Doug Nix, A.Sc.T.
Compliance InSight Consulting Inc.

New Thinking in Control Reliability

Or “Your Next Big Headache”

Product Safety Engineering Society

www.machinerysafety101.com
(519) 729-5704

Control Reliability

- ‘Burning Questions’ from the group?
- What is Control Reliability?
- How has it been described?
- What’s new?

Standards

ISO 13849
Non-Programmable
Controls

IEC 62061
Programmable
Electronic
Systems

PSES
Product Safety Engineering Society

Familiar Territory

- 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!)

Familiar Territory

- B – No special measures. Components suitable for the application and specified based on the design requirements (voltage, current, etc.).
- 1 – Cat B + Well-tried safety principles and well-tried components.
- 2 – Cat B + Well-tried safety principles + Automatic checks at suitable intervals

What does 'Well Tried' mean???

Well Tried?

A “well-tried component” for a safety-related application is a component which has been either

a) widely used in the past with successful results in similar applications, or

b) made and verified using principles which demonstrate its suitability and reliability for safety-related applications.

Newly developed components and safety principles may be considered as equivalent to “well-tried” if they fulfill the conditions of b).

The decision to accept a particular component as being “well-tried” depends on the application.

NOTE 1 Complex electronic components (e.g. PLC, microprocessor, application-specific integrated circuit) cannot be considered as equivalent to “well tried”.

Familiar Territory

- Cat 3

  Category B PLUS

  + Well-tried safety principles
  + No single fault can lead to the loss of the safety function
  + Whenever reasonably practical the single fault is detected

- Not all single faults may be detected
- Multiple undetected single faults can lead to the loss of the safety function

Familiar Territory

- Category 4

  Cat B PLUS

  +Well-tried safety principles

  +No single fault can lead to the loss of the safety function

  +Single faults are detected at or before the next demand on the safety system

  +Accumulation of single faults does not lead to the loss of the safety function

  +Fault exclusion is allowed

Familiar Territory

- North America
  - Simple
    - No special measures. Components selected to meet general design requirements. Programmable systems are acceptable.
  - Single Channel
    - Hardware based or use certified safety programmable controller
    - Use safety rated components
    - Use proven (read ‘well-tried’) circuit designs.

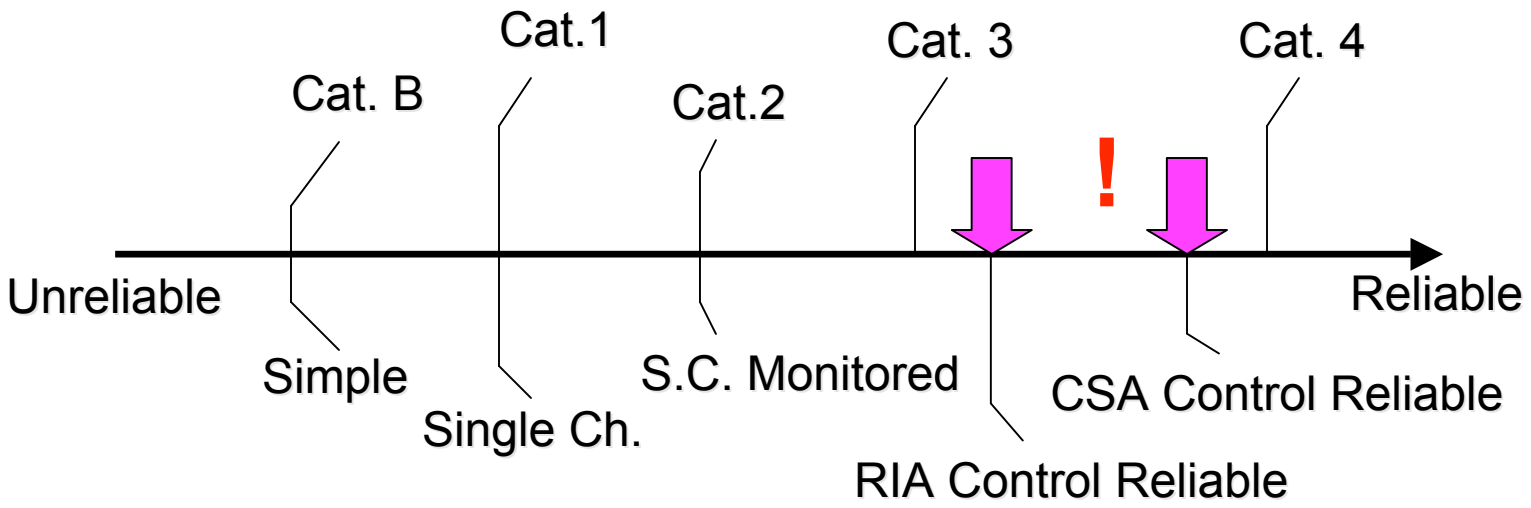
Familiar Territory

- Single Channel, Monitored
  - Single Channel Design +
  - Hardware checks at machine start and at suitable intervals thereafter (preferred at each state change)
  - Generate a stop condition if a fault is detected
  - Maintain a safe state until the fault is cleared.

Familiar Territory

- Control Reliable
  - No single component failure may cause the loss of the safety function. (remember this for later!)
  - Hardware based OR use certified programmable controller.
  - Generate a stop and maintain a safe state if a fault is detected
  - Design must consider common mode faults if probability is significant.
  - 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.

Familiar Territory



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

Questions

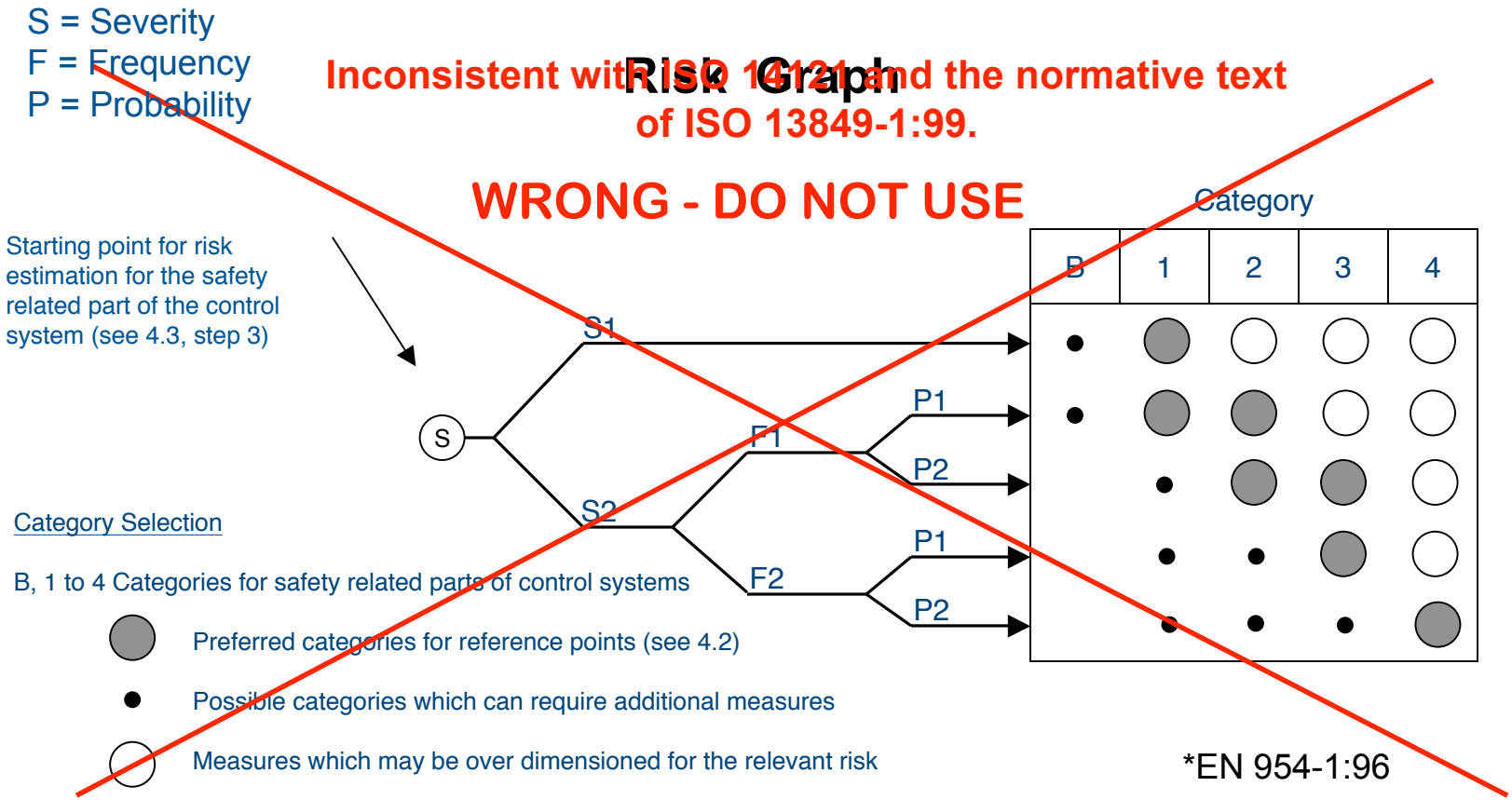
- What does all this mean, really?
  - What are the categories/performance criteria?
  - Do they represent risk?
  - How do I connect risk and control system performance?

ISO 13849-1:99* Annex B

S = Severity
F = Frequency
P = Probability

Inconsistent with ISO 14121 and the normative text of ISO 13849-1:99.

WRONG - DO NOT USE



*EN 954-1:96

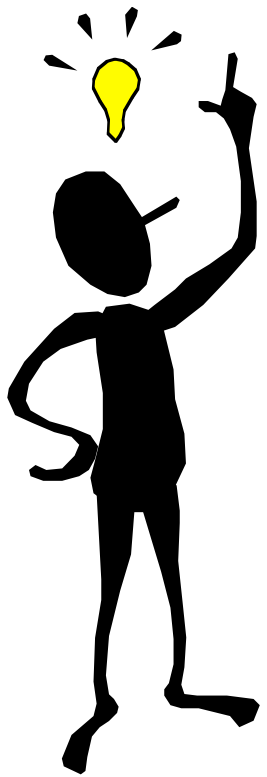
So What's the Problem?

- ISO 13849-1:99 says that the Categories are not a hierarchy, but the diagram illustrates them that way.
- You cannot draw a straight line from the risk assessment to the control reliability requirements as is shown.
- So how can we connect the two?

Now What?

- How do you make the link between risk and reliability?

ISO 13849-1:2006!



The Solution

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

Performance Levels

- PL's are the key to linking risk control reliability requirements

PL	Average probability of dangerous failure per hour
a	≥ 10^{-5} to < 10^{-4}
	≥ 3 x 10^{-6} to < 10^{-5}
	≥ 10^{-6} to < 3 x 10^{-6}
	≥ 10^{-7} to < 10^{-6}
e	≥ 10^{-8} to < 10^{-7}

1 Failure in 5 years of single shift operation

1 Failure in 25 years of single shift operation.

Determine Requirement

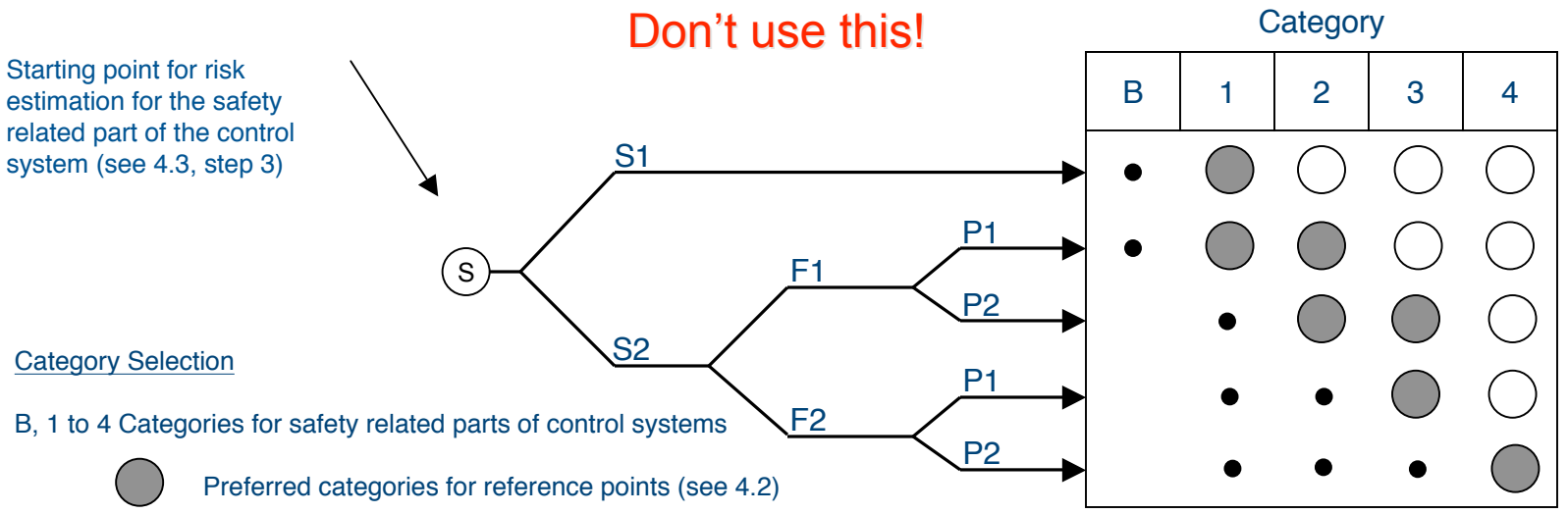
- Start by completing the Risk Assessment
- Analyze the PL required (PL_r) - See Annex A for guidance

ISO 13849-1:99* Annex B

S = Severity
F = Frequency
P = Probability

Risk Graph

Don't use this!



Category Selection

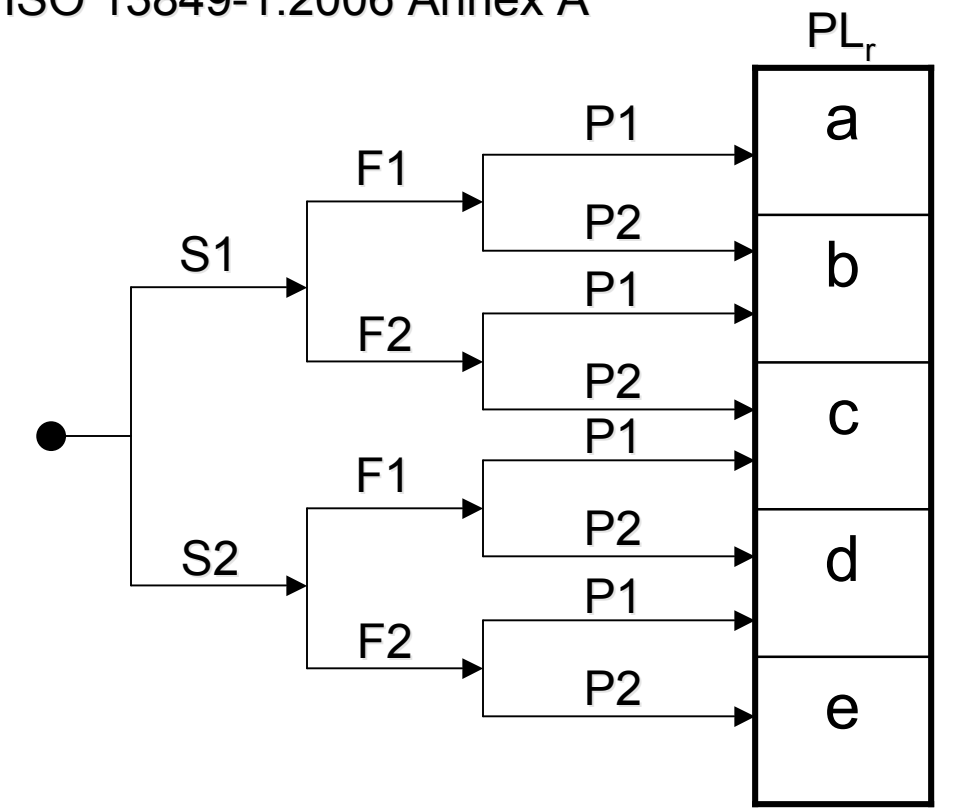
B, 1 to 4 Categories for safety related parts of control systems

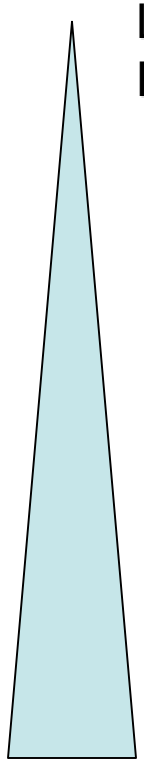
- Preferred categories for reference points (see 4.2)
- Possible categories which can require additional measures
- Measures which may be over dimensioned for the relevant risk

*EN 954-1

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

Performance Levels

- Once PL_r is determined based on the hazards, the current PL must be determined
- How to do this?
  - Annexes C,E, F,G,J provide guidance
  - Clause 6 covers Structures (remember the familiar categories B,1-4?)

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!

$MTTF_d$

- The time that will elapse until 63% of components fail.
- Calculated based on B_{10d}
- B_{10d} = Mean cycles until 10% of components fail (should be on the datasheet)

Calculation

$$MTTF_d = \frac{B_{10d}}{0.1 \times n_{op}}$$

- B_{10d} = Cycles to 10% of components fail
- n_{op} = Mean number of annual operations

Calculation

- $MTTF_d$ of all components is calculated and summed using methods in the annexes.
- PL is determined based on the calculated $MTTF_d$ using Tables 5 & 7.

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 %.

Table 7 — Simplified procedure for evaluating PL achieved by SRP/CS

Category	**B**	**1**	**2**	**2**	**3**	**3**	**4**
DC_{avg}	**none**	**none**	**low**	**medium**	**low**	**medium**	**high**
$MTTF_d$ of each channel							
Low	a	Not covered	a	b	b	c	Not covered
Medium	b	Not covered	b	c	c	d	Not covered
High	Not covered	c	c	d	d	d	e

Performance Levels

- What if you don't have the data to support the required calculations?
  - Means to estimate the required data for different types of components given in the standard.
- Use the predefined structures given as Category B through 4. (§4.5.4 and 6)

PSES
Product Safety Engineering Society

Diagnostic Coverage

- DC describes the ability of the system self-test to detect failures.
- Table E.1 gives examples

Table E.1 — Estimates for diagnostic coverage (DC)

Measure	DC
Input device	
Cyclic test stimulus by dynamic change of the input signals	90 %
Plausibility check, e.g. use of normally open and normally closed mechanically linked contacts	99 %
Cross monitoring of inputs without dynamic test	0 % to 99 %, depending on how often a signal change is done by the application
Cross monitoring of input signals with dynamic test if short circuits are not detectable (for multiple I/O)	90 %
Cross monitoring of input signals and intermediate results within the logic (L), and temporal and logical software monitor of the program flow and detection of static faults and short circuits (for multiple I/O)	99 %
Indirect monitoring (e.g. monitoring by pressure switch, electrical position monitoring of actuators)	90 % to 99 %, depending on the application
Direct monitoring (e.g. electrical position monitoring of control valves, monitoring of electromechanical devices by mechanically linked contact elements)	99 %
Fault detection by the process	0 % to 99 %, depending on the application; this measure alone is not sufficient for the required performance level e!
Monitoring some characteristics of the sensor (response time, range of analogue signals, e.g. electrical resistance, capacitance)	60 %

Table 6 — Diagnostic coverage (DC)

DC	
Denotation	**Range**
None	$DC < 60\ \%$
Low	$60\ \% \leqslant DC < 90\ \%$
Medium	$90\ \% \leqslant DC < 99\ \%$
High	$99\ \% \leqslant DC$

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 %.

Table 7 — Simplified procedure for evaluating PL achieved by SRP/CS

Category	**B**	**1**	**2**	**2**	**3**	**3**	**4**
DC_{avg}	**none**	**none**	**low**	**medium**	**low**	**medium**	**high**
$MTTF_d$ of each channel							
Low	a	Not covered	a	b	b	c	Not covered
Medium	b	Not covered	b	c	c	d	Not covered
High	Not covered	c	c	d	d	d	e

Faults

- Common Mode Failure:
  “A common-mode failure (CMF) is the result of an event(s) which because of dependencies, causes a coincidence of failure states of components in two or more separate channels of a redundancy system, leading to the defined system failing to perform its intended function”.

- Common Cause Failure:
  "A dependent failure in which two or more component fault states exist simultaneously, or within a short time interval, and are a direct result of a shared cause."

Common Cause Failures

- Annex F provides a scoring system
- Every part of the safety related part of the control system must be scored
- More extensive coverage of this topic is in ISO 13849-2.
- ‘Cascade’ failures are considered a single fault.
- Common Cause Faults are considered a single fault

Table F.1

Table F.1 — Scoring process and quantification of measures against CCF

No.	Measure against CCF	Score
1	**Separation/ Segregation**	
	Physical separation between signal paths: separation in wiring/piping, sufficient clearances and creep age distances on printed-circuit boards.	15
2	**Diversity**	
	Different technologies/design or physical principles are used, for example: first channel programmable electronic and second channel hardwired, kind of initiation, pressure and temperature, Measuring of distance and pressure, digital and analog. Components of different manufactures.	20

Common Cause Failures

- Add up the scores
- If the CCF score is ≥ 65, system is OK
- If the CCF score is < 65, additional measures required

Common Cause Failures

- Fault exclusion is specifically allowed under §7.3. What does CSA Z434-03 say about this?
- 4.5.5(c):
  - ‘Common mode failures shall be taken into account when the probability of such a failure occurring is significant.’
- Only common MODE failures addressed
- No guidance on what is considered to be “significant”

Faults and Failures

- This is the only place where any discussion of Common Mode Failures exists in the CSA standard
- There is no allowance for fault exclusion in the CSA or the RIA standard.
- Can you think of specific instances where it would be reasonable to exclude certain failures?

Fault Exclusion

Would it be reasonable to exclude mechanical failures in a system that used these gate interlocks?

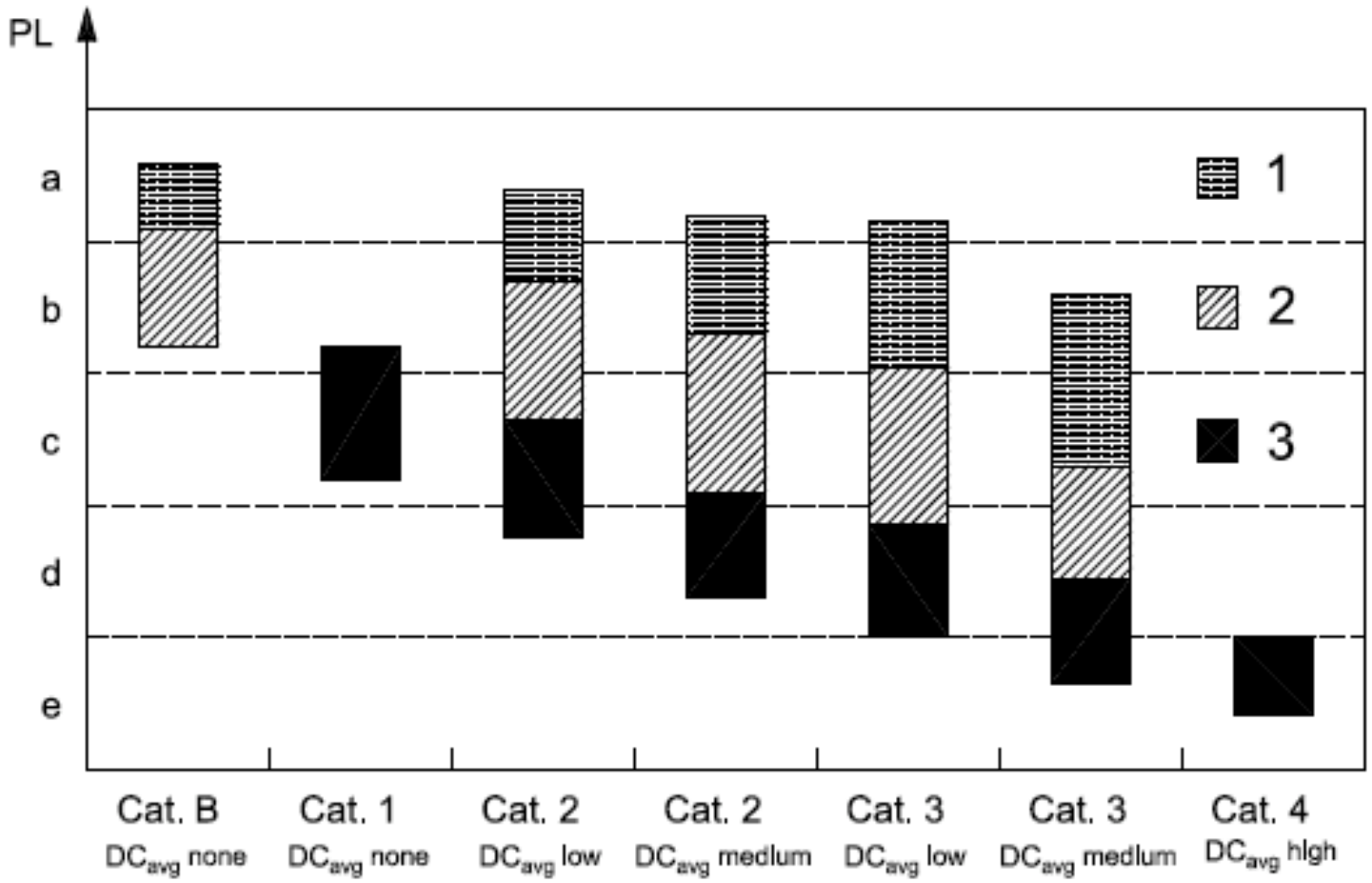
If YES, then how do we deal with the ‘no single component failure’ requirement in 4.5.5? Do we still need two devices on each gate?

Fault Exclusion

What about these switches?

Fault Exclusion

What about a switch like this one?



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

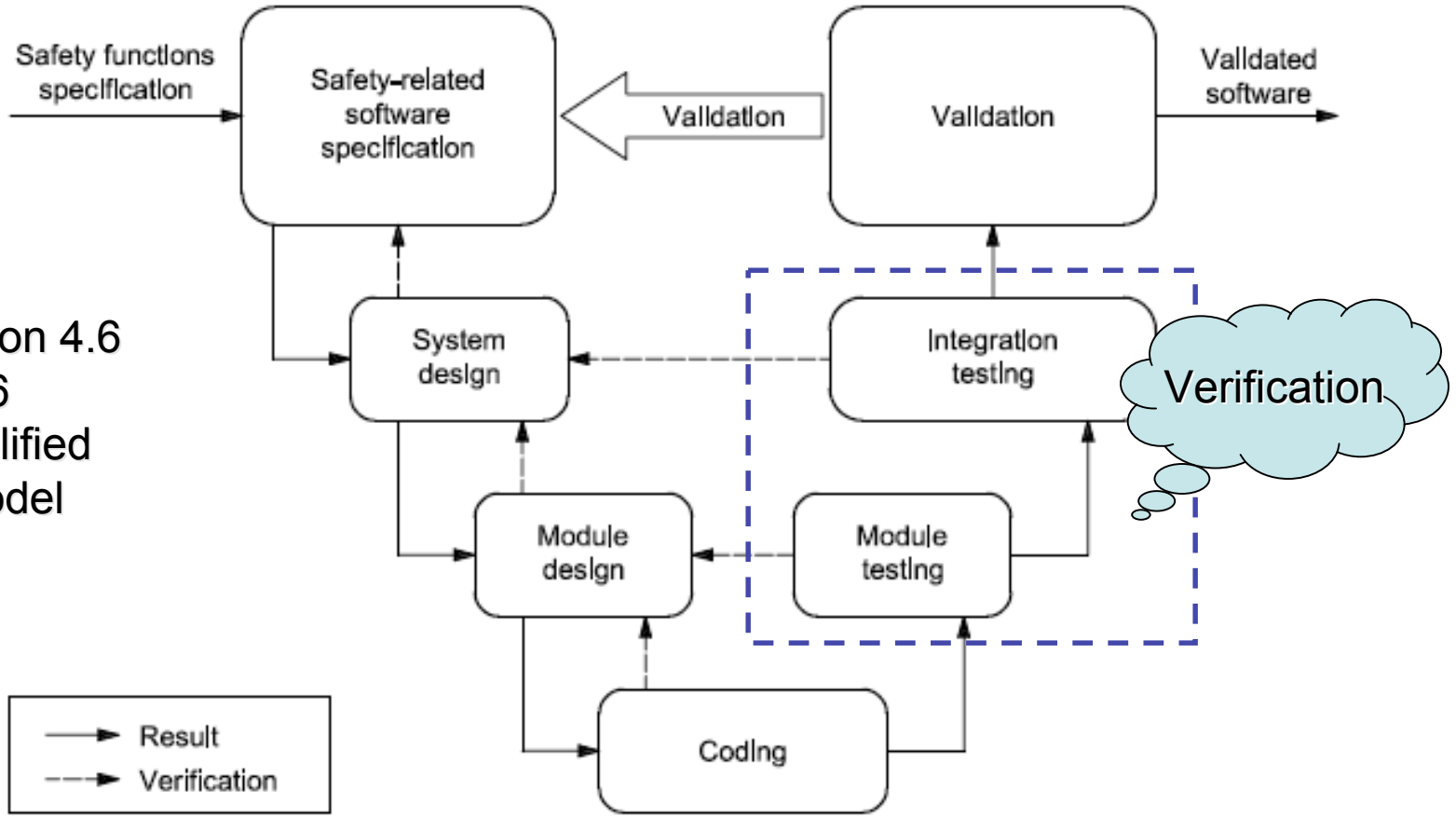
Figure 5 — Relationship between categories, DC_{avg}, $MTTF_d$ of each channel and PL

What About Software?

- Section 4.6
  - General V & V process
  - Requirements for Safety Related Embedded Software (SRESW)
  - Requirements for Safety Related Application Software (SRASW)

Software V & V

Section 4.6
Fig. 6
Simplified
V-Model



Avoiding Software V & V

- Purchased syste
  - Vendors condu
    &V
  - Users provide
  - Simplifies applicati
  - Runs process con ode as well (no formal V &V req d)
  - Certified systems come with a known Category rating.

Formal adoption of ISO 13849-1 by the EU has resulted in some products coming with a defined PL. Some products already have B_{10} or B_{10d} figures in their datasheets.

Wrapping Up

- Verify that the final PL of the system is greater than or equal to the PL_r determined at the beginning of the process.
- Section 8: Validation process is given in ISO 13849-2.

Wrapping Up

- Aspects not discussed:
  - Section 5: Defining Safety Functions
    - Emergency Stop
    - Safety Related Stop by Safeguard
    - Manual Reset
    - Muting
    - …
  - Section 7: Fault Considerations & Exclusions
  - Section 9: Maintenance
  - Section 10: Technical Documentation
  - Section 11: Information for Use

Wrapping Up

- Overall an excellent revision to an important standard
- Anyone designing safeguarding systems should study this standard and ISO 13849-2
- Implementation of ISO 13849-1 mandatory in the EU from 30-Nov-09
- ISO 13849 -2 has been mandatory since 20-Apr-04.
- Is influencing coming editions of other machinery standards

Other Relevant Standards

- ISO 13849-2 – Safety Of Machinery - Safety-related Parts Of Control System - Part 2: Validation

- ISO 13849-100 – Safety Of Machinery - Safety-related Parts Of Control Systems - Part 100: Guidelines For The Use And Application Of ISO 13849-1

Other Relevant Standards

- IEC 61508-1 – Functional Safety Of Electrical/electronic/programmable Electronic Safety Related Systems - Part 1: General Requirements

- IEC 62061 – Safety Of Machinery - Functional Safety Of Safety-related Electrical, Electronic And Programmable Electronic Control Systems

Thank You!

Compliance InSight Consulting Inc.
Know Risk…Design Safety™
Kitchener, Ontario, Canada

(519) 729-5704
www.machinerysafety101.com
dnix@mac.com