Arrow Industrial Solutions, LLC

8651 Freedom Road
Windham, OH 44288
1-877-444-8711
arrowsolutions.net
info@arrowsolutions.net

Machine safeguarding / Control Reliability

ASSP

Mark Stewart
mark@arrowsolutions.net
Cell: 330-730-4805
January 23, 2020

Don't Let Your Guard Down
'Safe Solutions by Design'

Machine Safeguarding
What is required?

The employer is required to provide " . . . employment and a place of employment which are free from recognized hazards that are causing or are likely to cause death or serious physical harm to his employees."
OSHAct 5(a)(1)

OSHA Part 1910, Subpart O - Machinery and Machine Guarding

The operator and other employees in the machine area must be protected (*29CFR1910.212(a)(1)* from hazards such as those created by:

Point of operation

In-running nip points

Rotating parts

Flying chips

Sparks

In general, anything that moves and can hurt an employee must be guarded!

P.O. Box 195, 8651 Freedom Road
Windham, OH 44288
1-877-444-8711
arrowsolutions.net
info@arrowsolutions.net

Control Reliability - Definition

Control reliability is the capability or portion of the machine control system that prevents exposing an Employee to a hazardous condition.

More specifically, control reliability is machine safeguarding, utilizing safety rated control components and related interfacing to achieve a safe state even in the event of a fault within their safety related functions.

P.O. Box 195, 8651 Freedom Road
Windham, OH 44288
1-877-444-8711
arrowsolutions.net
info@arrowsolutions.net

Machine Guarding – Control Reliability

- Control Reliability involves the integrated state of the Mechanical guarding and device interlocking / integrating, as determined by the Risk Assessment.
- Machine Safeguarding Evaluation / Design Phases:
  - Risk Assessment
  - Evaluate Access – Production, Maintenance, Set-up
  - Mechanical Guarding – Design
  - Control Reliability - Design
    - Device Selection
    - Category
  - Integration Methods
  - Verification

P.O. Box 195, 8651 Freedom Road
Windham, OH 44288
1-877-444-8711
arrowsolutions.net
info@arrowsolutions.net

Machine Safeguarding – System

Risk Assessment

Mechanical Guarding	Electrical Interlocking	Methods / Integration
PHYSICAL BARRIER	**CONTROL INTERLOCKS**	**FAILS SAFE CONDITION**
Barrier to the Hazard	Devices, Access, Distance	Risk Assessment helps to identify Category
Non-removable without specific tool	Shutdown – Reset to restart	Safety Rated Controller / Devices
Opening vs. Distance	Evaluate machine coast to stop for device distance / method	Redundant Input – Fault Checking
Mechanical Guarding alone is not Functionally Safe	Hazard isolated with safety rated output device – Motor, air, hydraulic	Output device switching verification

P.O. Box 195, 8651 Freedom Road
Windham, OH 44288
1-877-444-8711
arrowsolutions.net
info@arrowsolutions.net

Control Reliability

- If there is only one aspect of machine guarding to be implemented, it would have to be **Control Reliability**.
- Many safety-related control systems do not have this vital aspect.
- If a hazardous machine does not have Control Reliability and an accident occurs, you are subject to fines, lawsuits, and increased insurance costs.
- Often times, employers and OEM's:
  - Are unaware of the necessity
  - Have mistakenly used an improper design
  - Used the wrong components.

- OSHA doesn't really address Control Reliability except in relation to mechanical power presses.
- ANSI addresses Control Reliability in most types of machines based on Risk Assessment.

P.O. Box 195, 8651 Freedom Road
Windham, OH 44288
1-877-444-8711
arrowsolutions.net
info@arrowsolutions.net

Machine Safeguarding Regulations

P.O. Box 195, 8651 Freedom Road
Windham, OH 44288
1-877-444-8711
arrowsolutions.net
info@arrowsolutions.net

Primary Regulating Standards:

OSHA 29 CFR 1910, Subpart O – Machinery and Machine Guarding

ANSI B11.19 – Performance Standards for Safeguarding - Control Reliability

ISO 13849 – Safety of Machinery

NFPA 79 – Electrical Standard for Industrial Machinery

EN 954-1 – Safety Related Control Standards

ANSI B11.0-2010 –Safety of Machinery –General Requirements and Risk Assessment

P.O. Box 195, 8651 Freedom Road
Windham, OH 44288
1-877-444-8711
arrowsolutions.net
info@arrowsolutions.net

Machine Safeguarding - Minimum General Requirements

- **Prevent contact**
  - The safeguard must prevent hands, arms or any other part of a worker's body from making contact with dangerous moving parts - “over, under, around or through”.
- **Be secure**
  - Workers should not be able to easily remove or tamper with the safeguard.
  - Guards and safety devices should be made of durable material that will withstand the conditions of normal use and be firmly secured to the machine or elsewhere if attachment to the machine is not possible.
- **Protect from flying objects**
  - The safeguard should ensure that no projectiles or allow objects to fall into moving parts.
- **Create no new hazards**
  - A safeguard defeats its own purpose if it creates a hazard of its own such as a shear point, a jagged edge, or an unfinished surface.

P.O. Box 195, 8651 Freedom Road
Windham, OH 44288
1-877-444-8711
arrowsolutions.net
info@arrowsolutions.net

Safeguarding Considerations

- **Safeguarding Design:**
  - Guarding closer to the Process – Typically, Higher Capital Cost & Productivity
  - Fence Approach – Generally, Lower Capex and reduced productivity
- **Create no interference - Perception**
  - Any safeguard which impedes a worker from performing the job quickly and comfortably might soon be bypassed or disregarded.
  - Proper safeguarding can actually enhance efficiency since it can relieve a worker's apprehensions about injury.
- **Allow safe Maintenance / Interfacing the Process**
  - If possible, one should be able to lubricate the machine without removing the safeguard.
  - Machine can not be started while performing maintenance or clearing a jam.

- Unless all guards are bolted and secured, requiring a specific tool to remove, Control Reliability must be deployed.
  - Reality – Will they be properly reinstalled after being removed for maintenance?

P.O. Box 195, 8651 Freedom Road
Windham, OH 44288
1-877-444-8711
arrowsolutions.net
info@arrowsolutions.net

What are the options?

- **Guards**
  - Mechanical barrier or covers that separate the Employee from the hazard.
- **Devices**
  - Sensing devices or controls that force the Employee to operate the machine in a safe manner or senses Employees location / proximity to the hazard and shutdown the process in time to protect.
- **Location**
  - Hazard is far enough from Employees that they can not be harmed from projectiles from the process
  - Distance of presence devices or access gates from hazards is critical to ensure Employee can not reach hazard in a coast-to-stop situation.
- **Combination**
  - Various above methods can be deployed in unison on a particular machine / process to ensure safety.

P.O. Box 195, 8651 Freedom Road
Windham, OH 44288
1-877-444-8711
arrowsolutions.net
info@arrowsolutions.net

Risk Assessment – Safeguarding Overview

P.O. Box 195, 8651 Freedom Road
Windham, OH 44288
1-877-444-8711
arrowsolutions.net
info@arrowsolutions.net

Risk Assessment Concepts – Machine Guarding

- The risk assessment process includes identifying hazards regardless of the existence of risk reduction (safeguarding) measures.
- The machine should not be considered harmless as shipped and guarded.
- To assure that all hazards are included, hazard identification should be conducted with all safeguards conceptually removed.
  - **This is to assure that hazards are not ignored due to an assumption that the safeguard supplied is adequate for all tasks, including reasonably foreseeable misuse.**
- Existing safeguards that help meet the risk reduction objectives can be retained after evaluating their performance.
  - **This decision will be confirmed during the validation / verification part of the risk assessment.**

P.O. Box 195, 8651 Freedom Road
Windham, OH 44288
1-877-444-8711
arrowsolutions.net
info@arrowsolutions.net

ANSI B11.TR3

Risk is the "combination of the likely **severity of harm** and the **probability of occurrence** of that harm"

- Severity of harm: The degree of injury or illness that could occur.
  - Catastrophic – death or permanently disabling injury / illness (unable to return to work)
  - Serious – severe debilitating injury or illness (able to return to work at some point)
  - Moderate – significant injury /illness requiring more than first aid (able to return to same job)
  - Minor – no injury or slight injury requiring no more than first aid (little or no lost work time)
- Probability of occurrence: Accounts for the frequency, duration and extent of exposure, including training and awareness.
  - Very likely – near certain to occur
  - Likely – may occur
  - Unlikely – not likely to occur
  - Remote – so unlikely as to be near zero

When determining risk, the worst credible severity of harm is selected.
When estimating probability, select the highest credible level of probability.

P.O. Box 195, 8651 Freedom Road
Windham, OH 44288
1-877-444-8711
arrowsolutions.net
info@arrowsolutions.net

The Risk Assessment is primary in determining the Control Reliability Category and Methods of Design

- Ex. Gate access must be limited until zero-motion determined if a “coast to stop” situation

It is important that the entire system be considered:

- Devices (interlock switches, light curtains, etc.)
- Hardware (gates, posts, etc.)
- Control system (safety rated controller / PLC, force guided relays)
- Wiring (conduit, etc.)
- Methods
- Category – Redundancy
- Installation Methods

P.O. Box 195, 8651 Freedom Road
Windham, OH 44288
1-877-444-8711
arrowsolutions.net
info@arrowsolutions.net

Control Reliability

P.O. Box 195, 8651 Freedom Road
Windham, OH 44288
1-877-444-8711
arrowsolutions.net
info@arrowsolutions.net

Control Reliability - Origin

Control Reliability Categories

–First published in EN 954-1 1996

–Gave us a means of describing the fault tolerance of circuits

–Did NOT give us a way to relate the degree of risk to the fault tolerance requirements (more on this later!)

P.O. Box 195, 8651 Freedom Road
Windham, OH 44288
1-877-444-8711
arrowsolutions.net
info@arrowsolutions.net

Some of the basics include:

- No single device or wiring fault can cause an unsafe condition.
- Control Reliability cannot be ensured using traditional PLC's. Safety rated controllers and devices must be integrated.
- Generate a stop and maintain a safe state if a fault is detected.
- Design must consider common mode faults if probability is significant.
  - Devices and control systems need to be designed to fail in the safe condition.
- Devices must be designed and installed to avoid the ability to by-pass their operation.

P.O. Box 195, 8651 Freedom Road
Windham, OH 44288
1-877-444-8711
arrowsolutions.net
info@arrowsolutions.net

Some of the basics include:

- Faults should be detected as they occur or at the next demand on the safety system Independent of the process control system and not easily bypassed.
  - Circuit redundancy is required to avoid a single point failure causing an unsafe condition.
    - Input safety devices (E-stops, gate switches, light curtains, scanners, etc…)
    - Output controls (motor starters, hydraulic / pneumatic solenoids, etc…)
  - Monitoring of the dual inputs compensates for shorts, broken wires or failed devices.
- Safety Devices must comply with standards to ensure adequate diagnostic coverage, component failure rates, avoidance of common cause failures and meeting the maximum performance levels.

P.O. Box 195, 8651 Freedom Road
Windham, OH 44288
1-877-444-8711
arrowsolutions.net
info@arrowsolutions.net

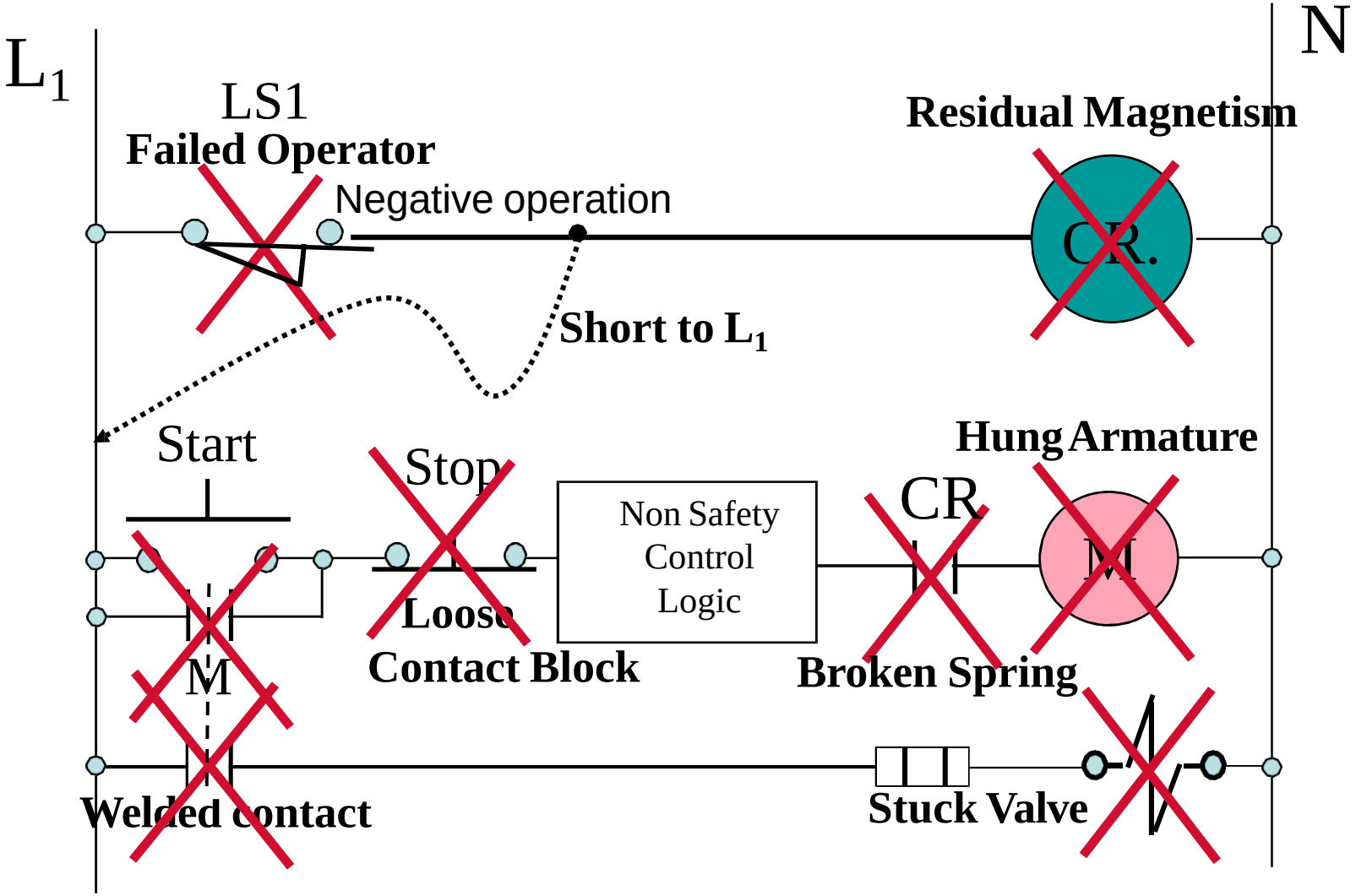
Category Level - Determination

- The necessary category depends upon the risk assessment (Likelihood / Consequences), the nature of the process and complexity of the device or control system.
- **The higher the category, does not always mean it provides the best protection.**
    - Cat 3 safety circuit is not necessarily “safer” than a Cat 2
        - Depends on application and components used.
        - Function may be compromised by control system construction and environmental conditions
- **The categories provide a description of the functional performance of the entire safety system including the methods and devices incorporated.**

P.O. Box 195, 8651 Freedom Road
Windham, OH 44288
1-877-444-8711
arrowsolutions.net
info@arrowsolutions.net

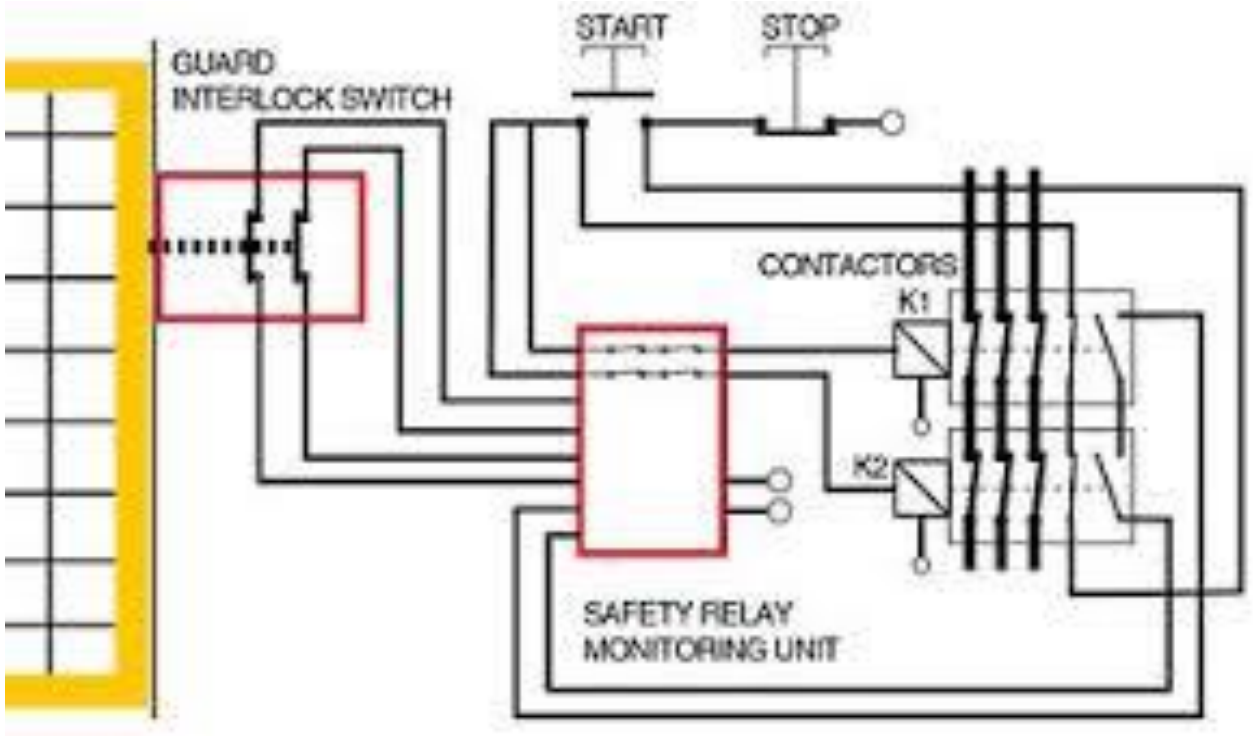
What if the relay contact fails to OPEN OR OR OR OR

Hazard is not eliminated



P.O. Box 195, 8651 Freedom Road
Windham. OH 44288
1-877-444-8711
arrowsolutions.net
info@arrowsolutions.net

Example of Control Reliable Circuit



P.O. Box 195, 8651 Freedom Road
Windham, OH 44288
1-877-444-8711
arrowsolutions.net
info@arrowsolutions.net

Control Reliability Categories

P.O. Box 195, 8651 Freedom Road
Windham, OH 44288
1-877-444-8711
arrowsolutions.net
info@arrowsolutions.net

EN / ISO – Safety of Machinery

CATEGORY B:

- Safety related parts of a machine control systems and/or their protective equipment, as well as their components, shall be designed, constructed, selected, assembled and combined in accordance with relevant standards so that they can withstand the expected influence.
- **When a fault occurs, it can lead to a loss of the safety function.**
- Category B in itself has no special measures for safety but it forms the base for other categories.

- Category 1-4 defines general requirements.
- ANSI has similar categories.

P.O. Box 195, 8651 Freedom Road
Windham, OH 44288
1-877-444-8711
arrowsolutions.net
info@arrowsolutions.net

EN / ISO – Safety of Machinery

CATEGORY 1:

- Includes the requirements under Category B along with the use of well-tried safety components and safety principles.
- This Category has a higher safety reliability of the safety related function. The higher the reliability of the device, the less the likelihood of a fault.
- **Primary increase Control Reliability through the selection of components**, moving closer towards the prevention of faults

P.O. Box 195, 8651 Freedom Road
Windham, OH 44288
1-877-444-8711
arrowsolutions.net
info@arrowsolutions.net

EN / ISO – Safety of Machinery

CATEGORY 2:

- Includes the requirements under Category B along with the use of well-tried safety components and safety principles.
- In addition, the safety function(s) shall be checked at machine start-up and periodically by the machine control system. **If a fault is detected, a safe state shall be initiated or if this is not possible a warning shall be given.**
- The loss of a safety function is detected by the check. The occurrence of a unknown fault can lead to the loss of safety function between the checking intervals.
- Primary increases Control Reliability through the selection of components, moving closer towards the prevention of faults by the structure of the safety control system.

P.O. Box 195, 8651 Freedom Road
Windham, OH 44288
1-877-444-8711
arrowsolutions.net
info@arrowsolutions.net

EN / ISO – Safety of Machinery

CATEGORY 3:

- Includes the requirements under Category B along with the use of well-tried safety components and safety principles.
- **The system shall be designed so that a single fault in any of its parts does not lead to the loss of a safety function.**
- When the single fault occurs, the safety function is always performed. Some but not all faults will be detected. **An accumulation of undetected faults can lead to the loss of safety function**
- Primary increases Control Reliability through both the selection of components and the prevention of faults by the structure of the safety control system.

P.O. Box 195, 8651 Freedom Road
Windham, OH 44288
1-877-444-8711
arrowsolutions.net
info@arrowsolutions.net

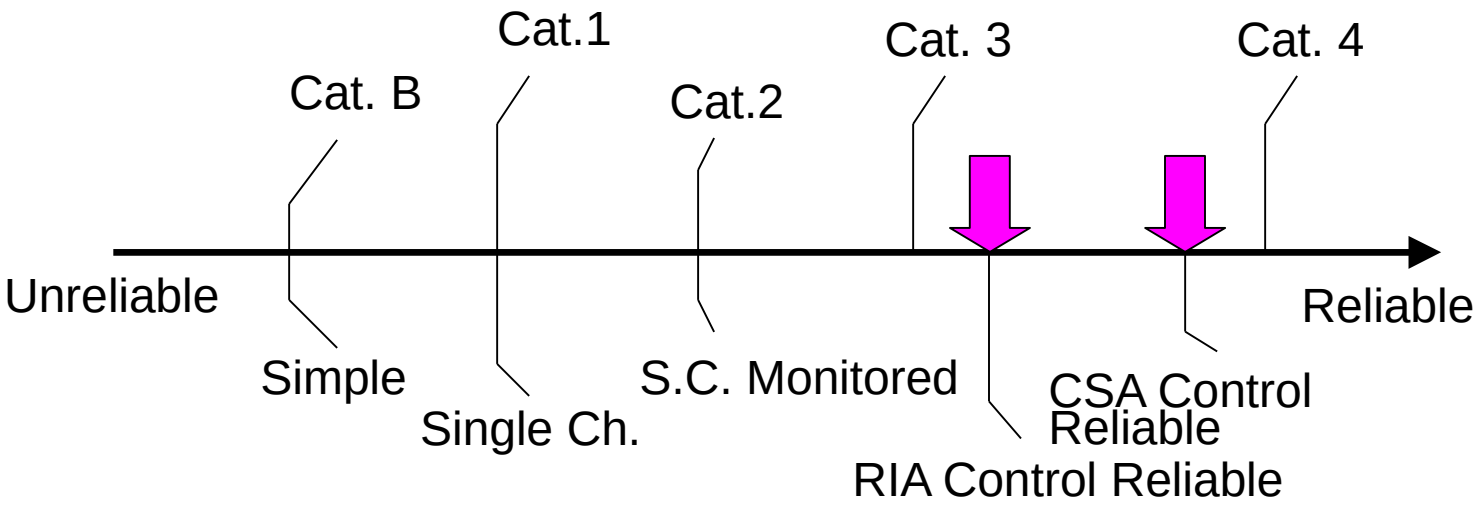
EN / ISO – Safety of Machinery

CATEGORY 4:

- Includes the requirements under Category B along with the use of well-tried safety components and safety principles.
- **The system shall be designed so that a single fault in any of its parts does not lead to the loss of safety function.** The single fault is detected at or before the next demand on the safety function. If this detection is not possible then an **accumulation of faults shall not lead to a loss of safety function.**
- **When the faults occur, the safety function is always performed.** The faults will be detected in time to prevent the loss of safety functions.
- Primary increases Control Reliability through both the selection of components and the prevention and prediction of faults by the structure of the safety control system.

P.O. Box 195, 8651 Freedom Road
Windham, OH 44288
1-877-444-8711
arrowsolutions.net
info@arrowsolutions.net

Control Reliability – ISO Categories



NOTE: There is no intent to imply direct equivalence between the ISO categories and the ANSI/CSA performance criteria (but they are similar!).

RIA – Robotics Industries Association
CSA – CSA Group – Certification

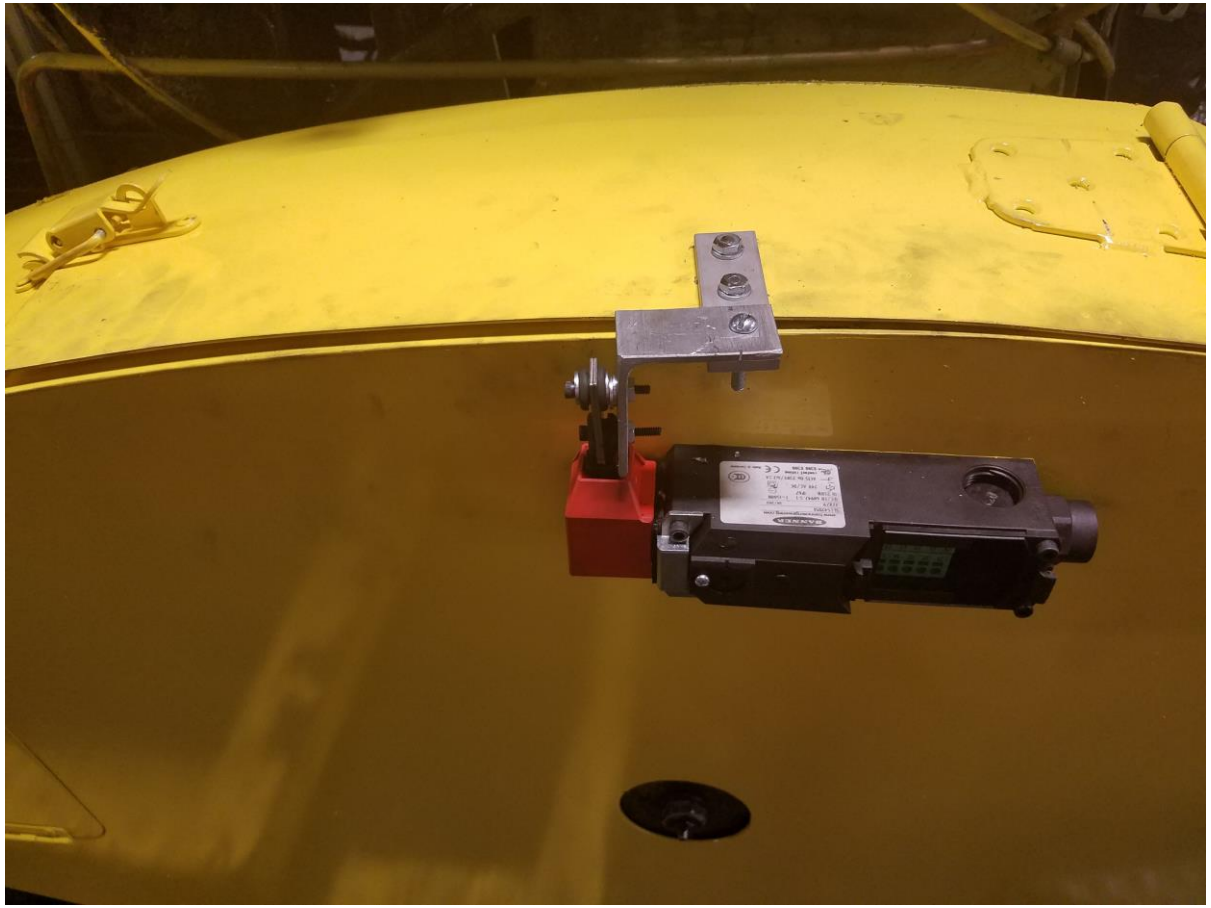
P.O. Box 195, 8651 Freedom Road
Windham, OH 44288
1-877-444-8711
arrowsolutions.net
info@arrowsolutions.net

Examples:

P.O. Box 195, 8651 Freedom Road
Windham, OH 44288
1-877-444-8711
arrowsolutions.net
info@arrowsolutions.net

Example of Access Gate Locking Solenoids with/without Passkey
Used in coast to stop processes, sensing zero-motion required.

Flywheel Guard Interlocked to Machine Safety Circuit
Example 1:



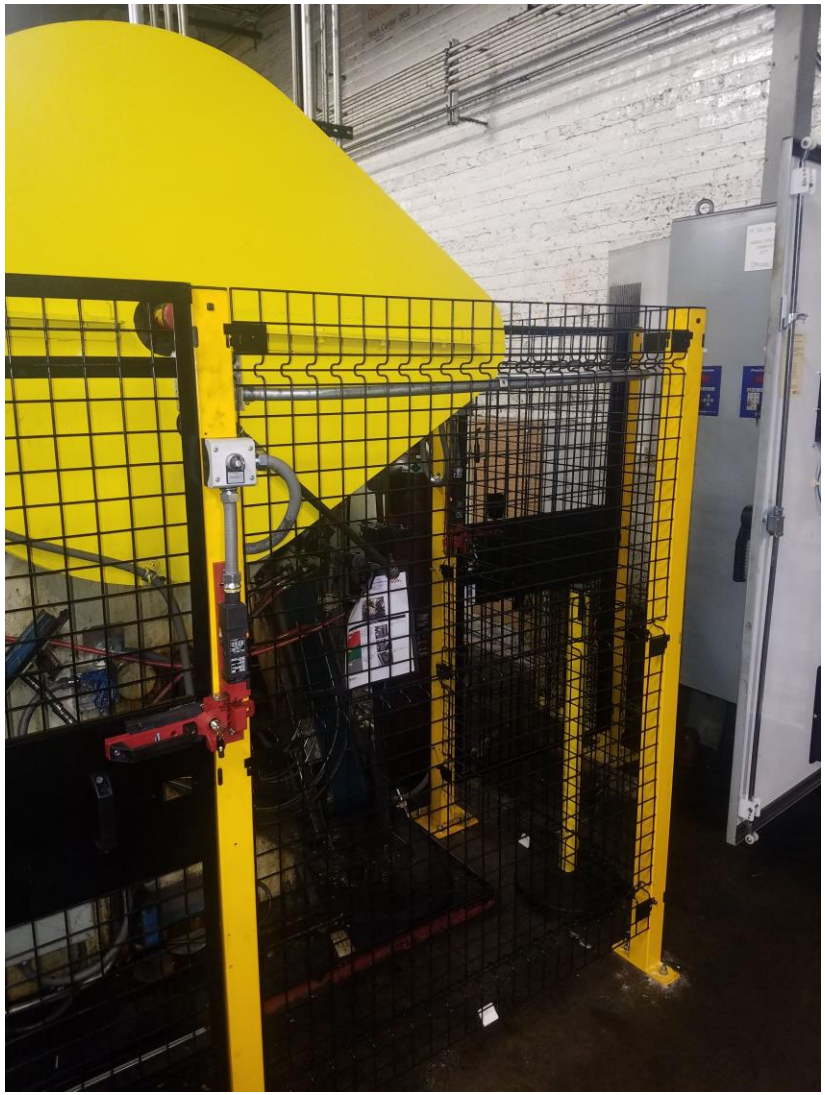
1). Sensed Zero-motion before allowing access.

2). Requires guard replacement And reset before restarting machine.

3). Category 3 – Redundancy of Inputs, with diagnostic checking.

4). Direct guard mount, allowing Operator access around machine.

Flywheel Guard Interlocked to Machine Safety Circuit
Example 2:



1). Sensed Zero-motion before allowing access.

2). Requires guard replacement
And reset before restarting machine.

3). Category 3 – Redundancy of Inputs, with diagnostic checking.

4). Safety Fence further from the process.

- **Same safety features**
- **Simpler installation**
- **Reduced productivity to interact with process.**

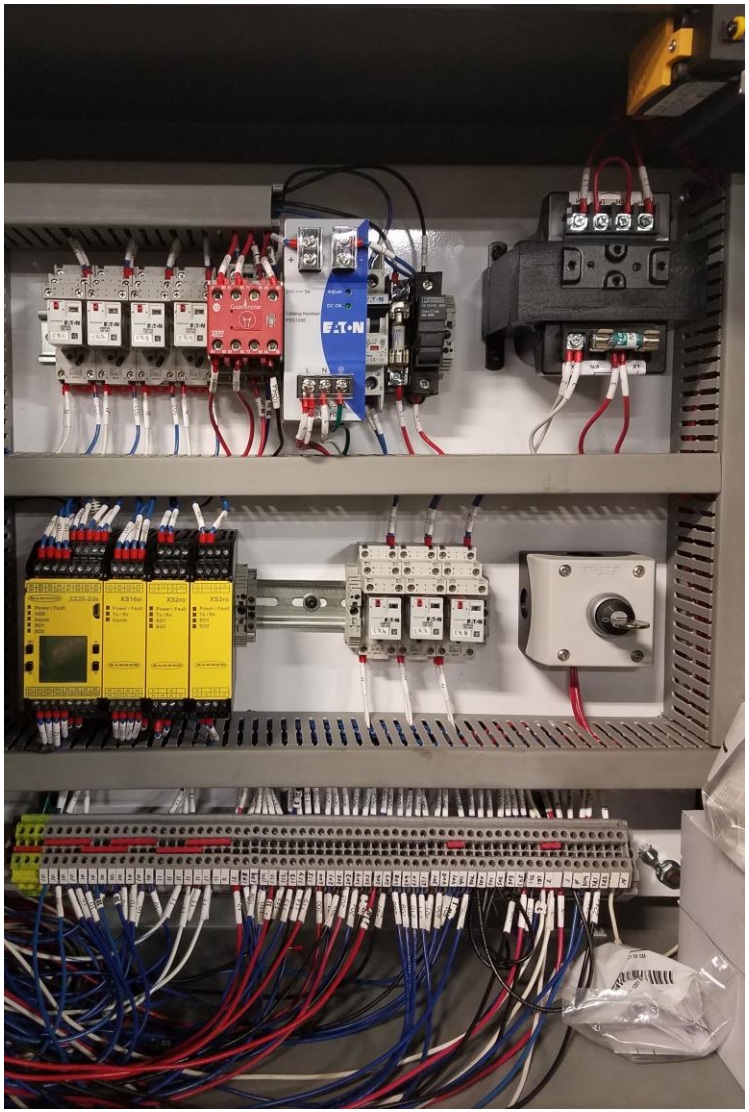
Example of:

1). Effective Guard allowing direct safe access to the process.

2). Solenoid locked, allowing Guard to be open only once “zero” motions verified.

3. Met Category 3, safety rated devices with dual inputs, zero-motion detection and appropriate Safety Controller.

Category 3 Retrofit of existing Stamping Machine



1). Safety Controller

2). Force Guided Safety Rated Control Relays

3). Category 3 – Redundancy of Inputs, with diagnostic checking.

4). 24V system – Fails to Safe Condition

5). Existing Machine Control not affected

P.O. Box 195, 8651 Freedom Road
Windham, OH 44288
1-877-444-8711
arrowsolutions.net
info@arrowsolutions.net

Evaluating Components/Devices and System Risk

P.O. Box 195, 8651 Freedom Road
Windham, OH 44288
1-877-444-8711
arrowsolutions.net
info@arrowsolutions.net

Safety Design is a matter of managing the failures What are the options?

- Have such a low risk that failure of the risk reduction circuit to failure is acceptable
- Use Extremely large failure interval components so that failure is not a concern for the intended mission life
  - Impossible to accomplish over any reasonable length of use
- Manage the failures so that they do not cause the loss of the safety function
  - Assure that the safety function continues to eliminate the hazard with one failure
  - Detect that failure and shut down the hazard
  - Prevent further operation until the failure has been repaired

Arrow Industrial Solutions, LLC

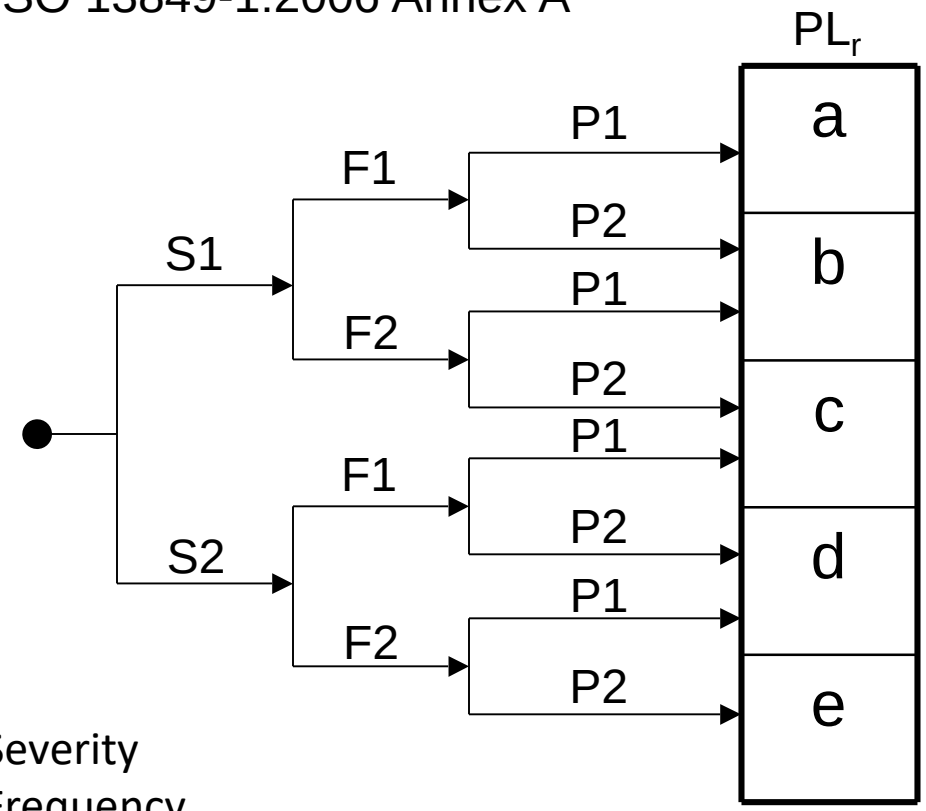
How do you make the link between risk and reliability?

- The Second Edition of ISO 13849-1:
  - Keeps the existing Category structure
  - Adds:
    - Performance Levels (PL)
    - Diagnostic Coverage (DC)
    - Common Cause Failures (CCF)

P.O. Box 195, 8651 Freedom Road
Windham, OH 44288
1-877-444-8711
arrowsolutions.net
info@arrowsolutions.net

Revised Risk Graph

ISO 13849-1:2006 Annex A



Low contribution to Risk Reduction

S1 - Slight Injury
S2 - Serious Injury
F1 - Seldom or Short
F2 - Frequent or Long
P1 - Avoidable
P2 - Unavoidable

High contribution to Risk Reduction

S – Severity
F – Frequency
P - Probability

P.O. Box 195, 8651 Freedom Road
Windham, OH 44288
1-877-444-8711
arrowsolutions.net
info@arrowsolutions.net

Performance Levels

- A number of factors contribute to PL:
  - $MTTF_d$, Mean time to dangerous failure
  - DC, Diagnostic Coverage
  - CCF, Common Cause Failures
  - Structure or architecture
  - Software
  - Systematic failures
  - More than can be covered in this presentation!

P.O. Box 195, 8651 Freedom Road
Windham, OH 44288
1-877-444-8711
arrowsolutions.net
info@arrowsolutions.net

$MTTF_d$

The time that will elapse until 63% components fail.

Calculated based on B_{10d}

B_{10d} = Mean cycles until 10% of components fail (should be on the datasheet)

Table 5 — Mean time to dangerous failure of each channel ($MTTF_d$)

$MTTF_d$	
Denotation of each channel	**Range of each channel**
Low	3 years $\leqslant$ $MTTF_d$ < 10 years
Medium	10 years $\leqslant$ $MTTF_d$ < 30 years
High	30 years $\leqslant$ $MTTF_d$ $\leqslant$ 100 years

NOTE 1 The choice of the $MTTF_d$ ranges of each channel is based on failure rates found in the field as state-of-the-art, forming a kind of logarithmic scale fitting to the logarithmic PL scale. An $MTTF_d$ value of each channel less than three years is not expected to be found for real SRP/CS since this would mean that after one year about 30 % of all systems on the market will fail and will need to be replaced. An $MTTF_d$ value of each channel greater than 100 years is not acceptable because SRP/CS for high risks should not depend on the reliability of components alone. To reinforce the SRP/CS against systematic and random failure, additional means such as redundancy and testing should be required. To be practicable, the number of ranges was restricted to three. The limitation of $MTTF_d$ of each channel values to a maximum of 100 years refers to the single channel of the SRP/CS which carries out the safety function. Higher $MTTF_d$ values can be used for single components (see Table D.1).

NOTE 2 The indicated borders of this table are assumed within an accuracy of 5 %.

P.O. Box 195, 8651 Freedom Road
Windham, OH 44288
1-877-444-8711
arrowsolutions.net
info@arrowsolutions.net

Diagnostic Coverage

DC describes the ability of the system to self-test and detect failures.

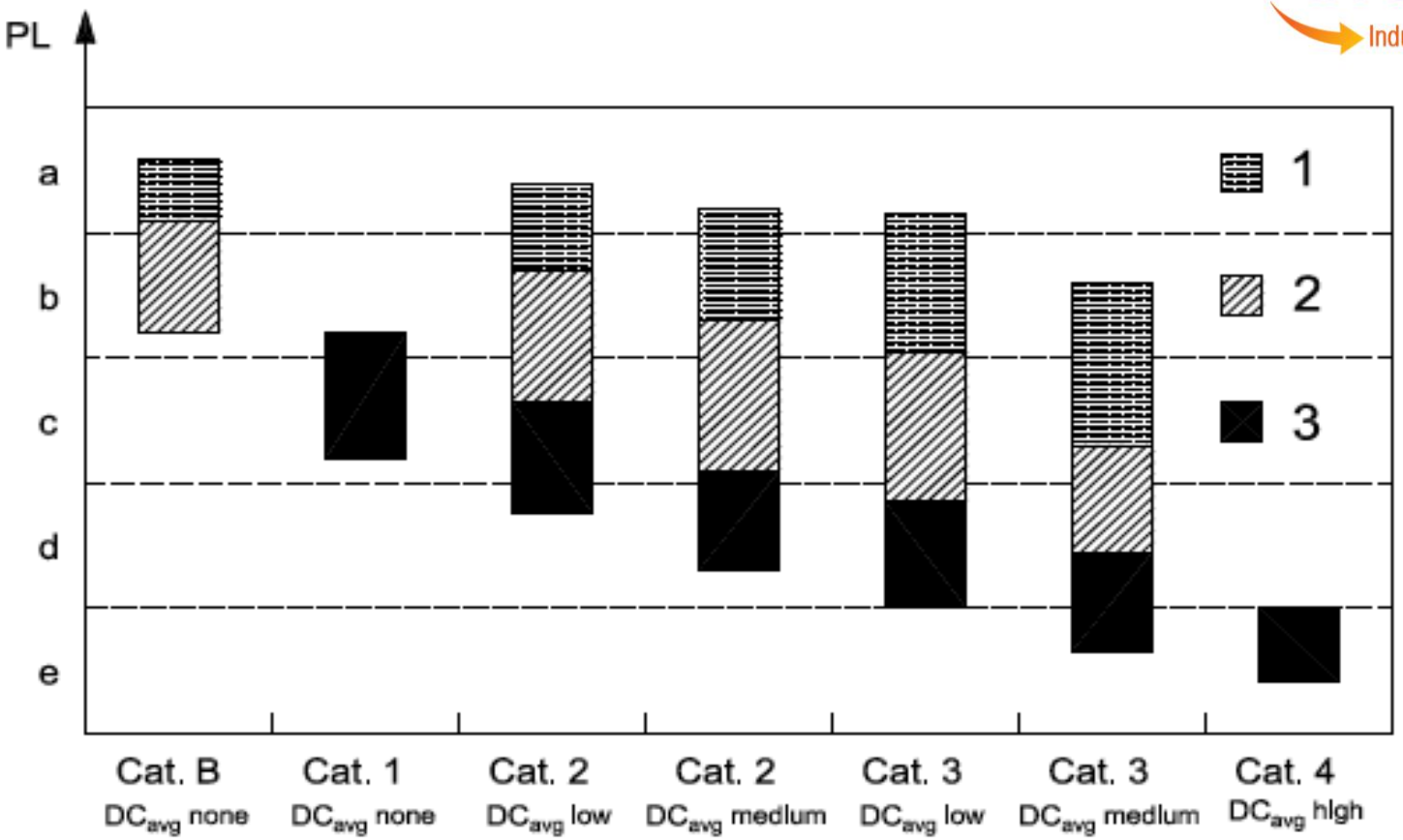
Table 6 — Diagnostic coverage (DC)

Denotation	DC Range
None	DC < 60 %
Low	60 % ⩽ DC < 90 %
Medium	90 % ⩽ DC < 99 %
High	99 % ⩽ DC

NOTE 1 For SRP/CS consisting of several parts an average value DC_{avg} for DC is used in Figure 5, Clause 6 and E.2.

NOTE 2 The choice of the DC ranges is based on the key values 60 %, 90 % and 99 % also established in other standards (e.g. IEC 61508) dealing with diagnostic coverage of tests. Investigations show that (1 - DC) rather than DC itself is a characteristic measure for the effectiveness of the test. (1 - DC) for the key values 60 %, 90 % and 99 % forms a kind of logarithmic scale fitting to the logarithmic PL-scale. A DC-value less than 60 % has only slight effect on the reliability of the tested system and is therefore called "none". A DC-value greater than 99 % for complex systems is very hard to achieve. To be practicable, the number of ranges was restricted to four. The indicated borders of this table are assumed within an accuracy of 5 %.

P.O. Box 195, 8651 Freedom Road
Windham, OH 44288
1-877-444-8711
arrowsolutions.net
info@arrowsolutions.net



Key

PL performance level

1 $MTTF_d$ of each channel = low

2 $MTTF_d$ of each channel = medium

3 $MTTF_d$ of each channel = high

Figure 5 — Relationship between categories, DC_{avg}, $MTTF_d$ of each channel and PL

P.O. Box 195, 8651 Freedom Road
Windham, OH 44288
1-877-444-8711
arrowsolutions.net
info@arrowsolutions.net

In Summary

- Control Reliability is the core requirement for successful Machine Safeguarding.
- It is a complex comprehensive system involving the:
  - Machine Guarding
  - Component/Control Reliability
  - Identification and elimination of Faults
- It starts with a Risk Assessment determining Tolerable Risk, thereby identifying the appropriate Control Reliability Category.
  - Involves Performance Level (PL) by evaluating the nature of the Safety Risks:
    - S – Severity of a Potential Injury
    - P – Probability of a Potential Injury
    - F – Frequency of a Potential Injury
- Requires the proper device selection, control and integration to ensure a reliable safe condition.

P.O. Box 195, 8651 Freedom Road
Windham, OH 44288
1-877-444-8711
arrowsolutions.net
info@arrowsolutions.net

Arrow Industrial Solutions, LLC

Machine safeguarding / Control Reliability

QUESTIONS?

Mark Stewart
January 23, 2020
mark@arrowsolutions.net
Ph: 330-730-4805

Don't Let Your Guard Down
'Safe Solutions by Design'