ICALEPCS 2015
International Conference on Accelerator & Large Experimental Physics Control Systems

Building an Interlock: Comparison of Technologies for Constructing Safety Interlocks

Melbourne, Australia
17-23 October 2015

T. Hakulinen, F. Havart, P. Ninin, F. Valentini –
CERN, Geneva, Switzerland

Interlocks are an important feature of both personnel and machine protection systems for mitigating risks inherent in operation of dangerous equipment. The purpose of an interlock is to secure specific equipment or entire systems under well defined conditions in order to prevent accidents from happening. Depending on specific requirements for the level of reliability, availability, speed, and cost of the interlock, various technologies are available. We discuss different approaches, in particular in the context of personnel safety systems, which have been built or tested at CERN during the last few years. Technologies discussed include examples of programmable devices, PLCs and FPGAs, as well as wired logic based on relays and special logic cards.

Safety systems

Safety system components:
- **Sensors** – collection of data on measurable conditions important for safety
- **Actuators** – manipulation of important safety equipment when necessary
- **Interlock** – logic solver for computing the safety logic

Safety system types:
- **Personnel protection systems (PPS)** – protection of humans
- **Machine protection systems (MP)** – [in accelerator world] protection of equipment and the immediate surroundings
- **Nuclear plant safety systems** – protection of public and environment
- **Process industry safety systems** – idem.

Basic requirements for safety systems:
- **Reliability** – must be able to trust that the system will function when solicited
- **Simplicity** – should be able to easily understand the functionality
- **Speed** – system must be able to react fast enough to danger

Principles of safety engineering

Safety engineering standards [1]:
- **IEC 61508** – Functional safety of electrical/electronic/programmable electronic safety-related systems
- **IEC 61511** – Functional safety – Safety instrumented systems for the process industry sector
- **IEC 61513** – Nuclear power plants – Instrumentation and control for systems important to safety

Safety integrity level (SIL):
Measure of risk reduction required by the safety system:
SIL 1: 10-100, SIL 2: 100-1000 , SIL 3: 1000-10000, SIL 4: 10000-100000

Basic engineering principles:
- **Redundant** – no single point of failure
- **Diverse** – no single cause or mode of failure
- **Failsafe** – equipment failure puts the system in a safe state

CERN personnel safety and access systems

LACS (LHC Access Control System) – who enters LHC and when [5]
LASS (LHC Access Safety System) – is it safe for beam or access at LHC [5]
PACS (PS Access Control System) – who enters the PS Complex and when [6]
PASS (PS Access Safety System) – is it safe for beam or access at PS [6]
SPS PSS – integrated personnel safety system for SPS
SPS Primary Ion Interlock – personnel safety during SPS mixed ion/proton runs [7]
SUSI (Surveillance des Sites) – who enters CERN sites and areas other than the accelerators
CSAM (CERN Safety Alarm Monitoring) – alarms for the fire brigade
Sniffer – gas detection in CERN tunnels and caverns
SIP/SAM (Site Information Panels / Simple Access Messages) – display relevant info at access points
SSA (Safety System Atlas) – personnel access and safety system for the Atlas detector.

Programmable Logic Controllers (PLC)

Technology
- Mainstay technology for safety systems
- Cyclic operation: read inputs, compute state, write outputs
- Certified components, up to SIL 3
- Response times of the order of 1-10ms
- Remote supervision via network
- Long-distance connections / remote I/Os with Profibus [2]
- Integrated programming environment
- Integrated safety and non-safety programs in the CPU
- Vendors: Siemens [3], HIMA [4]

Advantages
- Certification easy
- Changing logic and testing easy
- Well-known technology
- Long product life-cycles

Disadvantages
- Expensive hardware and software
- Complicated hardware/software environment
- Complicated upgrades/patching

Use in CERN personnel protection systems
- LASS [5]
- PASS [6]
- SPS PSS
- SPS Primary Ion Interlock [7]

Siemens S7 400 CPU and ET200 remote I/O modules of the PASS key controller.

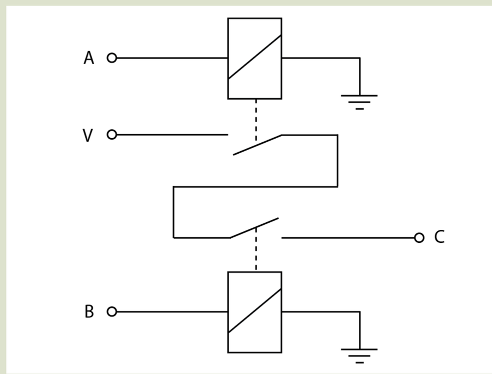
Relay-based logic

Technology
- In-house design and implementation
- Switching time of the order of 0.1-10ms
- Use of standard relays and electrical components
- Safety relays exist with high MTBFs
- Relay lifetimes of the order of 1M switches

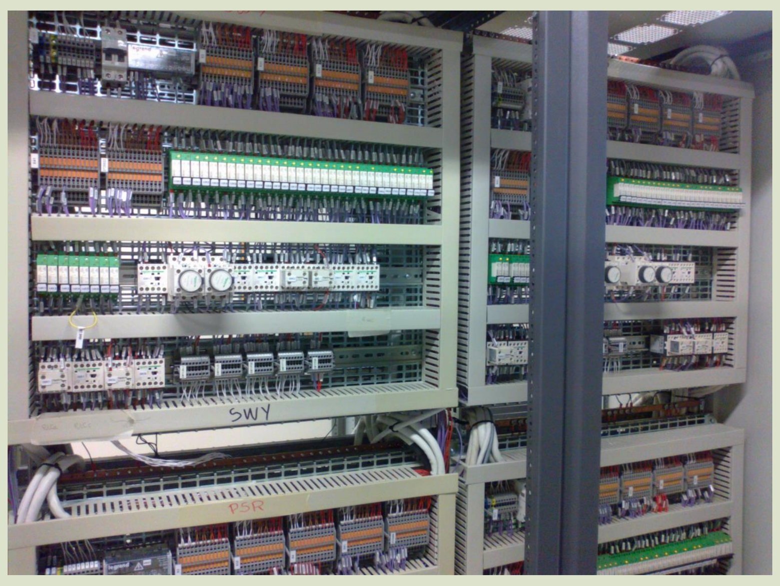
Advantages
- Straightforward implementation
- Robust to disturbances
- Implementation well visible and easy to understand

Disadvantages
- Certification hard (computation via individual components)
- Bulky (racks/connections/wiring/relays)
- Labor-intensive implementation
- Safety relays are expensive
- Contact issues (oxidation/sulphurisation / arcing) on rarely used relaysSupervision hard (requires extra logic)
- Changing logic hard and error prone (rewiring of connections)
- Complicated logic components laborious to implement
- Not suitable for very high switching frequency apps
- Realistically only suitable to straightforward and fairly small-scale logic (redundant chain for critical functions)

Use in CERN personnel protection systems
- LASS - redundant chain of outer perimeter
- PASS - idem.



A relay-based AND gate. A and B are the inputs, C is the output, and V is a constant voltage.



Hardwired relay-based wired logic of the PASS cabled loop. Green LEDs indicate contact states.

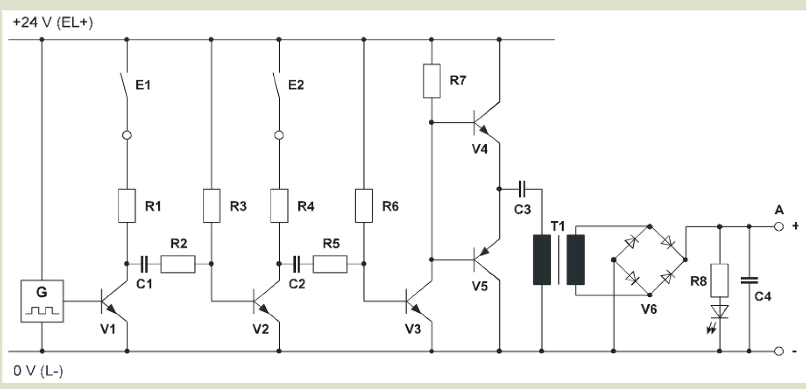
Dedicated logic cards

Technology
- Used in the highest-rated systems (people transport, critical process safety)
- Wired logic with dedicated interchangeable electronic cards that implement the logic gates
- Interconnections by soldering or wrapping
- Very high safety certification (SIL 4)
- Gate switching times of the order of 2-15ms
- Supervision via Profinet or Ethernet using a special module

Advantages
- Certification easy
- Very high level of safety and reliability
- Exchange of faulty components easy

Disadvantages
- Relatively slow
- Logic optimization necessary for performance (OR-based logic)
- Complicated logic components hard to implement (latches, flip-flops, etc.)
- No 2-channel complementary (ambivalent) I/O

Use in CERN personnel protection systems
- SPS primary ion interlock (HIMA Planar4 [4])



HIMA Planar4 AND-gate demonstrating the safety-related design. E1 and E1 are the inputs and A is the output. The internal design is based on dynamic signaling driven by signal generator G. A simultaneous failure of up to three separate components leads to the output being de-energized.

HIMA Planar4 wired logic in a 19-inch sub-rack of the SPS primary ion interlock. From the left: fuse module, two timing modules, logic modules, and far right a Profibus supervision module.

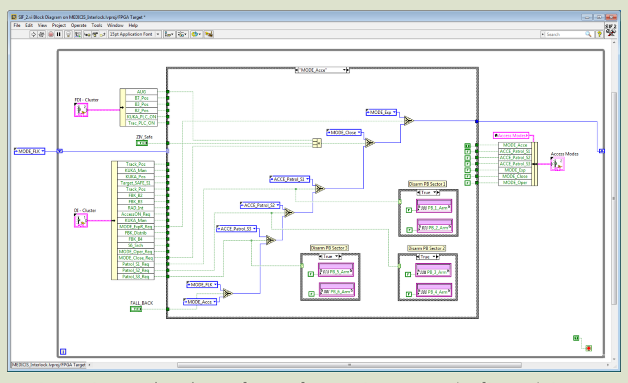
Field-programmable gate arrays (FPGA)

Technology
- Used in design requiring very fast response times
- Compilation of a schematic program into an array of gates on the circuit
- Coupled with a general-purpose processing unit running RT-Linux
- Currently not certified SIL, but certified I/O modules likely to be introduced soon
- Response times of the order of ns
- Supervision via Ethernet / special module
- A few vendors: National Instruments [8]

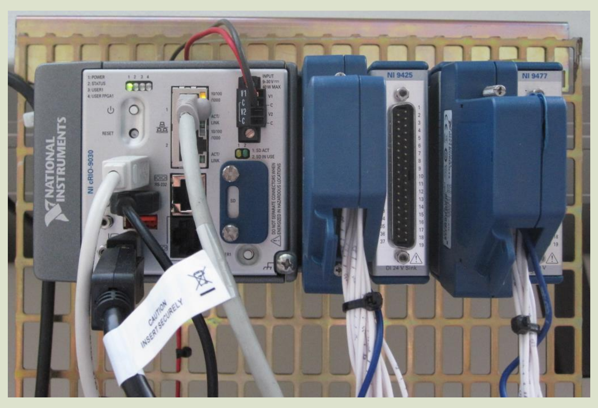
Advantages
- Very fast
- Changing logic / testing easy
- Integrated graphical dev environment (National Instruments LabVIEW)

Disadvantages
- Currently not certified SIL

Use in CERN personnel protection systems
- Being tested for use in a pilot project



One interlock safety function as defined in LabView for the FPGA.



NI cRIO 9030 FPGA controller test bench. The RT-Linux unit is on the left and the FPGA unit on the right with I/O modules.

Comparison of technologies

	Certification	Time scale	Communication	Supervision	Logic changes	Logic implementation	Space requirements	Scalability
PLC	Up to SIL 3	ms	TCP/IP Profibus	SCADA Custom	Easy	Programming	Medium	Good Large scale
Relay logic	None	ms	Wired	Custom	Hard	Manual Hard-wired	High	Limited Small scale
Logic cards	Up to SIL 4	ms	TCP/IP Profibus	SCADA Custom	Hard	Manual Hard-wired	Medium	Limited Medium scale
FPGA	None yet	ns	TCP/IP Profibus	SCADA Custom	Easy	Programming	Small	Good Large scale

Comparison of some of the most important metrics between the different interlock technologies.

References

[1] http://www.iec.ch
[2] http://www.profibus.com
[3] http://www.siemens.com
[4] http://www.hima.com
[5] T. Ladzinski et al., "The LHC Access System," ICALEPCS09, Kobe, Japan, WEP102, p. 600 (2009); http://www.JACoW.org
[6] P. Ninin et al., "Refurbishing of the CERN PS Complex Personnel Protection System," ICALEPCS13, San Francisco, USA, MOPPC059, p. 234 (2013); http://www.JACoW.org
[7] T. Hakulinen et al., "Personnel Protection of the CERN SPS North Hall in Fixed Target Primary Ion Mode," ICALEPCS13, San Francisco, USA, MOPPC067, p. 66 (2013); http://www.JACoW.org
[8] http://www.ni.com
[9] F. Valentini et al., "Integration of Heterogeneous Access Control Functionalities Using the New Generation of NI cRIO 903x Controllers," MOPGF143, this conference.

CERN