SAFETY INTERLOCK DESIGN CHALLENGES

SEMICONDUCTOR INDUSTRY WAFER PROCESSING EQUIPMENT

Mark Fessler (ASMI) 2019 SESHA - Safety Interlock Design Challenges

REMEMBER: HIERARCHY OF CONTROLS

Inherently Safe Design Focus

~ redesign to completely remove or greatly reduce the severity of hazard!
change materials, change chemicals; 100% H_2 to 2% H_2; or 110 VAC to 24 VDC

Today's Focus Area

Hazard Zone Area Focus

~ add a fixed guard
~ add 2nd containment / local exhaust
~ add EMO
~ add safety interlocks

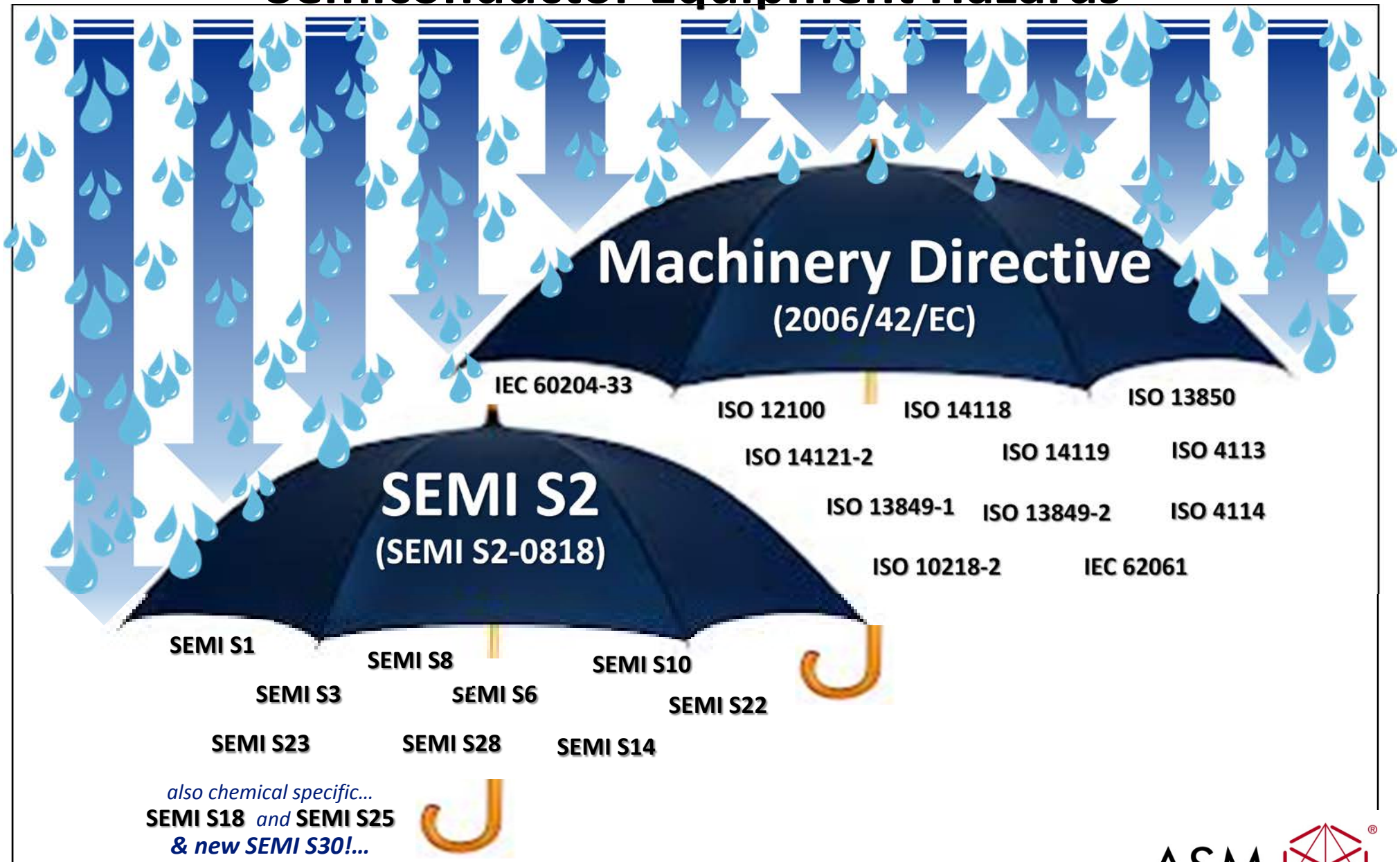
We do not want to have to rely on any human being "perfect"!

~ add warning devices
~ add warning labels
~ ensure documented procedures
~ ensure proper training
~ ensure proper PPE

AGENDA

- Safety Interlock Requirements Evolution
- Safety Interlock Related - Misused Terms
- ASM Safety Rated Interlock Components
- ASM's Component Selection Flowchart

Semiconductor Equipment Hazards



ASM

SAFETY INTERLOCK REQUIREMENTS EVOLUTION

SEMI® International Standards

"*Umbrella*" Standards

LET'S LOOK AT THE 2 TIMELINES...

"*International*" Standards

2 KEY TIMELINES: SAFETY INTERLOCK REQUIREMENTS

89/392/EEC

Machinery Directive (1989)
Annex 1.2.1 Safety / Reliability of Control Systems

- ~ Must be Safe and Reliable
- ~ Withstand rigors of normal use and external factors
- ~ Errors do not lead to dangerous situations
- ~ Entry into force Jan 1st 1993 / Mandatory Jan 1st 1995
- ~ (24 pages)

SEMI S2 (1991)
Section 3: Interlocks

- ~ FAIL-SAFE Hardware Interlocks
- ~ Operator notification
- ~ Manual Reset To Restart
- ~ No Definitions
- ~ (12 pages)

SEMI S2 (1993)
Section 5: Safety-Related Interlocks

- ~ Added Definitions between H/W and S/W
- ~ Added Definition (Fail-Safe)
- ~ Rest remained basically the same…
- ~ No "Suitability for Use" criteria yet!
- ~ (18 pages)

"European Only"
Harmonized EN Standards

EN 1088 (1995)
Interlocking Devices Associated with Guards

- ~ intended for electrical interlocking devices
- ~ mechanical & non-mechanical actuators
- ~ power-actuated guard locking devices
- ~ "Positive-Mode" actuation defined
- ~ (38 pages)

EN 954-1 (1996)
Introduced Safety Related Parts, & Control Categories

- ~ Safety-Related Parts of Control Systems
- ~ Based on non-programmable elements
- ~ Defined Risk Versus Design Categories
- ~ Fault Exclusion Concept
- ~ (22 pages)

2 KEY TIMELINES: SAFETY INTERLOCK REQUIREMENTS

89/392/EEC

Machinery Directive (1989)
Annex 1.2.1 Safety / Reliability of Control Systems

- ~ Must be Safe and Reliable
- ~ Withstand rigors of normal use and external factors
- ~ Errors do not lead to dangerous situations
- ~ Entry into force Jan 1st 1993 / Mandatory Jan 1st 1995
- ~ (24 pages)

SEMI S2 (1991)
Section 3: Interlocks

- ~ FAIL-SAFE Hardware Interlocks
- ~ Operator notification
- ~ Manual Reset To Restart
- ~ No Definitions
- ~ (12 pages)

SEMI S2 (1993)
Section 5: Safety-Related Interlocks

- ~ Added Definitions between H/W and S/W
- ~ Added Definition (Fail-Safe)
- ~ Rest remained basically the same…
- ~ No "Suitability for Use" criteria yet!
- ~ (18 pages)

IEC 61508 (1998)
Introduced SIL: Safety Integrity Levels

- ~ Included programmable systems
  (Software, Firmware, PLC's)
- ~ It literally changed the process industries!
- ~ 7 Total Volumes – it changed industry!
- ~ (328 pages in 1998, & 815 pages by 2000)

EN 1088 to ISO 14119 (1998)
Interlocking Devices Associated with Guards

- ~ Technical content stays the same
- ~ Now International consensus, versus just EU
- ~ More detailed description of applications
- ~ (50 pages)

EN954-1 to ISO 13849-1 (1999)
Safety-Related Parts of Control Systems

- ~ S, F, P selection determines Category
- ~ Focused on component selection
- ~ Introduced "Well-Tried Safety Principles"
- ~ Introduced "Well-Tried Safety Components"
- ~ (31 pages)

2 KEY TIMELINES: SAFETY INTERLOCK REQUIREMENTS

SEMI S2 (2000)
Section 11: Safety-Related Interlocks

- ~ Added new definition (fault tolerant)
- ~ Added "Suitability-for-Use" criteria which was significant for evaluating the safety interlock components used in the design
- ~ (75 pages)

SEMI S2 (2003)
Section 11: Safety-Related Interlocks

- ~ Added new definition (FECS)
- ~ Added New RI14 Recommendations for Designing and Selecting Fail-to-Safe (FECS) with Solid-State Interlocks
- ~ (90 pages)

Machinery Directive (2006) 2006/42/EC
Annex 1.2.1 Safety / Reliability of Control Sys

- ~ Must consider ***reasonably foreseeable misuse!***
- ~ Safety and reliability of control systems expanded to apply to all parts of a control sys
- ~ New guard locking requirements
- ~ (90 pages)

ISO 13849-2 (2003)
Introduced
Verification / Validation Methods

- ~ Introduced validation methods for Mechanical, Hydraulic, Pneumatic and Electronic components
- ~ Verification of Control Category (CAT B, 1, 2, 3, 4)
- ~ (50 pages)

IEC 62061 (2005)
Introduced SIL's
Safety Integrity Levels

- ~ Introduced a simplified "Machinery Sector" version of Process Industry IEC 61508 (Software, Firmware, PLC's)
- ~ NOTE: mechanical, hydraulic, pneumatic components are not in scope!
- ~ (205 pages)

ISO 13849-1 (2006)
Introduced Required PL_r ;
& achieved Performance Levels

Performance Level (PL) was introduced, quantitatively expressed as combination

- ~ Reliability of component = $MTTF_d$,
- ~ Diagnostic Coverage = DC_{AVG}
- ~ Control Category (B,1,2,3,4)
- ~ (100 pages)

2 KEY TIMELINES: SAFETY INTERLOCK REQUIREMENTS

SEMI S2 (2015)

New Related Information 17 (RI 17)

- ~ RI 17 provided additional guidance for safety functions used in conjunction with FECS.
- ~ Safety Functions with direct references to both ISO 13849-1 (Required Performance Levels, PL_r) and IEC 60261 (Safety Integrity Levels, SIL)
- ~ (124 pages)

SEMI S2 (2018)

Section 11: New Interlock Requirements

- ~ New FECS / Safety PLC compliance references
- ~ Safety PLC's now have new Management of Change Requirements as specified in SEMI S22
- ~ Equipment needs to have ability to verify Safety PLC's version installed on tool, and verify compatible H/W exist.
- ~ (150 pages)

ISO 13849-2 (2012)

Expanded Verification / Validation Methods

- ~ New Annex E with Examples for Validation
- ~ Validation of Control Category; $MTTF_d$; DC_{AVG}, and CCF
- ~ Validation of Systemic Failures, Safety S/W
- ~ Validation and Verification of Performance Level
- ~ (79 pages)

ISO 14119 (2013)

Interlocking Devices Associated with Guards

- ~ Minimizing interlock defeat is a requirement
- ~ Four types of interlocking devices defined
- ~ New Guard-Locking requirements
- ~ Became mandatory April 2015
- ~ (68 pages)

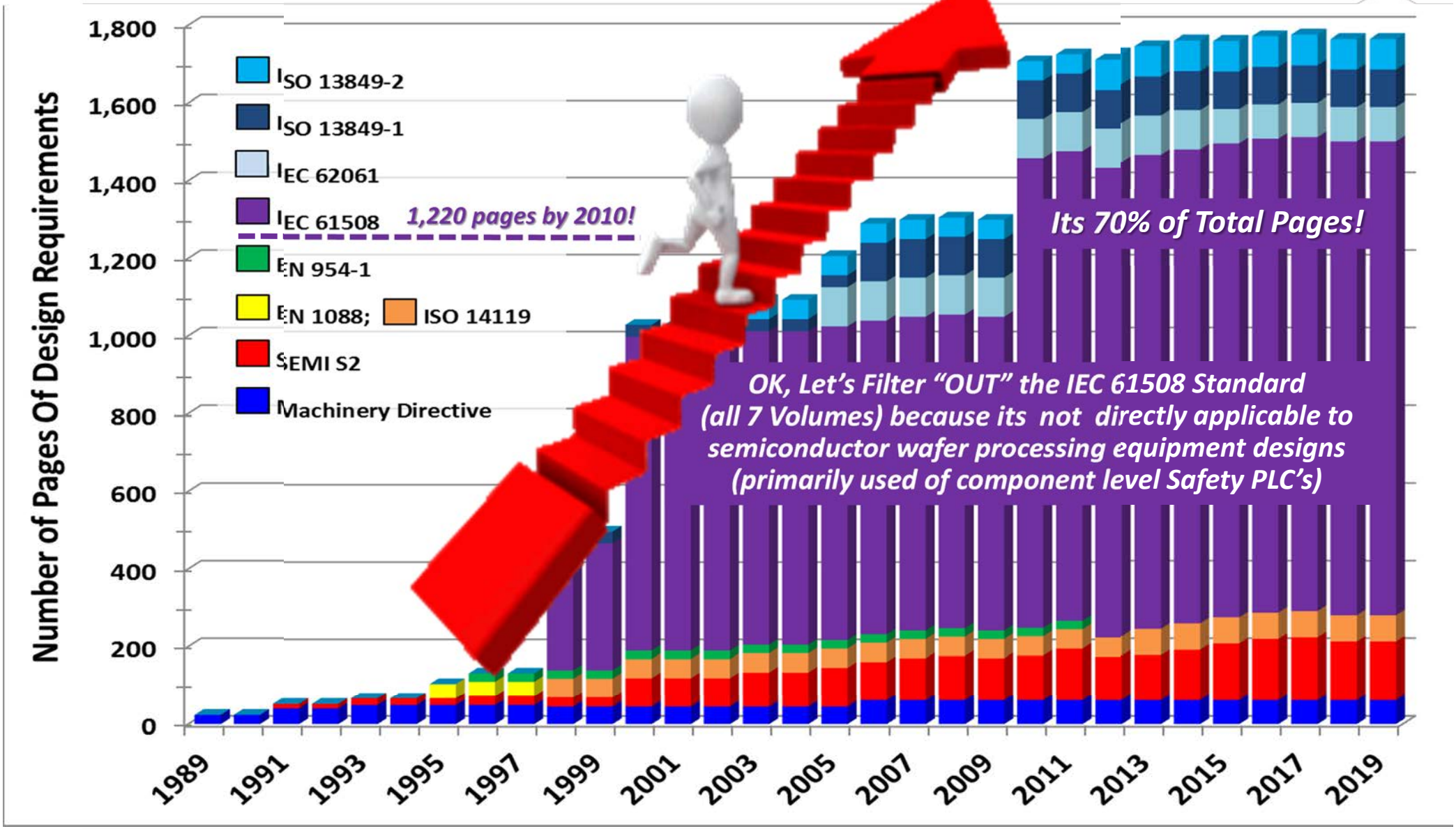
ISO 13849-1 (2015)

Clarified Mis-Interpreted Sections

- ~ Risk matrix renamed: required PL_r for safety function
- ~ ANNEX A Prob. of occurrence allowances, if not 100%
- ~ CAT 2 Demand Rate Changes
- ~ CAT 4 subsystems capping limit raised to 2500 yrs
- ~ (96 pages)

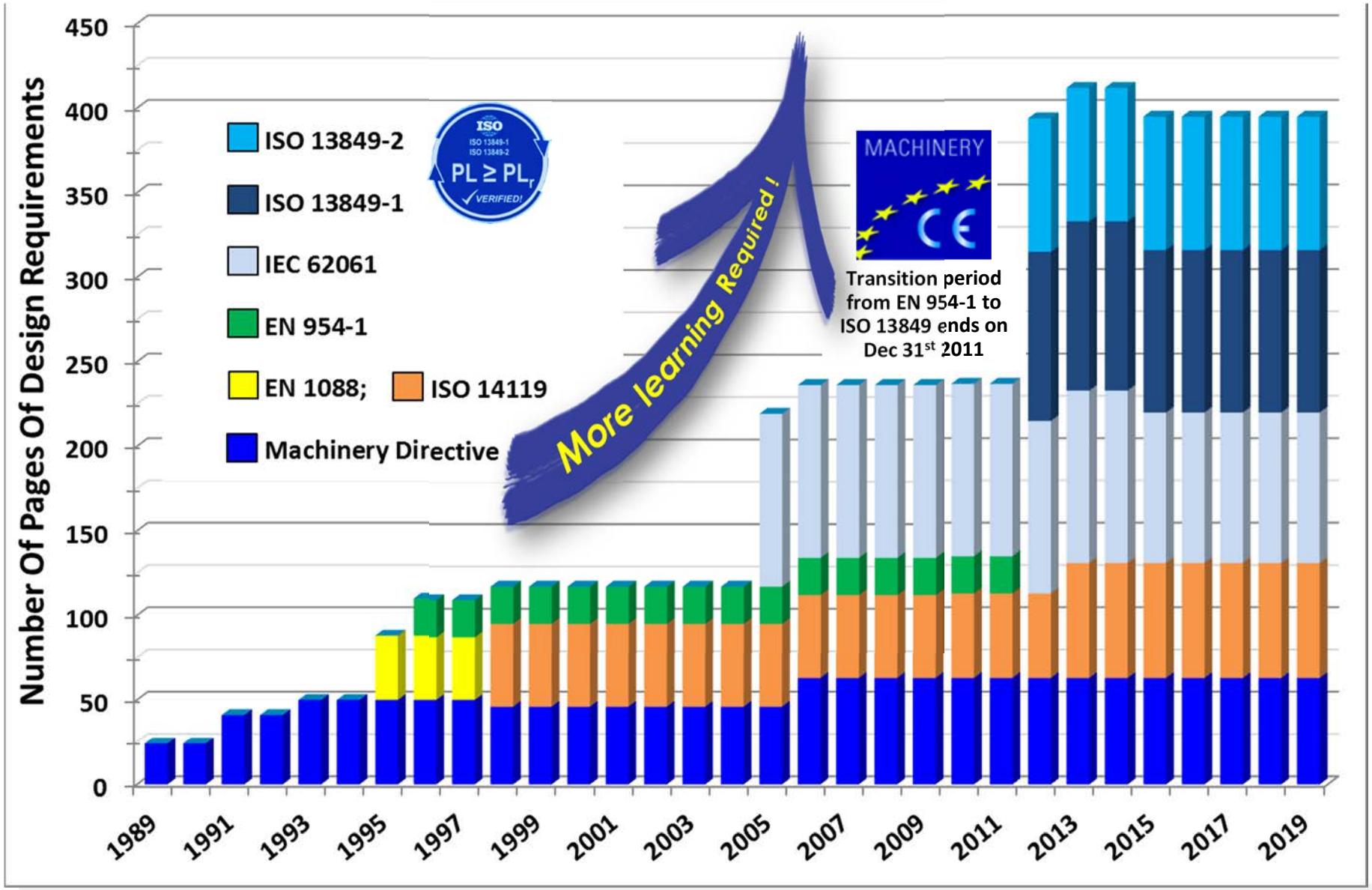
Continued Increase In Safety Interlock Design Requirements!

(History Of The the 9 Key Safety Interlock Standards For Semiconductor Equipment)



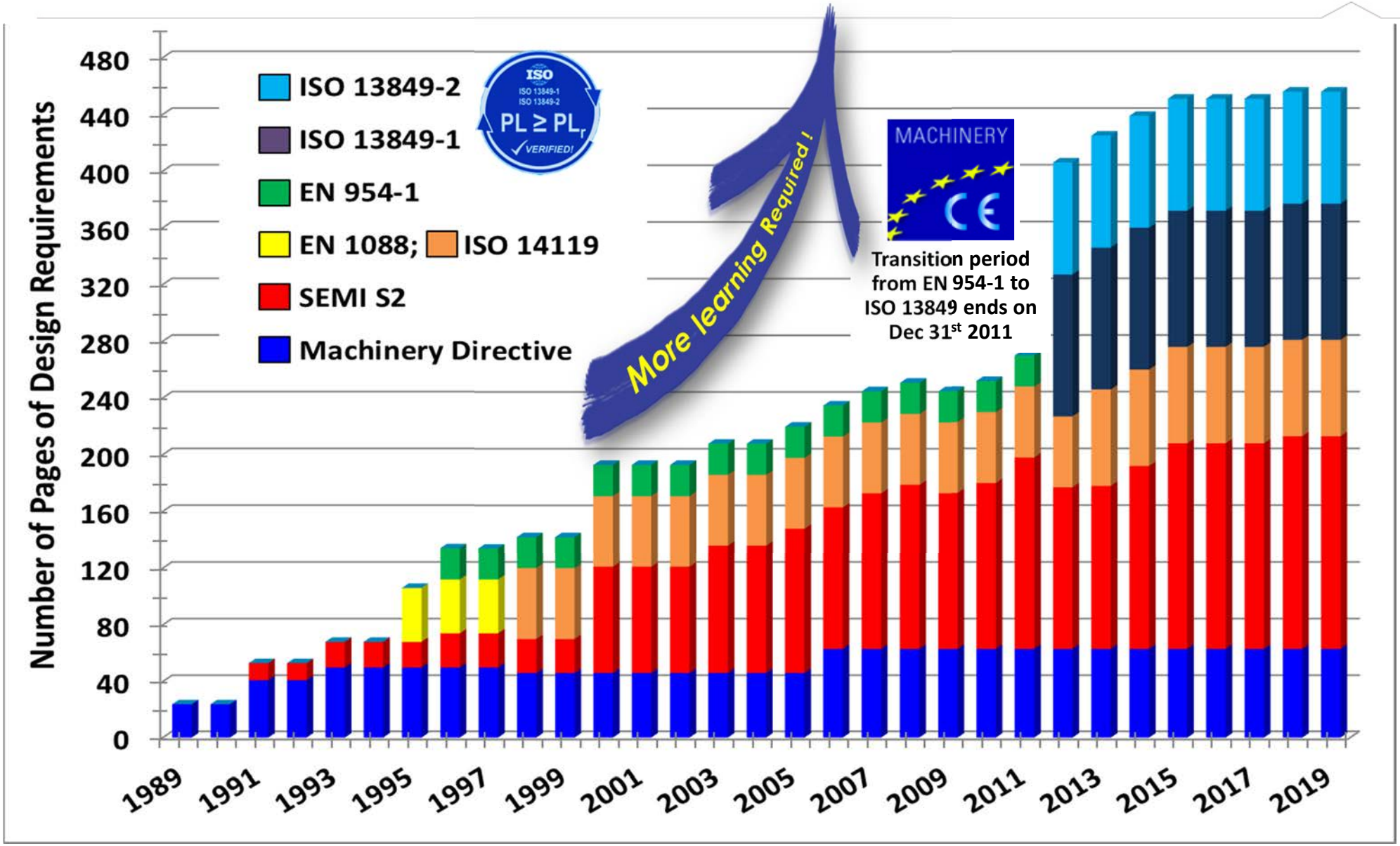
Rapid Increase In Safety Interlock Design Requirements

(History Of The 7 Safety Interlock Standards For Machinery)



Rapid Increase In Safety Interlock Design Requirements

(History Of The 7 Most Applicable Safety Interlock Standards For Semiconductor Equipment)



Summary:

- **Safety Interlock design requirements have steadily increased in complexity over past 30 years (> 20 different new or revised design standards) with much more detailed design and validation requirements, especially in the *last 7 years* (since January 1st 2012).**

- **A new knowledge base is required, and new education is also required to our design engineers as the concepts of such specifics are simply *not taught* in today's higher Engineering education**
  (e.g. Only through self-learning, OTJ training, formal technical training seminars)

AGENDA

- Safety Interlock Requirements Evolution
- **Safety Interlock Related - Misused Terms**
- ASM Safety Rated Interlock Components
- ASM's Component Selection Flowchart

SAFETY INTERLOCK RELATED - MISUSED TERMS

Before we dive into more details of design Challenges, let's spend a little bit of time to explain these 4 important, and often misused, terms/phrases as they relate to safety interlock components.

1) **What Does a *"Listed"* Electrical Component Mean?**
2) **What Are the Differences between UL , UR, CE and another CE ?**
3) **What Does *"Functional Safety"* Mean?**
4) **What does a *"Safety-Rated"* Mean?**

SAFETY INTERLOCK RELATED - MISUSED TERMS

What Does a *"LISTED"* Electrical Component Mean?

It's from OSHA…. NOT from SEMI!

This is a term from United States OSHA regulation, ***1910.303 = Subpart: S (Electrical)***

This subpart addresses design safety standards for electrical systems, and states that they are ***"acceptable"*** to the Assistant Secretary of Labor (as defined in ***Sec. 1910.399***) if they are…

determined to be safe (a.k.a. "Listed") by an Nationally Recognized Test Lab (NRTL)

This subpart addresses design safety standards for electrical systems, and states that they are "acceptable" to the Assistant Secretary of Labor if and only if they meets 1 of the following 3 requirements as defined in Sec. 1910.399. (Definitions)

1) If it is accepted, or certified, or listed, or labeled, or otherwise determined to be safe by a nationally recognized testing laboratory recognized pursuant to § 1910.7; (definitions and requirements for a NRTL)

OR

2) With respect to installation that no NRTL accepts, if it is inspected by another federal Agency, or by a State, or local authority responsible for enforcing occupational safety provisions of the NEC (NFPA 70) and found compliant.

OR

3) With respect to custom made equipment, that are designed for a particular customer, if it is determined to be safe by its manufacturer on basis of test data which employer keeps and makes available for inspection to the Assistant Secretary.

SAFETY INTERLOCK RELATED - MISUSED TERMS

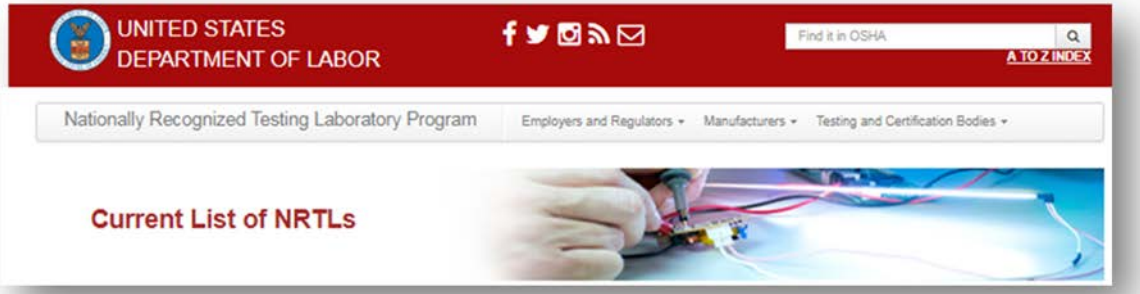
What Does a *"LISTED"* Electrical Component Mean?

It's from OSHA…. NOT from SEMI!

This is a term from United States OSHA regulation, ***1910.303 = Subpart: S (Electrical)***

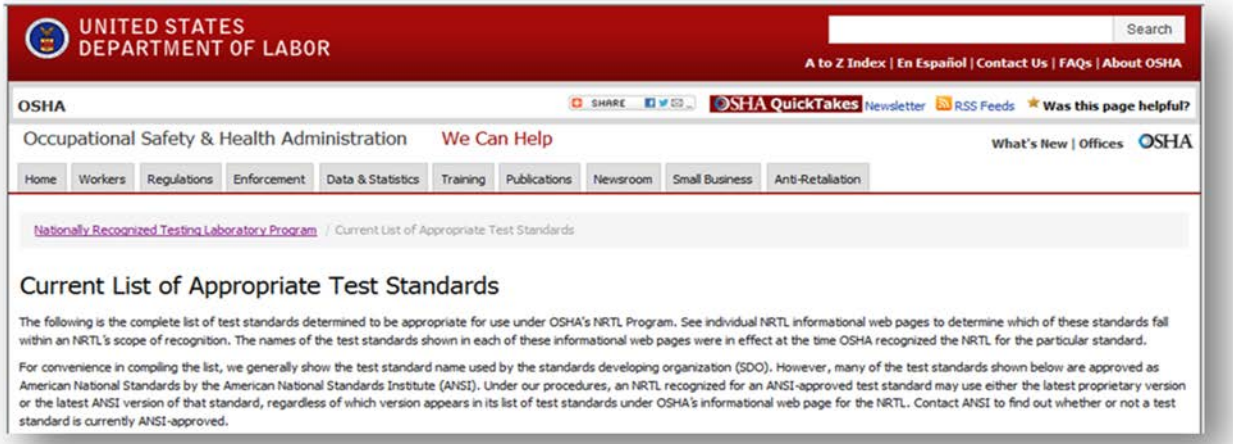
This subpart addresses design safety standards for electrical systems, and states that they are ***"acceptable"*** to the Assistant Secretary of Labor (as defined in ***Sec. 1910.399***) if they are…

determined to be safe (a.k.a. "Listed") by an Nationally Recognized Test Lab (NRTL)



SAFETY INTERLOCK RELATED - MISUSED TERMS

What Does a *"LISTED"* Electrical Component Mean?



- ***As of March 2019, There are total of 790 "appropriate" standards listed by OSHA as being applicable for NRTL evaluations (i.e. ASME, CGA, CSA, FM, IEEE, ISA, NEMA, NFPA, UL, …)***

But… SEMI S2 is NOT one of them!

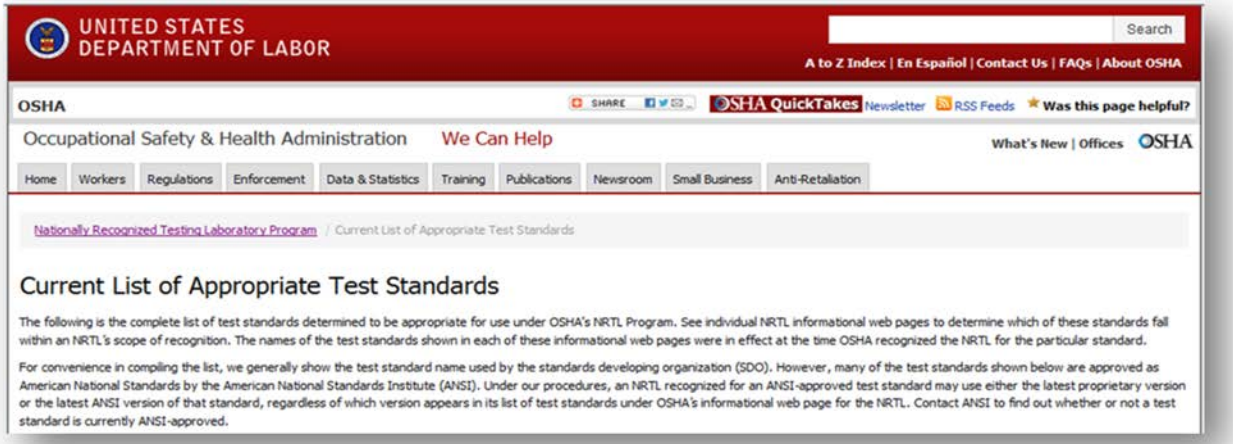
- ***However, NRTL is "similar" but not the same as SEMI S2 Definition for ATL = Accredited Test Laboratory (this term is not as US-centric!)***

SEMI S2 Section 5 Definitions

5.2.2 *accredited testing laboratory* — an independent organization dedicated to the testing of components, devices, or systems that is recognized by a governmental or regulatory body as competent to perform evaluations based on established safety standards.

SAFETY INTERLOCK RELATED - MISUSED TERMS

What Does a *"LISTED"* Electrical Component Mean?



- ***As of March 2019, There are total of 790 "appropriate" standards listed by OSHA as being applicable for NRTL evaluations (i.e. ASME, CGA, CSA, FM, IEEE, ISA, NEMA, NFPA, UL, …)***

But… SEMI S2 is NOT one of them!

SUMMARY: A so-called ***"Listed"*** component or assembly simply means that an OSHA approved **NRTL** has determined that it does not have reasonably foreseeable risk of fire, electric shock or related hazards, based on actual testing to a specific standard, and reoccurring QA audits.

Key Point: *"Listed" components* do NOT guarantee *"safety interlock performance"*!

What Are Differences: *UL Listed* Versus *UL Recognized*?

Well… It's from UL…. NOT OSHA!

It applies to specific country standards/regulations such as US and Canada, EU, Japan, etc.

- **UL LISTED:** Means UL has determined the manufacturer can reliably and dependably make part which ***does not have reasonably foreseeable risks of fire, or electric shock*** and related hazards. UL establishes ***"Quality Assurance"*** re-inspections to ensure compliance over product lifetime!

- **UL Recognized**: Consumers rarely see this mark because they are specifically used on component parts that are part of a larger product. It means components have been *"tested and evaluated"*, ***but are incomplete by themselves***, and have restricted performance capabilities once installed in end-product.
- At ASM, Product safety team must ensure we obtain the conditions of recognition from the mfg. and install accordingly, to ensure the UR mark is NOT voided..
  - ***For example, conditions of recognition requires the installation of additional upstream protective devices (e.g. fuse or circuit breaker)***

SAFETY INTERLOCK RELATED - MISUSED TERMS

What Are Differences: UL Versus CE Versus another CE ?

UL LISTED (USA/Canada, etc.):

This mark does requires 3rd party certification. Its focus is preventing electrical shock and fire hazards ONLY; ***It does NOT cover all other hazards of semiconductor equipment (e.g. chemical, mechanical, UV, IR, noise, etc.).*** Not all UL marks are same - you need to know the UL standard its listed to!

CE Marking (EU):

"Conformité Européenne"

The ***Conformité Européenne*** (CE) mark is required on "certain" products sold in the Europe. It does NOT require 3rd Party certification for semiconductor equipment – only self-declaration to Machinery Directive and EMC Directive. Other sub-assembles and components may have a CE marking to a specific directive for that component, but not all CE marks are the same - you need to know to which "EU Directive" its declaring conformance.

- **CE does NOT always = Product Safety. (Example: CE Mark for EMC Directive is NOT a for safety!)**
- **Having CE marks alone on components used in interlocks is usually not sufficient for SEMI S2 or MD!**

China Export Mark (China):

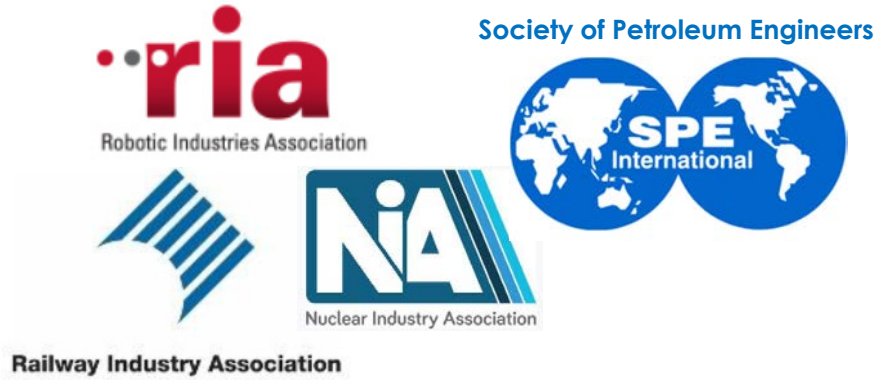
"China Export"

The China Export Mark means that the product was manufactured in China. There is no registration, testing, or auditing required in order to use it. The mark can be used arbitrarily by Chinese manufacturers.

- **Do NOT be misled… This Is NOT a product safety mark!**

SAFETY INTERLOCK RELATED - MISUSED TERMS

What Does the Phrase "*Functional Safety*" Mean?



Safety Function
(Other Industries)

Safety Interlock
(SEMI Industry)

Functional Safety
"Performance"

Safety Interlock Circuit
"Performance"

Emphasis Is Placed on "Performance Criteria" !

SAFETY INTERLOCK RELATED - MISUSED TERMS

What Are The Functional Safety Standards?

There are various international Functional Safety standards that address both the design engineering requirements, and the validation requirements for Safety Functions (SF's), and they are specified based on different industries sectors:

International Functional Safety "Related" Standards:			***SF Metric***
– IEC 61508	=	Original Functional Safety Standard (used to verify safety PLC's)	SIL
– IEC 62034	=	Medical Industry (Software) Functional Safety	--
– IEC 61513	=	Nuclear Power Plants Functional Safety	--
– IEC 61511	=	Process Industry (Chemical /Petroleum) Functional Safety	SIL
– ISO 23125	=	Machine Tools Safety - Turning Machines	PL
– ISO 13849	=	Equipment (Machinery) Functional Safety	PL
– IEC 62061	=	Equipment (Machinery) Functional Safety	SIL
– EN 50128	=	Railway Industry Functional Safety	SIL
– EN 50129	=	Railway Industry Functional Safety	SIL
– ISO 25119	=	Agriculture / Forestry Machinery Functional Safety	Ag-PL
– ISO 26262	=	Road Vehicles Functional Safety	A-SIL
– ISO 10218	=	Safety Requirements For Industrial Robots	PL / SIL

There are two most commonly used performance metrics for safety function design requirements:

1) Required Performance Level, PL_r (per ISO 13849-1, ISO 13849-2)

2) Target Safety Integrity Level, SIL (per IEC 61508, IEC 62061)

SEMI S2: "ADDITIONAL GUIDANCE FOR SAFETY FUNCTIONS"

SEMI® International Standards

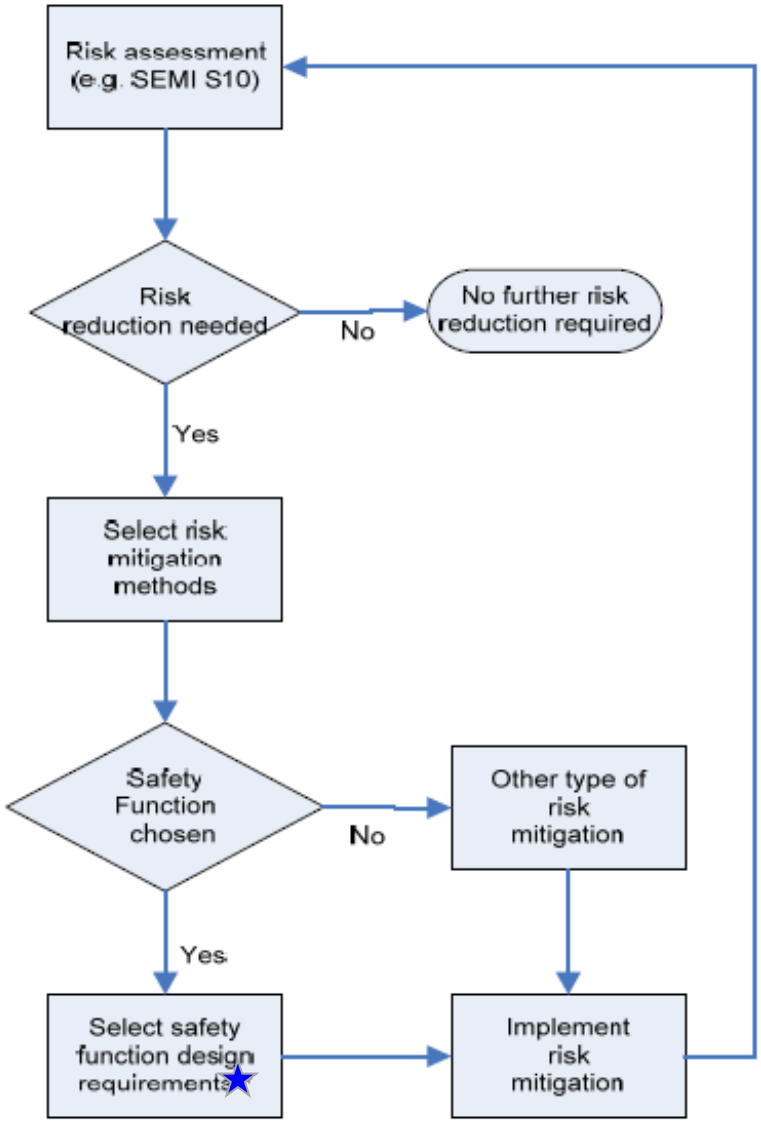


Figure R17-1
Relation Between Risk Assessment (e.g., SEMI S10) and Safety Function Selection

It's Now in SEMI S2!

The **ISO 13849-1** standard is repeatedly discussed within the 2 different SEMI S2 Related Information sections: **RI 13 (2003)** and **RI 17 (2015)**!

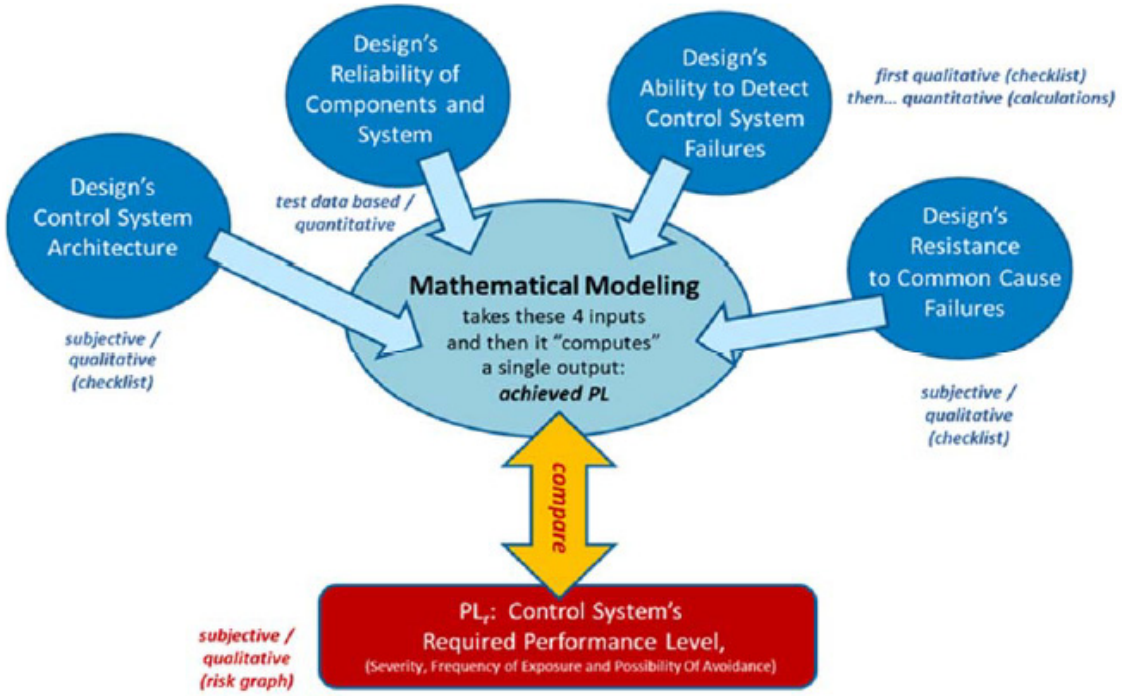


Figure R17-3
Overview of ISO 13849-1 Design Validation Process

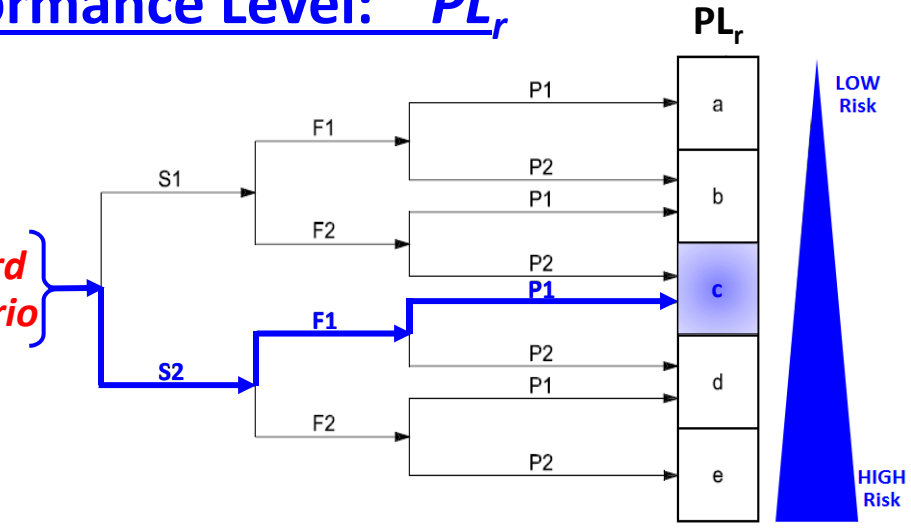
★ *asterisk directs you to follow ISO 13849-1*

PERFORMANCE CRITERIA – ISO 13849-1 EXAMPLE

STEP #1: Determine the Required Performance Level: "PL_r"

Based on a known hazard scenario, determine the required performance level of the safety function (assuming the interlock is not there to protect you)

1) ***Severity of Harm:*** **S1 or S2?**
2) ***Frequency or Duration of Exposure:*** **F1 or F2?**
3) ***Possibility of Avoidance:*** **P1 or P2?**



STEP #2: Engineer to ensure the design's "*Achieved PL*" ≥ "PL_r"

Engineering can look at the ***design requirements*** trade-offs, and can best decide how to reach the necessary "Achieved Performance Level" of the safety function.

1) ***Component Reliability:*** **$MTTF_D$ = ?**
2) ***Control System's Diagnostic Coverage:***
   Fault Detection, % Undetected Failures to Danger **DC_{avg} = ?**
3) ***Design's Control System Architecture:***
   Series Channel?, Parallel? Redundancy,? Diagnostics? **CAT = ?**
   (i.e. CAT B, CAT 1, CAT2, CAT 3, CAT 4)

Table 6 — Simplified procedure for evaluating PL achieved by SRP/CS

Category	B	CAT 1	CAT 2	CAT 2	CAT 3	CAT 3	4
DC_{avg}	none	DC = 0	low	medium	low	medium	high
$MTTF_D$ of each channel							
Low	a	Not cov-ered	a	b	b	c	Not cov-ered
Medium	b	Not cov-ered	b	c	c	d	Not cov-ered
High	Not cov-ered	c	c	d	d	d	e

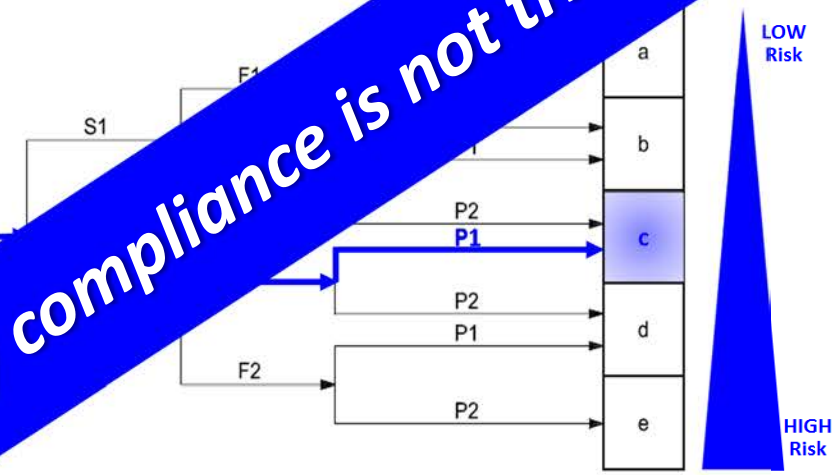
PERFORMANCE CRITERIA – ISO 13849-1 EXAMPLE

STEP #1: Determine the Required Performance Level: "PL"

Based on a known hazard scenario, determine the required performance level of the safety function (assuming the interlock is not there to protect you)

1) *Severity of Harm:* **S1 or S2?**
2) *Frequency or Duration of Exposure:* **F1 or F2?**
3) *Possibility of Avoidance:* **P1 or P2?**

Hazard Scenario



STEP #2: Engineer to ensu… …n's "Achieved PL" ≥ "PL$_r$"

Engineering can look at the *de… …ts* trade-offs, and can best decide how to reach the necessary "Achieved Perfo… …f the safety function.

1) *Component Reliabili…* **MTTF$_D$ = ?**
2) *Control Syste… …age:*
   Fault Dete… …es to Danger **DC$_{avg}$ = ?**
3) *D… …em Architecture:*
   …nel? Redundancy,? Diagnostics? **CAT = ?**
   …B, CAT 1, CAT2, CAT 3, CAT 4)

Table 6 — Simplified procedure for evaluating PL achieved by SRP/CS

Category	B	CAT 1	CAT 2	CAT 2	CAT 3	CAT 3	4
DC_{avg}	none	DC = 0	low	medium	low	medium	high
$MTTF_D$ of each channel							
Low	a	Not covered	a	b	b	c	Not covered
Medium	b	Not covered	b	c	c	d	Not covered
High	Not covered	c	c	d	d	d	e

The design effort for functional safety compliance is not trivial!

SEMI S2 SECTION 11 - "SAFETY INTERLOCK SYSTEMS"

Competent Design Engineers Can Be "Certified":

This program covers all areas of industry, not just our own semiconductor manufacturing industry. It tests on your working knowledge on these first 4 standards shown here: ***ISO 12100, ISO 13849-1, IEC 62061, IEC 60204-1*** *plus… the* ***Machinery Directive, 2006/42/EC****.*

- **Currently TÜV Rhineland has one of the accredited programs for Machine Design Functional Safety and is the most applicable to ASM Equipment.**

  - **Functional Safety Engineer (FSEng)**
  - **Functional Safety Expert (FSExpert)**

- **Other Functional Safety Programs exist for Chemical Plants, Railways, Automotive and Nuclear Industries which is outside scope of ASM equipment.**

  - **Certified Functional Safety Engineer (CFSE)**

SEMI S2 SECTION 11 - “SAFETY INTERLOCK SYSTEMS”

Competent Design Engineers Can Be “Cert

This program covers all areas of industry, nc *g*
industry. It tests on your working knowlec *e:*
ISO 12100, ISO 13849-1, IEC 62061, IEC 60204-1

- **Currently TÜV Rhineland has one of t** **n**
  Functional Safety and is the most applical

  - **Funct**
  - **Funct**

- **Other Functional Safety Programs exist f** **d**
  Nuclear Industries which is outside scope

  - **Certified F**


TÜVRheinland®

certifies that

Your Name Here!

has successfully completed the course

Functional Safety of Machinery
of ROCKWELL Automation – USA

Contents:
- European Guidelines, Standards
- Risk Analysis
- ISO 13849-1:1999 (EN 954-1)
- Safety Devices
- Safety functions of machines
- Circuits, schematics, examples
- New standards regarding safety of machinery
- EN ISO 13849-1:2006
- Validation
- EN 62061

and has met the approval criteria for a

TÜV Functional Safety Engineer
Machinery

Certificate Number: TÜVFSEng 6085/12

Issue date: December 2012
Expiry date: December 2017

Cologne, December 2012

TÜV Rheinland Industrie Service GmbH
Automation, Software
and Information Technology (ASI)

Dipl.-Ing. Heinz Gall
Head of TÜV Functional Safety Program

Functional Safety Engineer
Machinery
ID: 6085/12
TÜVRheinland® FSEngineer

SEMI S2 SECTION 11 - "SAFETY INTERLOCK SYSTEMS"

KEY POINT: ***The newer safety interlock requirements are much more complex than when our semiconductor industry first started out… special skillsets are required to understand, design, and then validate our safety functions correctly!***

- **Currently TÜV Rhineland has one of the accredited programs for Machine Design Functional Safety and is the most applicable to ASM Equipment.**
  - **Functional Safety Engineer (FSEng)**
  - **Functional Safety Expert (FSExpert)**

- **Other Functional Safety Programs exist for Chemical Plants, Railways, Automotive and Nuclear Industries which is outside scope of ASM equipment.**
  - **Certified Functional Safety Engineer (CFSE)**

SAFETY INTERLOCK RELATED - MISUSED TERMS

KEY POINT:

- ***"Safety Functions"*** are just safety interlock circuits with very specific design requirements (e.g. **PL_r** = c, or **SIL** = 1) to ensure that they will reliably work as their design intended, when they called upon to work (i.e. during the foreseen hazard scenario!)
- ***"Functional Safety"*** is achieved when all of the equipment's safety interlocks (safety functions) successfully operate at, or above, their required performance levels.

For More On Functional Safety: Older SESHA members may recall my SESHA Presentation from 8 years ago entitled:

"Performance Levels – Why Now?" ***(May 18th, 2011)***

2011 Presentation's PDF Link: ***http://seshaonline.org/viewfile.php3?filename=2011proceedings/42.pdf***

SAFETY INTERLOCK RELATED - MISUSED TERMS

What does a *"Safety-Rated"* Mean?

It's bad "SLANG" from 3rd party auditors and product safety engineers!

This is NOT a term that is ever defined within SEMI, or Machinery Directive, or even within the previous functional safety standards discussed today.

However, a part of this phrase is defined within the international industrial robotic standard: ISO 10218-1.

INTERNATIONAL STANDARD **ISO 10218-1**

Robots and robotic devices — Safety requirements for industrial robots —

Part 1:
Robots

3 Terms and definitions

3.19
safety-rated
characterized by having a prescribed safety function with a specified safety-related performance

The term "Safety Rated" simply means it has a prescribed safety function, with a specified safety-related performance – sounds very familiar to "Functional Safety Performance"

SAFETY INTERLOCK RELATED - MISUSED TERMS

What does a *"Safety-Rated"* Mean?

It's bad "SLANG" from 3rd party auditors and product safety engineers!

This is NOT a term that is ever defined within SEMI, or Machinery Directive, or even within the previous functional safety standards discussed today.

However, a part of this phrase is defined within the international industrial robotic standard: ISO 10218-1.

KEY POINT:

For safety interlock components, the intent of saying "*Safety-Rated*" implies much more than the component just having low risk of fire, or an electrical shock , or related hazards. (e.g. *OSHA NRTL Listed*)

The term "Safety Rated" simply means it has a prescribed safety function, with a specified safety-related performance – sounds very familiar to "Functional Safety Performance"

AGENDA

- Safety Interlock Requirements Evolution
- Safety Interlock Related - Misused Terms
- **ASM's Safety Rated Interlock Components**
- ASM's Component Selection Flowchart

ASM - SAFETY RATED INTERLOCK COMPONENTS

What Does A "*Safety Rated Interlock Component*" Mean?

Well… this is also NOT specifically defined anywhere, … but ASM has chosen to define it ourselves - based on the industrial robot standards "safety-rated", which means it should attempt to have a specified safety performance level.

- ***As a global company, ASM needed to standardize for internal use/alignment, and our initial focus will be on component selection only.***
- ***Last year ASM presented how we rolled out specific product safety awareness training to our global design engineers. ASM's is focused on proper component selection for single channel interlock circuits.***

ASM - SAFETY RATED INTERLOCK COMPONENTS

What Does A "*Safety Rated Interlock Component*" Mean?

Well… this is also NOT specifically defined anywhere, … but ASM has chosen to define it ourselves - based on the industrial robot standards "safety-rated", which means it should attempt to have a specified safety performance level.

ASM DEFINITION: *"Safety Rated Interlock Component"*

A component which is either:

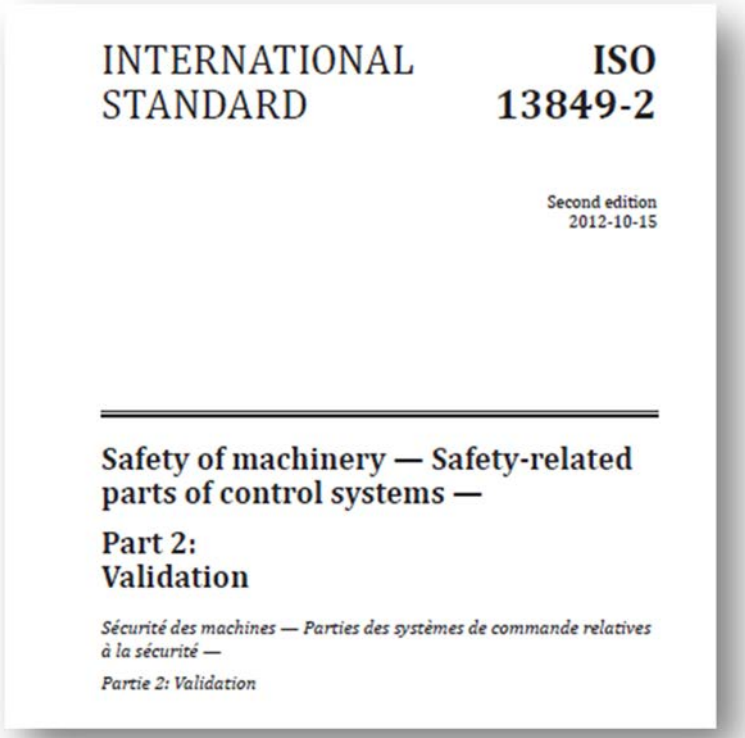
1) **Fully compliant to criteria as outlined within ISO 13849-2's "*Well-Tried Component*" which will be used within a CATEGORY 1 circuit (i.e. single-channel) with a PL_r = c.**

or

2) **It has been deemed as equivalent, per the additional evaluation and testing requirements specifically outlined within the new ASM Safety–Rated Interlock Component Selection Flowchart.**

Our So-Called "*Plan A*": Use the Standard!

The most easily defendable solution it to follow the ISO 13849-2 standard to justify our component selection. It is THE equipment specific harmonized international consensus standard for machine safety!



INTERNATIONAL STANDARD

ISO 13849-2

Second edition
2012-10-15

Safety of machinery — Safety-related parts of control systems —

Part 2: Validation

Sécurité des machines — Parties des systèmes de commande relatives à la sécurité —

Partie 2: Validation

VALIDATION!

Our "Plan A": Use the Standard!

The most easily defendable solution it to follow the ISO 13849-2 standard to justify our component selection. It is THE equipment specific harmonized international consensus standard for machine safety!

Table D.3 — Well-tried components

Well-tried component	Additional conditions for "well-tried"	Standard or specification
Switch with positive mode actuation (direct opening action), e.g.: — push-button; — position switch; — cam-operated selector switch, e.g. for mode of operation	—	IEC 60947-5-1:2003, Annex K
Emergency stop device	—	ISO 13850 IEC 60947-5-5
Fuse	—	IEC 60269-1
Circuit-breaker	—	IEC 60947-2
Switches, disconnectors	—	IEC 60947-3
Differential circuit-breaker/RCD (residual current device)	—	IEC 60947-2:2006, Annex B

For single channel safety interlock circuits, Safety-Rated = Well-Tried ☺

ISO 13849-2:2012(E)

Annex D

Validation tools for electrical systems

Our "Plan A": Use the Standard!

The most easily defendable solution it to follow the ISO 13849-2 standard to justify our component selection. It is THE equipment specific harmonized international consensus standard for machine safety!

Table D.3 *(continued)*

Well-tried component	Additional conditions for "well-tried"	Standard or specification
Relay	Only well-tried if	IEC 61810-1 ✓
	a) other influences are taken into account, e.g. vibration, ✓	IEC 61810-2 ✓
	b) positively energized action, ✓	
	c) failure avoided by appropriate methods, e.g. overdimensioning (see Table D.2), and ✓	
	d) the current in the contacts is limited by fuse or circuit-breaker to avoid the welding of the contacts. ✓	
	NOTE Fault exclusion is not possible.	

We also need to meet these 4 additional design conditions too!

Lets look at Table D.2

- **IEC 61810-1:2015** Electromechanical Elementary Relays - Part 1: General and Safety Requirements
- **IEC 61810-2:2017** Electromechanical Elementary Relays - Part 2: Reliability

IMPORTANT: There are additional design requirements listed in the middle column, and these must ALSO be followed (in addition to) your selection of a **IEC 61810** compliant safety relay!

ASM - SAFETY RATED INTERLOCK COMPONENTS

Lets look at Table D.2

Additional conditions for "well-tried"
Only well-tried if c) failure avoided by appropriate methods, e.g. overdimensioning (see Table D.2), and

Table D.2 *(continued)*

Well-tried safety principle	Remarks
Overdimensioning	De-rate components when used in safety circuits, e.g. by the following means:
	— the current passed through switched contacts should be less than half their rated current;
	— the switching frequency of components should be less than half their rated value;
	— the total number of expected switching operations should be no more than 10 % of the device's electrical durability.
	NOTE De-rating can depend on the design rationale.

Our "Plan A": Use the Standard!

The most easily defendable solution it to follow the ISO 13849-2 standard to justify our component selection. It is THE equipment specific harmonized international consensus standard for machine safety!

Table D.3 — Well-tried components

Well-tried component	Additional conditions for "well-tried"	Standard or specification
Main contactor	Only well-tried if	IEC 60947-4-1
	a) other influences are taken into account, e.g. vibration,	
	b) failure is avoided by appropriate methods, e.g. overdimensioning (see Table D.2),	
	c) the current to the load is limited by the thermal protection device, and	
	d) the circuits are protected by a protection device against overload.	
	NOTE Fault exclusion is not possible.	
Control and protective switching device or equipment (CPS)	—	IEC 60947-6-2

We also need to meet these 4 additional design conditions too!

For single channel safety interlock circuits, Safety-Rated = Well-Tried ☺

ISO 13849-2:2012(E)

Annex D

Validation tools for electrical systems

Our "Plan A": Use the Standard!

The most easily defendable solution it to follow the ISO 13849-2 standard to justify our component selection. It is THE equipment specific harmonized international consensus standard for machine safety!

Table D.3 — Well-tried components

Well-tried component	Additional conditions for "well-tried"	Standard or specification
Temperature switch	—	For the electrical side, see EN 60730-1
Pressure switch	—	For the electrical side, see IEC 60947-5-1 For the pressure side, see Annexes B and C.
Solenoid for valve	—	—

For Pneumatic switch, lets look at Annex B

For single channel safety interlock circuits, Safety-Rated = Well-Tried ☺

ISO 13849-2:2012(E)

Annex D

Validation tools for electrical systems

ISO 13849-2:2012(E)

Annex B

Validation tools for pneumatic systems

ASM - SAFETY RATED INTERLOCK COMPONENTS

Our "Plan A": Use the Standard!

The most easily defendable solution it to follow the ISO 13849-2 standard to justify our component selection. It is THE equipment specific harmonized international consensus standard for machine safety!

ISO 13849-2:2012(E)

Annex B

Validation tools for pneumatic systems

When pneumatic systems are used in conjunction with other technologies, Annex B should also be taken into account. Where pneumatic components are electrically connected/controlled, the appropriate fault lists in Annex D should be considered.

NOTE Additional requirements can exist in national legislation.

Tables B.1 and B.2 list basic and well-tried safety principles.

A list of well-tried components is not given in Annex B of this edition. The status of "well-tried" is mainly application-specific. Components can be described as "well-tried" if they are in accordance with ISO 13849-1:2006, 6.2.2 and ISO 4414:2010, Clauses 5 to 7. A well-tried component for some applications could be inappropriate for other applications.

Safety-Rated Pneumatics = Well-Tried Pneumatics

ISO 13849-2 *directs ASM designers to* ***ISO 4414*** *for compliance.*

(not as prescriptive as electrical systems)

Importance of Dangerous Undetected Failures

ASM Safety-Rated Interlock components follow international standard design criteria to ensure they are both reliable, and have a very high likelihood to fail-safe.

Note: Safe failures may also be **detectable** or **undetectable**, but the distinction is irrelevant.

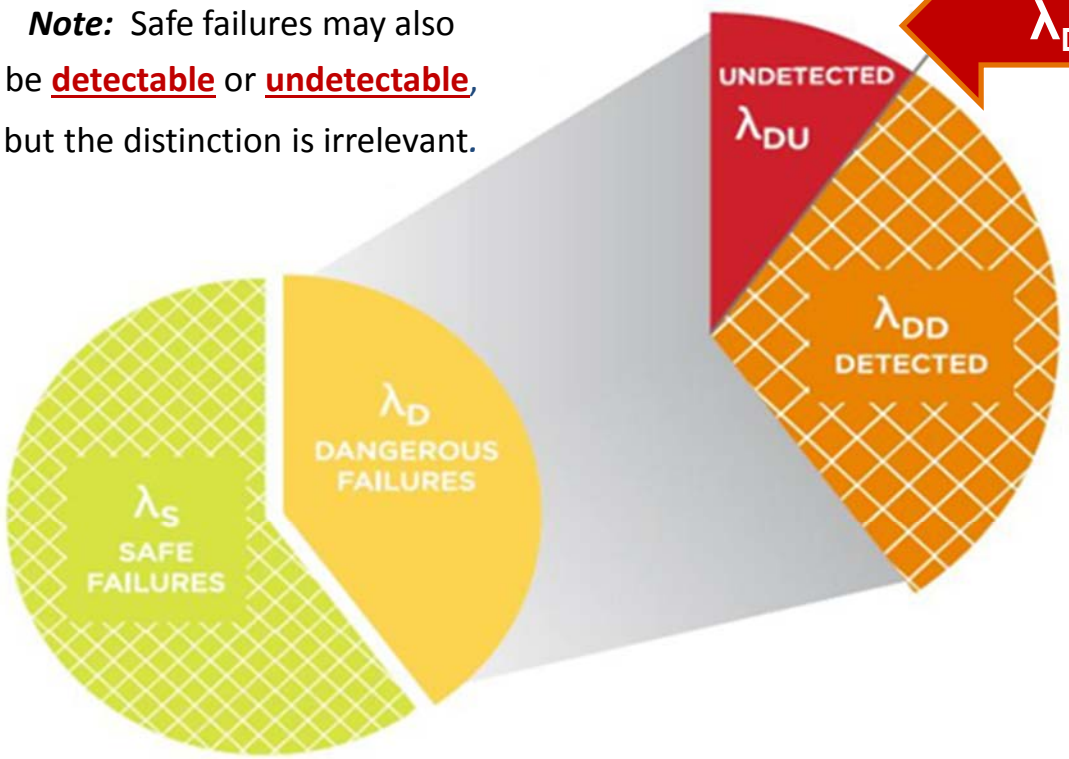


Chart Reference: ***Relays in Safety-Related Control Systems"***
Alice Matthews; 9th January 2017.

λ_{DU}: This is designer's biggest concern!

- ***For a safety interlock circuit, the most hazardous outcome is if the component fails to danger, but it goes undetected.***
- ***No one knows it failed!***
- ***Everyone believes it is OK! Its NOT.***
- ***The design has no way to protect itself when the hazard arises. …***

AGENDA

- Safety Interlock Requirements Evolution
- Safety Interlock Related - Misused Terms
- ASM Safety Rated Interlock Components
- **ASM's Component Selection Flowchart**

ASM - SAFETY RATED INTERLOCK COMPONENTS

What Does A "*Safety Rated Interlock Component*" Mean?

Well… this is also NOT specifically defined anywhere, … but ASM has chosen to define it ourselves - based on the industrial robot standards "safety-rated", which means it should attempt to have a specified safety performance level.

ASM DEFINITION: *"Safety Rated Interlock Component"*

A component which is either:

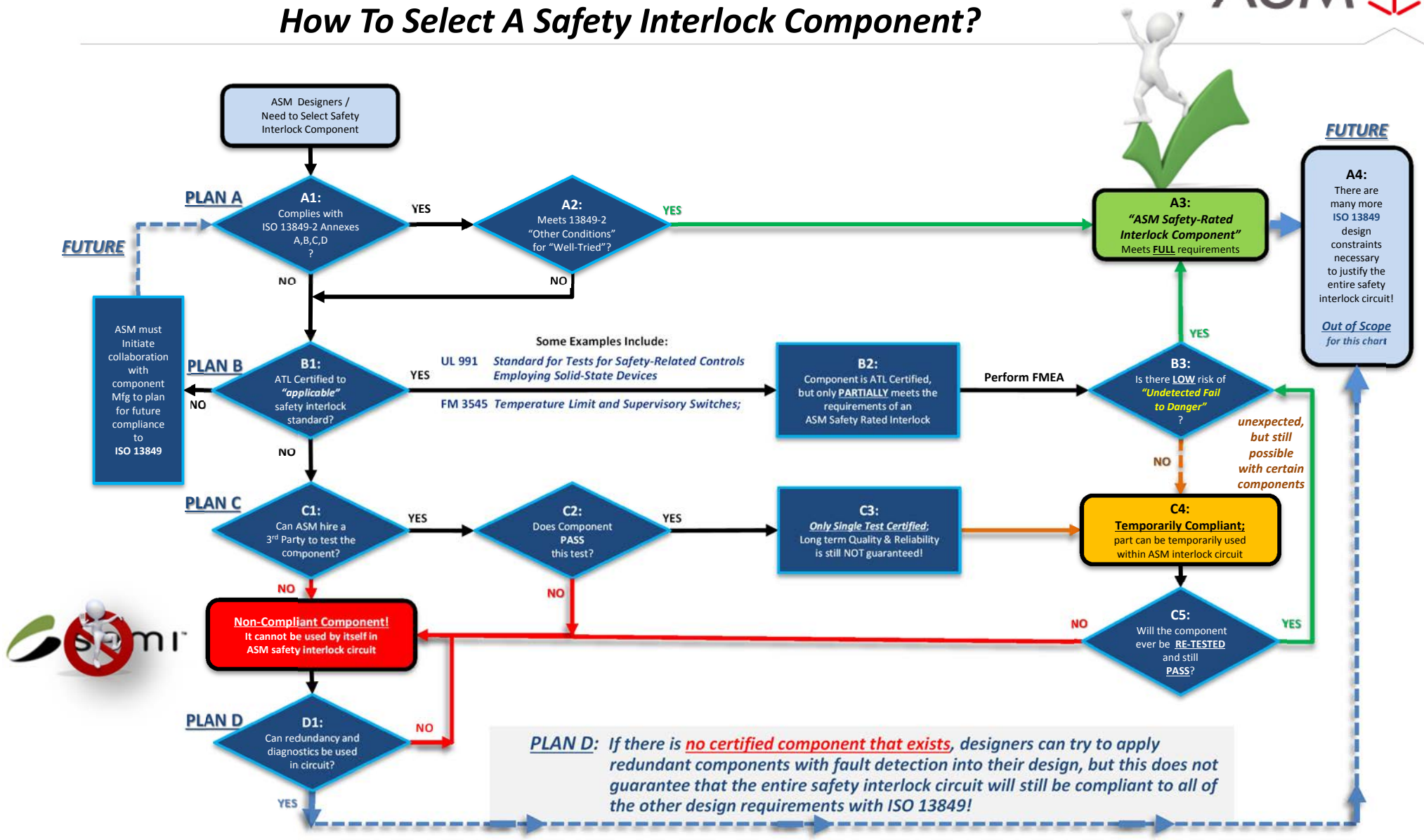
1) *Fully compliant to criteria as outlined within ISO 13849-2's "Well-Tried Component" which will be used within a CATEGORY 1 circuit (i.e. single-channel) with a PL_r = c.*

or

2) ***It has been deemed as equivalent, per the additional evaluation and testing requirements specifically outlined within the new ASM Safety–Rated Interlock Component Selection Flowchart.***

New ASM Design Decision Flowchart

How To Select A Safety Interlock Component?



SUMMARY: ITS ALL ABOUT LEARNING!

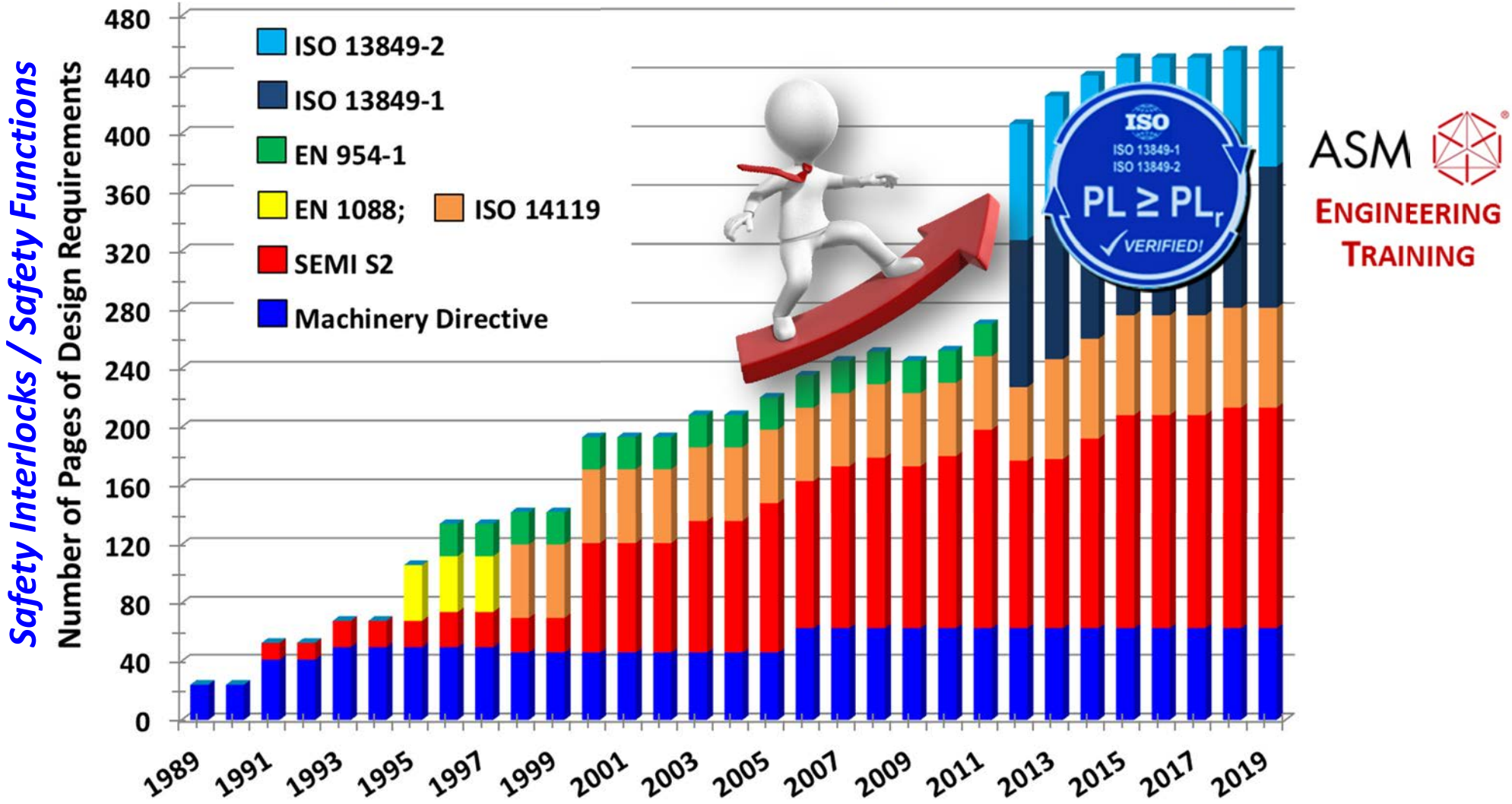
- **In semiconductor industry, our safety interlock design requirements have *steadily increased in complexity over the last 30 years*, (since 1989), but especially since Jan 1st, 2012 when ISO 13849-1 Performance Levels was harmonized as presumption of conformity to the Machinery Directive!!**
- **Today, new *training* and *certification* is required to ensure proper understanding to design, and then validate our safety functions correctly!**

- ***"Listed"* electrical component only means it's approved an OSHA NRTL, ensuring low risk of fire or an electrical shock, but it *does NOT guarantee* safety interlock performance".**
- ***"Safety Functions"* are just safety interlock circuits with very specific performance requirements (*examples only*: PL_r = c, PL_r = d, SIL = 1, SIL = 2) to ensure that they will reliably work as their design intended, when they called upon to work.**
- ***"Functional Safety"* is achieved when all of the equipment's safety interlocks successfully operate at, or above, their required performance levels.**
- ***"Safety Rated Interlock Component"* has not yet been defined, so ASM created a custom Flowchart to guide design engineers on the proper steps to take (i.e. Plans "A" through "D").**

SUMMARY: ITS ALL ABOUT CONTINUOUS LEARNING!

It's getting harder to surf the increasing "WAVE" of design requirements!

History Of The 7 Key Safety Interlock Standards for Semiconductor Equipment



SAFETY INTERLOCK DESIGN CHALLENGES

SEMICONDUCTOR INDUSTRY WAFER PROCESSING EQUIPMENT

IT'S ALL ABOUT CONTINUOUS LEARNING!

Let's ensure SESHA continues to promote this type of important *"Knowledge Sharing"* through its monthly webinars, local chapter meetings, and this Symposium!

ASM