

Health and Safety
Executive

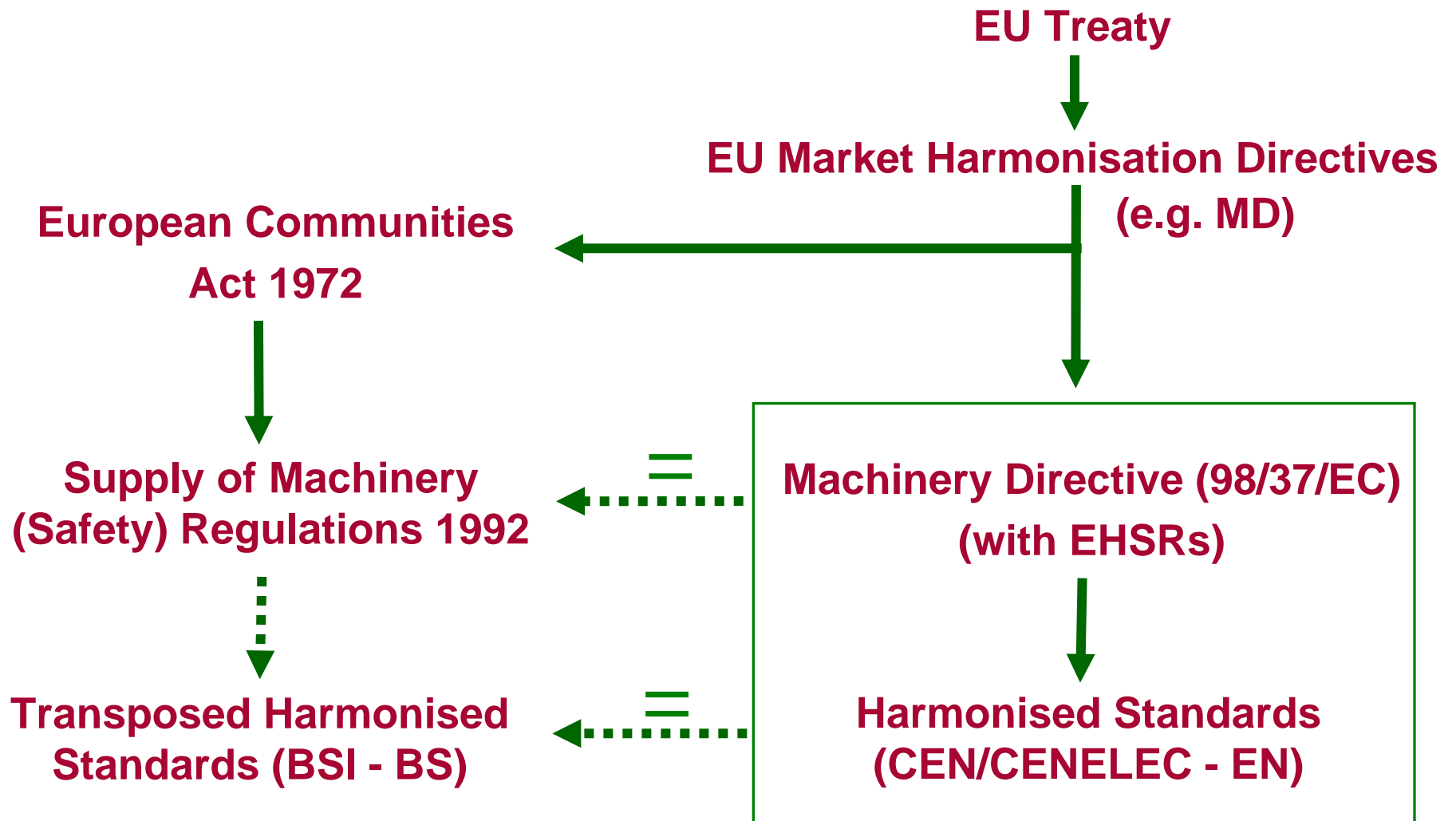


PABIAC SAFETY-RELATED CONTROLS SEMINAR
14TH NOVEMBER 2006
LEEDS, UK

Application of key standards

Philip Parry
HSE Electrical and Control Systems Group

Route into UK legislation of Supply of Machinery (Safety) Regulations 1992



Machinery Directive (98/37/EC)



- **A New Approach Directive**
 - **Essential Health & Safety Requirements (EHSRs)**
 - **Harmonised Standards**
 - Presumption of conformity with specific EHSRs (see Annex ZB/ZZ)

Harmonised Standards

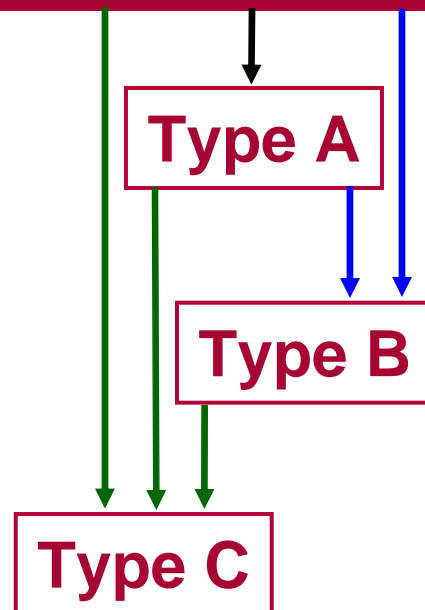


- **European standards bodies (CEN/CENELEC) granted a mandate by the EC to produce ENs that address EHSRs**
- **Listed in EC Official Journal as ‘harmonised’ under the Machinery Directive:**
 - Type A – basic safety (e.g. EN 12100-1 & EN 1050)
 - Type B – generic safety
 - B1 – particular safety aspects (e.g. EN 954-1)
 - B2 – particular safeguards (e.g. EN 1088)
 - Type C – machine safety standards (e.g. EN 1034-1)

Harmonised Standards



Essential Health & Safety Requirements



- **Published by British Standards Institution (BSI) in the UK**
 - Prefix BS EN (or BS EN IEC, BS EN ISO)
 - Withdraw similar scope national standards
 - Use with Supply of Machinery (Safety) Regulations 1992

Type A Standards



Body	Reference	Title of the harmonised standard
CEN	EN 12100-1:2003	Safety of machinery - Basic concepts, general principles for design - Part 1: Basic terminology, methodology
CEN	EN 12100-2:2003	Safety of machinery - Basic concepts, general principles for design - Part 2: Technical principles
CEN	EN 1050:1996	Safety of machinery - Principles for risk assessment

Selected Type B Standards



Body	Reference	Title of harmonised standard
CEN	EN 294:1992	Safety of machinery - Safety distance to prevent danger zones being reached by the upper limbs
CEN	EN 349:1993	Safety of machinery - Minimum gaps to avoid crushing of parts of the human body
CEN	EN 418:1992	Safety of machinery - Emergency stop equipment, functional aspects - Principles for design
CEN	EN 574:1996	Safety of machinery - Two-hand control devices - Functional aspects - Principles for design
CEN	EN 811:1996	Safety of machinery - Safety distances to prevent danger zones being reached by the lower limbs
CEN	EN 953:1997	Safety of machinery - Guards - General requirements for the design and construction of fixed and movable guards
CEN	EN 954-1:1996	Safety of machinery - Safety-related parts of control systems - Part 1: General principles for design
CEN	EN 999:1998	Safety of machinery - The positioning of protective equipment in respect of approach speeds of parts of the human body
CEN	EN 1037:1995	Safety of machinery - Prevention of unexpected start-up

Selected Type B Standards (cont'd)



Body	Reference	Title of harmonised standard
CEN	EN 1088:1995	Safety of machinery - Interlocking devices associated with guards - Principles for design and selection
CEN	EN 1760-1:1997	Safety of machinery - Pressure sensitive protective devices - Part 1: General principles for the design and testing of pressure sensitive mats and pressure sensitive floors
CEN	EN 1760-2:2001	Safety of machinery - Pressure sensitive protective devices - Part 2: General principles for the design and testing of pressure sensitive edges and pressure sensitive bars
CLC	EN 60204-1	Safety of machinery - Electrical equipment of machines - Part 1: General requirements
CLC	EN 61496-1:1997	Safety of machinery - Electro-sensitive protective equipment - Part 1: General requirements and tests
CLC	EN 62061:2005	Safety of machinery – Functional safety of safety-related electrical, electronic, and programmable electronic control systems

Also, although not a harmonised standard.....



BS PD 5304:2005

Guidance on safe use of machinery

- Based on a British Standard in use before Machinery Directive harmonised standards were transposed.
- Revised and updated as a British Standards 'Published Document' for guidance.

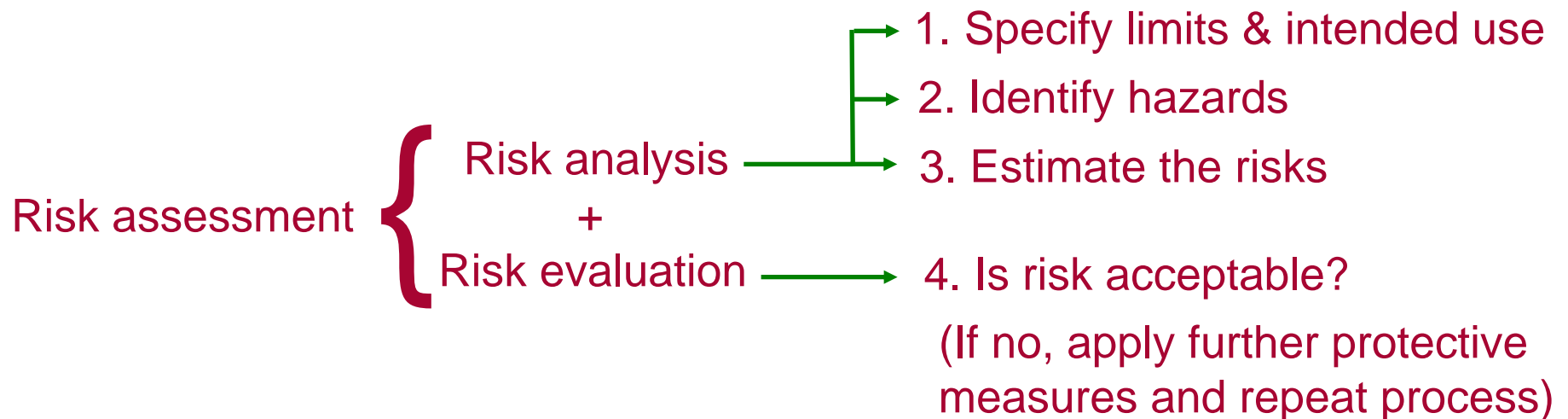
EN 12100

Part 1 – Basic terminology, methodology

Part 2 – Technical principles



- Strategy for risk reduction based on iterative process of conducting a **risk assessment** & applying **protective measures**
- Use in conjunction with **EN 1050:1996 - Safety of machinery - Principles for risk assessment**
- Requirement for risk assessment and risk reduction is embodied in EHSR 1.1.2. of the Machinery Directive.
- Protective measures remove the hazard or reduce its associated risk

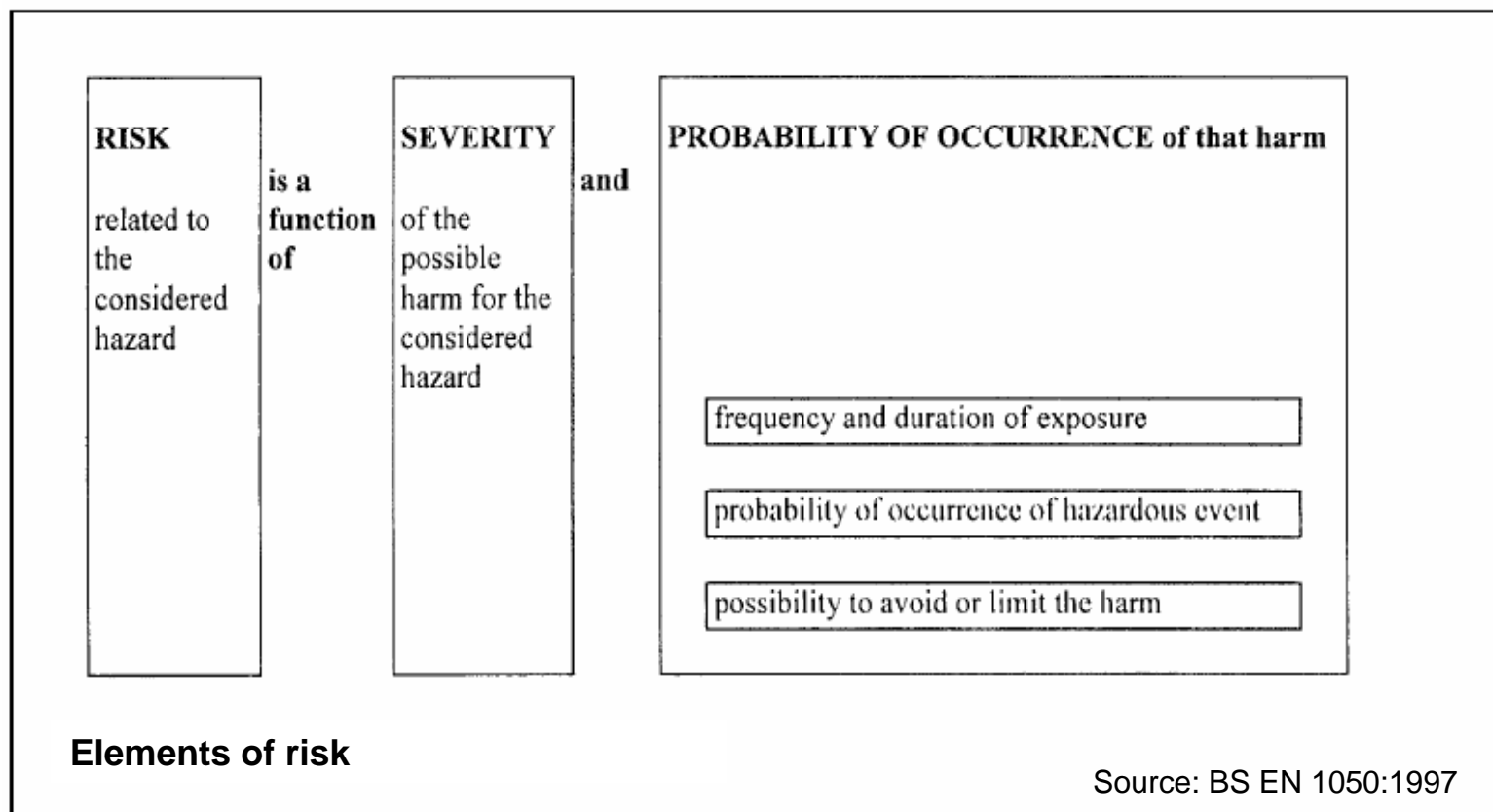


Risk Assessment – EN 1050



-
- Guidance and requirements for the risk assessment process, whereas EN 12100-1/2 covers risk reduction methods.
 - Will be replaced by ISO 14121-1/2.
 - Methodology:
 - Identify limits of machine
 - Identify hazards (list of common ones provided)
 - Identify tasks
 - Estimate risks

Risk Assessment – EN 1050



Risk reduction using the EN 12100 hierarchy of 'Protective Measures'



Inherently safe design measures
EN 12100-2, clause 4

Safeguarding and complementary protective measures
EN 12100-2, clause 5

Information for use
EN 12100-2, clause 6



Inherently safe design measures

Inherently safe design measures



Stage 1 in hierarchy of protective measures for risk reduction

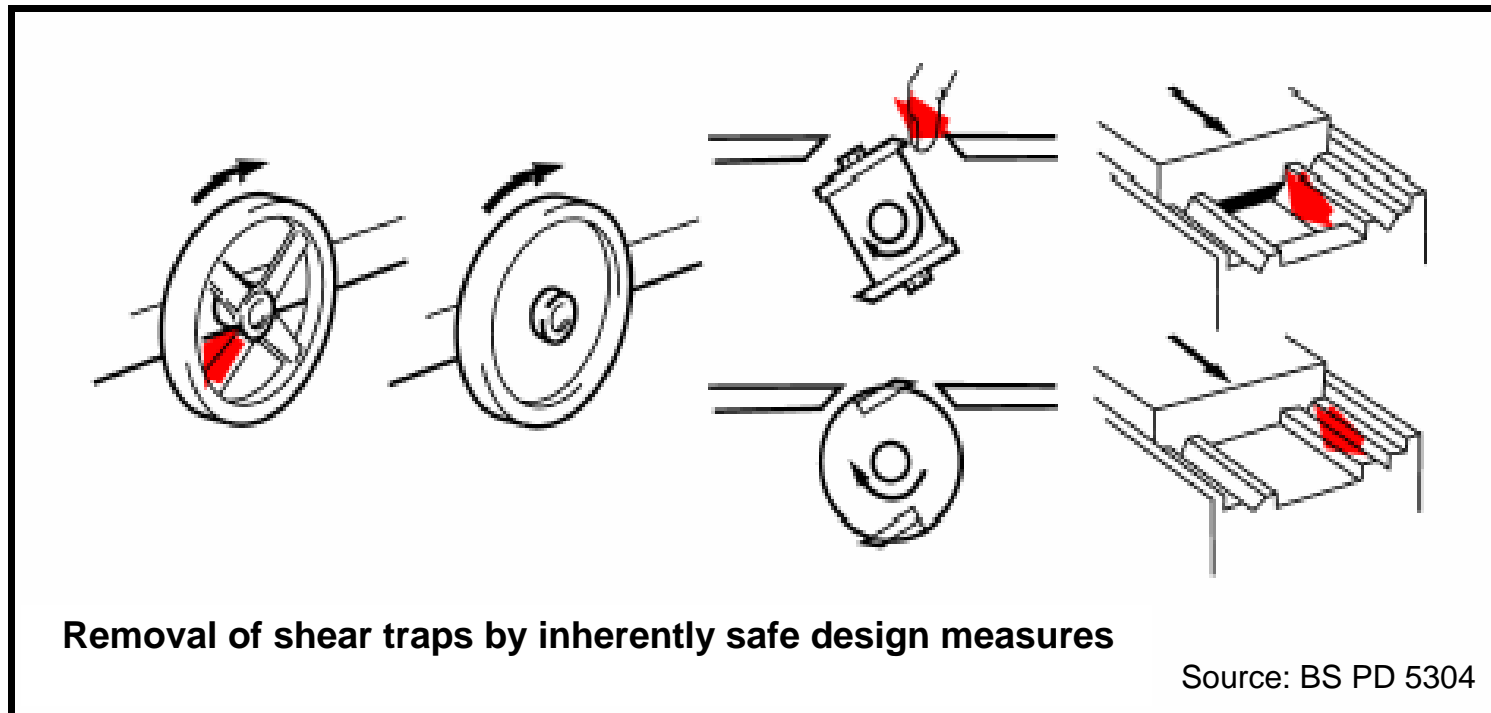
Redesign & substitution....

Avoid sharp edges, corners, protrusions, etc
Increase min gaps to avoid crushing – EN 349
Reduce max gaps to prevent body parts entering – EN 294/811

Reduced forces, pressures, speeds
Less hazardous substances, materials

Intrinsically safe electrical equipment, or
pneumatic/hydraulic

- Geometrical factors
- Physical aspects
- Choice of technology
- Positive mode operation
- Preventing electrical, pneumatic, hydraulic hazards
- Inherently safe design of control systems
- Extent of automation
- Maintainability
- Ease of use



Safeguarding and complementary protective measures

Safeguarding and complementary protective measures



Stage 2 in hierarchy of protective measures for risk reduction

- Safeguarding.....
 - Based on **guards** and **protective devices**
 - Protects persons from hazards that could not reasonably be eliminated, or their associated risks sufficiently reduced, through inherently safe design.
 - Prevents persons from coming into contact with hazards, or reduce hazards to a safe state, before a person can come into contact with them
- Complementary protective measures (e.g. emergency stop) may have to be used in conjunction with safeguards.

Safeguarding

– guards (fixed and movable)



EN 953:1998 – Safety of machinery – General requirements for the design and construction of fixed and movable guards.

EN 294:1992 - Safety of machinery - Safety distance to prevent danger zones being reached by the upper limbs

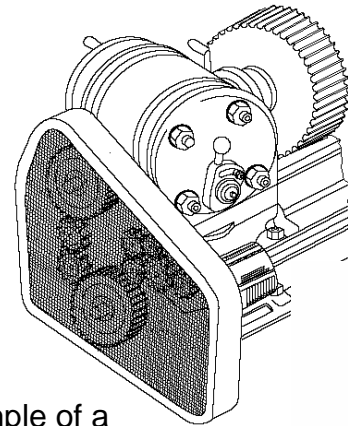
EN 811:1996 - Safety of machinery - Safety distances to prevent danger zones being reached by the lower limbs

- **Fixed guards**

- Enclosing
- Distance

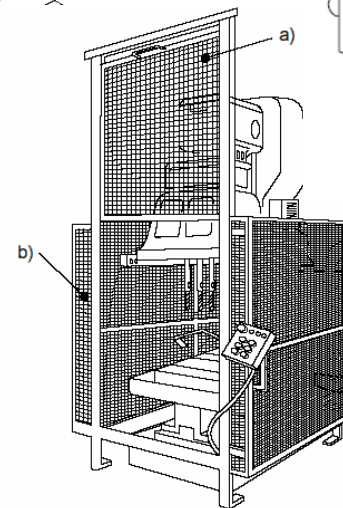
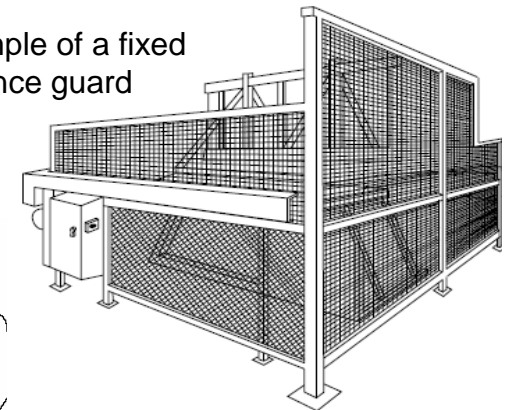
- **Movable guards**

- Self-closing
- Power-operated
- Interlocking



Example of a fixed enclosing guard

Example of a fixed distance guard



Example of a movable guard

Safeguarding

– protective devices



These are safeguards that are not physical guards.

For example:

- **Interlocking device**
- Enabling device
- Hold-to-run control device
- Two-hand control device
- Pressure sensitive mats and floors
- Light curtains and laser scanners
- Mechanical restraint device
- Limiting device
- Limited movement control device

Safeguarding

– movable guards



- **Generally used in conjunction with an interlocking device, which interacts with the machine's power supply or control system**
 - Power interlocking
 - Control interlocking
- **Consider whether interlocking is adequate for preventing an unexpected start-up of the machine when a movable guard is open?**
 - refer to risk assessment
 - nature of task - cleaning, setting, adjusting, etc
 - full isolation and energy dissipation may be required
 - EN 1037 and EN 60204-1
- **'Interlocking guard' or 'Interlocking guard with guard locking'**
 - stopping time relative to access time

Safeguarding –interlocking



EN 1088:1995 - Safety of machinery - Interlocking devices associated with guards - Principles for design and selection

- Types of interlocking devices
- Installation considerations
- Failure modes
- Resistance to defeat
- Etc..

Types of interlocking devices



-
- Mechanically actuated detectors
 - cam-operated detectors
 - tongue-operated detectors
 - Non-mechanically actuated detectors
 - magnetically actuated switches
 - electronic proximity switches
 - Captive-key or trapped-key systems
 - Mechanical interlocking
 - Plug and socket systems

Interlocking guard



-
- the hazards "covered" by the guard cannot operate until the guard is closed;
 - if the guard is opened while hazards are present, a command is given to bring the hazards to a safe state;
 - when the guard is closed, the hazards "covered" by the guard can operate, but closure of the guard does not normally by itself start the hazardous machine functions.

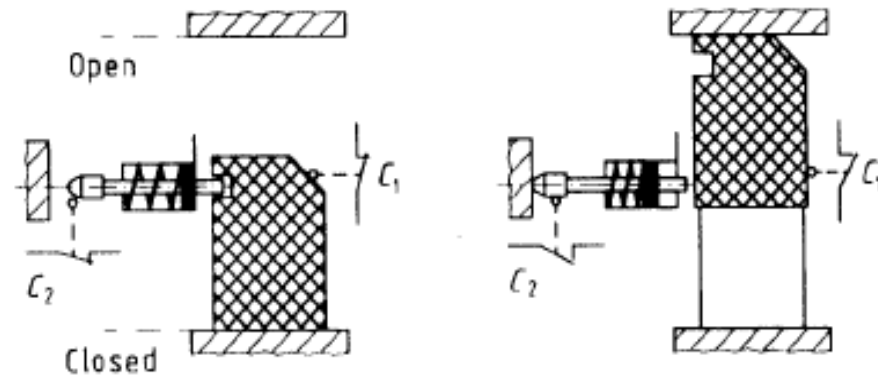
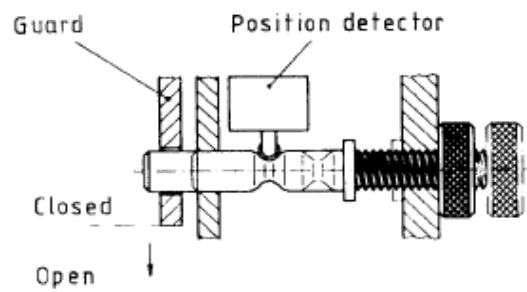
Interlocking guard with guard locking



- hazards "covered" by the guard cannot operate until the guard is closed and locked;
- the guard remains closed and locked until the hazards "covered" by the guard have been brought to a safe state;
- when the guard is closed and locked, the hazards "covered" by the guard can operate, but closure of the guard does not normally by itself start the hazardous machine functions.

Interlocking device with guard locking

- When stopping time would otherwise exceed access time.
- **Unconditional locking** or **conditional locking**



- Possible to open at any time, but time required is of sufficient duration for hazard to disappear
- Fixed time delay
- Possible to open only when a condition is fulfilled, e.g. the moving parts have stopped
- Fixed time delay or timed until hazard disappearance

Interlocking devices - principle of positive mode actuation



Positive mode actuation

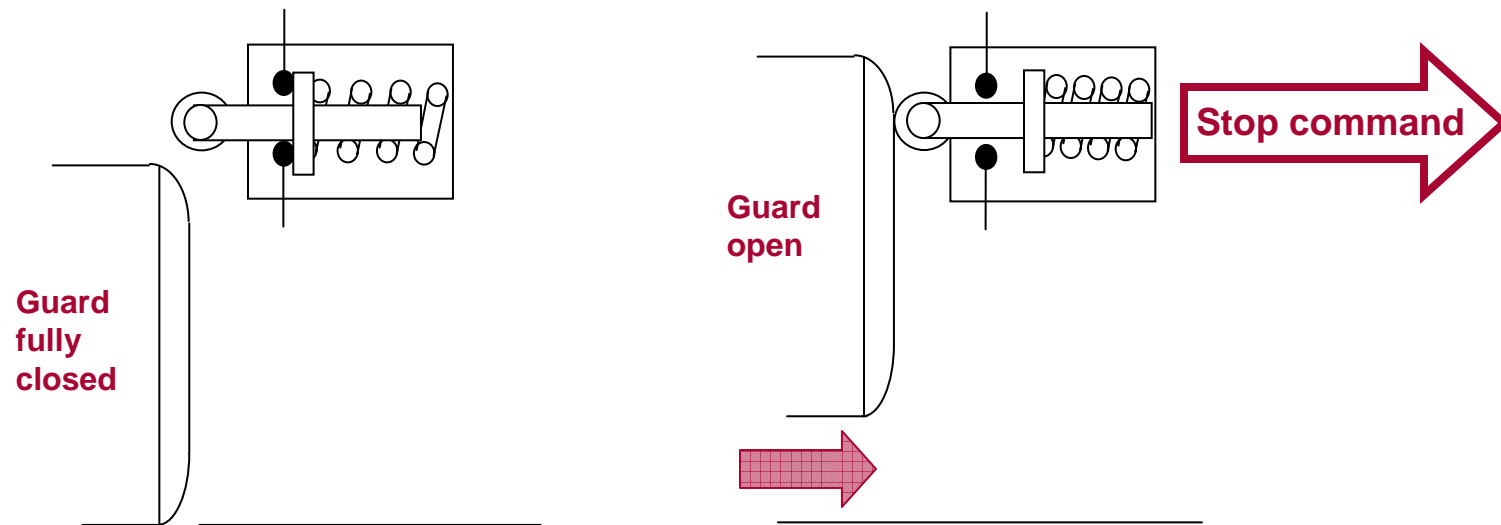
- If a moving mechanical component inevitably moves another component along with it, either by direct contact or via rigid elements, the second component is said to be actuated in the positive mode (or positively) by the first one.

Positive opening operation of contact elements

- Achievement of contact separation as the direct result of a specified movement of the switch actuator through non-resilient members (e.g. not dependent upon springs).

Interlocking devices - principle of positive mode actuation

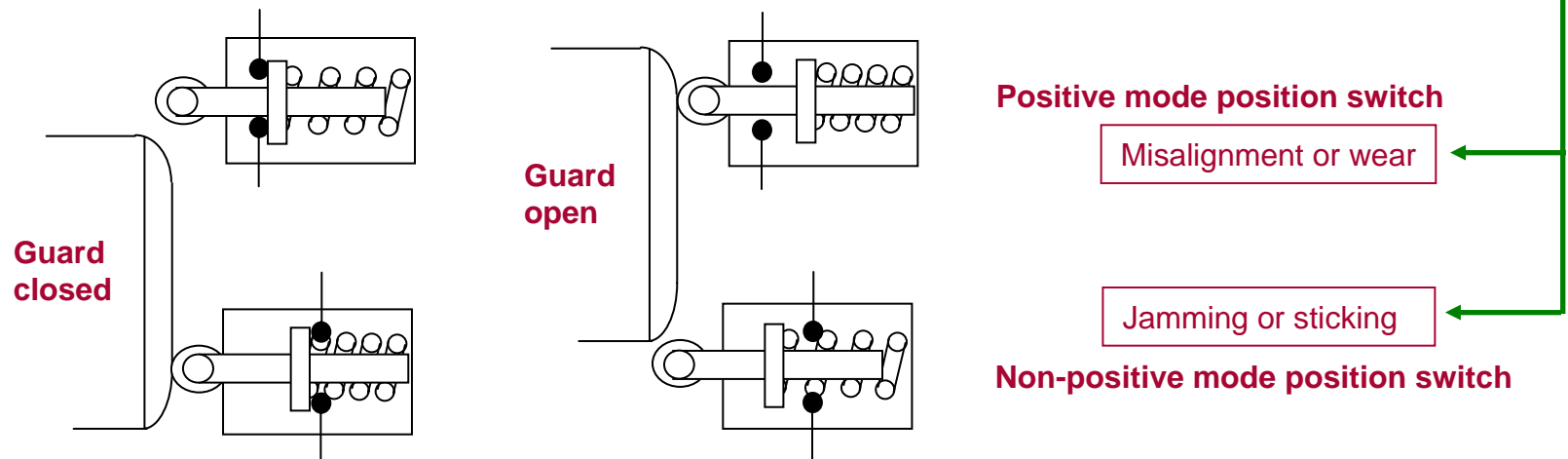
- E.g. illustrated for a cam-operated detector:



- Stem of positive mode position switch is held depressed against the spring force when the guard is any position other than fully closed. Contacts are positively (directly) opened by the guard's cam.
- Final closing movement of the guard releases the switch stem, allowing the spring force to non-positively close the contacts.

Non-positive mode actuation

- **Cam operated non-positive mode detector** in conjunction with a positive mode detector
 - one detector with normally-closed contacts
 - other detector with normally-open contacts
 - complementary failure modes (no common cause failures) *



- **Non-mechanically actuated detectors**
 - non-positive mode actuation
 - redundancy and monitoring of contact elements

Interlocking devices - application



- **Interlocking devices should be selected and installed with regard to minimising the possibility of defeat and failure, and the overall safeguard should not unnecessarily impede production tasks.**
 - devices fastened securely in a (fixed) place and requiring a tool to remove or adjust;
 - coded devices or systems, e.g. mechanically, electrically, magnetically or optically;
 - physical obstruction or shielding to prevent access to the interlocking device when the guard is open;
 - the support for devices shall be sufficiently rigid to maintain correct operation;

Interlocking devices - application



-
- movement produced by actuation shall remain within the specified operating range of the device to ensure correct operation and/or prevent overtravel;
 - displacement of the guard before the device changes state shall not compromise the protective effect of the guard (reach into danger zone);
 - devices shall not be used as mechanical stops;
 - the devices shall be located and, if necessary, protected so that damage from foreseeable external causes is avoided;
 - appropriate redundancy and monitoring.

Other protective devices



-
- Fixed or movable guards are not always practical
 - Very frequent access situations
 - Not a physical barrier
 - Usually require (and form part of) a safety-related control system
 - Not suitable if:
 - Machine can eject materials or components
 - Risk of injury from thermal or other radiation
 - Excessive noise levels
 - Environment impedes device functionality
 - Often use in conjunction with guards

Other protective devices



-
- Enabling device
 - Hold-to-run control device
 - Two-hand control device (EN 574)
 - Pressure sensitive mats and floors (EN 1760-1)
 - Light curtains and laser scanners (EN 61496)
 - Mechanical restraint device
 - Limiting device
 - Limited movement control device

IEC TS 62046 provides extensive guidance on application of pressure sensitive mats, laser scanners and light curtains, whilst HSG 180 provides guidance on the application of light curtains.

EN 999:1998 - Safety of machinery – The positioning of protective equipment in respect of approach speeds of parts of the human body



- Determines suitability and position of light curtains, pressure sensitive mats, etc.
- Based on an equation of motion:

$$\mathbf{S = KT + C}$$

- S** - minimum distance, in millimetres, from the danger zone to the detection point, line, plane or zone;
 - K** - parameter in millimetres per second, derived from data on approach speeds of the body or parts of the body;
 - T** - overall system stopping performance in seconds;
 - C** - additional distance in millimetres, based on intrusion towards the danger zone prior to actuation of the protective equipment.
- Will have been applied in some Type C standards
 - Iterative calculation and design

Stopping time can vary due to:

- time taken for the protective device to operate;
- time delays introduced by the control system (consider effect of programmable or networked technologies);
- time taken for the machine primary control element (e.g. contactor) to respond
- varying inertia of the moving parts (speeds, loads etc);
- degeneration of parts (brakes or clutch wear etc);

Protective Measures - recap

Hierarchical application of:

- Inherently safe design
- Safeguarding and complementary protective measures
- **Information for use** - utilised by the user to implement:

- Organisation
 - Safe working procedures
 - Supervision
 - Permit-to-work systems
- Provision and use of additional safeguards
- Use of personal protective equipment
- Training
- Etc..

A green bracket groups the 'Information for use' items. A vertical box to the right of the bracket contains the text 'Not hierarchical' written vertically.

Not hierarchical

Safety-related control systems of machinery



-
- When the protective measures that reduce risk to an acceptable level include protective devices, such as interlocking devices or light curtains, these generally interface with the machine's control system.
 - Risk reduction is being performed by a control system
 - Safety-related control systems
 - Safety functions
 - Functional safety

Harmonised standards relevant to safety-related control systems of machinery



EN 60204-1 - Safety of machinery – Electrical equipment of machines - Part 1: General requirements

EN 954-1 – Safety of machinery – Safety-related parts of control systems – General principles for design

EN 62061 - Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems

Essential Health & Safety Requirements



- 1.1 General
- 1.2 Controls
 - **1.2.1 Safety and reliability of control systems**
 - 1.2.2 Control devices
 - 1.2.3 Starting
 - 1.2.4 Stopping device (including e-stop)
 - 1.2.5 Mode selection
 - 1.2.6 Failure of the power supply
 - **1.2.7 Failure of the control circuit**
 - 1.2.8 Software
- 1.3 Protection against mechanical hazards
- 1.4 Guards and protection devices
- 1.5 Protection against other hazards (*inc. elec.*)
- 1.6 Maintenance (*maintainability of machine*)

Safety-integrity of machinery control systems



- Machinery Directive EHSRs:
 - **1.2.1 – Safety and reliability of control system**
 - **1.2.7 – Failure of the control circuit**
- Concerned with safety-related control systems that implement safety functions of machines
- Addressed by 2 current harmonised standards:

BS EN 954-1:1997



Safety of machinery –
Safety related parts of control
systems – Part 1. General
principles for design

BS EN IEC 62061:2005



Safety of machinery –
Functional safety of safety-related
electrical, electronic and programmable
electronic control systems

A few words on.....



Functional Safety

&

Power Drive Systems

Terminology.....



PDS - adjustable speed electrical Power Drive System

PDS(SR) - PDS that is suitable for use in a safety-related application

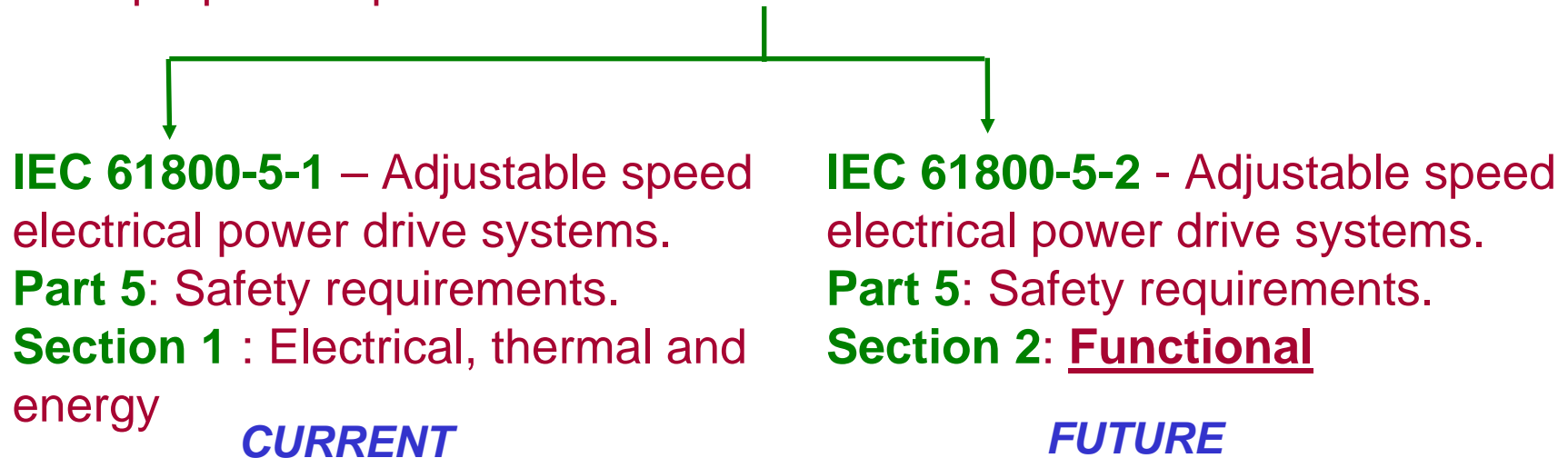
PDS(SR)s are emerging because....

- Increasing automation and use of PDSs in general
- Control systems increasingly relied upon for overall safety
- Demand for safety functions based on the typical functions offered by a PDS

PDS(SR)s



- Range of safe stopping, holding and motion control functions
- Can eliminate standstill/speed monitors, limit switches, position cams, contactors, etc..
- But complex safety functions require complex E/E/PE technology
- Product standard based on IEC 61508 therefore being developed
- UK proposed split of draft **IEC 61800-5**



IEC 61800-5-2



-
- Product standard for PDS(SR) functional safety considerations, based on IEC 61508
 - IEC Standard by mid-2007 – intention is for adoption by CENELEC and harmonisation to the Machinery Directive
 - Considers E/E/PE technology of all complexity – including electronic and programmable electronic (considers systematic failures)
 - Requirements and recommendations for design, development, integration and validation of a PDS(SR)
 - Applicable to a product when:
 - Functional safety (of a PDS) is claimed
 - High demand or continuous mode of operation
 - Max SIL*3 capability (*Safety Integrity Level)
 - PDS(SR)s considered to be:
 - Subsystems of higher level safety-related systems (e.g. IEC 62061)
 - Contributing to risk reduction for particular safety functions

IEC 61800-5-2



As IEC 61800-5-2 will be a product standard for PDS(SR) manufacturers, users of PDS(SR)s will need to:

- Carry out a hazard and risk analysis for the application
- Identify all safety functions required and required safety integrity for each
- Interface the PDS(SR) with other subsystems and consider the validity of signals and commands from these
- Select a PDS(SR) that provides appropriate:
 - Safety functions
 - Safety integrity (SIL Capability & PFH_D)
- Design, integrate and validate the overall safety-related control system - hardware, software, parameterisation, etc..

Simply using a ‘*safe drive*’ in an application does not necessarily make that application safe!

Safety functions of a PDS(SR)



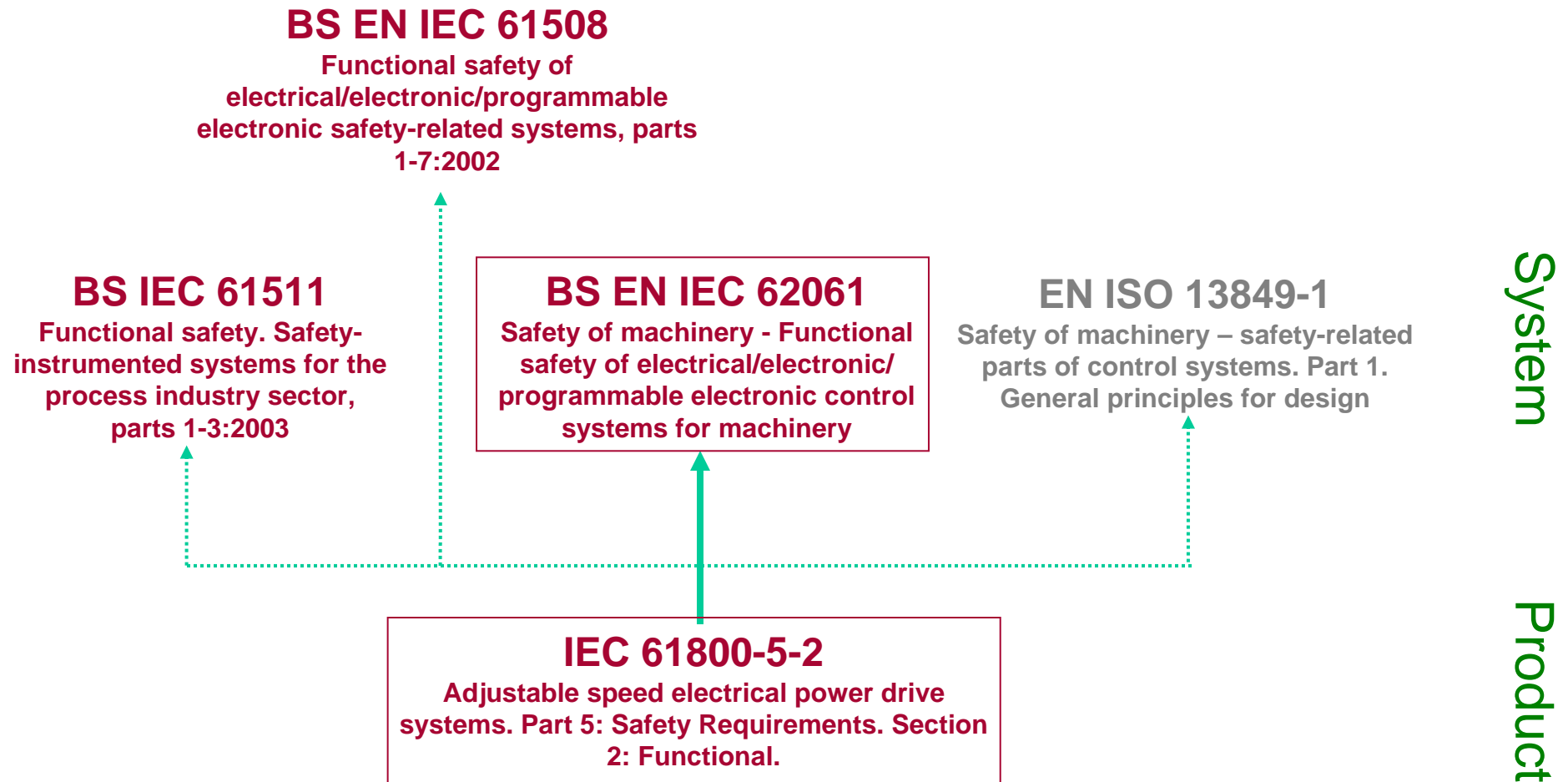
..... functions with a specified safety performance to be implemented in whole or in part by a PDS(SR), which are intended to maintain the safe condition of the installation or prevent hazardous conditions arising at the installation (IEC 61800-5-2)

SIL or SIL Capability & PFH_D

Typical safety functions of PDS(SR)s:

- Safe Torque Off
- Safe Stop 1
- Safe Stop 2
- Safe Operating Stop
- Safely-Limited Speed
- Safe Speed Range
- Safely-Limited Acceleration
- Safe-Acceleration Range
- Safely-Limited Torque
- Safe Torque Range
- Safely Limited Position
- Safely-Limited Increment
- Safe Direction
- Safe Motor Temperature
- Safe Brake Control
- Safe Cam
- Safe Speed Monitor

Relevance to machinery control system designers, system integrators, etc.

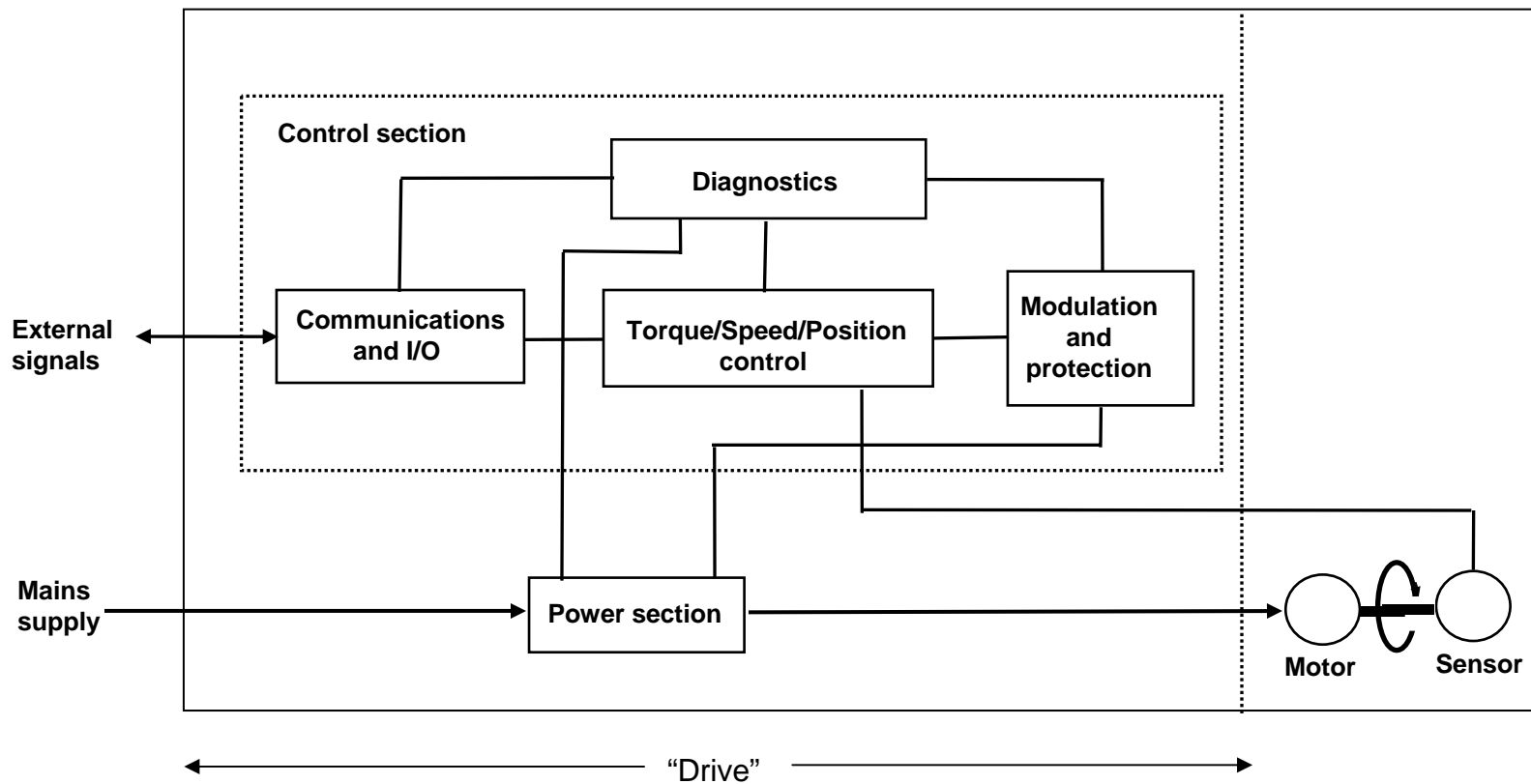




Thank You

Questions?

General architectural model of a PDS

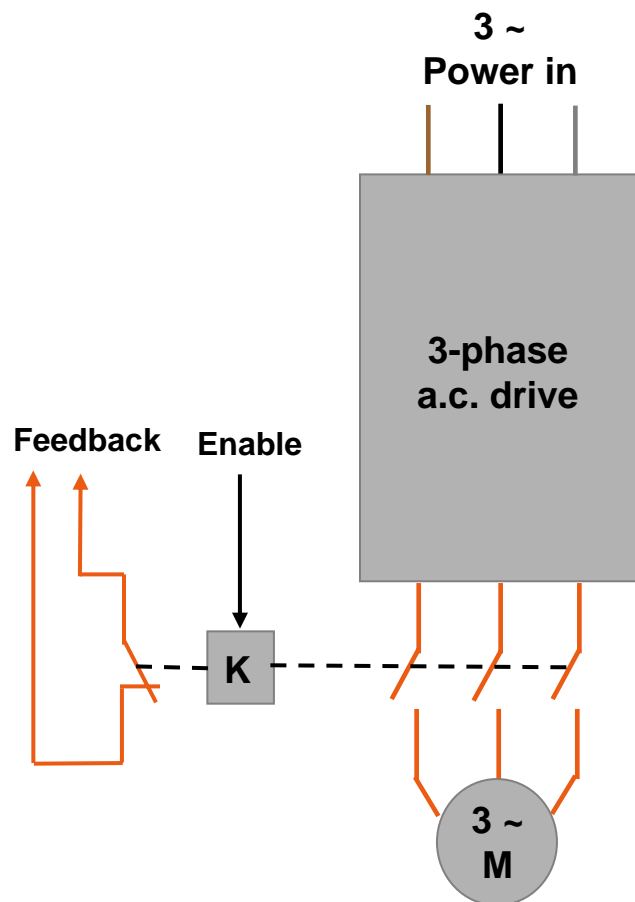


Removal of power to prevent an unexpected start-up – Safe Torque Off (STO)



- A fundamental safety function – mechanical hazards
- Isolation device required?
- Non-safety-related (conventional) PDS with safety-related control of external contactor(s)
- PDS(SR) with integrated safety function(s)

Conventional PDS incorporating safety-related control of external contactor(s)



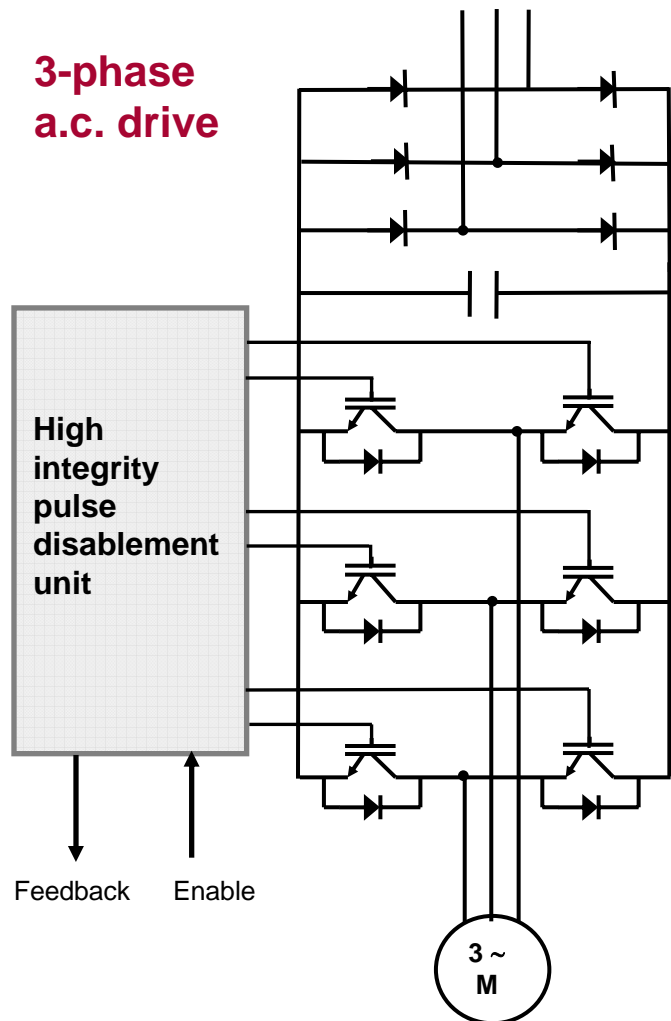
- Electromechanical contactor(s)
 - Location – input/output?
 - Premature opening – arcing and uncontrolled stop?
- Low complexity external control systems – comply with **EN 954 – 1**.
- Limited (monitoring) range of safety-functions, with no contribution from PDS
 - Safe Torque Off (to disable at rest)
- Safety-related stopping functionality:
 - Safe Torque Off (uncontrolled stop) (IEC 60204-1 cat 0 stop)
 - Safe Torque Off after a controlled stop (IEC 60204-1 cat 1 stop)

Controlled stop with Safe Torque Off using conventional PDS and output contactor(s)



1. Command the drive to perform a rapid controlled deceleration
 - No safety integrity
 - Drive retains motion control
2. When motion has ceased (time delay 1), switch off power semiconductors
 - No safety integrity
3. When power semiconductors are off and motor current has decayed (time delay 2), open output contactor(s)
 - Safety integrity - external safety-related control system including contactor(s)

PDS(SR) with integrated Safe Torque Off safety function



- Typically use high integrity disablement of power semiconductor firing pulses
- Offers 'contactorless' Safe Torque Off
- Power semiconductors v contactors
 - Internal diode paths – prevent arcing
 - Power semiconductor switches – effect of leakage currents?
 - Short-circuit failures of power semiconductors?
- Complexity of E/E/PE technology used in disablement unit - EN 954–1, IEC 61508, IEC 61800-5-2 (future).

PDS(SR) with integrated Safe Torque Off safety function



However....

- May be no safety-related motion control – only the disablement of power semiconductors may have any safety integrity.
- Other functions performed may not have any safety integrity
- Deceleration to standstill may have no safety integrity
- Premature disablement (whilst motor rotating) – uncontrolled stop

