

SAFETY COURSE ON SAFETY RISK ASSESSMENTS, SAFETY VALIDATION, IIOT IMPACT

Safety risk assessments, safety
validations, and the impact to IIoT /
Industry 4.0 / smart manufacturing

» **Terry Meister**





TABLE OF CONTENTS

Overview.....	2
Maximizing Safety.....	2
Safety Risk Assessments.....	3
Why Are Risk Assessments Important?.....	3
Who Should be Involved in a Risk Assessment?.....	3
What Terminology Goes Along with Risk Assessments?.....	4
What Procedure Should be Followed?.....	5
What Documentation is Needed?.....	6
Deliverables.....	7
Design Advice.....	7
Example 1.....	7
Example 2.....	8
Safety Validation.....	9
The Principles of a Safety Validation.....	9
Safety Validation Process Overview.....	10
Validation Record.....	10
Software.....	10
Tools.....	11
Safety Validation by Testing.....	12
Information Needed for Safety Validation.....	12
Who Should be Included?.....	12
When are Validations Normally Performed?.....	13
Validation Example.....	13
SAFETY IN THE IIoT / INDUSTRY 4.0 / SMART MANUFACTURING WORLD	13
Summary.....	13



TERRY MEISTER TEACHES SAFETY COURSE ON SAFETY RISK ASSESSMENTS, SAFETY VALIDATION, IIOT IMPACT

EBOOK BY: TERRY MEISTER | CONTROLS AND ROBOTICS ENGINEERING MANAGER

As part of the 2021 CFE Media and Technology Virtual Training Week, AMT's Controls and Robotics Engineering Manager Terry Meister recently taught a course concentrating on safety risk assessments, safety validations, and the impact to IIoT / Industry 4.0 / smart manufacturing.

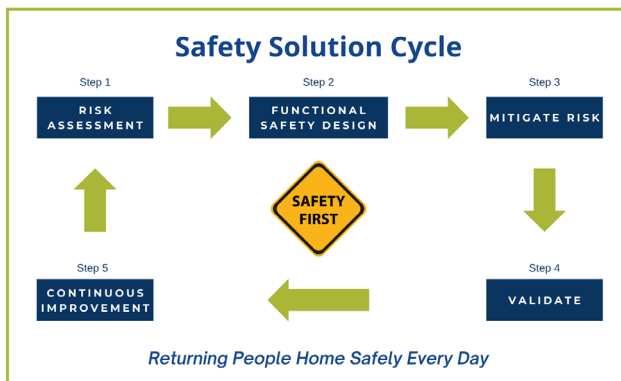
[Click this link](#) to watch the full session.

Terry Meister recently taught a CFE Media and Technology continuing education session focusing on safety validation in an IIoT / Industry 4.0 / smart manufacturing world. Meister leads the controls and robotics team for AMT's Automated Systems Group delivering turnkey automation solutions. His focus on people has allowed him to build a team that ensures all systems from AMT are of the highest quality and meet today's safety standards. As part of every system delivered by AMT, safety risk assessments are conducted to RIA and industry standards. His expertise in electrical and pneumatic hardware engineering is a result of 26 years in the industry. As Meister continues his focus on safety, he is the chairman of AMT's safety committee and also has been a valuable resource on its technical council looking at emerging technologies and industry trends.

“ Safety can be implemented effectively and efficiently provided the right skill sets and resources are maintained. ”

Terry Meister

The topics covered in this course are safety risk assessments, safety validations, and the impact to IIoT / Industry 4.0 / smart manufacturing.



MAXIMIZING SAFETY

Safety is not just a piece of the engineering or a piece of the equipment, it must be thought about as a whole solution in the life cycle of a system or machine. When aiming to maximize safety, there are five different categories that companies typically fall into. They can be complacent, combative (not good), competitive, cooperative, or collaborative.

1. Complacent - most or all of the people at that company don't recognize safety as an integral part of the process
2. Combative - quick to dismiss or argue that safety is a hindrance
3. Competitive - quick to discount safety within their own process
4. Cooperative - understand the need for safety, may not understand totally how to implement it, but they understand that there is a definite need
5. Collaborative - understand the benefits of safety and they are in full implementation on their systems and machines



The first type is **complacent**, meaning that most or all of the people at that company don't recognize safety as an integral part of the process. Today, there are very few companies that fall into category one; most understand safety to a certain extent and understand the need for it.

A **combative** company dismisses or argues that safety is a hindrance. When we look at a company as **competitive**, they're quick to discount safety within their own process.

The fourth type is **cooperative**, which is good. These companies understand the need for safety, but may not completely understand how to implement it. The fifth type of company is one that is **collaborative**; they understand the benefits of safety and they desire full implementation on their systems and machines. Most companies that AMT works with that are building systems and machines are in category four or five.

There are five steps to follow to ensure safe operation on all systems:

1. Risk assessment: this provides an understanding of what must be done to protect the operator
2. Functional safety design: this is the design phase for safety systems for the mechanical and electrical equipment
3. Mitigate risk: there is a risk on many machines and systems; how can you mitigate that to keep people safe?
4. Validation: this is a very important point, but many companies skip it because they run out of time during the manufacturing of the equipment
5. Continuous improvement: systems, safety devices, and programming software are constantly evolving; it's important to finish the safety cycle thinking about how to make improvements on the next event that could happen

Ensuring Safe Operation

1. Risk assessment
2. Functional safety design
3. Mitigate risk
4. Safety validation
5. Continuous improvement

SAFETY RISK ASSESSMENTS

During the safety risk assessment process, the following questions must be answered:

- **Why are risk assessments important?**
- **Who should be involved in them?**
- **What terminology goes along with risk assessments?**
- **What procedure needs to be followed?**
- **What documentation is needed?**

Safety Risk Assessments

1. Importance
2. Team
3. Terminology
4. Procedure
5. Documentation

Why Are Risk Assessments Important?

Completing a risk assessment is the first step in producing a safe solution and it gives a systematic analysis and evaluation of the risk associated with that system over the whole lifecycle of the equipment.

Remember, a risk assessment isn't just for protecting an operator. Risk needs to be evaluated for all stages in the use of a machine or system, all the way from building and programming it, to when it gets to the customer and then when it's demolished. All of those things need to be considered in a risk assessment over the whole life cycle. The risk assessment gives an approach to do that methodically to catch all of the risk. It also allows for an impact on supporting the coworkers. The more that the workers get involved in a risk assessment, the more buy-in that they have.

Who Should be Involved in a Risk Assessment?

There are a variety of parties that should be involved in the risk assessment: end user, operators, maintenance, safety officer, and engineering staff, including controls, simulation, programming and software. All of these people can be part of the group that collaborates on the risk assessment.

Who is Involved?

- Integrator
- Machine builder
- Designers
- End user
- Operators
- Maintenance

What Terminology Goes Along with Risk Assessments?

The following terms relating to safety risk assessment must be understood:

- **Task:** a piece of work that's done or undertaken
- **Hazard:** the potential source of harm from the task that could create physical injury or damage to health
- **Severity:** if contact is made with the hazard, how badly will someone be hurt? Is it a potential pinch, broken bone, or even death?

- Exposure: the estimated incidence of the operator being in the presence of the hazard. Is it once a minute, once a day, or once a year?
- Avoidance: the ability to sense and elude the hazard. How fast can we react to avoid the hazard?
- Risk: a combination of the probability of the occurrence of harm and the severity of that harm
- Functional safety: the piece of equipment or part of the overall safety system which creates the safe environment

Terminology

- Task
- Hazard
- Severity
- Exposure
- Avoidance
- Risk
- Functional safety

What Procedure Should be Followed?

Risk assessments are governed by standards and there are two documents that are primarily used. The RIA R15.06-2012 code is used to evaluate robots and robot systems. The ANSI/ISO 12100:2012 code gives a basis for risk assessments.

There are five pieces to the strategy for risk assessment and reduction, as outlined in ISO 13849-2. The first is to determine the limits of the machinery, which includes the intended use and reasonably foreseeable misuse. An example of a reasonably foreseeable misuse, is that the designer must make sure that the safety devices cannot easily be bypassed. The next strategy is to identify the hazards and associated hazardous situations then estimate the risk for each identified hazard and finally, make a decision about the need for risk reduction. The following six steps are the life cycle of a risk assessment and should be followed each time a system is designed.

- Step 1, identify usage: identify the intended equipment use and the reasonably foreseeable misuse
- Step 2, hazard identification: identify tasks or hazards that may present when an operator interacts with the system
- Step 3, risk estimation: evaluate and assess the risks. For example, look at a task or a hazard and the risk that is involved with it. How badly can a person be injured?
- Step 4, risk evaluation: identify the risk reduction and what countermeasures could be used to protect the operator
- Step 5, risk reduction: mitigate the risk. Put the learning from step four into practice and mitigate the risk with the appropriate countermeasures.
- Step 6, validation: verify that the mitigated risk meets the acceptable level

Risk Assessment References

- RIA R15.06-2012
- ANSI / ISO 2100:2012



What Documentation is Needed?

When it comes to both risk assessments and safety validation, documents are important as they are proof that due diligence was completed to make sure the systems are safe. Understand that the specifications do not give the required documentation.

The documentation can be created by working through a risk assessment and developing custom templates. Also, risk assessment software can be purchased to aid in creating documentation, understanding that the background knowledge and mastery of the principles are still required to produce good outcomes.

Here is the required documentation:

- Cover page: a simple system overview and sequence of operations
- Notes: a list of determinations and assumptions that have been made about the system
- Customer acceptance: the customer signs off to indicate they understand the risks associated with the machine and agreement that the risks have been mitigated to an acceptable level
- Tasks and hazards: what would the hazards be for the task if there was no safety equipment? This can be an extensive section, but it becomes easier with subsequent risk assessments by building a library of hazards associated with particular tasks and equipment.
 - Risk is evaluated by documenting:
 - Severity: what is the severity for each task?
 - Exposure: how likely is it that the operator will be injured by the hazard if there were no safety systems installed?
 - Avoidance: how likely is it that the operator can avoid the hazard based on its speed and process?
- Risk reduction / countermeasures: these are employed to get the equipment into the “safe” category
- Data: this includes information such as robot safe stop times, safe distance calculations, etc.

RISK ASSESSMENT REPORT

Company: _____ Location: _____ Date: 10/11/2017

Robot Cell Identification: _____ Assessed by: _____

Robot Manufacturer and Model Number: _____ Job # of Manufacture: _____

Approved by: _____ Review/Revision Status: _____

Project Identification: _____ PRE REL READY FOR INITIAL REVIEW 8/11/2017
REL RELEASE TO CUSTOMER 10/11/2017

General Description of Application (Narrative):
 Robotic system consisting of _____ equipment, Fanuc collaborative CR35 robot, and Motion RT350 inverter. Robot will perform measurement by way of the _____ equipment in conjunction with the motion of the inverter as a seventh axis. Robotic system is desired to run in an open space or with minimal safeguarding as determined through the risk assessment process.

Sequence of Normal Use:
 1) Operator returns part to loading on inverter dial plate
 2) Operator leaves robotic area
 3) Robot calibrates if required with _____ book
 4) Robot begins measurements functions
 5) Once complete Operator returns area to unload product
 Repeat cycle.

SYSTEM IMAGES

General Comments:
 Procedures shall be developed by _____ to address tasks requiring procedural mitigation as noted within the risk assessment.
 While not specific to the application, foreseeable mis-use by operators or nearby personnel has been considered as closely as possible.
 For maintenance and servicing tasks, reference manufacturer specific documentation.
 Robot 7th axis does not have force monitoring capability and has the potential to be a hazard for personnel in the working area. Procedures and secondary protections have been planned to be put in place. _____ has determined that turntable motion of 10 degrees does not pose a significant hazard to personnel, and residual risks can be mitigated by way of _____ procedures policy and training.

Prepared by: _____ Date: _____
 System Integrator: _____ Signature: _____ Date: _____
 System End User: _____ Signature: _____ Date: _____

Deliverables

Although there is often a heavy burden of documentation for risk assessments, it is for the important purpose of keeping people safe and alive. The deliverable package should be easy to understand and have buy-in from relevant parties. Having good documentation can answer any questions that come up in the future about mitigation strategies, testing methods, and more.

Hazards							Tasks					
ITEM	ISSUE	EVIDENCE	EXPOSURE	AVOIDANCE	RISK	SAFETY CATEGORY	ITEM	TASK	ISSUES	PERSONNEL	EFFECTS	NOTES
1	Shock to equipment	Measure	Low	None	MEDIUM	PL-C Category 2	1	Testing Program to Run	Shock to equipment Exposure to heat Control by the robot Unprotected motion	Programmer	Use and production	
2	Exposure to noise	Measure	Low	None	HIGH	PL-C Category 3	2	Testing Program to Run	Unprotected motion			
3	Controlled fire hazard	Measure	Low	None	HIGH	PL-C Category 3						
4	Unprotected motion	Measure	Low	None	MEDIUM	PL-C Category 2						
5	Trailing joints	Measure	Low	None	MEDIUM	PL-C Category 2						
6	Walking joint	Measure	Low	None	LOW	PL-C Category 2						
7	Physical strain	Measure	Low	None	LOW	PL-C Category 2						
8	Lubrication (Sharp parts)	Measure	Low	None	NEGOTIABLE	PL-C Category 1						
9	Electrical shock	Measure	Low	None	HIGH	PL-C Category 3						
10												
11												
12												
13												
14												
15												
16												
17												
18												
19												
20												
21												
22												
23												
24												
25												
26												
27												
28												
29												
30												
31												
32												
33												
34												
35												
36												
37												
38												
39												
40												

Design Advice

Risk assessments and safety systems must be considered as part of the overall project budget and timeline. A good rule of thumb is to keep safety systems simple; if it is a very complicated safety system, people are going to try to bypass it. Make sure that the schedule includes adequate time for the completion of the risk assessment. Safety can be implemented effectively and efficiently if the right resources and skill sets are allocated to do so.



Example 1

The chart illustrates the risk level by examining the severity, exposure to the hazard, and potential avoidance of the hazard. As an example, what is the risk level of an industrial robot with no fencing or other safety devices? The harm from a robot would not be minor or moderate, it is in the S3 severe category; a person exposed to a robot would get seriously injured. For exposure, anyone could walk up to a robot without an enclosure, so that's in the E2 high risk category. For avoidance, it's not likely that a robot moving at 3000 millimeters per second can be avoided, which is A2 category, resulting in a risk level of high. With the RIA standard for a robot, the performance level and structure category require a minimum PLD category 3. The risk has been evaluated and the minimum safety standard that needs to be protected against has been determined. To mitigate this risk, countermeasures are employed, such as fencing for the robot.

Take All Concerns Into Account

- Safety
- Preserving the process
- Profitability
- Budget
- System complexity
- Schedules

To continue the robot example, the data required is robot safe stop times, safety distance calculations, device response times, and software response times. Knowing robot safe stop times is imperative because after the e-stop is hit and the robot gets a stop signal, it cannot come to a complete stop immediately because of its inertia. For safe distance calculations, a light curtain or a safety scanner may be in use and those have associated times that it takes to react to the input signal of the broken beam. It's important to realize that a relay doesn't work instantaneously. Software also takes time to respond. Even times measured in milliseconds matter when it comes to safety. Designers need to understand these principles and collect all the data to produce a good risk assessment and ensure the risk is properly mitigated.

Severity of Injury	Exposure to the Hazard	Avoidance of the Hazard	Risk Level
S1 - Minor	E0 - Prohibited	A1 - Likely	NEGLIGIBLE
	E1 - Low	A2 - Not Likely	LOW
	E2 - High	A3 - Not Possible	
S2 - Moderate	E0 - Prohibited	A1 - Likely	MEDIUM
	E1 - Low	A2 - Not Likely	HIGH
	E2 - High	A3 - Not Possible	
S3 - Serious	E0 - Prohibited	A1 - Likely	LOW
	E1 - Low	A2 - Not Likely	HIGH
	E2 - High	A3 - Not Possible	

Risk Level	Minimum SRP/CS requirements	
	PL _r	Structure Category
NEGLIGIBLE (see 5.6.1)	c	1
LOW	c	2
MEDIUM	d	2
HIGH	d	3
VERY HIGH (see 5.6.2)	e	4

Functional Safety

Risk Assessment Data Collection

1. Robot stop times
2. Safety distance calculations
3. Device response times
4. Software response time



Example 2

The chart shows the hazards associated and the evaluation of risk. Currently the risk is at a medium level, but it is possible to negate that risk to an even lower level. In the example of someone teaching a robot, as is shown in the chart under countermeasures, are there additional countermeasures that can further lower the risk? If the robot is in teach mode, it is often limited to 250 millimeters a second, which is a safe speed for humans to avoid, which is

Item / Who	Task	Hazard - Risk	Evaluation		Countermeasure Sketch or description of safety protection and reason why level of safety device was chosen	Safety Device Integrity	Check		Notes				
			Severity	Exposure			Severity	Exposure					
1 See Task List	Teaching/Programming	Crushed by the robot	Severely	Moderate	1 Compliant robot per ISO10218-Part 1	PL d, Category 2	Severity	Moderate					
	Struck by robot/gripper	Exposure	Low	2 Teach speeds of 250mm/s	Prohibited								
	Uninspected motion	Avoidance	Not Likely	3 POS enable switch	Likely								
	Risk Level				4 Single man operation	Ranking associated to the highest level of risk for an identified hazard related to the task. Reference Hazard List for individual device integrations if required for purposes of design. Each hazard to be re-assessed once counter measures are in place to find any higher risks.	Risk Level						
	Conveyor pinch	5 Guarding per RIA	MEDIUM		LOW								
	Tooling motion	6 Clear of wireway and obstructions per 5.5.3											
	Projectiles	7 CDLR functions removed during entry/teach											
	Slip & trip	8 Destacker functions removed during entry/teach											
	Falling part	9 Vacuum air prep always live											
		10 PPE - Eyewear, Steel toes, Hardhat, Gloves, Etc.											
		11											
		12											
		13											
		14											
		15											
! LOCKOUT & CONTROL SOURCES OF ENERGY !													
Validated By:		Validation Date:					Validation Notes:						

one countermeasure. Another way to mitigate that risk is to have a single-person operation, in other words, don't have more than one person with a teach pendant inside the cell while teaching the robot. Teach pendants have a three-position enable switch requiring the user to hold the switch in the center. If anything were to happen, the user would quickly let go of the

pendant and the switch would no longer be in the center enabling position, stopping the robot instantly. Countermeasures like these allow the designer to negate the risk which results in a higher level of protection. This process is used for every task by examining what the hazard is without any safeties around it and employing countermeasures to negate that risk.


SAFETY VALIDATION

After the risk assessment is complete and the system is fully designed and built, the next step is to validate that the system is at the expected risk level and the higher-risk hazards have been negated. The validation plan should be considered from the start; it should not be an afterthought at the very end of building the system.

Safety validation consists of applying analysis and executing functional tests as written into a validation plan under foreseeable environmental conditions. In addition, safety function categories two, three, and four also must include testing the system under fault conditions.

Safety Validation

- Principles
- Plan
- Designs
- Testing
- Documentation

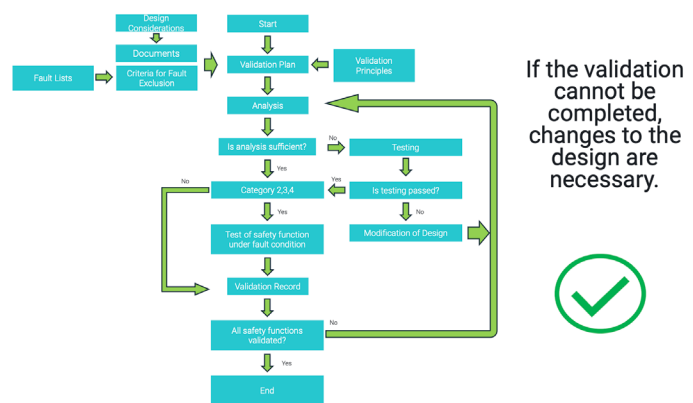


The Principles of a Safety Validation

The validation should confirm the design of the safety related parts (SRP) / controls system (CS) meets the requirements ISO 13849-1. To meet those requirements, several items must be part of the validation:

- Meet the requirements of the performance level (PL)
- Meet the requirements of the specified category
- Measures for control and avoidance of systemic failures
- If applicable, the requirements of software
- Ability to perform a safety function under expected environmental conditions
- Design of operator interface such that the operator is not tempted to act in a hazardous manner

The design must meet the requirements of the performance level mentioned earlier, and meet the requirements of the specified category, which comes from the risk assessment. The control devices must be measured for the avoidance of systematic failures. If applicable, any safety software must also meet requirements.



The safety function must be tested under expected environmental conditions as well. What is the environment that the system is going into? It may have been built in a controlled environment, such as 70 degrees with low humidity, but what if the machine will be used in a freezer and the safety devices and functions are not able to work there?

The operator interface is a key part of the design and must be created so that the operator is not tempted to act in a hazardous manner, such as defeating the SRP or CS. Also, the safety validation principles 13849-2 state that the validation should be carried out by persons who are independent of the design. It's imperative that the checker is someone who was not involved in the design; a second set of eyes can find those small things that may potentially cause a safety issue.

Safety Validation Process Overview

The first step in the validation plan is to implement the validation principles. The validation plan should describe the requirements for carrying out the validation process. It should:

- Specify safety functions
- Specify categories and performance levels
- Identify specification documents
- Identify operational and environmental conditions during testing
- Identify analysis and tests to be applied
- Reference test standards to be applied
- Identify the person(s) responsible for each step

The design considerations documents must be planned; these are the reference documents such as the risk assessment. The validation plan also includes the faults lists to make sure that those critical faults are actually built into our validation plan. Finally, the analysis is conducted. In the analysis, the individual parts of the safety system, including software, are inspected to make sure they have been tested and proven to meet the required safety function and performance level. AMT uses only quality equipment and software from reputable manufacturers who provide the necessary documentation, reducing headaches during the analysis portion of the validation.

If the risk assessment determines that the system is in category two, three or four, testing under fault conditions is also required in order to catch a single failure and react to it.

Validation Record

The validation record consists of the full documentation of the validation process and should contain the paperwork to prove every step of the process has been properly completed and encompasses the entire safety system as it exists in the equipment. Should it be found that a device was excluded from the process, the steps must be repeated until the validation record reflects the actual complete system that is in use.

When making a plan for the safety validation, goals must be kept in mind. It is very important to describe the requirements needed to carry out for the validation. From the beginning of the process, it is crucial to understand the specific safety functions, category, and performance levels required to meet and validate the system. Additionally, it is important to assign a person who is responsible for each of these tasks to ensure that nothing is missed.

Software

There are two types of software that are covered under ANSI 13849-1, part 7: safety-related software; they are SRASW (safety-related application software) and SRESW (safety-related embedded software).

If an engineer is creating a system design that contains any associated software, the designer must follow the code to identify its category and performance level. All aspects of the software must be fully validated, including the characteristics of it: the drawings, block diagrams, circuit diagrams, functional descriptions, time sequence for switching devices, analysis of relevant faults.

Don't be tempted to take a shortcut when software is present in the system. Software is being used for safety more frequently and it must be validated as well. The software specification must be clear and unambiguous and the person verifying it needs to understand the intent. The specification should state the safety requirements, the performance level, evidence that it meets those requirements, and detailed testing of the validation.

The validation plan is the key. It helps on the plant floor to make sure that the system is safe from a software aspect. The safety-related software is either embedded or application software, but it needs to include certain things, such as the functional behavior performance criteria. The software must be verified that it measures up to the performance level of the safety function originating in the risk assessment.

To avoid and protect against systemic software faults, measures and activities should be taken during software development. For a small, simple system, a validation may be as straightforward as a walkthrough or review of that software. Again, a second set of eyes should be validating all systems. On bigger systems, someone needs to validate the software functions and safety blocks, tearing each one apart, making sure that they react and are written in a way that is safe.

In summary, where software is relevant, make sure the specification is clear and unambiguous. The specification needs to state the required safety performance and evidence that it meets those requirements. It should also detail the tests used to produce the evidence.

All software functions need to be validated, including safety blocks.

Safety Validation of Software Includes:

- Specified functional behavior & performance criteria
- Verification that software measures are sufficient for the specified performance level of the safety function
- Measures and activities taken during the software development to avoid systematic software faults
- Validation of all software functions and safety blocks

Safety Validation of Design: SISTEMA

- Meets ISO 13849-1
- Libraries available for many manufacturers
- Multi-lingual and industry accepted
- Assists with risk parameters for determining:
 - Required performance level (PLr)
 - Category
 - Measures against common core failures (CCF) in multi-channel systems
 - Mean component quality (MTTFd)
 - Mean test quality (Dcavg) of components or blocks

Tools

There are many tools that can help with validation. An example is SISTEMA, a free software tool for assisting in validating that the application meets the Control Standard in EN ISO 13849-1. SISTEMA, offered by German insurance association DGUV, is an industry accepted, multilingual tool which has libraries available for many component manufacturers. It assists with the risk parameters for determining required performance level (PLr), risk category, measures against common cause failures (CCF) in multi-channel systems, mean component quality (MTTFd), mean test quality (Dcavg) of components or blocks. SISTEMA takes the required risk category from the risk assessment and helps determine if the designed safety devices and wiring practices achieve that level. It also takes into consideration the common cause failures of a component, the mean time to failure of components, and the diagnostic coverage of components.

Safety Validation by Testing

The next step is to produce the test plan and making sure that the records cover the basis written into the specification, such as the name of the person carrying out the tests, the environmental conditions, the test procedures, the equipment used, the date of the test, and the results of the test, while making sure the validation is against systemic failures and also of faults if it's in category two, three, or four. All of these items need to be in the validation plan and during testing the engineer actually removes each wire, making sure that that fault is caught and the system can't be reset. Again, documentation is key. Every system must leave with documentation proving it is validated.

Information Needed for Safety Validation

- Varies with technology used
- Must document at all times
- Validate the safety-related parts:
 - Specified characteristics
 - Drawings and specifications
 - Block diagrams
 - Circuit diagrams
 - Functional descriptions
 - Time sequence for switching devices
 - Analysis of relevant faults

Who Should be Included?

For safety validation, use hardware, software, and testing safety engineers who did not write the software, work on the design or work on the project. Some clients request third-party validation, which is not required by the codes.

Include the following:

- Hardware - a safety engineer who did not work on the project
- Software - a safety engineer who did not work on the project
- Testing - a safety engineer who did not work on the project
- 3rd party validation may be required depending on the customer

When are Validations Normally Performed?

AMT completes at least two validations for each system.

The first is before the equipment leaves the plant at the factory acceptance test (FAT). A validation is also completed at the end user’s facility when the system is finished to make sure nothing has changed: no one has added devices and nothing has changed in the safety solution, ensuring the system is safe.

Validation Example

In this example, the category 3 PLD is what the device must meet. Take, for example, a simple push button e-stop. The e-stop has already been verified as meeting the correct category and PL level necessary to create the safety function based on the risk assessment, but it still needs to be physically tested. Some people may think it’s enough to hit the e-stop and verify that the machine stops. But, have the faults been tested? What if one of the wires becomes disconnected? Can it be proven that the e-stop is redundant?

Project Number and Description					
Unless otherwise stated, the system must be reset after each test Motion includes any moving parts in the system (robots, conveyors, cylinders, etc.)					
Safety Device Information					
Safety Device Name: Main Panel E-stop PB (0.085)					
Customer Name: Customer Name					
Project Number: 12345					
Test#	Test description	Cat3 PLD	Pass/Fail	Not Applicable	Checked By
Press E stop					
1	Motion has stopped and cannot be restarted Control power is not on Cannot reset				
Comments:					
Test#	Test description	Cat3 PLD	Pass/Fail	Not Applicable	Checked By
Remove channel 1 wire (0.0) in the main panel with E-stop reset (do not reset after this test)					
2	Motion has stopped and cannot be restarted Control power is not on Cannot reset				
Comments:					
Test#	Test description	Cat3 PLD	Pass/Fail	Not Applicable	Checked By
Replace channel 1 wire (0.0) (do not reset until after this test)					
3	Motion is still stopped and cannot be restarted				
Comments:					

SAFETY IN THE IIOT / INDUSTRY 4.0 / SMART MANUFACTURING WORLD

In the IIoT / Industry 4.0 / Smart Manufacturing world, more machines are getting interfaced with the cloud. At this point, most safety systems are still held on the plant floor directly at the machine and with the local PLC controller, but in the future this is likely to change.

As safety systems become connected to and accessible from the cloud, designers need to make sure that these systems cannot be altered by someone who is not on site. Network protection is necessary for connected systems, and the ramifications of hacking, ransomware and other scenarios need to be considered. Ask questions such as, if remote changes are allowed, how can accidents be prevented?

A corporate culture that consistently supports (and may have already implemented) these specifications is vital to the success of safety in a technology-driven world. As Industrial Internet of Things (IIoT) and Industry 4.0 continue to be defined, designers must stay up to date on specifications and do research on the security of these technologies and devices to stay at the forefront of this emerging technology.

To learn more on these topics, the full presentation is available [here](#).