



Machinery Safety Project Lifecycle

▶ Machinery Safety Project Lifecycle

- ▶ [Simplified Project Flow](#)
- ▶ [Common Issues Relating to Safety Compliance](#)
- ▶ [Conformity Assessment Procedure in Brief](#)
- ▶ [Methodology to Aid Compliance](#)

▶ **Simplified Project Flow**

- ▶ Define Requirements of the new Machine/Line
- ▶ Identify Machinery & Project Plan
- ▶ Create Purchasing Specification
- ▶ Appoint OEM's, System Integrators
- ▶ Factory Acceptance Test
- ▶ Receive New Machinery
- ▶ Install New Machinery/Line
- ▶ Site Acceptance Test
- ▶ Carry out Commissioning & Validation
- ▶ Complete Certification & Handover

RETURN TO CONTENTS



► Common Issues

▶ **Common Issues Within the Project**

- ▶ Applicable Directives to be complied to – Example - MD, LVD, EMC, ATEX, PED.....
- ▶ UK Specific Regulations not Considered
- ▶ Outdated Standards Referenced
- ▶ Machinery Specific Standards Not Identified
- ▶ Non-Compliances to Machinery Safety Standards
- ▶ Interpretation of Standards Between UK and OEM Native Country
- ▶ Unidentified Non-Compliances
- ▶ Rectifications Being Completed After Machinery Delivered
- ▶ Ownership of Overall Certification

▶ Regular On Machine Issues Found to Include

- ▶ Insufficient guarding (none / large gaps / damaged, wrong style, size, distance, fixings)
- ▶ Incorrect position of ESPE (light curtains, scanners)
- ▶ Possible fault masking issues in guard switch safety circuits (EN 14119 / EN 13849)
- ▶ Emergency & Guard Switches in the same circuit
- ▶ Open access into dangerous parts of machinery
- ▶ Uncontrolled access into moving machinery (no rotation / speed monitoring)
- ▶ Pneumatic / Hydraulic controls
- ▶ Old or non-existent PUWER assessments
- ▶ New machinery arriving on site that does not meet current regulations (from OEM or inter-company)
- ▶ Electrical Panel Non-Compliances to EN 60204-1
- ▶ Using Outdated Standards

This is not an exhaustive List

▶ Conformity Assessment Procedure

► Conformity Assessment Procedure – UKCA/CE Marking



▶ Who is Responsible for Certification

The responsibility for demonstrating that the machinery satisfies the Essential Health and Safety Requirements of the applicable Directives and can be CE Marked rests on:

- ▶ **Original Equipment Manufacturers (OEM's) and System Integrators**
- ▶ **Agents that import machines**
- ▶ **Companies that directly import machines**
- ▶ **Persons who build machines for their own use**
- ▶ **Persons who substantially modify machines beyond their original specification**

* Be aware of this if they are directly importing machines into the UK – Importers are responsible for signing the Declaration of Conformity.

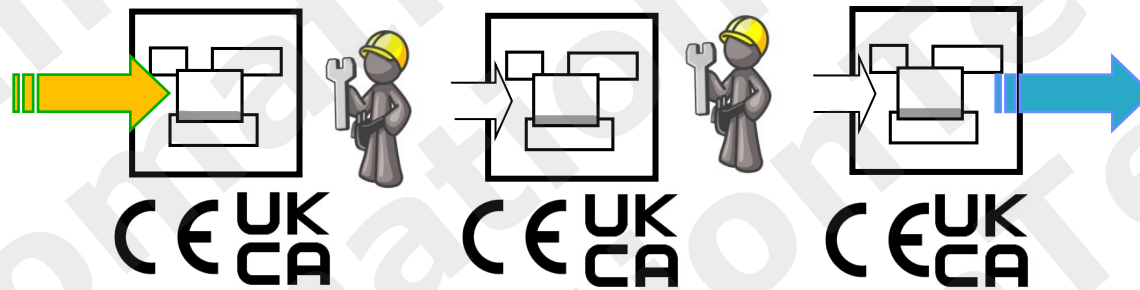




▶ Assemblies of machines CE/UKCA Marking

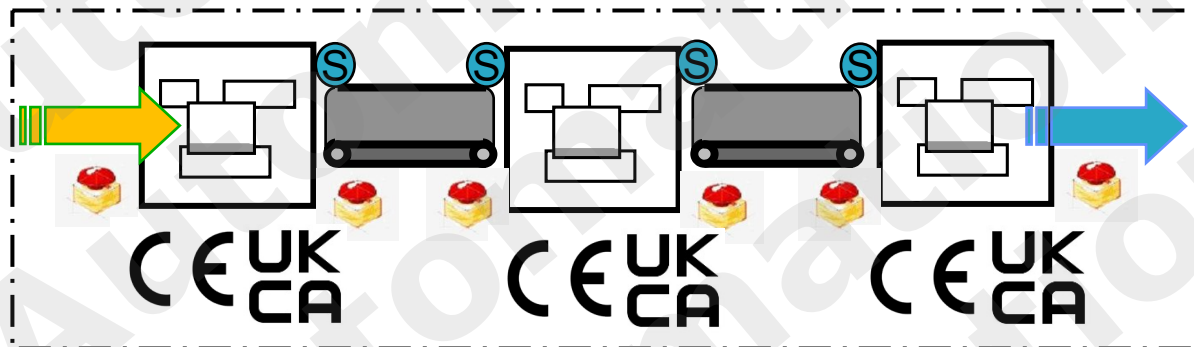
Examples

No process or safety-related connection



No overall
CE/UKCA

Process and safety-related connection



Overall CE/UKCA

► Methodology to Aid Compliance

► Pilz Machinery Lifecycle

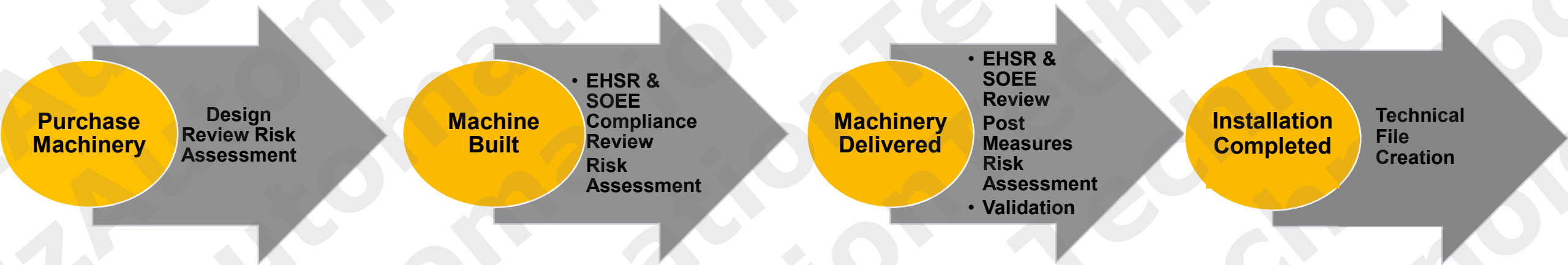


▶ Early Considerations

- ▶ Detailed RFQ Considering Safety Requirements
- ▶ Identify Machine Specific Safety Standards
- ▶ Define Role and Responsibilities for the Project from a Safety Perspective
- ▶ Create Specific Compliance Methodology



► Methodology to Aid Compliance



▶ EHSR's - Essential Health & Safety Requirements

According to Article 5 1.(a) of the Machinery Directive:

"Before placing machinery on the market and/or putting it into service, the manufacturer or his authorised representative shall: ensure that it satisfies the relevant essential health and safety requirements set out in Annex I;"



▶ EHSR's – Essential Health & Safety Requirements

EHSR 1 Essential Health and Safety Requirements

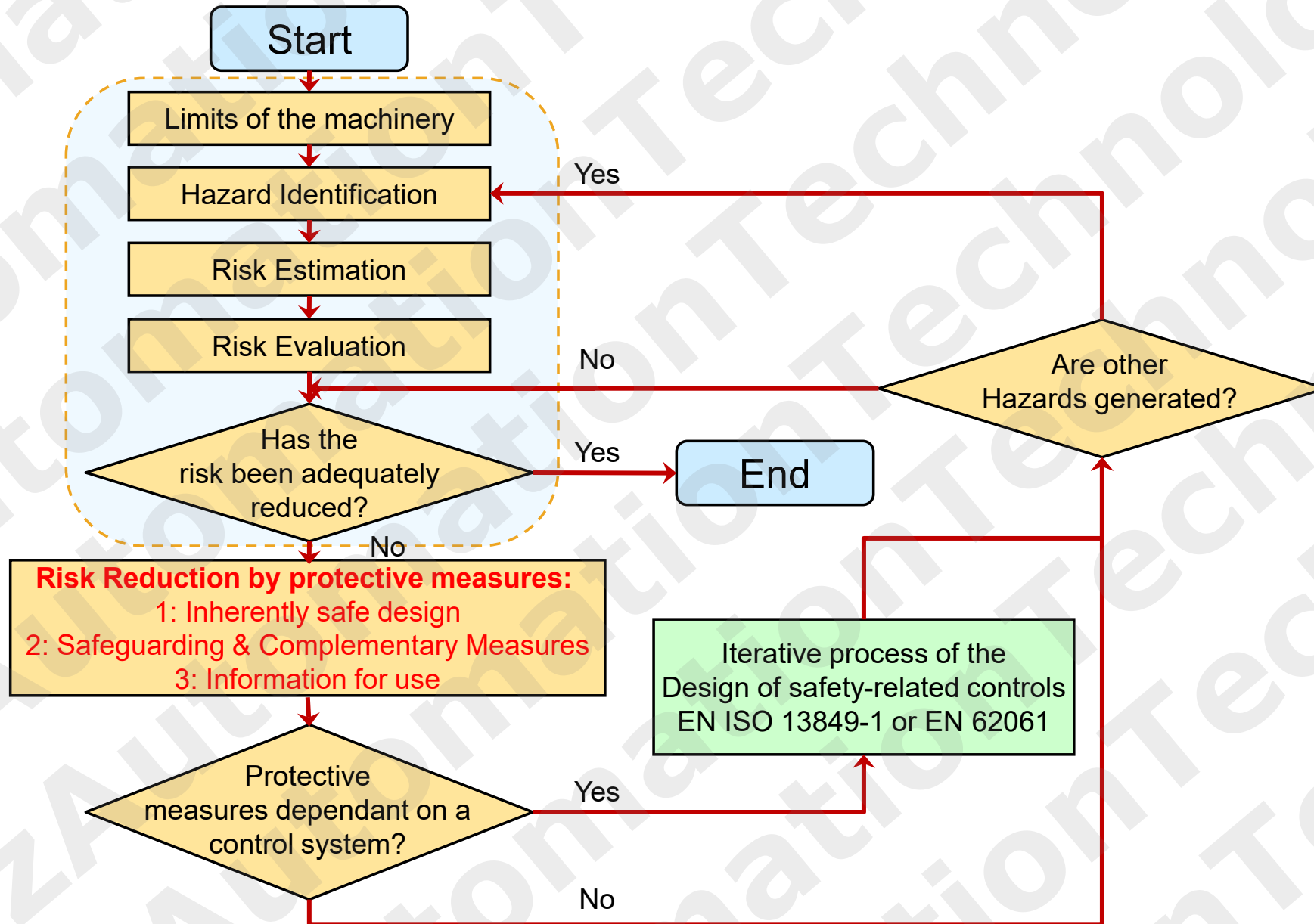
- ▶ EHSR 1.1 General
- ▶ EHSR 1.2 Control Systems
 - ▶ EHSR 1.2.4 Stopping
 - ▶ EHSR 1.2.5 Selection of Control or Operating Modes
- ▶ EHSR 1.3 Protection against mechanical hazards
- ▶ EHSR 1.4 Required characteristics of guards and protection devices
 - ▶ EHSR 1.4.2 Special requirements for guards
- ▶ EHSR 1.5 Risk due to other hazards
- ▶ EHSR 1.6 Maintenance
- ▶ EHSR 1.7 Information



► Risk Assessment



Risk Assessment - EN ISO 12100:2010 - Safety of machinery: General principles for design

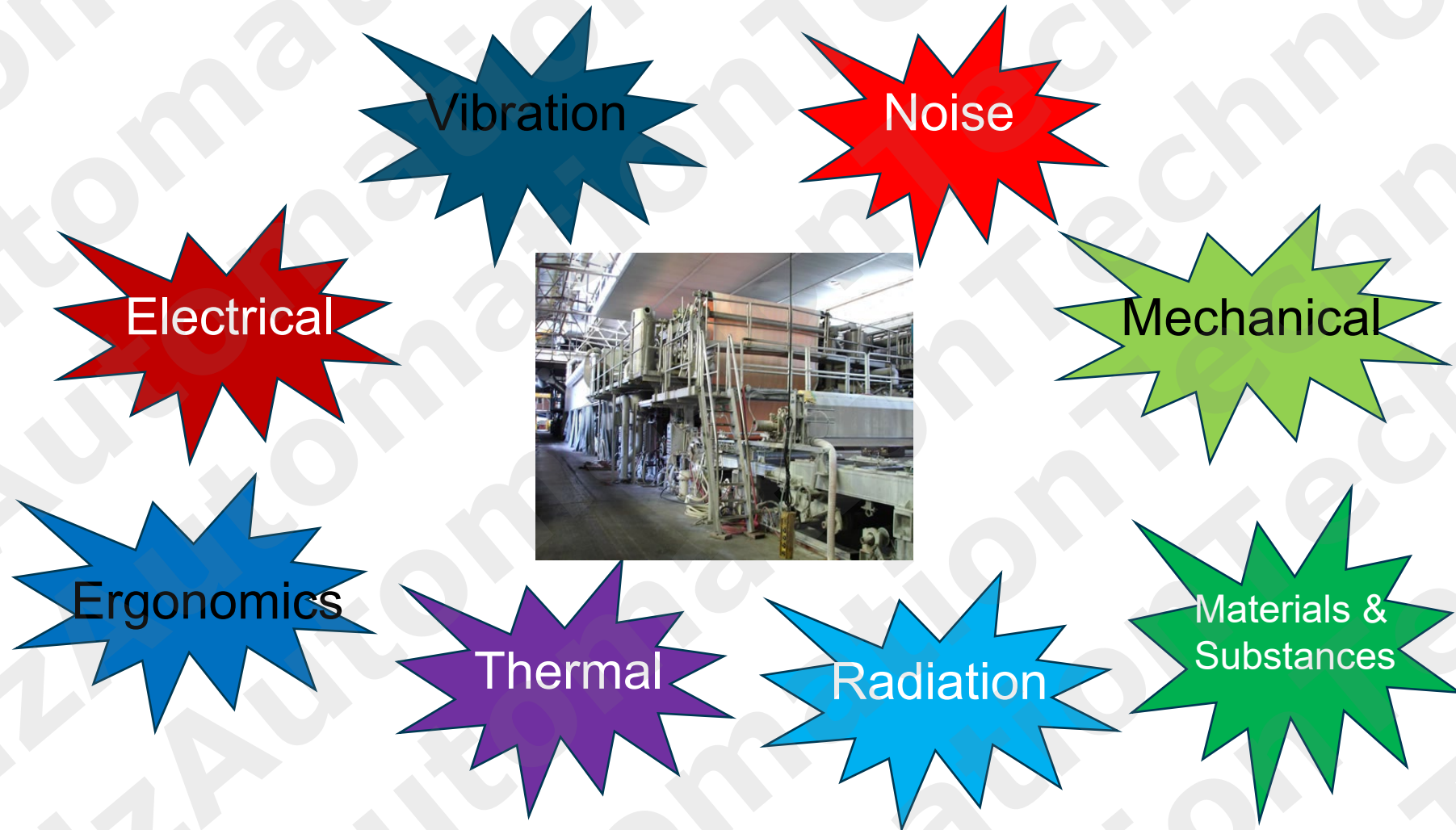


Risk Assessment - Determination of the machine's limits

- ▶ Aspects to be considered when determining the limits of use
 - The machine's operating modes
 - The possibilities for the user to intervene
 - The machine's area of application
 - The user's professional qualifications
- ▶ Aspects to be considered when determining the space limits
 - Room for manoeuvre
 - Space requirement for people handling the machine
 - Interaction between man and machine:
- ▶ Aspects to be considered when determining the time limits
 - "Machine's lifetime" – Operation, maintenance, disposal
 - Recommended maintenance intervals
 - HAZARDS IDENTIFIABLE IN ALL PHASES

► Risk Assessment - Hazard identification

Typical Machinery Hazards



► Risk estimation - PHR method

Four parameters to determine the risk level

- ▶ Possibility of occurrence of a hazardous event (PO)
- ▶ Possibility of avoidance (PA)
- ▶ Frequency of exposure to the hazard (FE)
- ▶ Degree of possible harm (DPH)

$$\text{Risk level PHR} = \text{PO} \times \text{PA} \times \text{FE} \times \text{DPH}$$

▶ Risk estimation - PHR method

▶ Possibility of occurrence of a hazardous event (PO)

<i>Criterion</i>	<i>Hazard rate</i>
Almost impossible	0.05
Unlikely	1.25
Possible	2.5
Likely	4
Certain	6

▶ Possibility of avoidance (PA)

<i>Criterion</i>	<i>Hazard rate</i>
Possible	0.75
Possible under specific circumstances	2.5
Not possible	5

▶ Risk estimation - PHR method

▶ Frequency of exposure to hazard (FE)

Criterion

Annually
Monthly
Weekly
Daily
Hourly
Constantly

Hazard rate

0.5
1
1.5
2.5
4
5

► Risk estimation - PHR method

► Degree of possible harm (DPH)

Criterion

Hazard rate

Scratch/bruise	0.25
Wound / cut / minor health impact / minor burns	0.5
Minor fracture – fingers, toes	3
Major fracture – hand, arm, leg	5
Loss of 1 or 2 fingers / toes or major burns	8
Amputation of leg / hand, partial loss of hearing or sight	11
Amputation of both legs/hands, full loss of hearing/sight in both ears / eyes	15
Critical injuries or long-term illness/injury or permanent condition	25
Single fatality	40
Catastrophic	65

► Risk Assessment – Risk Level

► The risk levels can be assessed and prioritised as follows :

	PHR	Risk	Comment
	1 - 10	Negligible Risk	Presents practically no risk to health and safety, no further risk reduction measures are required.
	11 - 20	Very Low Risk	Presents very little risk to health and safety, no significant risk reduction measures are required, may necessitate the use of personal protective equipment and/or training.
	21 - 45	Low Risk	Risk to health and safety is present, but low. Risk reduction measures must be considered.
	46 - 160	Significant Risk	The risk associated with the hazard is substantial enough to require risk reduction measures. These measures should be implemented at the next suitable opportunity.
	161 - 500	High Risk	Potentially dangerous hazard, which requires risk reduction measures to be implemented urgently.
	501+	Very High Risk	Risk reduction measures should be implemented immediately, corporate management should be notified.

▶ Validation

- ▶ To make sure the safety system does what the designer required
- ▶ There has been no human error in the implementation
- ▶ The System is Safe
- ▶ If a fault occurs the safety system stops the machine/system where required
- ▶ It is suitable and sufficient for the application

► Functional safety – what's new in ISO 13849-1

- ISO 13849 consists of two parts
 - ISO 13849-1:2023
“Part -1: General principles for design” is published.
 - technically revised to clarify and detail some requirements without introducing new major technical concepts
- ISO 13849-2:2012
“Part -2: Validation” will remain as it is for a while. The normative parts of Part 2 are embedded within the Part 1 update



► Validation Principles

Validation consists of applying analysis and executing functional tests under foreseeable conditions in accordance with the validation plan. Figure 1 gives an overview of the validation process. The balance between the analysis and testing depends on the technology used for the safety-related parts and the required performance level.

For Categories 2, 3 and 4 the validation of the safety function **shall** also include testing under fault conditions.

The analysis should be started as early as possible in, and in parallel with, the design process. Problems can then be corrected early while they are still relatively easy to correct, i.e. during steps

- design and technical realization of the safety function
- evaluate the performance level PL
- It can be necessary for some parts of the analysis to be delayed until the design is well developed.

► Validation Principles

Where necessary due to the system's size, complexity or the effects of integrating it with the control system (of the machinery), special arrangements should be made for

- validation of the SRP/CS separately before integration, including simulation of the appropriate input and output signals, and
- validation of the effects of integrating safety-related parts into the remainder of the control system within the context of its use in the machine

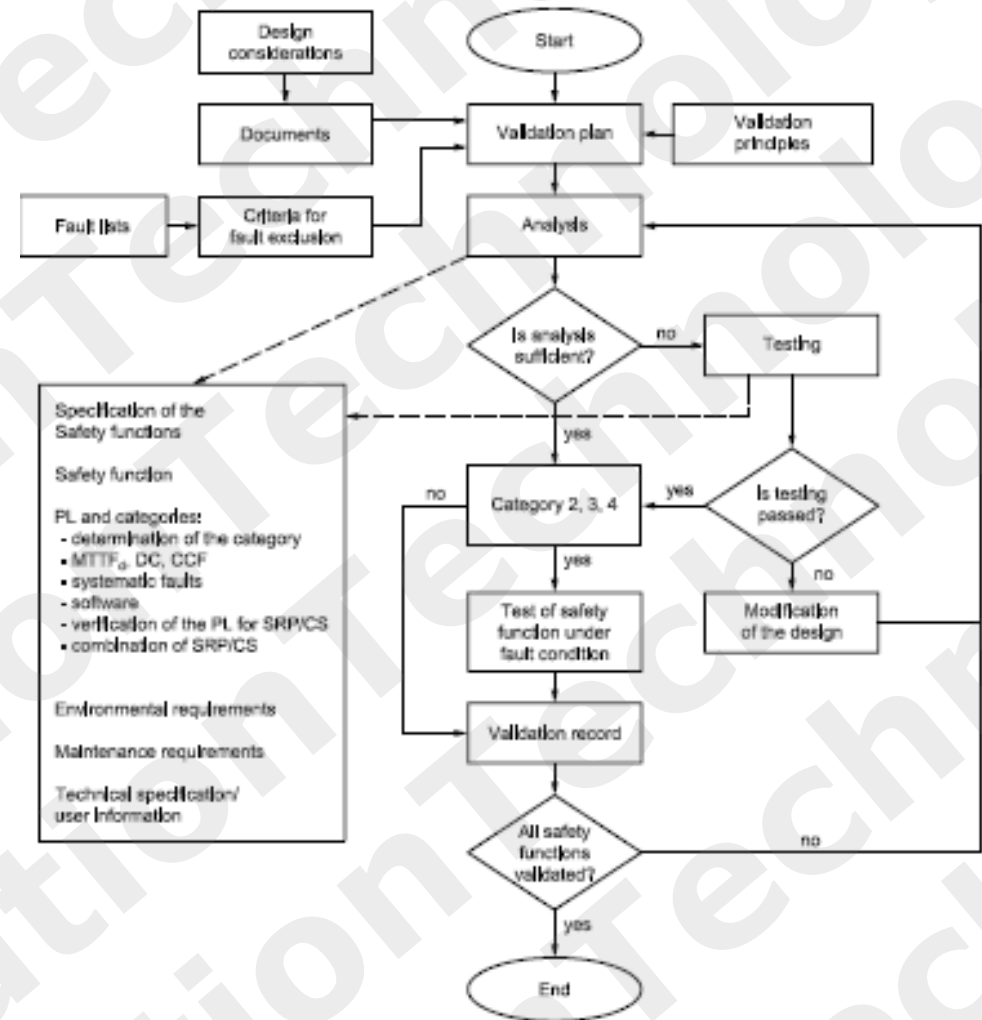


Figure 1 — Overview of the validation process

► Validation Plan

The validation plan shall identify and describe the requirements for carrying out the validation process for the specified safety functions, their categories and performance levels.

The validation plan shall also identify the means to be employed to validate the specified safety functions, categories and performance levels. It shall set out, where appropriate

- a) the identity of the specification documents,
- b) the operational and environmental conditions during testing,
- c) the analyses and tests to be applied,
- d) the reference to test standards to be applied, and
- e) the persons or parties responsible for each step in the validation process.

Safety-related parts which have previously been validated to the same specification need only a reference to that previous validation.

Validation Documented

Component Name	Initiating Event	Initial Status	Resulting Action	Component Name	Initial Status	Resulting Action	Component Name	Initial Status	Resulting Action
				1 - DEPALLETER	ON	OFF	Emergency Stop to Container Conveyor	ON	OFF
				STO to Drive Transport (XV4)	ON	OFF	Emergency Stop	ON	OFF
				Emergency Stop Shutdown (25Q1)	ON	OFF	- Pallet Conveyor (XV4.2)	ON	OFF
				Emergency Stop - Control Voltage	ON	OFF	24VDC Machine (XV3.2.1)	ON	OFF
				Drive inputs, Drive STOs, Relief Valves (XV3)	ON	OFF	Servo Drives - 24VDC for Drive Stroke Brakes (3.12)	ON	OFF
				Drives Safety Stop (XV2.3)	ON	OFF		ON	OFF
				2 - LABELLER	ON	OFF	Emergency Stop to Label Control	ON	OFF
				Emergency Stop to Transport, STO to Drive	ON	OFF	Emergency Stop to Date Marking 4/Robotch	ON	OFF
				Emergency Stop Potential 3	ON	OFF		ON	OFF
				3 - PACKER	ON	OFF	Shut down valve	ON	OFF
				Control voltage on	ON	OFF		ON	OFF
				Main drive on/off	ON	OFF		ON	OFF
				STO Emergency stop	ON	OFF		ON	OFF
				STO Safety device Feed Belt	ON	OFF		ON	OFF
1 - DEPALLETER	Emergency Stops Internal (12 Estops)	Button(s) depressed	X	X	X	X	X	X	X
	Emergency Stops - Internal and Container Conveyor	Button(s) depressed	X	X	X	X	X	X	X
	Safety Light Barrier 1	Beam(s) broken	X	X	X	X	X	X	X
	Safety Light Barrier 2	Beam(s) broken	X	X	X	X	X	X	X
	Safety Door 1	Door open	X	X	X	X	X	X	X
	Safety Door 2	Door open	X	X	X	X	X	X	X
2 - LABELLER	Emergency Stop	Button(s) depressed	X	X	X	X	X	X	X
	Emergency Stop +P2	Button(s) depressed	X	X	X	X	X	X	X
	Emergency Stop +P3	Button(s) depressed	X	X	X	X	X	X	X
	Enabling Sw Emergency Stop +P4	Button(s) depressed	X	X	X	X	X	X	X
	Enabling Button +P4	Switches not activated	X	X	X	X	X	X	X
	Safety door 1	Door open	X	X	X	X	X	X	X
	Safety door 2	Door open	X	X	X	X	X	X	X
	Safety door 3	Door open	X	X	X	X	X	X	X
	Safety door 4	Door open	X	X	X	X	X	X	X
	Safety door 5	Door open	X	X	X	X	X	X	X
	Safety door 6	Door open	X	X	X	X	X	X	X
	Safety door 7	Door open	X	X	X	X	X	X	X
	Emergency Stop from Container Conveyor	Button(s) depressed	X	X	X	X	X	X	X
	Emergency Stop from Label Control	Button(s) depressed	X	X	X	X	X	X	X
3 - PACKER	E/Stop Panel	Button(s) depressed	X	X	X	X	X	X	X
	E/Stop Machine Feed	Button(s) depressed	X	X	X	X	X	X	X
	E/Stop Machine Outlet	Button(s) depressed	X	X	X	X	X	X	X
	E/Stop Machine External	Button(s) depressed	X	X	X	X	X	X	X
	Power Packer on/off	Switch in off position	X	X	X	X	X	X	X
	E/Stop Tunnel	Button(s) depressed	X	X	X	X	X	X	X
	E/Stop Film Wrapping	Button(s) depressed	X	X	X	X	X	X	X
	Power Packer on/off 2	Switch in off position	X	X	X	X	X	X	X
	Safety device 1	Guard open	X	X	X	X	X	X	X
	Safety device 2	Guard open	X	X	X	X	X	X	X
	Safety device 3	Guard open	X	X	X	X	X	X	X
	Safety device 4	Guard open	X	X	X	X	X	X	X
	Safety device 5	Guard open	X	X	X	X	X	X	X
	Safety device 6	Guard open	X	X	X	X	X	X	X
	Safety device 7	Guard open	X	X	X	X	X	X	X
	Safety device 8	Guard open	X	X	X	X	X	X	X
	Safety device 9	Guard open	X	X	X	X	X	X	X
	Safety device 10	Guard open	X	X	X	X	X	X	X
	Safety device 11	Guard open	X	X	X	X	X	X	X
	Safety device 12	Guard open	X	X	X	X	X	X	X
	E/Stop Machine feed	Button(s) depressed	X	X	X	X	X	X	X

► Validation Documented

DT	Description Sensors	Signals		OK	nOK
		Input	Output		
27ES	E-STOP, pushbutton, CP27 Main Panel	(27ES) A4.i0		<input type="checkbox"/>	<input type="checkbox"/>
27PBRESET	RESET Pushbutton (N/O), CP27 Main Panel	(CP27_RESET) A8.i0		<input type="checkbox"/>	<input type="checkbox"/>
SS1 active	VFD45108 Safe Standstill 1 is ACTIVE	(VFD45108_SS1_ACTIVE) A10.i0		<input type="checkbox"/>	<input type="checkbox"/>
STO active	VFD45108 Safe Torque Off is ACTIVE	(VFD45108_STO_ACTIVE) A10.i1		<input type="checkbox"/>	<input type="checkbox"/>
	Description Logic				
-1120.A1	PNOZmulti m B 1 (772101)			<input type="checkbox"/>	<input type="checkbox"/>
	Description Actuator				
VFD45108_SS1	Safe Stop 1 (SS1) (OG1A)		A10.o0 (VFD45108_SS1)	<input type="checkbox"/>	<input type="checkbox"/>
-KM_SORTER	Contacteur SORTER (OG1B)		A4.o0 (-K_SORTER)	<input type="checkbox"/>	<input type="checkbox"/>
-KM_Merge and Infeed	Contacteur Merge and Infeed (OG2)		A4.o1 (-K_Merge and Infeed)	<input type="checkbox"/>	<input type="checkbox"/>
-KM_Takeaways	Contacteur Takeaways (OG3)		A4.o2 (-K_Takeaways)	<input type="checkbox"/>	<input type="checkbox"/>
-KM_Decline	Contacteur Decline (OG4)		A4.o3 (-K_Decline)	<input type="checkbox"/>	<input type="checkbox"/>
-KM_Recirc	Contacteur Recirc (OG6)		A5.o1 (-K_Recirc)	<input type="checkbox"/>	<input type="checkbox"/>
-KM_Acc to Merge	Contacteur Acc to Merge (OG7)		A5.o2 (-K_Acc to Merge)	<input type="checkbox"/>	<input type="checkbox"/>
-KM_F_Acc to merge	Contacteur F_Acc to Merge (OG8)		A5.o3 (-K_F_Acc to merge)	<input type="checkbox"/>	<input type="checkbox"/>
-CE1_27ESR1	Contact Expander 1			<input type="checkbox"/>	<input type="checkbox"/>
-CE3_27_ESR1_1	Contact Expander 2			<input type="checkbox"/>	<input type="checkbox"/>
-CE3_27ESR2	Contact Expander 3			<input type="checkbox"/>	<input type="checkbox"/>
-CE4_27ESINT26	Contact Expander 4			<input type="checkbox"/>	<input type="checkbox"/>
-CE5_27R1ESR1	Contact Expander 5			<input type="checkbox"/>	<input type="checkbox"/>
-CE6_27R1ESR2	Contact Expander 6			<input type="checkbox"/>	<input type="checkbox"/>
CE7_27R1ESR_new	Contact Expander 7			<input type="checkbox"/>	<input type="checkbox"/>
-CE8_27R1ESINT1	Contact Expander 8			<input type="checkbox"/>	<input type="checkbox"/>
-CE10_26ESR3	Contact Expander 10			<input type="checkbox"/>	<input type="checkbox"/>

► Validation Documented

Designation	OK	nOK	NA
Modules used as expected/planned	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Visual inspection for mechanical damage and fixings	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Check mechanical practicability	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Check regarding interlocking function (independent engagement)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Check trigger process	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Check optical indication of trigger process	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
No independent restart after release	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Detection of short across contacts	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
On two-channel version, disconnect channels alternately and check function	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<u>Fault exclusions? If yes, give reasons:</u> None			
<u>Notes:</u> Single channel input device (pushbutton).			

▶ **Methodology to Aid Compliance**

▶ **Design Review Risk Assessment**

- ▶ Remote Video Call with Machinery Safety Consultant, OEM & End User

▶ **EHSR & SOEE Compliance Check and physical Risk Assessment**

- ▶ Carried out at OEM Facility

▶ **EHSR & SOEE Review and Post Measures Risk Assessment**

- ▶ Inspections of Machinery in operation conditions

▶ **Validation & Verification**

- ▶ Functional Test with Fault Injection and Confirmation PLr has been Achieved

▶ **Technical File Completion and UKCA/CE Certification**

- ▶ Signing of DOC & Issuing of Technical File

RETURN TO CONTENTS

