Yaskawa Electric America Training Café

Today's topic is

Functional Safety Standards & Safe Disable Inputs

Presenter is
Joe Pottebaum
Senior Applications Engineer

To make this Café enjoyable for all, please follow these tips on web class etiquette.

***Please do not put us on hold**. Others will hear the hold music.*

***Do not use a speaker phone**. Background noise can be heard.*

Don't be shy, we welcome comments and questions.
*(Press ***6*** to **mute or unmute** your phone)*

*Questions not answered during the Café can be emailed to **training@yaskawa.com** or can be entered into the survey at the end of the class.*

‘English’ Definition - Safety

Safety

1. *the state of being safe; freedom from the **occurrence** or **risk** of **injury**, **danger**, or **loss**.*
2. *the quality of averting or not causing injury, danger, or loss.*
3. *a contrivance or device to prevent injury or avert danger.*

safety. Dictionary.com. Dictionary.com Unabridged (v 1.1). Random House, Inc. http://dictionary.reference.com/browse/safety (accessed: April 21, 2009).

Safety Standard's Definition of Safety

'Safety' = Freedom from Unacceptable Risk

What makes risk acceptable?

Who determines?

Determination of Risk Acceptability

Individuals and Society determine what risk is acceptable.

Standards, Codes and Laws reflect those expectations.

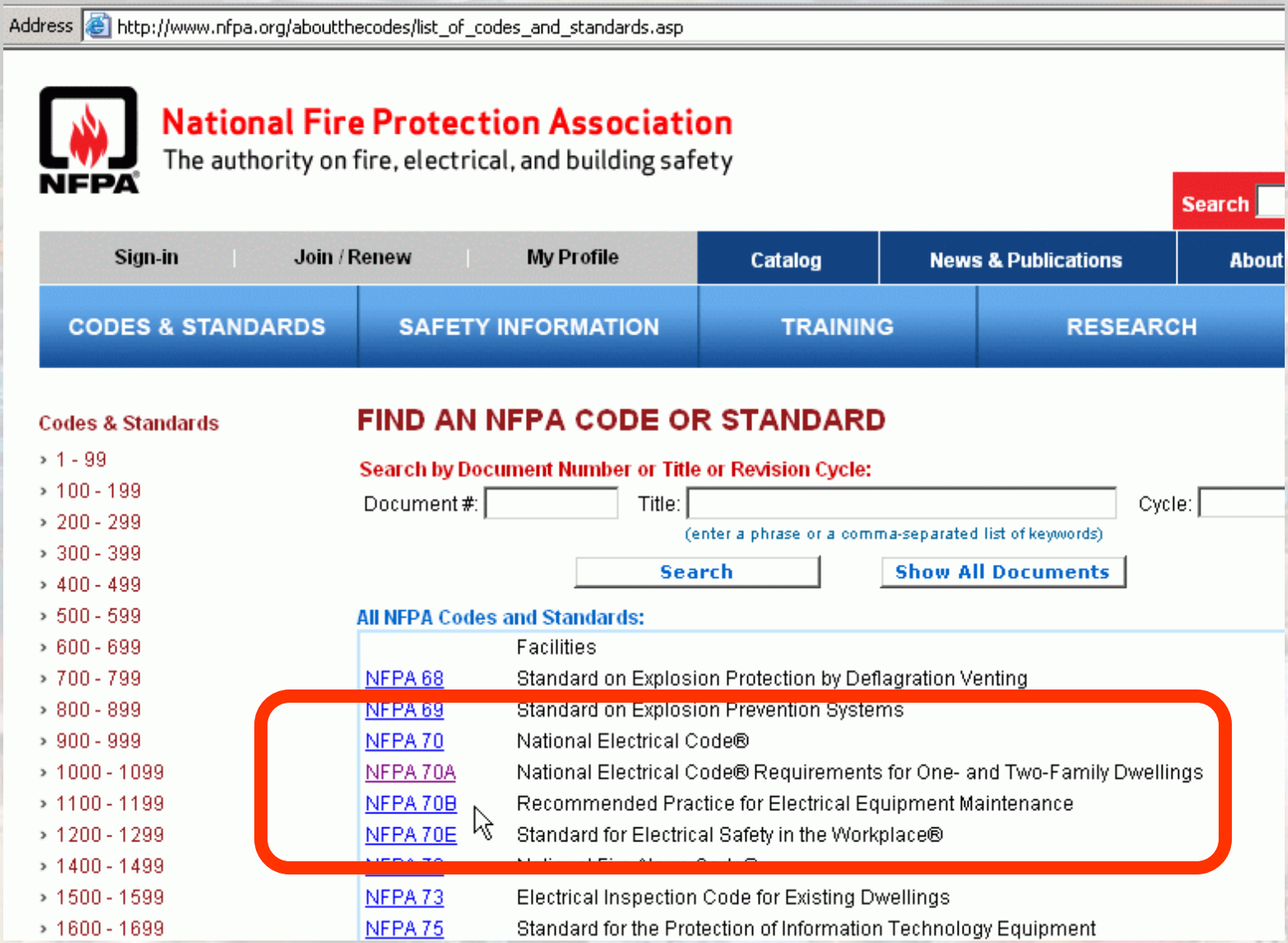
Traditional Approach

- *Make each piece of equipment safe by constructing it according to appropriate standards (UL, CSA, etc.).*
- *Slather it with warning labels.*
- *Install it according to code (NEC).*
- *Train operators in its proper safe use.*
- *Assume operators will always follow safe practice.*

History: IEC 61800-5-1

CONTENTS

History: NFPA 70 = NEC



Traditional Equipment Safety Standards

Historical Equipment Safety Concerns:

Don't Start Fires

Don't Electrocute Anybody

Safe is Safe, Right?

- ***A system comprising all safe components can still function in an unsafe manner.***

Equipment Safety vs. Functional Safety

Equipment Safety

- *Is the individual piece of equipment safe?*
- *Is electrical insulation adequate?*
- *Is the ground wire fat enough?*
- *Is the door interlocked with the circuit disconnect?*
- *Etc. etc. etc.*
- *Meet UL, CSA, CE, etc.*

Functional Safety

- *Will the machine as a whole always function safely?*
- *Can this be guaranteed to within an acceptable level of risk?*

Drive is Only a Component

- ***No matter how big they are,***

Yaskawa Drives are only Components in the Safety System.

Equipment Safety vs. Functional Safety

- *We must distinguish between*
  - *safety functions* ***integrated into equipment***
  - *the safety of a facility or enforcing safe practices.*

Functional Safety Definition

- *Functional Safety is part of overall safety that depends on a system of equipment operating correctly* ***in response to its inputs****.*

Directives, Standards & Laws in EU

- *EU formulates general safety objectives via **directives**.*
- *Directives are not binding until set into law by individual countries.*
- ***Standards** are 'legal' when published in "Official Journal of the EU" and referenced by domestic laws, ie. '**harmonized**'.*
- ***Adherence** to harmonized standards confers "**Presumption of Conformity**".*

Presumption of Conformity

- '***Presumption of conformity***' *means that* ***if*** *a manufacturer has complied with the* ***standard****,* ***then*** *it can assume it has met the requirements of the* ***directive****.*

- *Legal effect is* ***reversal of the burden of proof****.*

Reversal of the Burden of Proof

When there is a problem:

- *Where the manufacturer applies a standard, misconduct must be proved.*
- *Where the manufacturer has **not** applied a standard, the manufacturer must prove it has acted in compliance with the directive.*

The CE Mark

- *'CE' = 'Communauté Européenne'*
- *The CE mark documents that the manufacturer has considered all the EU directives relevant to the product and*
- *applied the appropriate conformity assessment procedures, ie. tested to the relevant standards.*

Machinery Directive

- *Machinery Directive covers Yaskawa Drives.*
- *Revised **Machinery Directive 2006/42/EC** took effect **December 29, 2009**.*
- *EU domestic laws require that machines meet the Essential Health and Safety Requirements (**EHSR**) defined in the Machinery Directive.*

CE Mark

Comply with the Standards → CE → Meets the Directive ↓

*Fulfill Essential Health and Safety Requirements (**EHSR**)*

Functional Safety Systems

- *Safety is integrated into machine's functionality*
- *not just warning labels added to meet regulations*
- *So what standards apply to meet Essential Health and Safety Requirements (EHSR)?*

What is a Machine?

- *Article 2 of Machinery Directive:*
  An assembly of linked parts or components, at least one of which moves, and which are joined together for a specific application.

Functional Safety Standards

Was

- *EN 954-1*

Now

- ***Either*** *EN (IEC) 62061*
- ***Or*** *EN (ISO) 13849-1*

Take your pick !

What Changed

- *Old EN 954-1 defined safety categories – meet them and you are done.*
- *New standards based on **probability**. Manufacturer must ensure safety by performing assessment calculations.*

YASKAWA
Yaskawa Training Cafe

Alphabet Soup

Take Your Pick

- *EN ISO 13849-1:2008 (Safety of Machinery -Safety-related Parts of Control **Systems** - General Principles for Design)*
- *EN (IEC) 62061:2005 (Safety of Machinery - Functional Safety of Safety-related Electrical, Electronic and Programmable Electronic Control **Systems**).*

International

- *IEC = International Electrotechnical Commission*
- *ISO = International Organization for Standardization*

ISO vs. IEC

- *ISO: standardization in all fields except electrical and electronic engineering*
- *IEC: electrical and electronic engineering standards*
  - *Both ISO and the IEC operate according to similar rules.*
  - *Members are national standards organizations like ANSI, DIN, etc.*
  - *The adoption of ISO and/or IEC standards into the national collections is voluntary.*
  - *Adoption may be complete or partial.*

IEC 61508, ISO 13849-1, IEC 62061

- *IEC 61508 = Functional Safety of Electrical / Electronic / Programmable Electronic (E/E/PE) Safety Related Systems.*
- *Seven parts of **IEC** 61508 were published by CENELEC in December 2001 as **EN** 61508*
- *Principles in IEC **61508** carried into both ISO **13849-1**:2008 and IEC **62061**:2005*

Differences

- ***ISO 13849-1***
- *Any type of control*
- *Uses Performance Levels – PL*
- *PL a, b, c, d, or e*
- *PL a is lowest*

- ***IEC 62061***
- *Electrical Control*
- *Use Safety Integrity Levels – SIL*
- *SIL 1, 2, or 3*
- *SIL 1 is lowest,*

Safety Related System & IEC 61508

What is a safety-related system in the context of IEC 61508?

- *A safety-related system comprises everything (hardware, software and human elements) necessary to carry out one or more safety functions, where failure of the safety function would give rise to a significant increase in the risk to the safety of persons and/or the environment.*
- *A safety-related system can comprise stand-alone equipment dedicated to perform a particular safety function (such as a fire detection system) or can be integrated into other plant or equipment (such as motor speed control in a machine tool).*
- *3.4.1 of IEC 61508-4 gives a formal definition.*

What is Functional Safety in 61508

What is functional safety?

- ***Functional safety is part of the overall safety that depends on a system or equipment operating correctly in response to its inputs****. Functional safety is achieved when every specified safety function is carried out and the level of performance required of each safety function is met.*
- *For example, an overtemperature protection device, using a thermal sensor in the windings of an electric motor to de-energise the motor before they can overheat, is an instance of functional safety. But providing specialised insulation to withstand high temperatures is not an instance of functional safety (although it is still an instance of safety and could protect against exactly the same hazard).*
- *See the document Functional safety and IEC 61508 for further details.*

ISO 13849-1 Performance Levels

- *Similar to EN954-1 Levels B, 1, 2, 3 and 4*

IEC 62061 'SIL'

- ***What is a safety integrity level (SIL)?***
- *A safety integrity level is one of four levels, each corresponding to a range of target likelihood of failures of a safety function. Note that a safety integrity level is a property of a safety function rather than of a system or any part of a system.*

SIL for Component

What is meant by a SILn system, subsystem or component?

- *A safety integrity level (SIL) is not a property of a system, subsystem or component. The correct interpretation of this phrase is that the system, subsystem or component is capable of supporting safety functions with a safety integrity level up to n. This in itself is not sufficient to achieve a safety function of the required safety integrity level.*
- *The safety integrity level capability of a subsystem determines the highest safety integrity level that can be claimed for any safety function that uses the subsystem. For this reason, the term safety integrity level claim limit is sometimes used instead. A SILn capability or claim limit (where n is 1,2,3 or 4) is determined for each subsystem by achieving a or b below.*
- *The design requirements for SILn to prevent and control systematic faults in accordance with IEC 61508-2 and IEC 61508-3; or*
- *The proven in use requirements for SILn in accordance with 7.4.7.6 to 7.4.7.10 of IEC 61508-2.*
- *Other information about the system, subsystem or component is also necessary to facilitate a demonstration that the required safety integrity level of the safety function in the E/E/PE safety-related system will be achieved.*

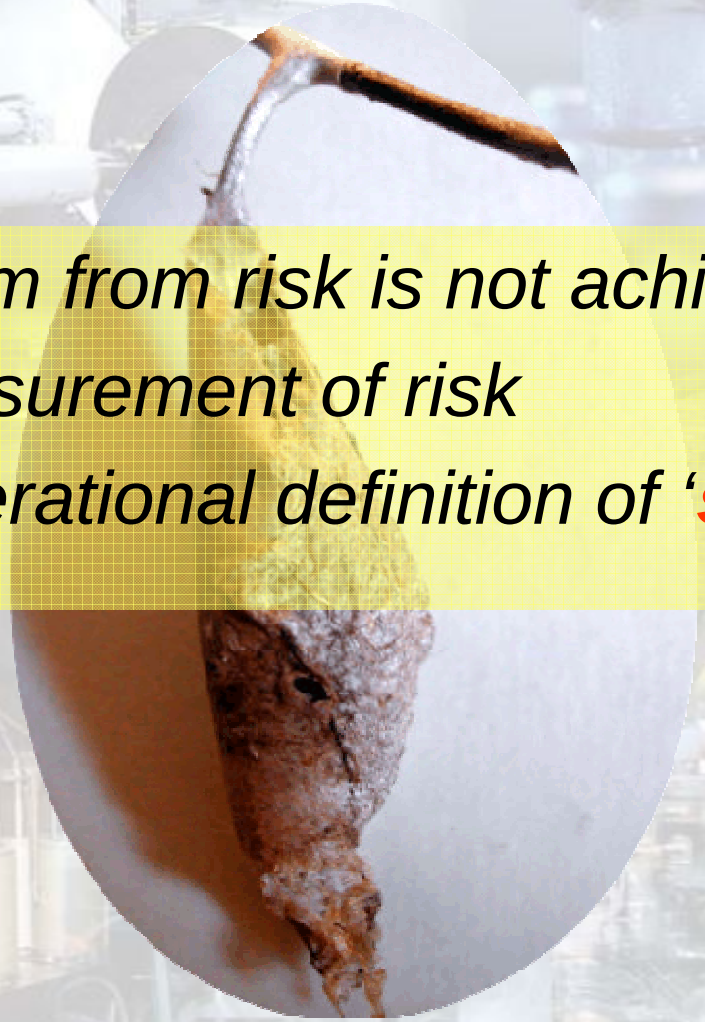
Functional Safety Requirement

- *NOT ONLY --*
  - *Equipment must have reliable safe construction*

    → ***UL, CE, CSA, etc.***
- *BUT ALSO --*
  - *Equipment must **function correctly** in response to safety related inputs*

    → ***Functional Safety***

Freedom from **Risk** of Injury



- *Total freedom from risk is not achievable*
- *Need a measurement of risk*
- *Need an operational definition of '**safety**'*

Risk Assessment

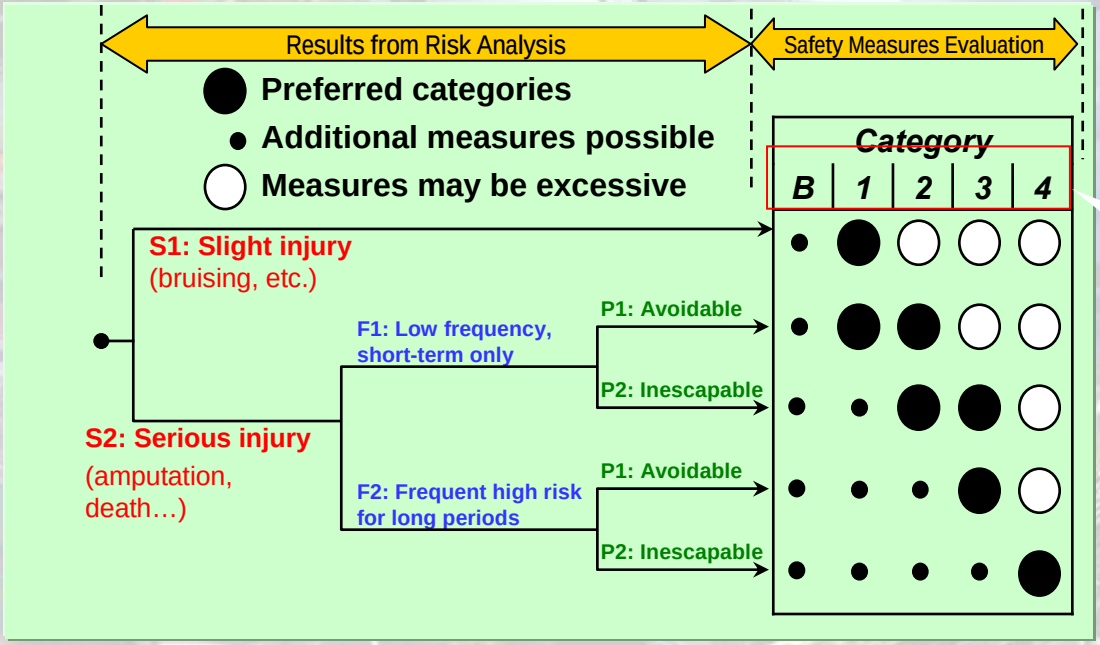
- *How safe is safe enough?*
- *To find out – do a **Risk Assessment**.*

ISO13849-1 (Successor to EN954-1)

Safety-related parts of control systems
Part1: General principles for design
ISO13849-1, JIS B 9705

- *Covers the design procedures for components related to safety in a system.*
- *Determines the danger level by looking at the **severity of potential injury** and the **probability** of an accident causing those injuries.*
- *Specifies what **types of safety measures** are needed for control to cover each of the five levels of danger.*

Category Assessment Table



S: Severity of injury
F: Frequency and/or duration of exposure to the hazard
P: Possibility of avoiding the hazard

Safety Categories Based on ISO13849-1

Determines the danger level by looking at the severity of potential injury (serious injuries vs. light injuries) and the probability of an accident causing those injuries.

The higher the values are for B,1,2,3, and 4, the more safety measures are required.
When there is a high possibility of severe injuries, then the safety category will indicate that more comprehensive steps be taken (parts, system design) to ensure safety.

EN954-1: the five categories for safety-related parts of control systems

Category B

The basic category --The occurrence of a fault can lead to loss of safety function;

•Category 1

Improved resistance to faults is achieved predominantly by selection and application of components. This is achieved by **using well-tried components and well-tried safety principles**.

•Category 2

Category 1 requirements plus control system is designed so safety-related functions are checked at suitable intervals by the machine control system. After detection of a fault, a safe state will be maintained until the fault has been cleared**.**

•Category 3

Improved so that a **single fault will not lead to loss of a safety function**. Common mode faults need to be taken into account when the probability of such a fault occurring is significant. Whenever reasonably practical, the single fault should be detected at or before the next demand for the safety function. **All faults are not required to be detected**, thus an accumulation of undetected faults could lead to hazardous situation.

•Category 4

All faults will be detected and there will the **protection against an accumulation of faults** which needs to be specified. The safety-related parts of the control need to be designed so the a single fault does not lead to a loss of safety function and the **single fault will be detected** at or before the next demand for the safety function. This category of safety requires that when faults occur the safety function is always performed and the faults will be detected in time to prevent the loss of the safety function.

Reality for Yaskawa

- *The **Drive** is only a **Component** in the overall safety system*
- *The **drive's only responsibility** is to respond predictably to its safety inputs – Safe Disable*
- *For Yaskawa V1000, A1000 drives:*

  Opening Safe Disable input => Motor Coasts

EN 60204-1

- *This part of IEC 60204 is applicable to the electrical equipment or parts of the electrical equipment that operate with nominal supply voltages not exceeding 1000 V for alternating current and not exceeding 1500 V for direct current, and with nominal supply frequencies not exceeding 200 Hz.*
- *Covers all aspects of electrical equipment and machinery in regards to control circuits, functions, devices, and safety measures, as well as documentation explaining installation, operation, and maintenance.*

Stop Categories & Safe Disable Input

Electrical equipment of machines
Part1: Specification for general requirements
IEC standards: IEC60204-1 JIS standards: JIS B 9960-1

Yaskawa's Safe Disable feature satisfies both Category 0 defined in EN60204-1 (STO defined in IEC 61800-5-2) for an uncontrolled stop

and Category 3 of EN954-1.

Safe Disable can be integrated into any sequences or circuits the user has set up for machine safety.

Stop Categories

0 or STO: Stopping by immediate removal of power to the machine actuators (i.e., an uncontrolled stop or "coast to stop" or Safe Torque Off)

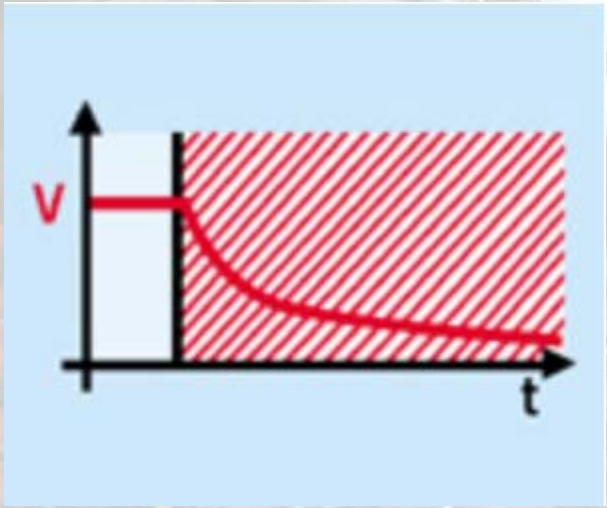
1 or SS1: Stopping in a controlled manner, with power made available so that the machine actuators can achieve the stop, the power removal when the stop is achieved (ramp to stop followed by STO)

2 or SS2: Stopping in a controlled manner, with power left available to the machine actuators (Zero Servo or SOS Safe Operating Stop)

Stop Categories Illustration

STOP Categories / IEC61800-5-2

V1000, A1000, F7(option)

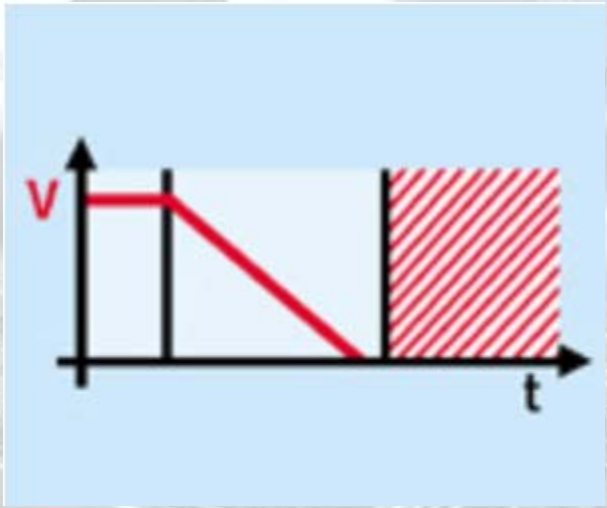


EN 60204-1 (VDE 0113):
Stop Category 0

IEC 61800-5-2:
Safe Torque Off (STO)

Remove Energy

Servo + Options

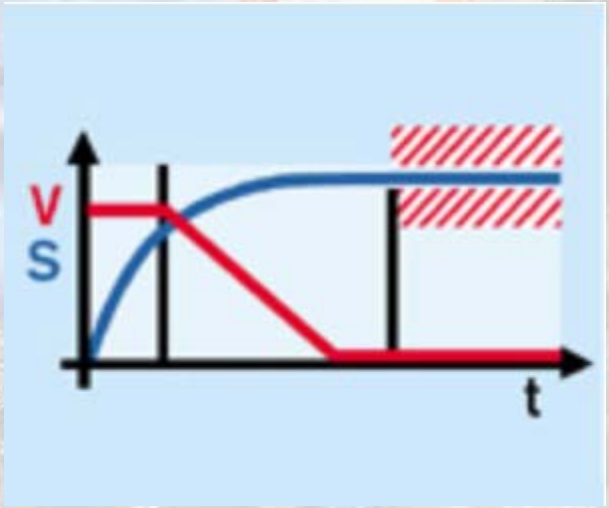


EN 60204-1 (VDE 0113):
Stop Category 1

IEC 61800-5-2:
Safe Stop 1 (SS1)

Controlled ramp down, followed by STO

Servo + Options



EN 60204-1 (VDE 0113):
Stop Category 2

IEC 61800-5-2:
Safe Stop 2 (SS2)

Controlled ramp down, followed by SOS (Safe Operating Stop)

On Board Safety Function

Standard on Board:

EN 954-1:

Safety Category 3

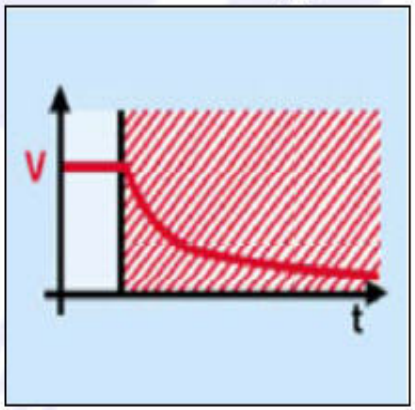
EN 60204-1 (VDE 0113):

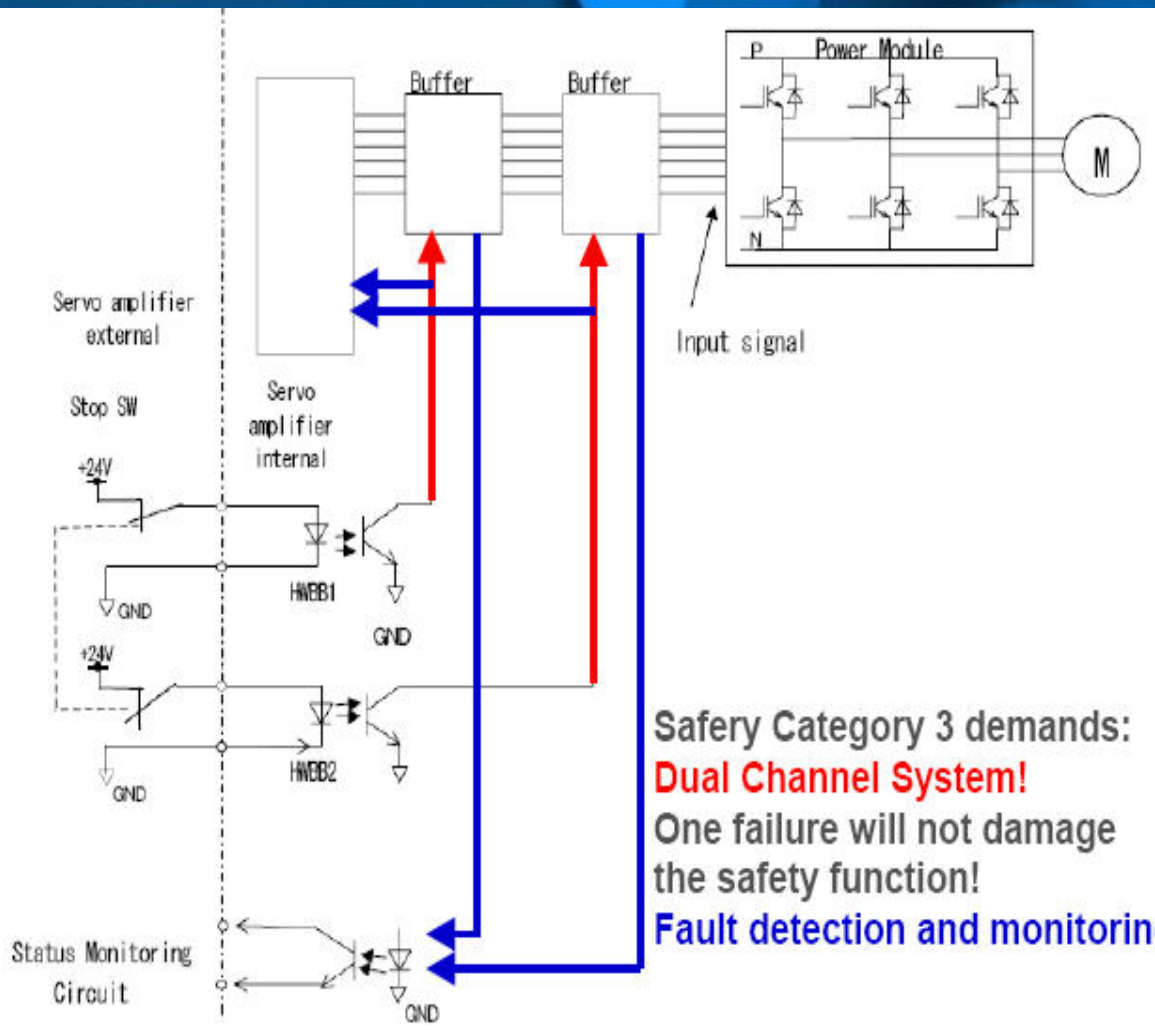
Stop Category 0

IEC 61800-5-2:

Safe Torque Off (ST0)

Remove Energy!





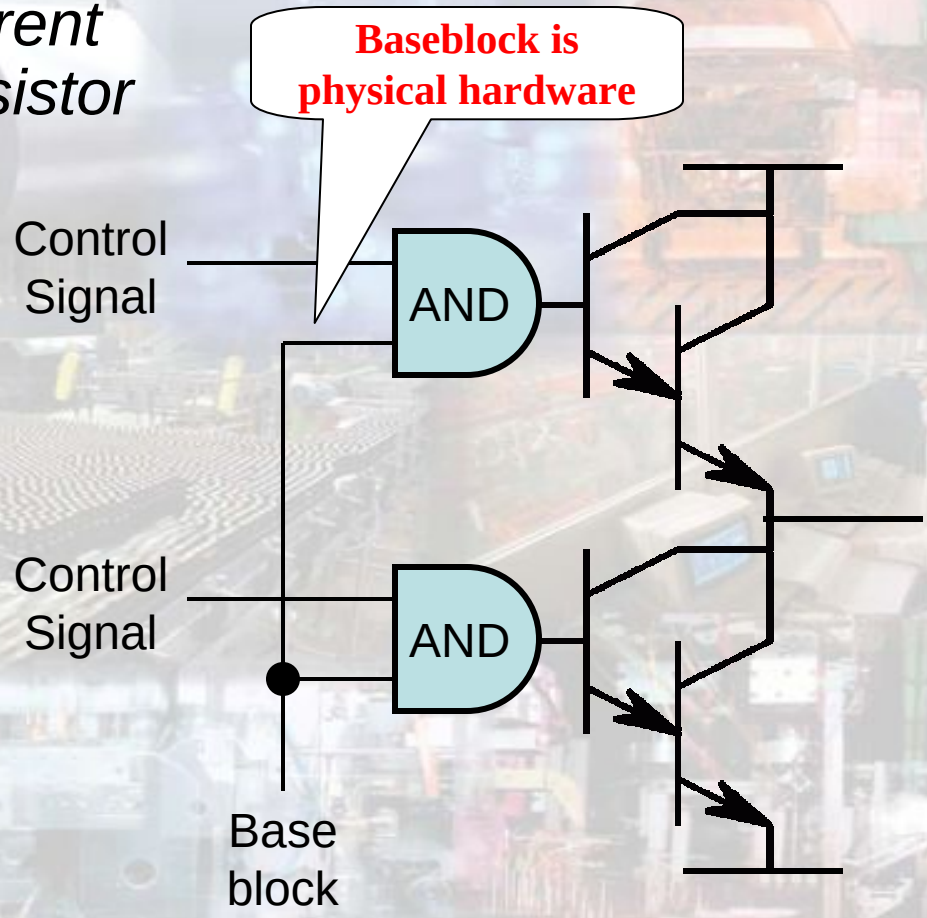
Safety Category 3 demands:
Dual Channel System!
One failure will not damage the safety function!
Fault detection and monitoring!

Base Block

Why doesn't the standard baseblock multi-function input satisfy Stop 0 or STO?

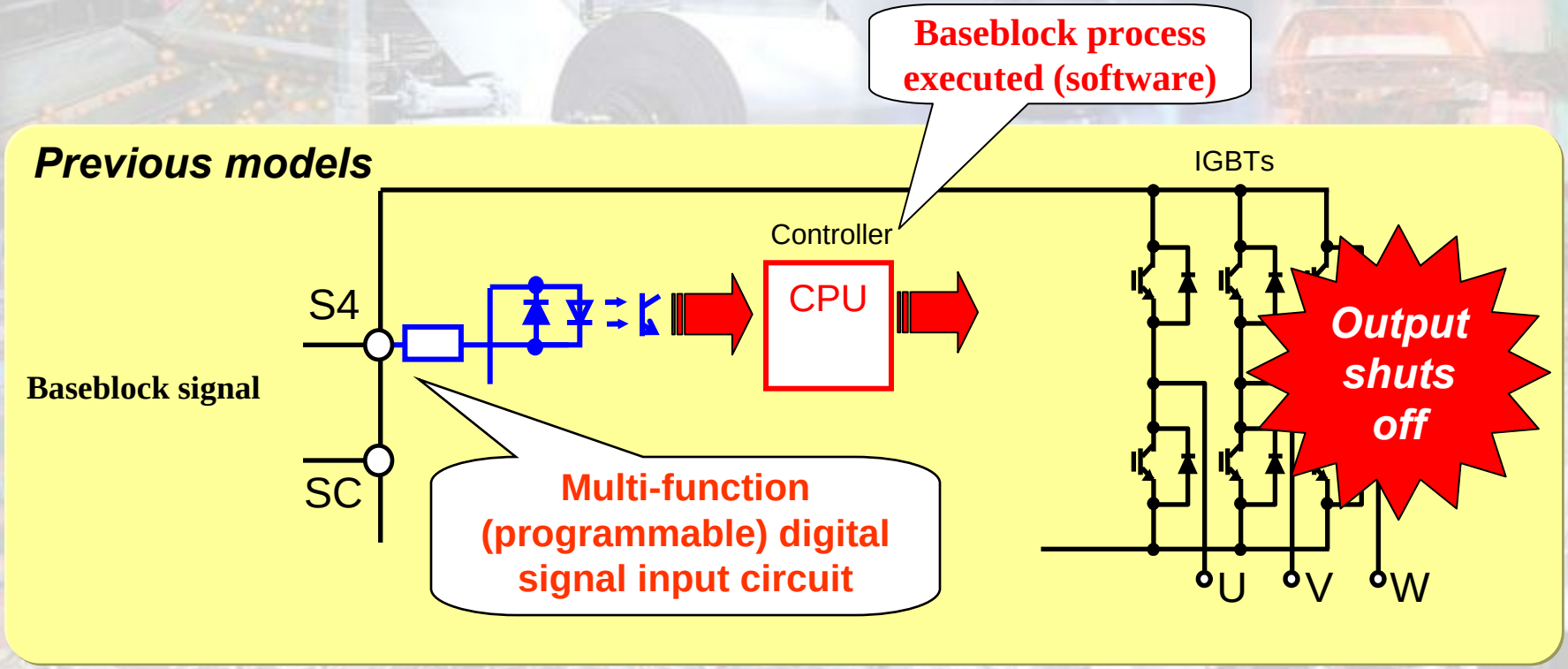
Evolution of the Base Block

- *Originally "base block" was hardware that blocked current to the base of bipolar transistor to turn it off during a fault.*



Software Base Block

Baseblock implemented in software.



Issues with Software Baseblock

- *Safety Issues with Software Baseblock command.*
  - *Safety can't be guaranteed for every step in the program.*
    - *Someone may re-program the baseblock input –*
      - ***after all, it is programmable***
    - *Input scan time can cause delayed response.*
    - *The controller could malfunction*
    - *Software bug.*

EN954-1: the five categories for safety-related parts of control systems

Category B

The basic category --The occurrence of a fault can lead to loss of safety function;

•Category 1

Improved resistance to faults is achieved predominantly by selection and application of components. This is achieved by **using well-tried components and well-tried safety principles**.

•Category 2

Category 1 requirements plus control system is designed so safety-related functions are checked at suitable intervals by the machine control system. After detection of a fault, a safe state will be maintained until the fault has been cleared.

•Category 3

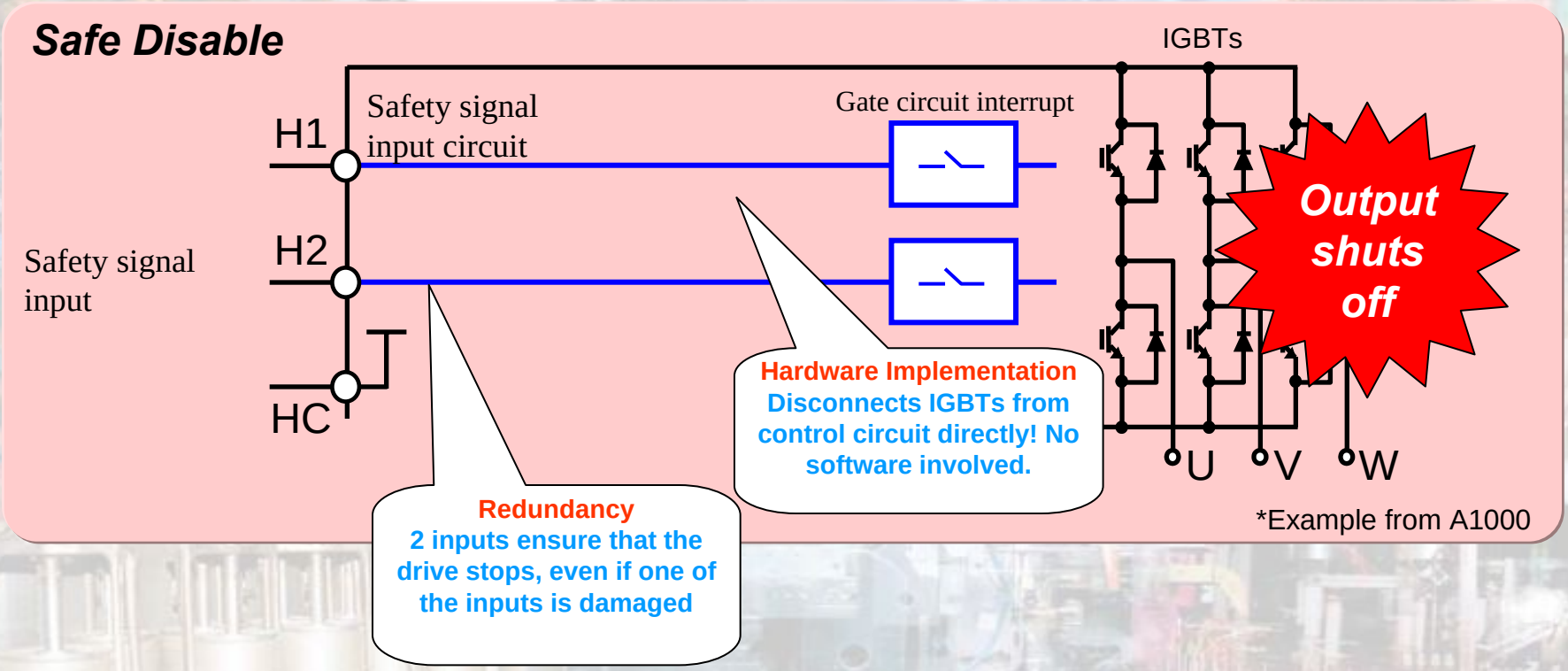
Improved so that a **single fault will not lead to loss of a safety function**. Common mode faults need to be taken into account when the probability of such a fault occurring is significant. Whenever reasonably practical, the single fault should be detected at or before the next demand for the safety function. **All faults are not required to be detected**, thus an accumulation of undetected faults could lead to hazardous situation.

•Category 4

All faults will be detected and there will the **protection against an accumulation of faults** which needs to be specified. The safety-related parts of the control need to be designed so the a single fault does not lead to a loss of safety function and the **single fault will be detected** at or before the next demand for the safety function. This category of safety requires that when faults occur the safety function is always performed and the faults will be detected in time to prevent the loss of the safety function.

Safe Disable (Safe Torque off)

- *Back to hardware base block.*



Safe Disable in V1000

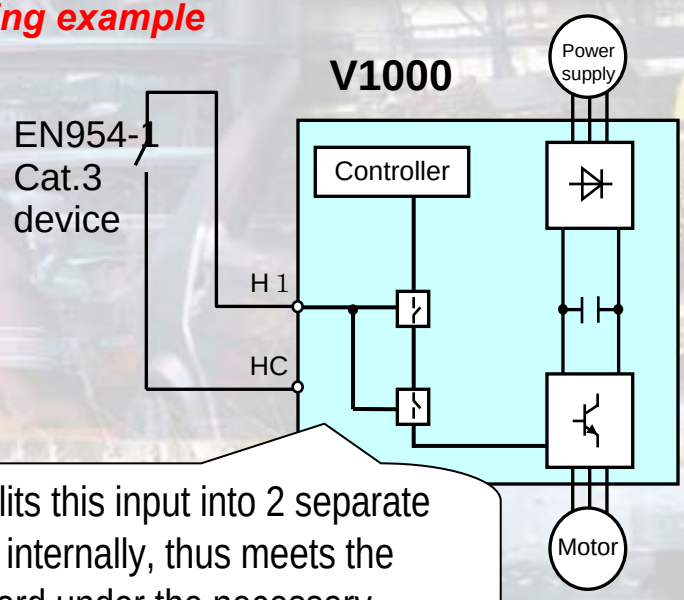
Safe Disable is triggered as soon as the current between terminals H1 and HC is interrupted.

Triggering Safe Disable blocks signals to the output transistors in accordance with safety standards.

Power to the motor is cut off, and the motor coasts.
The operator display reads "Hbb" to indicate that Safe Disable has been activated.

Safe Disable can be used with both induction motors and synchronous PM motors.

Wiring example



V1000 splits this input into 2 separate circuits internally, thus meets the standard under the necessary requirements described in Note1.

***Note that output is shut off within 1 ms.**

- To use the Safe Disable input function, remove the short between H1 and HC (a temporary jumper is placed between the two terminals for shipping).
- A safety switch or other components for safety that ranks above Cat. 3 in EN954-1 can be added to terminals HC and H1.

Note 1
Any enclosures must at least satisfy protective levels defined in IP54.

Remove the jumper from terminals used for Safe Disable.

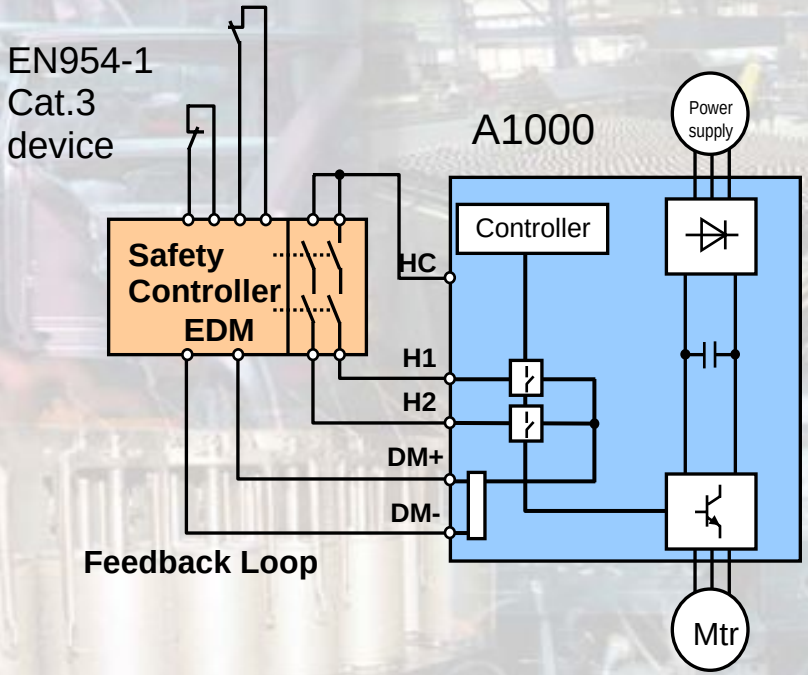
Safe Disable in A1000

A1000 has two Safe Disable input terminals and a single monitor output terminal.
Safe Disable is triggered by interrupting current to terminal H1 or H2 from HC.

Output DM notifies external devices that the Safe Disable feature has been triggered.

The user can therefore expand drive capability by adding a device with an External Device Monitor (EDM) input.

Wiring example



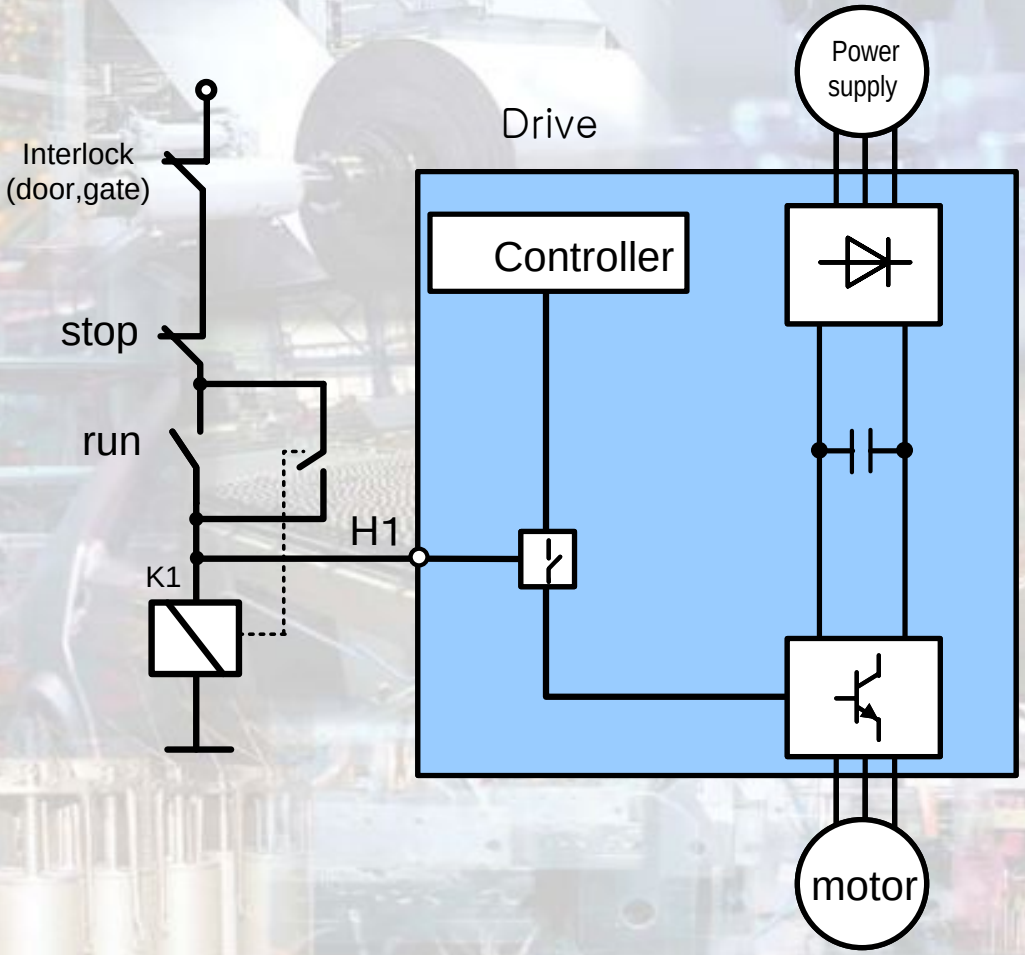
To use the Safe Disable input function, remove the short between H1/H2 and HC (**a temporary jumper is placed between these terminals for shipping**).

A safety switch or safety components that rank above Cat. 3 in EN954-1 can be added to terminals HC and H1 & H2.

Never short the terminals used for Safe Disable.

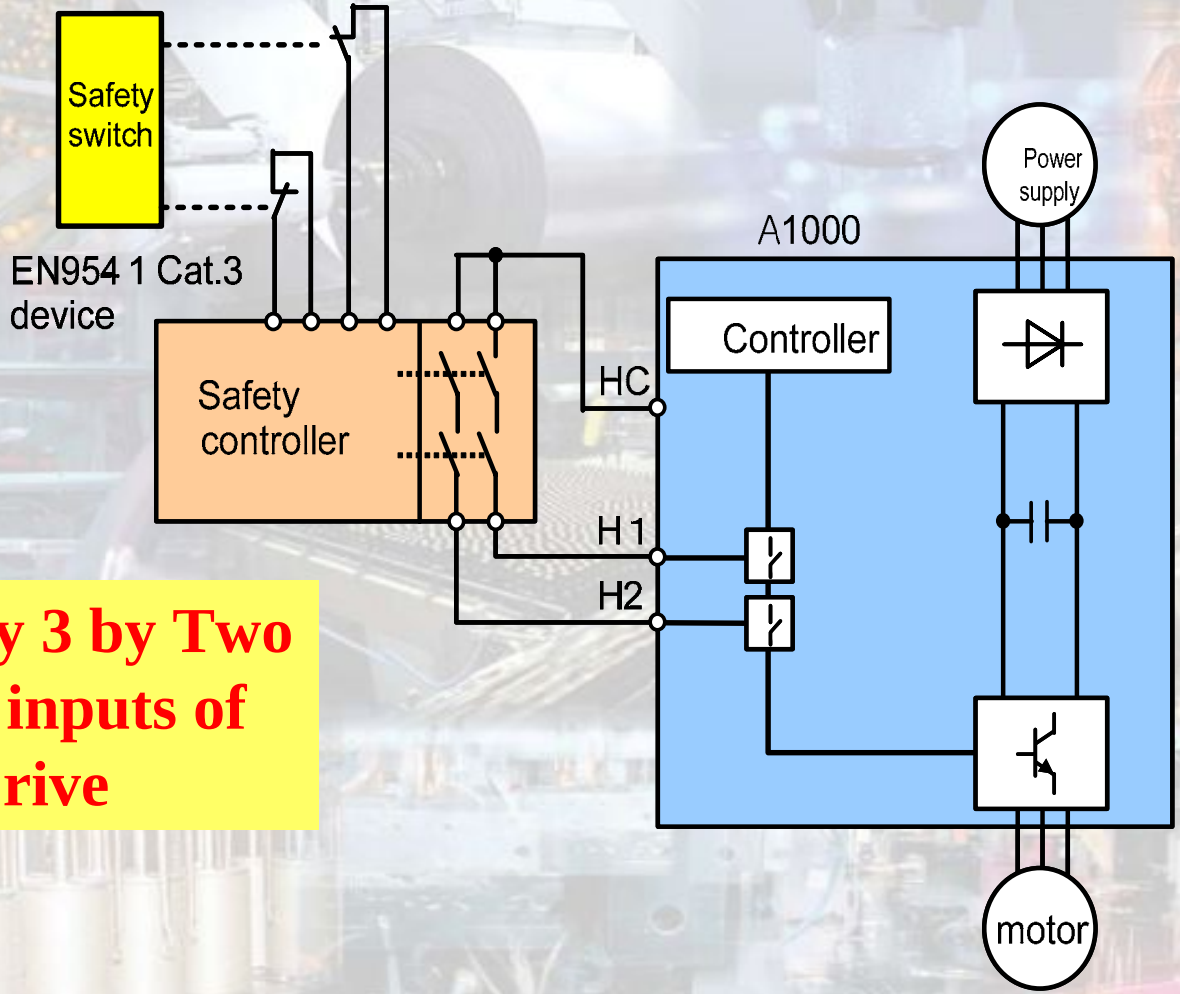
Category 1 Safe Disable

Run/stop with use of well tried components and safety principles



Category 3 Safe Disable

Single fault must not lead to the loss of the safety function

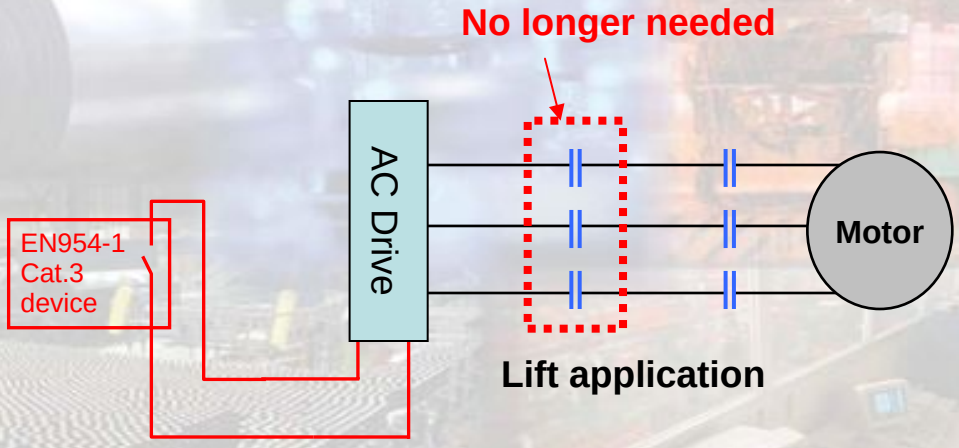


Category 3 by Two Safety inputs of Drive

Lift Example

The benefits of the Safe Disable feature differ by the type of application, as safety requirements vary by the type of machinery.

The two contactors on the output side can be reduced to a single switch.



Note that a safety switch in compliance with EN954-1 Cat. 3 is required.

EN81-3: Safety regulations for lift applications (Part 3: Industrial hydraulic lifts)

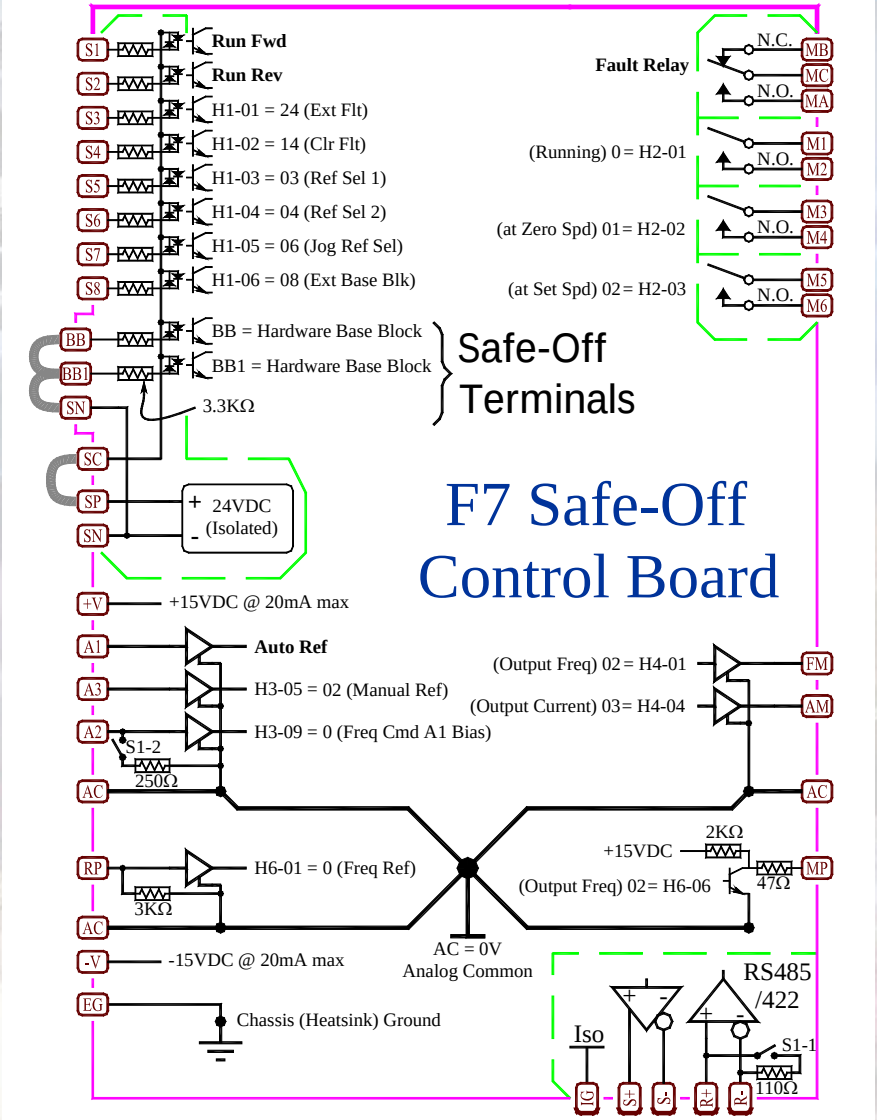
◆EN115: Safety standards for escalator and moving walkway installations

EN201: Engineering safety requirements for the design and construction of plastic and rubber injections molding applications.

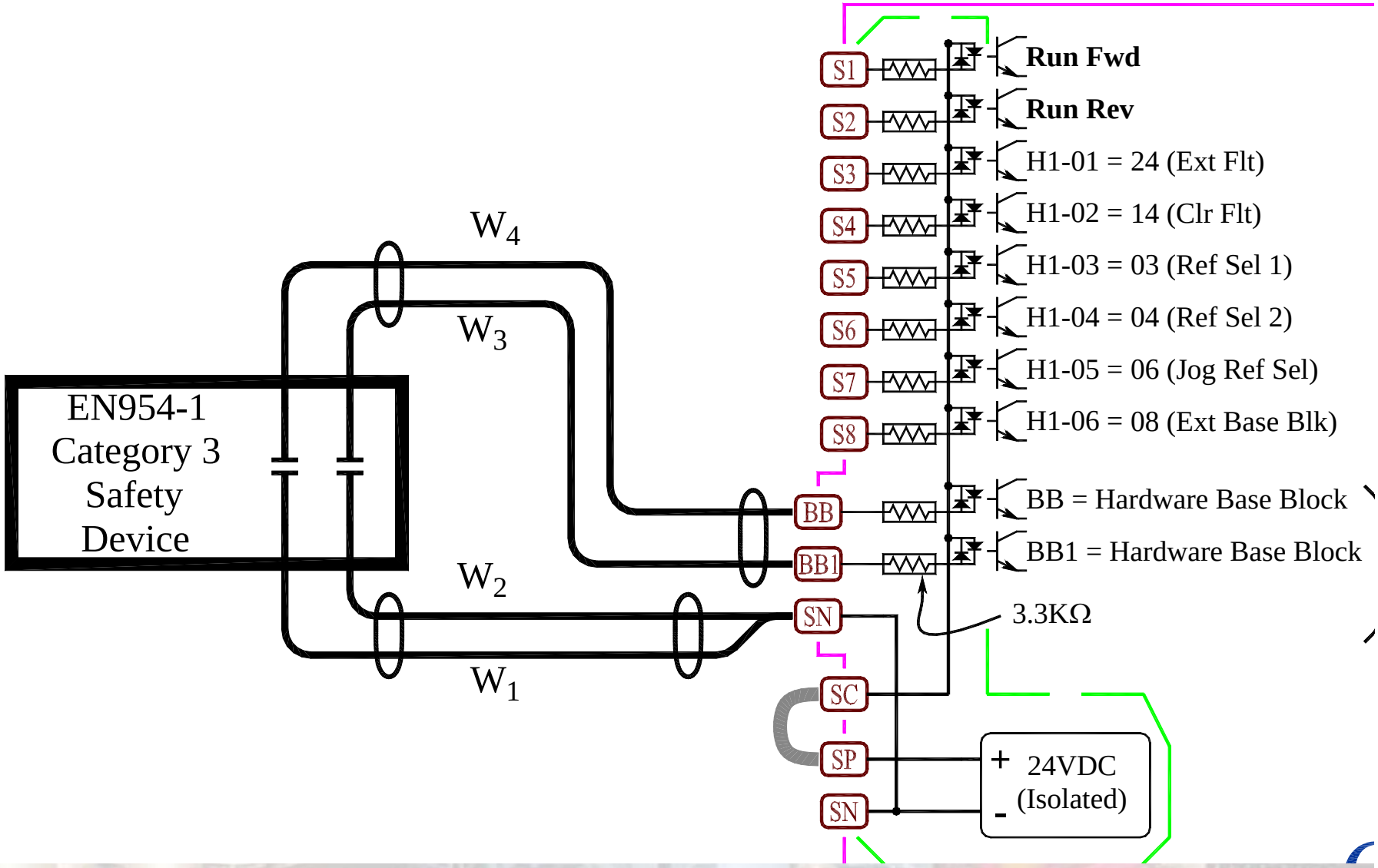
F7 Option

- *For the customer who just can't wait for the A1000*
- *Special F7 with Safe Disable*
- *Requires special Control Board & special I/O Board*

F7 Option


S1
Run Fwd
S2
Run Rev
S3
H1-01 = 24 (Ext Flt)
S4
H1-02 = 14 (Clr Flt)
S5
H1-03 = 03 (Ref Sel 1)
S6
H1-04 = 04 (Ref Sel 2)
S7
H1-05 = 06 (Jog Ref Sel)
S8
H1-06 = 08 (Ext Base Blk)
BB
BB = Hardware Base Block
BB1
BB1 = Hardware Base Block
SN
3.3KΩ
Safe-Off Terminals
SC
SP
SN
+ 24VDC
- (Isolated)
F7 Safe-Off Control Board
Fault Relay
N.C.
MB
MC
N.O.
MA
(Running) 0 = H2-01
M1
N.O.
M2
(at Zero Spd) 01 = H2-02
M3
N.O.
M4
(at Set Spd) 02 = H2-03
M5
N.O.
M6
+V
+15VDC @ 20mA max
A1
Auto Ref
A3
H3-05 = 02 (Manual Ref)
A2
H3-09 = 0 (Freq Cmd A1 Bias)
S1-2
250Ω
AC
(Output Freq) 02 = H4-01
FM
(Output Current) 03 = H4-04
AM
AC
RP
H6-01 = 0 (Freq Ref)
3KΩ
AC
-V
-15VDC @ 20mA max
EG
Chassis (Heatsink) Ground
AC = 0V
Analog Common
2KΩ
+15VDC
(Output Freq) 02 = H6-06
47Ω
MP
RS485
/422
Iso
S1-1
110Ω
IG
S+
S-
R+
R-

F7 Wiring


EN954-1
Category 3
Safety
Device
W4
W3
W2
W1
S1
S2
S3
S4
S5
S6
S7
S8
BB
BB1
SN
SC
SP
SN
Run Fwd
Run Rev
H1-01 = 24 (Ext Flt)
H1-02 = 14 (Clr Flt)
H1-03 = 03 (Ref Sel 1)
H1-04 = 04 (Ref Sel 2)
H1-05 = 06 (Jog Ref Sel)
H1-06 = 08 (Ext Base Blk)
BB = Hardware Base Block
BB1 = Hardware Base Block
3.3KΩ
+ 24VDC
- (Isolated)

F7 Physical Terminals

The End – Any Questions?

Functional Safety

- ***Remember –***
  - ***A Drive is only a Component in the Safety System.***
  - ***Its only responsibility is to turn off the motor when a Safe-Disable input is opened.***