

2012

A warm welcome by **Omron**, **FSE** Global,  
and host **Factory Controls**

**From Inspiration to Installation:**  
and how the WH&S Act and Standards assist.  
*And off course congratulations to the Cats!*



Richard Davies  
Manager **Factory Controls**

John Merrett  
safety product specialist  
**Omron** Electronics

Maurits Funke-Kupper  
machine safety expert  
**FSE** Global

2012

## Functional Safety Engineering Global

- FSE Global is a brand independent internationally operating organization specialised in safety-related consulting and training services for the machine and process industries.
- **Facilitating** Risk Management (HAZOP/HAZID study, Plant/Risk Assessment, Safety Design Verification, Audit/Validation)
- Assisting in Safety Control Design (Safety-by-Design, Safety Requirement Specification, SIL/PL Determination study, FMEA study)
- Providing Training (Certification in Functional Safety, Applying Safety standards, Machine Safety-by-design, Optimised Process Safety)

*Maurits has more than 25 years of Industrial Automation and Machine/Process Safety expertise and is a Certified ISA84/AS61511 Safety Instrumented Systems specialist.*

Welcome

2012

## Welcome to all participants today!

(Please ask questions during the presentations, your query will be valuable to all of us)

Safety is no longer just a **responsibility** between Employer and Employee,

Or a responsibility that can **handballed** to an OH&S representative, supplier, designer, manufacturer, system integrator, electrician, or contractor,

The responsibility of safety in the workplace is a **shared** responsibility of all people and organisations involved in a business or undertaking.

The new Act and Regulations, and newly introduced Standards and Guidelines will assist us in working together achieving our collective goals.

# Participants

2012

Who must comply with and gain knowledge of the WH&S Act 2010 and new Standards?  
As you might have guessed after the previous slide: **We are all participants in the process!**

Responsibility for Safety in the Workplace includes **Management and 'Workers'** .

'Workers' have been redefined not only as employees of the business or undertaking, (sub) contractors, labour hire company, apprentice, trainee, student for work experience, volunteers, and visitors. (The last two must take care of health and safety of themselves and others, and only proven negligence can lead to prosecution)

Persons conducting business are required to prove **compliance** with the Act and

Regulations include: (Case: lost arm in abattoir, company and contracting agency fined. Non-interlocked guarding and no training records. **Electrical contractor had to prove compliance and demarcation**)

- Management or control of Workplace, Structures, Plant and Equipment
- Designers and Manufacturers of Structures, Plant and Equipment
- Importers and Suppliers of Structures, Plant and Equipment
- Installers/electricians, Constructors or Commissioners of Plant and Equipment

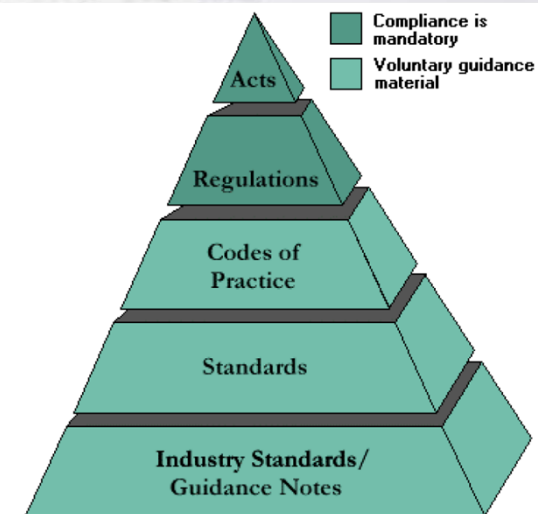
# Compliance

2012

- New Work Health & Safety Act (215 pages)
- New Work Health & Safety Regulations (582 pages)
- Codes of Practice (64 pages)
- (Inter)National Standards (dozens)
- Industry specific Standards and Guidelines (Notes)
- White Papers, Manuals and Guidelines of Manufacturers and Integrators
- Industry forums and other sources of knowledge and experience

So if nothing much has changed, what is the history behind:

- The new WHS Act and Regulations? ([www.SafeWorkAustralia.gov.au](http://www.SafeWorkAustralia.gov.au))



(Source: National Occupational Health and Safety Commission)

# History

2012



National **OHS Strategy** 2002-2012 and its targets:

- Reduce work-related fatalities by >20% by June 2012
- Reduce workplace injuries by >40% by June 2012

Stock-take in 2007 revealed goals were not going to be met requiring more action!

The five **key points** of change in the new **Work Health & Safety Act**:

- Legal compliance to WH&S applies to all with decision making **responsibilities**
- Duty of care to include **any person** who works in **any capacity** in the business
- Obligation to **acquire appropriate knowledge** about the hazards and risks, and eliminate/minimise these to ALARP, preferably in the design phase
- The importance of **specialised consultation** has been recognised and has been made into a specific obligation for all duty holders (ignorance is no excuse)
- Strengthened capacity of **government to enforce** WH&S compliance

# Responsibility

2012

Every person has the responsibility for providing and maintaining a safe work environment throughout the complete Safety Lifecycle

- Workplace Owner, Manager, Team-leader, Operator, etc. (Risk assessments)
- Engineering team (HAZID, Design assessments, Verification)
- Control System design team (SRS, SIS, SIF, Verification)
- Component manufacturer (Third-party Certification)
- Sales/Import/Distributor of parts (Risk assessment)
- System Integrator, Programmer (SRS, SIS, SIF, Verification)
- Installer, Electrician, etc. (Risk assessment)
- Service and Maintenance engineer (Risk assessment)
- Visitor, Contractor, Temporary staff (Risk assessment)

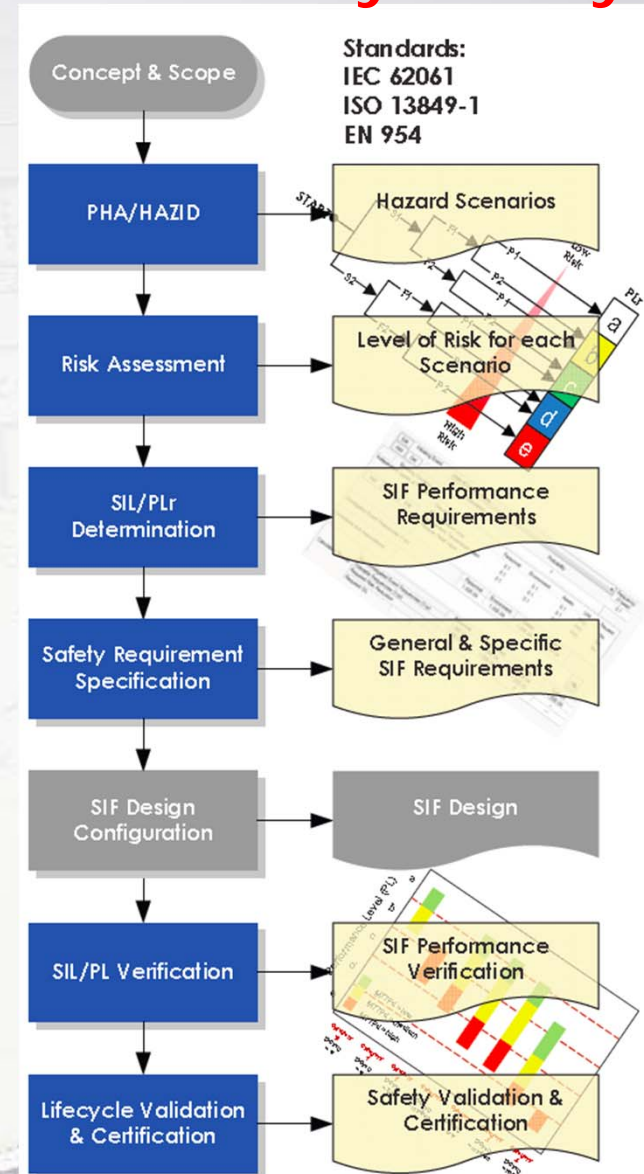
**Never assume! Ask and ask again! Document everything!**  
**When in doubt: stop and ask! Communicate at all levels!**



# Safety Lifecycle

2012

- "I have a dream" (**Inspiration**)
- Analyse the dream (Intended and **misuse**)
- Brainstorm (dream) about all possible **risks**
- Severity, Frequency, Likelihood, Avoidance
- **Re-design** the idea to eliminate these hazards  
(Practice **Safety-by-Design** methodologies)
- Consider IPL's (Independent Protection Layers)
- Determine the (**Acceptable**) Residual Risk Level
- Safety Requirements Specifications (rSIL/rPL)
- Design the SRP/CS, **Verify** the Design (Re-assess)
- Build, Test and **Validate** the SRP/CS as a whole
- **Document** all steps and ensure regular updates  
(WH&S Act and Machine Directives are very similar)



2012

When we find hazards with machines, processes or workplace, these risks must be eliminated or minimised for as far as is reasonably practicable.

**Note: A Hazard has the potential to cause harm, Risk is the likelihood that harm will come from exposure to the hazard. No hazard, no risk!**

- **Hazards** can be found in relation to:
  - People, Environment, Capital goods, and the Community
- Risks must be **eliminated** for as is reasonably practicable (ALARP)
  - Eliminate, Substitute, Isolate, Control, Administer, PPE, Warning
- Risks must be considered in all **operating modes** and life cycle stages:
  - Commissioning, Operation, Cleaning, Maintenance, Fault-finding, etc.
- The **factors** to influence in order to eliminate or minimise Risks are:
  - **Consequence, Exposure, Probability and Avoidance!**

# Reasonably Practicable

2012

Reasonable practicable and hierarchy of risk control:

- Reasonable: 'Based on good sense' and 'Appropriate'
- Practicable: 'Useful', 'Realistic', 'Workable' and 'Viable'
- Hierarchy of Risk Control: Elimination or Safety-by-Design, Substitution, fixed Isolation, monitored and/or controlled Isolation, Engineered control, Administrative control and Training, PPE and awareness (Signage, SOP's).

*Note: you can reduce safety costs by applying **Standard Automation** (Control systems, Robots, Vision systems) to reduce the frequency of exposure and possibly positively influence production capacity and/or quality.*

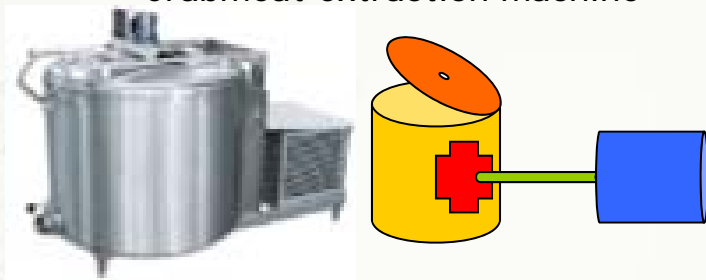
*This is Safety-by-Design and regarded as an **Independent Protection Layer** (IPL).*

# Safety by Design

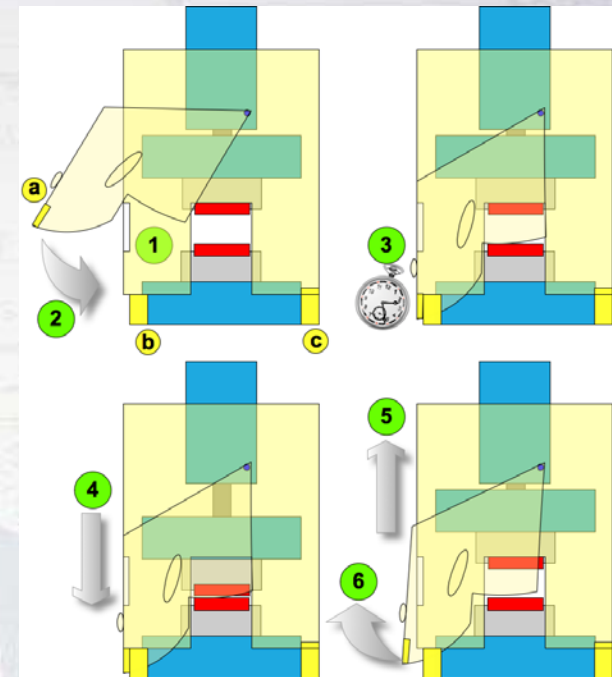
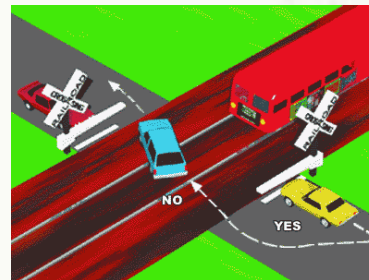
2012

Safety by Design and assessing the four factors to influence is where we benefit:

- Pneumatic Press and Guillotine
- Bag filler with dust build-up to lumps problem
- Crabmeat extraction machine



- Road/Railway intersection
- CNC machine (access)
- Quarry (mobile crusher)



When creating a Design Concept, do you know the required integrity level and consequent architectures?

# Design Concept

2012

- Four Risk reduction factors: Consequence, Exposure, Probability, Avoidance
- Select the most applicable Standards for guidance
- Eliminate at source (crabmeat machine)
- Investigate all Sources of risk (mechanical, pneumatic, electric, hydraulic)
- Guarding (apply hierarchy)
- Look for the weakest link (Failure Mode and Effect Analysis)
- What about the Reset function (time, position)
- Can we use Photo electrical sensing (delay, speed)
- Choice of technologies (single point of failure, again FMEA)
- Safety Requirement Specifications (required to be able to verify and validate)
- Verification (design meets SRS objectives by analysis)
- (Validation: installation meets SRS objectives by demonstration)

# Failure Mode And Effect

2012

The FMEA investigates the failure mode of each component and function: Failure to Safety or to Danger, Detected or Undetected, taking into account the consequence, probability and diagnostic coverage.

- Examples to take into account when designing safety solutions:
  - Contactor, Valve, Thyristor, VSD-drive (Positively guided, diagnostics)
  - Temperature sensor (Pt100 versus Thermocouple)
  - Mechanical Thermostat, Level or Flow Switch (Control versus Alarm)
  - Mechanical Brake (Power-to-Release versus Power-to-Brake)
  - Pump and valve application (Level, Pressure, Cooling, Heating)
  - Non-programmable Controller (Standard versus Safety)
  - Switches: Solenoid-to-Open Tongue Switch, RF and Magnetic Switches
  - Programmable Safety Controller (Verification versus Validation)

Detection by: monitoring, comparison and indication.

What standards are available to assist us?

## Useful Standards

2012

AS 31000 (AS 4360): Risk Management

- Risk, Resources, Communication and Reporting, Monitoring and Review

AS 4024.1: Series of Machine safety

- Combines 26 European Norms and Standards

EN ISO 12100:2010, previously EN ISO 12100 and 14121: Machine safety

- Risk Assessment and Design and Practical guidance plus examples of Methods

AS 60812: Procedure for Failure Mode and Effect Analysis

AS 62061: Functional safety of safety related electrical, electronic and programmable electronic control systems

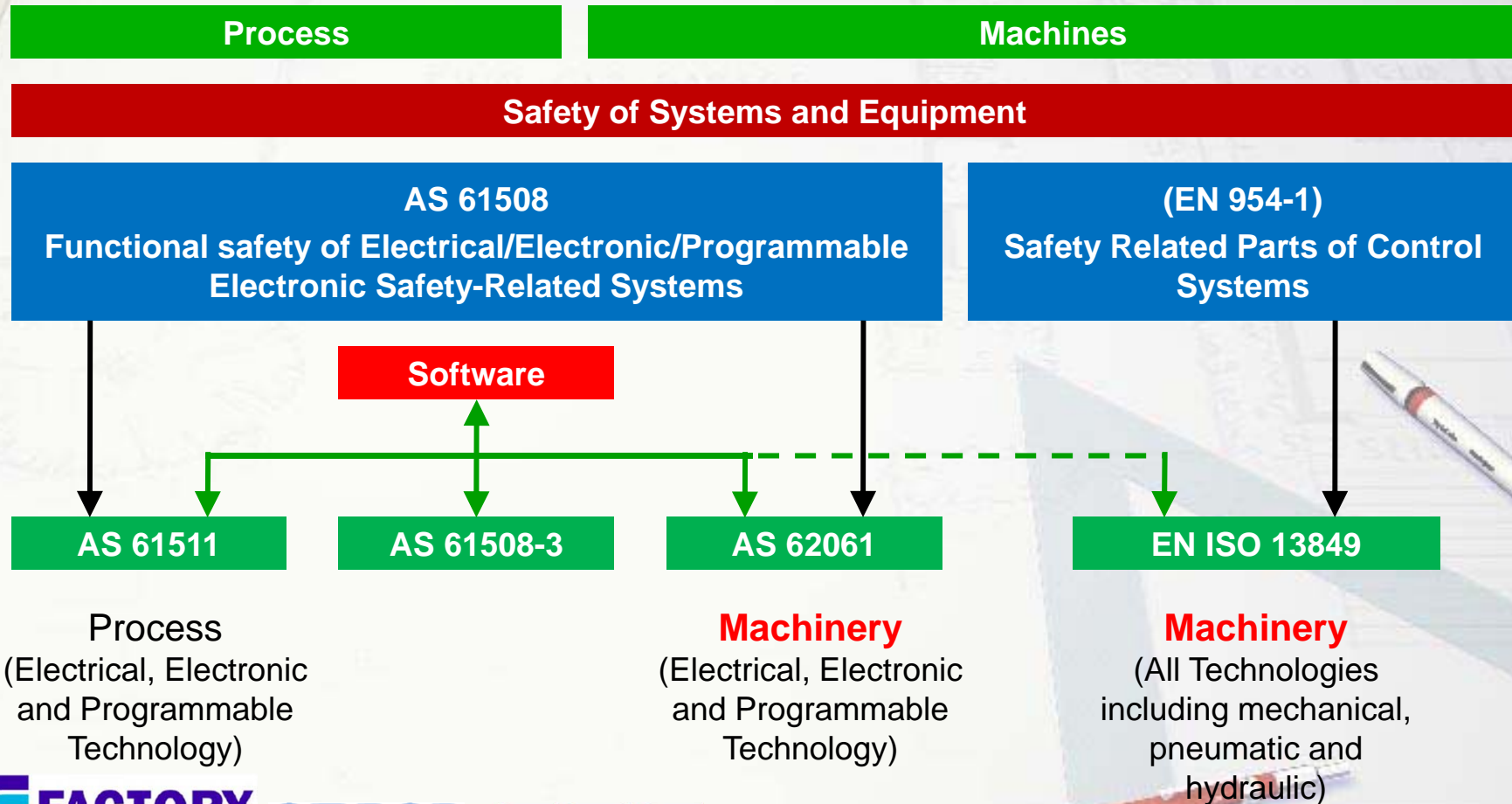
EN ISO 13849-1: SRP/CS General principles for design

EN ISO 13849-2: SRP/CS Validation

- ISO/TR 23849: Guidance on the application of ISO 13849 and IEC 62061

# Control Systems

2012



# Control Systems

2012

AS 61508: Functional safety of electrical/electronic/programmable electronic safety-related systems is the Design standard for the manufacturers of Safety Control Systems (product)

AS 61511: Functional safety of E/E/PE safety-related systems

- Standard for the design of Safety Instrumented Systems for the process industry sector

AS 62061: Functional safety of safety-related E/E/PE systems

- Defines requirements and gives recommendations for the design, integration and validation of safety-related E/E/PE control systems for machinery

[EN ISO13849](#): Safety Related Parts of the Control System

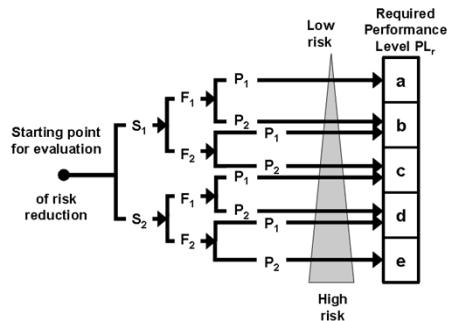
Note: AS 61508/61511/62061 do not define requirements for the performance of non-electrical (e.g. hydraulic, pneumatic, electromechanical) safety-related control elements for machinery. EN ISO 13849 does.

2012

- The Risk Assessment process will determine the required integrity level
- Engineered Risk Control: the benchmark for safety integrity levels is shifting from a 'deterministic' (mainly based on architecture) to a 'probabilistic' approach expressed as **Safety Integrity Levels** to PL (Performance Level to 13849) or SIL (Safety Integrity Level to 61508, 61511, 62061)

Table 1 — Relationship between PLs and SILs based on the average probability of dangerous failure per hour

Performance level (PL)	Average probability of a dangerous failure per hour (1/h)	Safety integrity level (SIL)
a	$\geq 10^{-5}$ to $< 10^{-4}$	No special safety requirements
b	$\geq 3 \times 10^{-6}$ to $< 10^{-5}$	1
c	$\geq 10^{-6}$ to $< 3 \times 10^{-6}$	1
d	$\geq 10^{-7}$ to $< 10^{-6}$	2
e	$\geq 10^{-8}$ to $< 10^{-7}$	3



Consequences	Severity Se	Class Cl					Frequency and duration, Fr	Probability of hzd. event, Pr	Avoidance Av	
		3 - 4	5 - 7	8 - 10	11 - 13	14 - 15				
Death, losing an eye or arm	4	SIL 2	SIL 2	SIL 2	SIL 3	SIL 3	$\leq 1$ hour	5	Very high	5
Permanent, losing fingers	3		OM	SIL 1	SIL 2	SIL 3	$> 1$ h - $\leq$ day	5	Likely	4
Reversible, medical attention	2			OM	SIL 1	SIL 2	$> 1$ day - $\leq$ 2wks	4	Possible	3
Reversible, first aid	1				OM	SIL 1	$> 2$ wks - $\leq$ 1 yr	3	Rarely	2
							$> 1$ yr	2	Negligible	1

# Safety Integrity Level

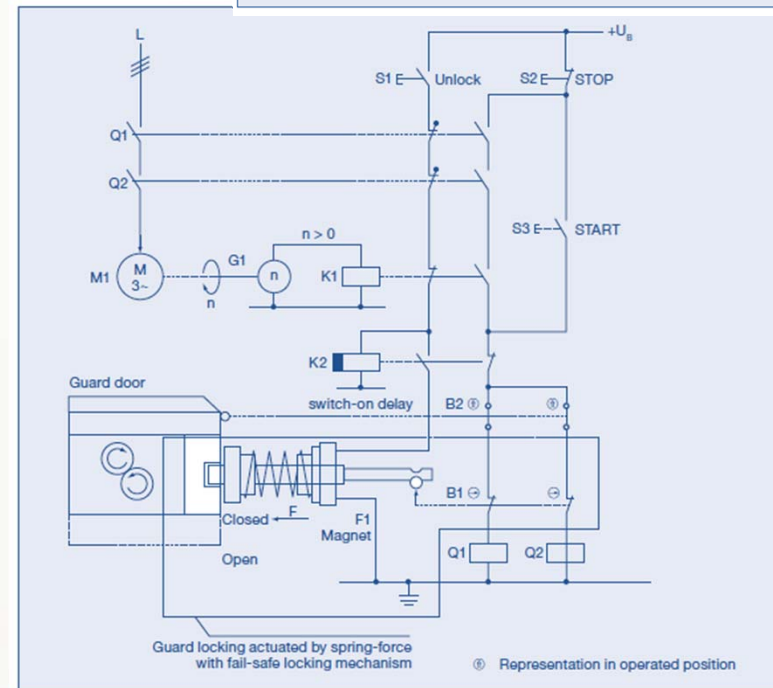
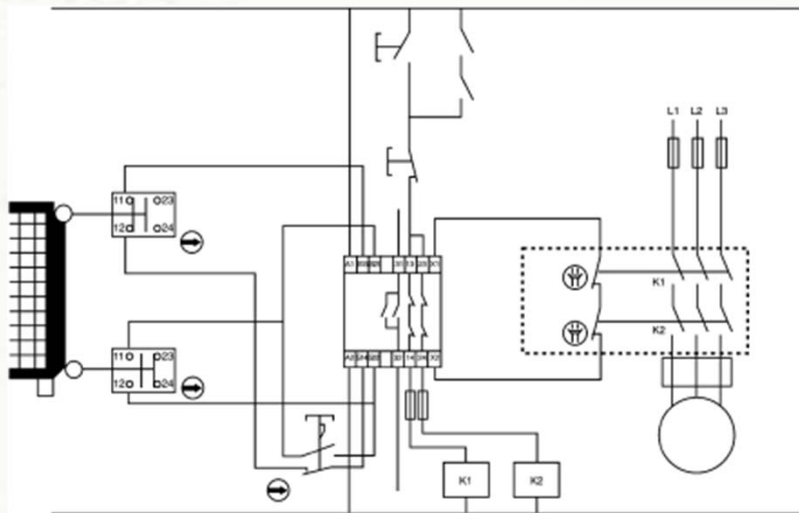
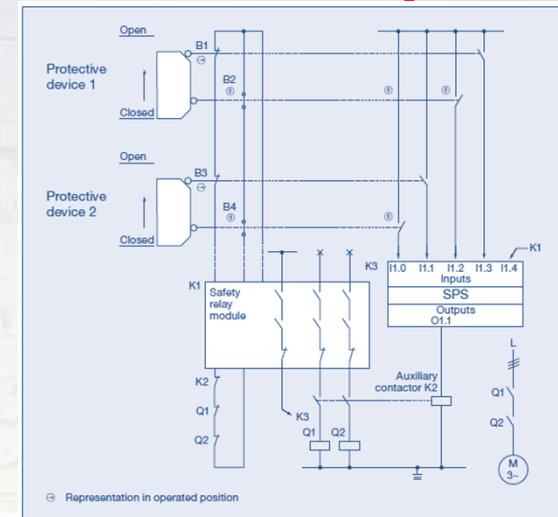
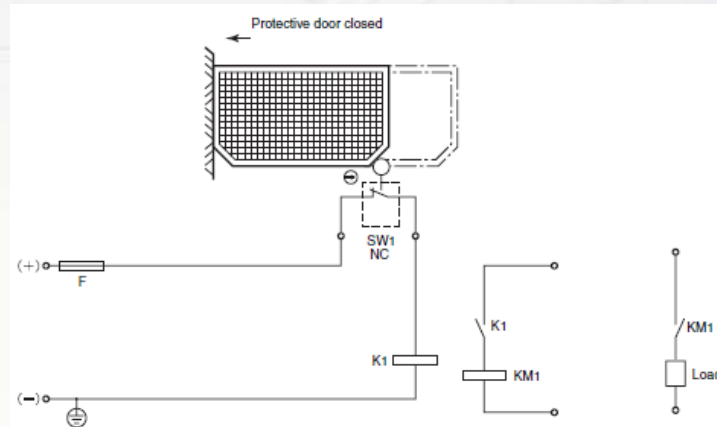
2012

Integrity relates to the Design and implementation of mechanical, electric, pneumatic and hydraulic systems and components

- An error or failure shall not lead to the loss of a safety function.
- Especially a 'failure-to-danger', shall be detected
- A possible failure shall not occur more than once per x hours of operation
- Category (Single/Dual channel structure),
- Mean Time To dangerous Failure (MTTFd), (Likelihood)
- Number of cycles by which 10% of a random sample of wearing components have failed dangerously (B10d). (Reliability)
- Diagnostic Coverage (DC), (Prevent undetected failures)
- Common Cause Failure (CCF), (Proper design)
- Mission Time <sup>TM</sup>. (Lifecycle)

# Systems

2012



2012

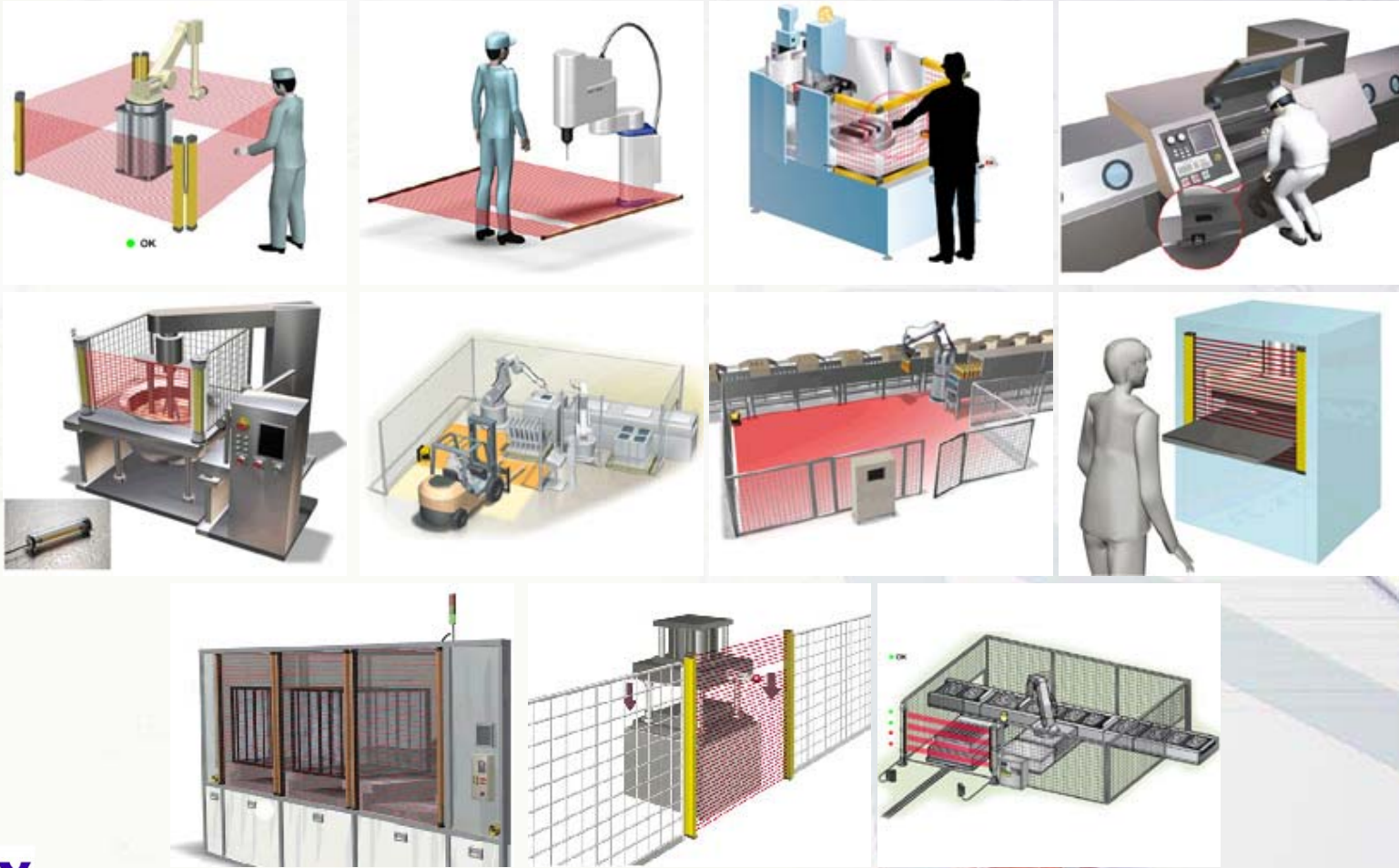
The screenshot displays the SISTEMA software interface. The main window title is "SISTEMA - Safety Integrity Software Tool for the Evaluation of Machine Applications". The interface includes a menu bar (File, Edit, View, Help), a toolbar with icons for New, Open, Save, Close Project, Library, Report, Help, and Wizard-Help, and a project tree on the left. The project tree shows a hierarchy of safety functions: PR 19 Interlocked guard with guard lock, SF No deactivation of guard locking, SB Activation of the magnet, CH Channel 1, BL Tachometer G1, BL Zero-speed relay K1, CH Channel 2, BL Contactor K2, TE Test channel, SB Magnet, spring and mechani, SF Prevention of unexpected start-u, and SB Monitoring of the safety guar. The main workspace shows two channels: Channel 1 and Channel 2. Channel 1 contains two blocks: BL Tachometer G1 (DC [Low] 60, MTTFd [High] 30) and BL Zero-speed relay K1 (DC [High] 99, MTTFd [-] 347.22). Channel 2 contains one block: BL Contactor K2 (DC [Low] 73.48, MTTFd [-] 257.73). The bottom left of the interface shows a table of safety parameters for the selected function.

Function	PLr	PL	PFH [1/h]	MTTFd [a]	DCavg [%]	CCF
No deactivation of guard locking at speeds	d	d	1,62E-7			
Activation of the magnet	d	d	1,62E-7	70,65 (High)	64,11 (Low)	70 (fulfilled)

Sistema: free Design Verification Tool maintained by industry

# Applications

2012



# Omron and **Sti** Products

2012



# Questions

2012

- If you have any questions, don't feel limited to 'here and now', my contact details are:
    - Maurits Funke-Kupper
    - Machine and Functional Safety expert
    - Mobile: +61 417 012 139
    - Fax: +61 3 8679 3682
    - maurits.funke@fse-global.com
    - <http://www.fse-global.com>
- Or via John Merrett @ Omron.  
Many thanks for your participation today.