Safety Circuit Design

Heinz Knackstedt
Safety Engineer
C&E sales, inc.
OBJECTIVE

• What are some of the “soft” issues which determine the final effectiveness of the Functional Safety risk reduction measure
• Identify the basic Functional Safety circuit design concepts to reduce risks, which may be applied to any machine tool or assembly machine control, including robots and fluid power systems
• Review control design basics as the backbone of ISO 13849-1:2015
Warning

• The intent of the diagrams offered is as a suggestion only. These diagrams simply show, in general, how the listed performance is obtained, and may vary with specific product or application requirements.

• These diagrams are not designed for any specific application or purpose nor to meet a specific application functional requirement.

• Capabilities and features of devices vary by manufacturer. If specific information is needed, contact the manufacturer directly. Failure to obtain specific product feature capability and assembly instructions could result in injury or death.

• Compliance to Federal, State, and Local requirements and safety standards in any application is the responsibility of the end user.
References

- ISO 10218-1, 2: 2011
- ANSI/RIA R15.06-2012
- RIA TR R15.306-2016
- ISO 13849-1-2015
- B11.26-(Final Draft) formerly B11-TR6
- B11.0:-2015
- B11.19:-2010
MACHINE SAFETY IS NOT AN OPTION!

The General Duty Clause 5(a) (1) of the OSH Act-1970 Public Law 91-596 requires that:

Each employer shall furnish to each of his employees, employment and a place of employment, which is free from recognized hazards that are causing or are likely to cause death or serious physical harm

Consensus standards help to identify hazards and risk reduction measures by which acceptable risk may be attained
Consensus Standards

• Seek to highlight the current state of the art and best practices
• May be referenced by OSHA in conjunction with the General Duty Clause
  – Proof that the hazard is known and that a means of remediation exists
  – Two of the four elements of proof for a General Duty Clause citation

An unfounded rumor
Are the Risks at an Acceptable Level?

- Risk Assessment is the first step in the Risk Reduction Process
- But first, a look at the reality of the production floor
Root Cause of Safeguarding Manipulation and Unauthorized Bypassing

POOR FUNCTIONAL DESIGN is most often the ROOT CAUSE for the circumvention of safeguarding devices and other risk reduction measures

Safe Guard “Value” Analysis by the Operator

Perceived Risk and its resultant Reduction ..vs....

Effort of Use of the Risk Reduction Measure

The POSITIVE vs the NEGATIVE
Influences Impacting Safety Behavior

• Perception
  – How hazardous is it now without the safeguard?
  – What is my personal risk?
  – How much is my risk reduced if I use the safeguard?

• Habit
  – “I’ve always done it this way ‘cause that’s a good way and I haven’t been injured”

• Obstacle

• Barriers
  – The safeguard prevents me from ..........

“Understanding Influences on Risks: A Four-Part Model”
Terry Mathis, Shawn Galloway
What is a “Good” Design?

• Without a “SAVINGS” the safeguarding device/measure will not be used

• A “GOOD” risk reduction measure design addresses these concerns:

• Those of the END user
Cause for Manipulation (Defeating) of Safeguarding Devices and Measures

![Bar chart showing the cause for manipulation (defeating) of safeguarding devices and measures. The categories include: Automatic mode, Set-up/adjustment, Programming/program test/test run, Commissioning, Dismantling, Inspection, Readjustment/alignment, Checking/sampling, Modifying/rigging/tool change, Component change, Troubleshooting in the machine, Troubleshooting in the work cycle, Feed/removal of material, Cleaning/servicing, Maintenance. The values range from 55 to 423.]

*Fig. 12* Subjectively perceived “necessity” of manipulating protective devices according to operating modes (n = specifications as part of an empirical study; multiple answers possible)
# Incentive to Defeat Safeguards

## Tasks:

<table>
<thead>
<tr>
<th></th>
<th>Automatic</th>
<th>Manual, etc.</th>
<th>Help</th>
<th>Help</th>
<th>Help</th>
<th>Help</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Initial Operation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Program test/ test run</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Setup/adjustment conversion/tooling/</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Machining</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Manual intervention for swarf removal</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Manual change of workpiece</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>Manual intervention for trouble shooting</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>Checking/random sampling</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>Manual intervention for measuring/ finetuning</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>Manual change of tools</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>Maintenance/ servicing</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>Rectification of faults</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

## Benefits without protective device:

- None
- Minor
- Substantial

## Modes of operation:

- Task permissible for the task
- Task possible in these modes of operation
- Faster, greater productivity
- Greater freedom of movement
- Improved flow of movement, etc.
- Avoidance of interruptions, etc.
- Better audibility
- Reduced travel

## Brief Instructions:

1. Add operating modes if appropriate
2. Determine relevant tasks
3. Complete one cells line by line
Causes of Process Safety Incidences
Safety Related Parts of the Control System (SRP/CS) did not provide the Required level of Risk Reduction

85% 65% Already wrong before start of operation. These are Quality issues not Hardware Failures. Systematic errors which must be Reduced by Fault Avoidance through specification and design quality measures and Validation.

- Specification
  - Lack of Definition and Clarity of Requirement and Purpose
- Design and Implementation
  - Omission and Errors
- Installation & Setting into Operation
  - No Validation Plan
- Modification after setting into Operation
  - Modified to accomplish tasks
- Operation and Maintenance
  - Unclear specifications cause incorrect repair

The Specification is defined as part of the Risk Assessment.

Errors in concept caused by lack of understanding of the task(s)

Only 15% are from operations and failure

Source: “Out of Control” UK Health and Safety Executive (HSE) (September 2004)
A Paradigm Shift

• There is **NO** plant which has not recently had an accident!!

• An accident is any UNPLANNED, UNEXPECTED, and typically UNWANTED event

• It does not necessarily result in an injury
  – Frequently known as an incident
  – A near miss is an accident which, if repeated through continued exposure, will ultimately result in an injury
  – The majority of injuries are preceded by unresolved close calls and near misses
  – **There are between 7 to 9 “Close Calls” for every 1 Injury**
    • The factors which resulted in a near miss at one exposure to the hazard, will not always be present in the same measure to prevent an injury at the next occurrence
Assess Risk

• Establish a risk assessment team
  – Most important member(s) of the Team are those who can identify and who actually perform each task:
    – Operators and Maintenance Personnel

• Identify the TASK/HAZARD pair

• Estimate the Level of Risk
  – Level or degree of harm and probability of occurrence

• Evaluate the Level of Risk
  – Risk is sufficiently low that no additional risk reduction measures are required
    • Typically even an initial low risk still requires some level of procedure and training
  – Identify the method and level of risk reduction required to achieve an acceptable risk
Reduce Risk

• Based on a Risk Assessment, develop a Hazard Control Strategy

• Using THE RISK REDUCTION HIERARCHY
  – Design Machine or Process to either
    • Eliminate Hazard
      – Substitution or elimination
      – Change in the process or operation
    • Reduce Risk
      – Reduce Force, Speed, Frequency of access

• This is why a preliminary Risk Assessment should be performed during DESIGN stage

OR
Reduce Risk

• Control exposure to hazards / reduce risk by risk reduction measures
  – Fixed Covers and Guards
  – Functional Safety
    • A controls based risk reduction measure which upon failure returns the risk to its former unacceptable level
      – Interlocked Guards
      – Safeguarding devices
      – Complementary devices
  – Warning and Alerting Techniques (Awareness Devices)
    • Active
    • Passive
  – Administrative controls
    • Personnel Protective Equipment (PPE)
    • Safe work procedures and practices
Verify the Risk Reduction Measure

• Verify that the risk reduction measure(s) chosen can achieve risk reduction to the level required
  – The risk reduction measure is sustainable and meets operational needs
  – The resultant residual level of risk is acceptable
    • Redesigned Task/Hazard pair is evaluated using same measures as used in the original risk estimation
    • The Functional Safety Performance Level chosen can achieve the level of risk reduction as determined by the level of risk
      – If the SRP/CS meets the Risk Reduction measure’s Performance Level requirement,
      – Then the proposed system is accepted as resulting in acceptable risk when correctly implemented
If the Functional Safety Control System fails to danger, the risk level of the task / hazard pair reverts back to its original level.

EX: If the risk of a task with exposure to a vicious dog represents is reduced by a restraining system and that system fails, the risk presented by the dog is the same as it was before the system was installed.

The risk is currently acceptable based on the assumption that its reduction system is appropriate for the application and will contain the risk.

Adding the restraint did not change the hazard (dog), nor the task, only the risk which their combination represented.

That is why we have “Beware of Dog” signs on fences.
Reduce Risk

• Install the risk reduction measure(s)
• Validate the performance of the risk reduction measure(s)
  – Use a written validation plan
    • How to safely test the system
    • What tests/simulation shall be run
    • What are the specific expected results for each test
    • Look for systemic errors since they do not depend on a failure, only the occurrence of the trigger event
  – Document the results
Monitor

• **EFFECTIVE** Personnel training of the hazards and safe operating procedures
  – Employees are required by the ACT to adhere to employer safety procedures

• Assure that Safeguarding System is:
  – Used
  – Functional as intended
  – Maintained in safe operating condition
  – Monitored
  – Use lessons learned as result of the above
What is Functional Safety

• A function performed by a safety related part of the control system to:
  – Reduce the level of risk by;
    • Achieving or maintaining a safe state of the hazard
If nothing ever failed, safety circuit design requirements *could have been* met by any circuit which can eliminate the hazard

**BUT........**
HOPE is not a safety strategy!

Is that the Back-Bone of your Safety Program?

http://www.txt2pic.com
Backbone of Safety Circuit Design

• Eliminate/Reduce the hazard
• Manage the failures
  – Reduce by the probability of occurrence
  – Detect failure and execute a safe shut-down of the hazard
• The performance level of functional safety
  – Based upon two fundamental issues
    • How frequently do the components and sub-systems fail to danger
    • What is the Probability of Failure to Danger of the system
• Fluid power devices are included in the failure analysis
  – The safety related parts of the controls system do NOT end at the termination of the copper wire
ISO 13849 in Perspective

• It is a Consensus Standard
• Harmonized: If followed provides “Presumption of Conformity” to the EU Machinery Directive
• Only standard requirement in U.S. if claiming conformity to RIA15.06:2012 (ISO 10218-1,2:2011)
• Categories B through 4 have been generally accepted in Industry but from ISO 954-1:1996
• Some U.S. Corporations have adopted it internally
• Calculations can provide GENERAL GUIDANCE for increasing the reliability of the Functional Safety Risk Reduction Measure and rank competing designs
• Its most important feature for us here in the United States is the discipline of the process
What are

- **MTTF\textsubscript{D}** Mean Time to Dangerous Failure
  - Average value of operating time without a failure to danger for a component or channel
  - Typically given in years

- **PFH\textsubscript{D}** Probability of Failure to Danger per Hour
  - Statistical probability of Failure to Danger of a system or sub-system based on its:
    - Channel(s) MTTF\textsubscript{D}
    - Ability to detect failures to danger and to eliminate the hazard having sustained that fault
    - Robustness against Common Cause Failure
  - For Cat B and Cat 1 and single components it is
    - $\lambda\textsubscript{D} = 1/(\text{MTTF}_{\text{D}})$ if MTTF\textsubscript{D} is expressed in hours
  - Given in Failure/hour
The FOUR Legged Stool of ISO 13849-1,2:2015

- **Verification and Validation**
- **The Basis of Design of the Safety Function**
- **Risk Assessment**
- **The Underpinning**

**FUNCTIONAL SAFETY**

**RISK REDUCTION MEASURE**

**CAPABILITY**

- **Category**
- **Circuit structure**
- **MTTF\(_D\)**
  - Mean Time To Dangerous Failure
- **DC**
  - Diagnostic Coverage
- **CCF**
  - Common Cause Failure

Does it meet the design requirements?
Risk Reduction by Safety Function

• ISO 13849-1-2015 Safety Function based on
  – Circuit Categories also known as Structure
    • Must follow architecture in order to use method simplifications
  – Mean time to dangerous failure, $\text{MTTF}_D$, of components and sub-systems
  – Diagnostic Coverage DC
    • Percentage of all failures to danger which can be discovered for each component or sub-system
    • Not to be confused with IEC 62016 Safe Failure Fraction
    • $\text{DCavg}$
      – Statistical average of all DC in system, rationalized based on probability of failure of the component or sub-system
  – Common Cause Failure CCF
    • System design minimizes CCF by use of at least a minimum number of CCF reduction design techniques
Functional Safety

• What does a Functional Safety circuit look like?
• How can its functionality be shown?
• Safety-related Block Diagrams
  – Show the components of failure modes of the circuit
Each circuit has these three elements of either:
- Individual components
- Sub-systems which perform that function, with internal monitoring

A failure in any block in the series safety-related block diagram, can lead to the loss of the safety function
- To evaluate safety performance, each proposed SRP/CS must be broken into a block diagram of Series Safety Failure Events
- This includes the interconnection/communication between the blocks
Safety-Related Function Block Rules

• All items which can lead to the loss of safety are shown in “Series”

• Items which provide an alternate means of performing the safe shut down function when another component fails are show in “Parallel”

• Do not confuse the electrical or fluid power flow with the orientation of the safety function block
  – EX: A Safety Interface Module (SIM) used for Manual Suspension of a Door Interlock has its contacts in parallel with those of the Door Interlock SIM. BUT:
    – The safety function block shows them in a series failure flow since the failure of the Manual-Suspension SIM to drop out, leads to a failure to danger of the Door Interlock Safety Function, as it can no longer perform its safety function
Safety-Related Function Block Rules

• Three main function blocks of:
  – Input, logic, output

• Include communication between blocks
  – Hard wire
  – Network, wireless, fiber optics

• May be sub-systems or simple components

• Each device may have multiple failure measures, each represented by its own block
  – Contacts have dry (no load) and load sensitive failure rates
  – PLC may have separate modules external to the basic main frame
    • Input/output modules
      – Local or remote
    • Communication modules
The SRP/CS must be rationalized into one of five categories in order to use the ISO 13849-1 methodology and statistical simplifications.

What does the “Category’s” structure look like?
- Are evaluated on the basis of their safety-related block diagram.
Category B or 1

- Single fault leads to the loss of the safety function
- Cat 1 uses “Well Tried” higher MTTF\(_D\) components
• When a component fails it will lead to the loss of the safety function
• Only protection against system failure is the use of components which have a sufficiently low failure rate, a long time between failures
• If used in a low risk application, this failure rate may be acceptable
• To increase performance:
  • **Components** to utilize lower failure rate components and/or “safety rated” devices which are less likely than “standard” devices to fail to danger over the same period of use.
  • **Safety Principles** which reduce the probability of specific modes of failure to danger of the SRP/CS

*Adapted From B11.26*
Category 1

• Not Allowed
  – Single Electronic Devices
  – Standard Electronic Logic
  – Standard Software

• A standard (non-safety certified) PLC is not allowed on all three basis of exclusion

• Uses “Well Tried” components which:
  – Have proven themselves in safety applications
  – Are designed using accepted best practices
    • See ISO 13849-2:2012
  – Typically have a higher MTTF$_D$ than standard components
Category B or 1

- Solenoid coils are connected to the single channel control and performance of the valve function is not monitored directly.
Category 2

- Cat 2 = Single channel with monitoring
- Warn or shut down hazard
- Dashed monitoring lines represent reasonably practicable fault detection
Category 2

• The occurrence of a component fault will lead to the loss of the safety function
• Safety function is tested at suitable intervals
• When a failure is detected by the circuit it shall provide warning or shut down the hazard
• Loss of the monitoring function causes the circuit to behave like a Cat B or 1

Adapted From B11.26
For a directional valve directly controlling an operation, a monitoring function may be inferred if the operation is continuously ongoing.

May also be used on a spring centered valve, however, the failure of the spring to center the spool must be considered.

Adapted From B11.26
Category 3

- Cat 3 = Dual Channel
- Single fault will not cause the loss of the safety function
- w/ Conditional Monitoring (May not detect all failures)
- Multiple undetected faults may cause the loss of the safety function

ISO 13849-1-2006
• A single fault does not lead to the loss of the safety function
• Whenever reasonably practicable, the single fault shall be detected at or before the next demand on the safety function
• Some but not all of the failures are detected
• An accumulation of undetected faults may lead to the loss of the safety function

Adapted From B11.26
Category 3

- Three way dump/exhaust valve is monitored with directly operated limit switch in the EDM
- 5 Ported 3 Position valve is indirectly monitored by process observation
  - Failure of valve to spring center is excluded

Adapted From B11.26
Category 4

- **Cat 4 = Dual Channel**
- **w/ Complete Monitoring**
- **Faults will not cause the loss of the safety function**
- **Must detect first fault or continue to protect with this and the next fault, this combination must be detected**
Category 4

- Single fault does not lead to the loss of the safety function
- Where possible, all failures will be detected
- The undetected fault will not lead to the loss of the safety function with the occurrence of the next fault.
- The safety system will continue to function without loss of the safety function until the combination of accumulated faults is detected, and the hazard eliminated
  - Typically at the detection of the second fault
Two three way dump/exhaust valves each are monitored by direct operating limit switches.

Limit switches are monitored in the EDM portion of the SRP/CS.
Category 4

- Dual solenoid dual spool Safety Rated blocking valve
  - Internal “logic” which monitors pressures and prevents one spool from shifting to pass fluid to the output port if the other spool has failed to block
  - Pressure switch transfers due to internal pressure at fault
    - Not part of the safety critical function

Adapted From B11.26
Safety-Related Block Diagram

• Proposed Safety Function circuit must be reduced to block diagram to identify category

• Necessary to correctly identify the failure contributions to the components and sub-systems

• Will confirm the category of the circuit as first part of the verification process
Devices may be simple or complex sub-systems, each with its own individual S, L, and O functions.

Adapted From Fig 6.13  BGIA Report 2-2008e
Fluid Power Example

Note: Suggested for horizontal cylinder, without a pilot check valve at the cylinder lower port, will drop in vertical applications

Adapted From B11.26
Safety-Related Block Diagram

- Direct acting Limit switches have both a mechanical (dry) and an electrical (load) B10 failure mode data
- K1 is a Category 4 PLe Safety Interface Module
- V1 and V2 are Pneumatic Valves built to ISO 13849-1 Annex C clause C.4.1 and
- Applied per ISO 13849-2 Annex B Tables B.1, through B.13
Figure 8.28: Detection zone monitoring by laser scanner with electro-hydraulic deactivation of the hazardous movement.
Applying Safety-Related Block Diagram

- To correctly represent the failure behavior of the SRP/CS in a safety-related block diagram, the circuit has to be correctly analyzed.
Dual Channel Pneumatic Circuit?

Adapted From B11.26
Safety-Related Block Diagram

- This is not a dual channel system
  - Cylinder up or down under power is dependent on V1 only
- For the check valve V2 to block down drift, V1 must have shifted to the spring centered position, venting the pilot stage of the check
  - Showing ONLY fluid power, add control blocks
Dual Channel Hydraulic Circuit?
Safety-Related Block Diagram

Safety performance requires that the block diagram is carefully constructed and analyzed

- Showing ONLY fluid power, add control blocks
- With A, B center to Tank would be single channel on Drift
Channels Defined by SBD

With a correct Safety-related Block Diagram for each Functional Safety requirement

- Identify the components’ failure metrics for each channel
  - Mean time to dangerous failure $MTTF_D$ for components
    - Limit switches, contactors, valves
  - $PFH_D$ for sub-systems
    - Safety Light Curtains, Safety Interface Modules, VFD Safe Stop controllers

- For channel $MTTF_D$ components
  - Determine DC of each component
  - Verify minimum design requirements for Common Cause Failure Annex F Table F.1
  - Develop the equivalent single channel $MTTF_D$ and $DC_{avg}$
  - With the data above, use Annex K Table K.1 to determine $PFH_D$ of the symmetrized channel
  - If system also contains $PFH_D$ sub-components their value is added to the channel to gain a total system $PFH_D$
Example

- Symmetrized MTTF$_D$ of valve dual channel single valve 150 to 100 = 88 yr.
- DC of both 1V3 and 1V4 is 99% via 1S3
- DC of 1V5 by process monitoring is 60%
- DC$_{avg}$ is calculated to be 86%, <90% therefore low
- Valve channel is Cat 3 DC$_{avg}$ Low
- CCF score from table F.1 >65
- From table K.1 closest lower values of 82 yr. and low DC$_{avg}$ (60%) hydraulic system PFHD s 1.14E-7
  - This is conservative due round down, actual calculations using SISTEMA would yield a value of 6.2E-8
- Resultant system performance is sum of the three PFH$_D$ Conservative 5.6E-7 PLd or calculated 5.1E-7 PLd
Software Requirements

We typically emphasize hardware failure concerns sometimes to the detriment of solid, well organized, and documented control

- Control design errors may lead to the loss of the safety function without the occurrence of a component failure
- Requires only the occurrence of the event leading to the error

Figure 6 ISO 13849-1:2015
Failure to Meet PLr

- The use of Table K.1 gives conservative values due to the graininess of the table
- Use a PL calculation program such as SISTEMA to fine tune the calculation
- As a first shot at increasing PFH$_D$
  - Look for the lowest MTTF$_D$ in the lowest MTTF$_D$ channel
    - Change component or loading
    - Reduce number of cycles per year
  - Increase DC for lowest MTTF$_D$ component
  - Exclude faults through application of safe design principles
    - See Annex A through D of ISO 13849-2:2012
    - Provide documentation
  - Change Category to a higher level
Heinz Knackstedt  
Safety Engineer  
TÜV Functional Safety Engineer  
C&E sales, inc.  
Dayton, Ohio USA  

Office: +1 (937) 434-8830  
Cell: +1 (937) 545-6494  

hknackstedt@cesales.com