

Health and Safety
Executive



PABIAC SAFETY-RELATED CONTROLS SEMINAR
7TH/14TH NOVEMBER 2006
SWINDON/LEEDS, UK

Functional Safety & Power Drive Systems

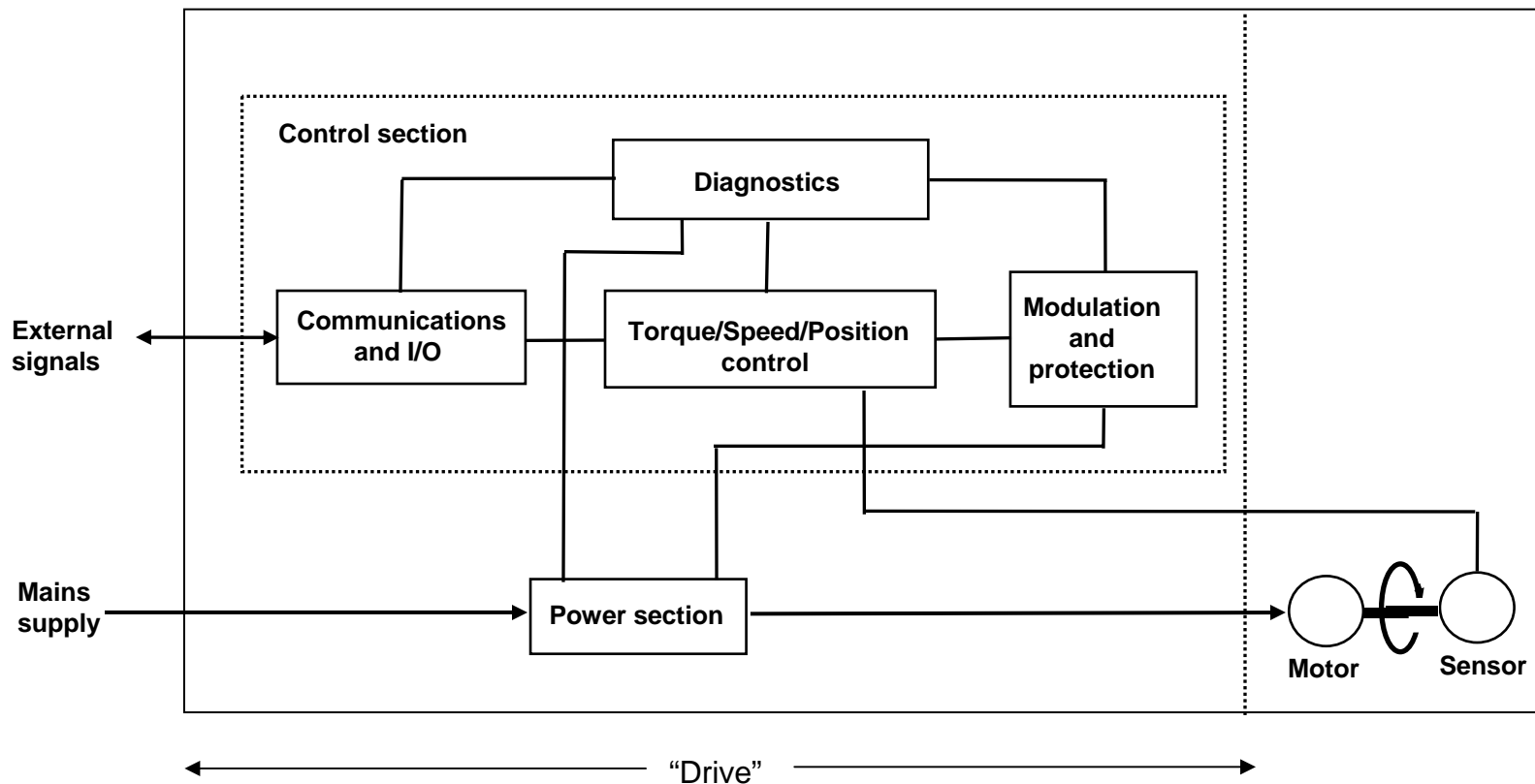
Philip Parry
HSE Electrical and Control Systems Group

Some terminology.....



-
- PDS - adjustable speed electrical Power Drive System
 - PDS(SR) - PDS that is suitable for use in a safety-related application

General architectural model of a PDS



Background



The ability of PDSs to perform safety functions is an issue because of

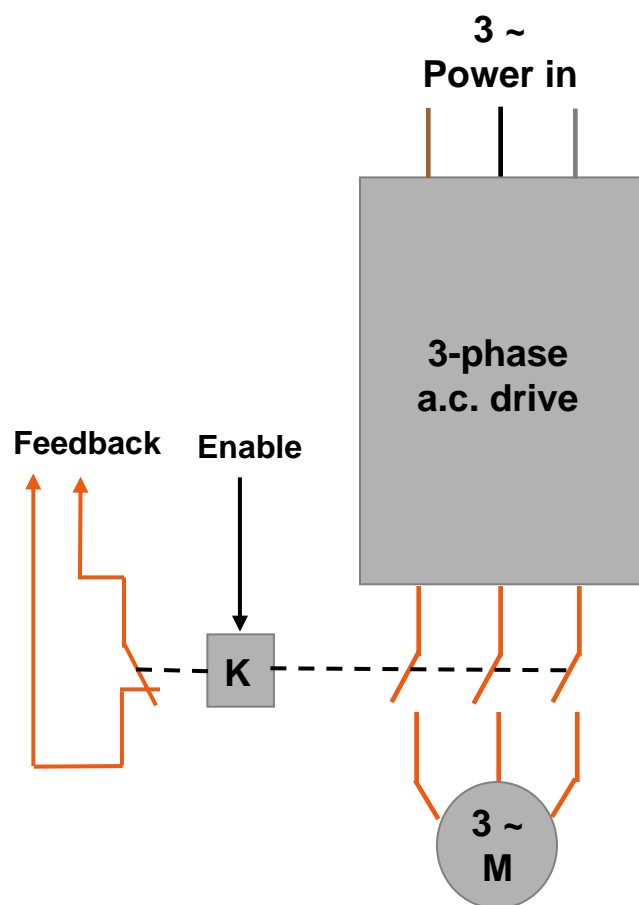
- Increasing automation
- Increasing use of PDSs
- Control systems relied upon for overall safety
- Capability/complexity of PDSs

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)



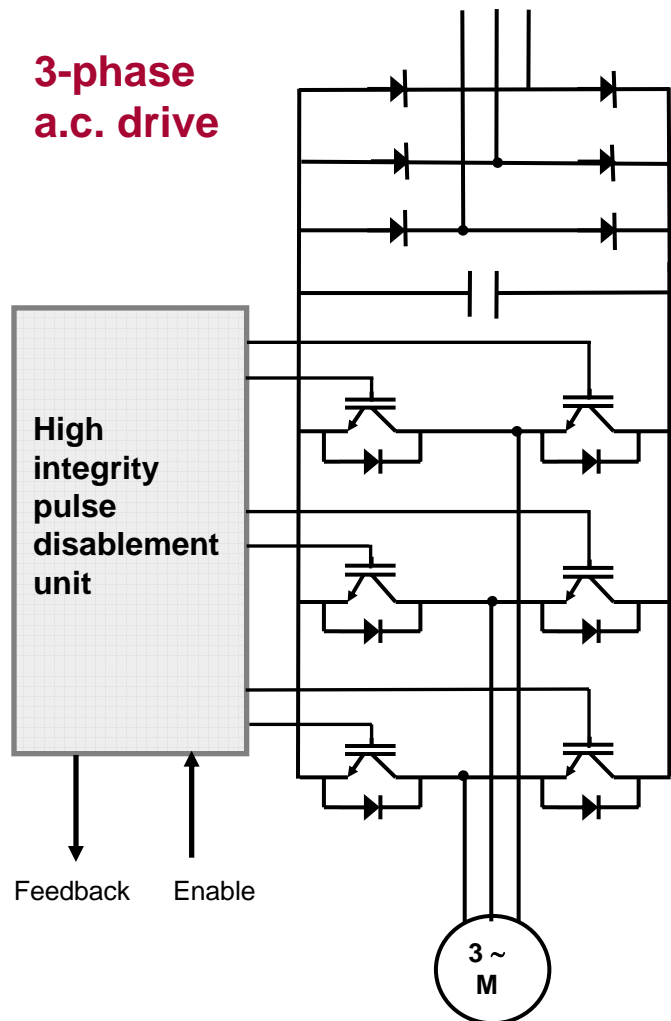
- Electromechanical contactor(s)
 - Location – input/output?
 - Premature opening – arcing and uncontrolled stop?
- Low complexity external control systems – comply with **EN 954 – 1**.
- Limited (monitoring) range of safety-functions, with no contribution from PDS
 - Safe Torque Off (to disable at rest)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



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
 - Diodes – 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

PDS(SR) with full motion control safety functions



- Safe stopping, holding and motion control functions
- Eliminate standstill/speed monitors, limit switches, position cams, contactors, etc..
- Complex safety functions require complex E/E/PE technology
- Development of product standard based on IEC 61508
- UK proposed split of draft **IEC 61800-5**

IEC 61800-5-1 – Adjustable speed electrical power drive systems.
Part 5: Safety requirements.
Section 1 : Electrical, thermal and energy

CURRENT

IEC 61800-5-2 - Adjustable speed electrical power drive systems.
Part 5: Safety requirements.
Section 2: **Functional**

FUTURE

IEC 61800-5-2



-
- PDS(SR) safety-related considerations based on IEC 61508
 - Currently progressing to FDIS, International Standard by mid-2007
 - 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
 - Contributing to risk reduction for particular safety functions

IEC 61800-5-2



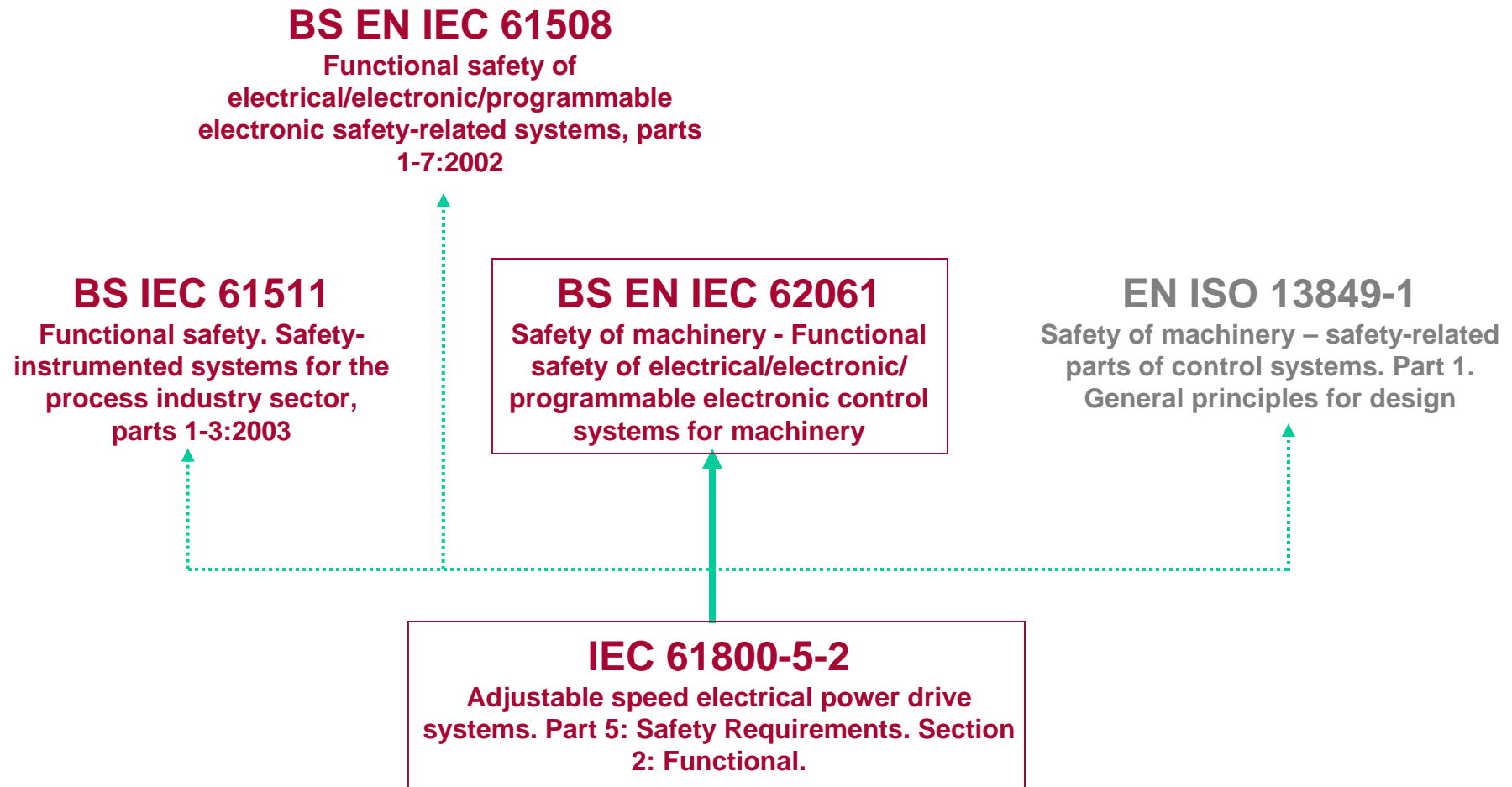
IEC 61800-5-2 is for manufacturers of PDS(SR)s, not users.

Users of PDS(SR)s are responsible for:

- Hazard and risk analysis of the application
- Identifying safety functions required and allocating SILs to each
- Other subsystems and the validity of signals and commands from them
- Selecting a PDS(SR) with appropriate capabilities
- Designing appropriate safety-related control systems (hardware, software, parameterisation, etc)

Using a ‘*safe drive*’ in an application does not necessarily make the application safe!

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



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 (CDV IEC 61800-5-2)

SIL or SIL Capability & PFH

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