

Safety Solutions

Safety Management

Deliver a measurable difference to plant safety, performance, and profitability

Optimize Performance

Machine Safety

Improve safety and performance, reduce development time to ISO 13849-1, IEC 62061

Increase Productivity

Process Safety

Safety instrumented systems to protect your people, assets, and the environment

Reduce Risk

Electrical Safety

Arc containment safety technologies and services

Reduce Exposure

Optimize Safety, Productivity, and Design Time

Services, Tools, and Technology for Best-in-class Performance

Numerous studies show that best-in-class performers achieve 5 to 7% higher OEE, 2 to 4% less unscheduled

www.machinesafetysolutions.com

- Whitepapers
- Videos
- Blog topics
- Application Examples
- Engineering Resources
- Self Maturity Self-Assessment tools
- Smart Safety Devices & Systems
- Software tools
- And more … !

Thank you!

www.rockwellautomation.com