BUILDING AN INTERLOCK: COMPARISON OF TECHNOLOGIES FOR CONSTRUCTING SAFETY INTERLOCKS

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

Abstract

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.

INTRODUCTION

There are three basic types of components in safety systems: *sensors* for collecting data on any measurable conditions important for safety, *actuators* for manipulating equipment important for safety when necessary, and *interlocks*, for computing the safety logic between the two. Sensors and actuators are always particular to the application in question, that is, the conditions to be surveyed and actions to be taken are different in each case. However, an interlock is just a unit for processing of logical information, and the technological choices for its implementation have usually more to do with requirements of overall throughput, reliability, cost, or technological diversity as mandated by principles of safety system design.

Safety interlocks are considered critical components that are subject to careful implementation and certification. International standards, such as IEC 61508 and 61511 for process industry, and IEC 61513 [1] for nuclear industry are often used in the design of entire safety systems, including the interlock. IEC 61508 and 61511 use the concept of safety integrity level (SIL) to quantify the required level of reliability of the safety system in its safety function as well as the ability of the system components to satisfy that requirement.

CERN GS/ASE group is responsible for all personnel safety systems, access control systems, and personnel safety alarm systems at CERN. We have a long experience of designing, building, and operating different personnel safety systems for CERN accelerators and experiments. Over the years, different approaches have been used for building interlocks for these systems, and this has given us some insight into the relative merits of the various technological choices. The technologies discussed in this paper are programmable logic controllers (PLCs), relay-based logic, wired logic with dedicated logic cards, and field-programmable gate arrays (FPGAs) with the examples based on actual implemented equipment.

PLC

Programmable logic controllers (PLCs) are the mainstay of modern process control applications. A PLC operates in a cyclic manner: during one cycle all inputs are collected, a new system state is computed in the CPU according to the program logic, and all outputs are set correspondingly. Cycle times of PLCs vary normally from a few to hundreds of milliseconds depending on the number of I/Os and the complexity of the program. I/Os are normally handled by separate modules, which can be placed some distance away from the CPU when connected via copper or fiber-optic cabling using a specific fieldbus protocol such as Profibus or Profinet [2]. Modern PLCs are also able to communicate via standard TCP/IP protocols via Ethernet, facilitating long-distance supervision of these systems. Special Supervisory Control and Data Acquisition (SCADA) systems are often used to integrate PLCs into a larger control framework.

Several manufacturers offer safety-related components certified for use in SIL-rated systems [3,4]. As a PLC-based system cannot be certified higher than SIL 3 (according to the standard, no system containing program code can be at SIL 4), that is normally the highest level of certification for the safety-related components as well. Some PLCs are able to integrate safety and non-safety-related programs and components within a single system, making communication between the two parts seamless.

At CERN, various generations of Siemens PLCs (S5, S7) are used in our personnel safety systems: LHC Access Safety System (LASS) [5], PS Access Safety System (PASS) [6], SPS Personnel Protection System, SPS Primary Ion Interlock [7]. This technology is fully mastered at CERN, and Siemens product life cycles are long allowing for a long utilization of installed hardware. Logic modifications and testing of PLC systems is fairly easy thanks largely to an integrated programming environment. Furthermore, PLC safety signatures provide a safeguard against unauthorized modifications of PLC code.

However, there are also drawbacks to PLC technology: For a large system, powerful CPUs are often needed to manage the logic coupled with sophisticated SCADA

ISBN 978-3-95450-148-9

systems, which can get quite expensive in hardware and license costs. Also, the entire system environment can get fairly complicated, where considerable expertise is required to manage different generations of hardware, firmware, and software for everything to work correctly together. Upgrading any of the system components, including patching firmware and software even for security reasons can be a complicated and risky affair, which will almost inevitably incur a period of unavailability of the entire system. Furthermore, changing safety system components in any way normally triggers a full suite of validation tests by the responsible safety officer, often requiring days to prepare and carry out, which further limits the usefulness of the otherwise easy programmability of PLC systems in production environments. Figure 1 shows one of PASS PLCs with its I/O modules.

Figure 1: Siemens S7 400 series CPU with ET200 remote I/O modules.

RELAY-BASED LOGIC

Possibly the oldest and still a highly relevant method of building reliable hard-wired logic systems is to use relays. All basic logic gates can be implemented in simple relays with hardwired connections. An example of a relay-based AND-gate is shown in Figure 2.

Implementation of a relay-based interlock is quite straightforward: standard electrical wiring, connectors, and relays are installed in a rack. Special safety relays are often used, which have high MTBFs and known fail-safe states. Generally relay-based systems are quite resistant to external disturbances, with the exception of high magnetic fields in rare cases, which can cause a magnetic relay to misbehave. Also any competent electrician is able to understand, maintain, and modify such a system based on simple circuit diagrams.

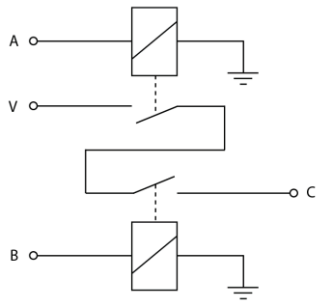

Figure 2: A relay-based AND-gate. A and B are the inputs, C is the output, and V is a constant voltage.

However, relay-based systems have several serious drawbacks compared to more modern approaches: Relay-based systems are bulky requiring plenty of rack space even for a small amount of logic, which limits the practical complexity of the application. Safety relays are expensive and implementation of the system is quite labour intensive. If supervision of interlock functions is required, extra logic needs to be implemented. Modifying the interlock logic can also obviously get quite hard.

As a relay-based system is necessarily built and designed in-house, its certification at a specific SIL-rating, if required, could be difficult requiring a calculation based on the individual SIL-rated components. Relays themselves may exhibit wear and tear over time: contact issues due to oxidation, sulphurisation, or arcing may happen. The upside is that in such a case, changing the defective component is relatively easy.

Relays are also not suitable for applications, where the switching frequency is high, since normal mechanical relays are typically only rated for around 1-2 million switches during their lifetime. Also, switching time of a mechanical relay is somewhere between 0.1-10ms and a certain resolution time is in any case required for the state change due to effects like contact bounce. Using solid-state relays could help in these cases, though.

Figure 3: Hardwired relay-based logic using relays. Green LEDs indicate contact states.

ISBN 978-3-95450-148-9

For these reasons, relay-based systems are realistically only suitable for fairly straightforward and small-scale logic. At CERN, they have mainly been used to build redundant chains of the most important safety functions of the LHC and PS access safety systems. Figure 3 shows part of the relay logic installed in the PASS cabled loop rack.

DEDICATED LOGIC CARDS

Another way of constructing a hard-wired interlock is by using dedicated electronic logic cards such as HIMA Planar4 series [4]. Logic gates are implemented in standard modular sub-rack-mounted cards and interconnections between these gates are realized by wiring the card inputs and outputs on the sub-rack backplane either by soldering or wrapping. A faulty card can easily be exchanged without having to touch the logic at all.

These kinds of systems can be used to build the highest rated safety systems. Most components of the Planar4 series are certified for use in SIL 4 systems, and consequently, they are often used in people transport systems or for critical process safety at chemical plants, oil rigs, and the like. Various I/O modules based on relays or line-monitored connections are available, and all gates in the sub-rack can be supervised by dedicated communication modules offering Profibus, Modbus, or OPC connectivity to an outside PLC or supervision post. Figure 4 shows the modules of the wired chain of CERN SPS North Area primary ion interlock [7] designed using HIMA Planar4.

Figure 4: Planar4 wired logic in a 19-inch sub-rack. From the left: fuse module, two timing modules, logic modules, and far right a Profibus supervision module.

One of the drawbacks of this technology is that due to a safety-related design and the additional diagnostic functions on each card, switching times are relatively long for active gates (AND, NOT), ranging from 2-15ms depending on the case (see Figure 5). Therefore, complicated logic may introduce a considerable delay of up to tens or hundreds of milliseconds. This may not be a problem in most applications, but should it be necessary to optimize this, careful design is required. For example, by application of De Morgan's theorem it is usually possible to construct the logic by using primarily OR-gates, which incur no internal processing delay. The HIMA wired chain of the SPS North Area primary ion interlock was designed this way [7]. The downside of this approach is that the logic becomes harder to understand from the diagrams.

HIMA provides logic cards for the basic logic operations as well as a variety of I/O options. However, any more complicated logic components, such as latches, flip-flops, etc. would have to be constructed from the basic gates. HIMA also does not provide 2-channel complementary (ambivalent) I/O, for which logic would also have to be custom built, if needed. As the logic programming is carried out with a soldering iron or a wrapper, changing this logic is not straightforward. Even small modifications may require unsoldering of a considerable number of connections to gain access, which is obviously both time consuming and error prone.

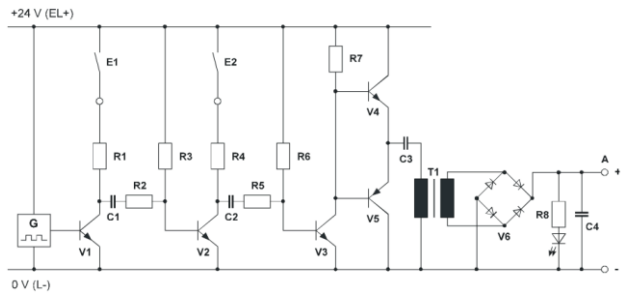

Figure 5: HIMA Planar4 AND-gate. E1 and E1 are the inputs and A is the output. The internal design is based on dynamic signaling driven by signal generator G. A simultaneous failure of up to three separate components leads to the output being de-energized. Compared to Figure 2, the added complexity due to safety-related design is clear.

FPGA

Designs requiring very fast logic processing have since long time used Application Specific Integrated Circuits (ASIC) or Field Programmable Gate Arrays (FPGA). An FPGA is an integrated circuit that can be programmed at the gate level to perform desired operations. In contrast to an ASIC, an FPGA can be reprogrammed in field if necessary. Both ASICs and FPGAs can be designed using a specific hardware description language (HDL). FPGA system vendors often also provide block-based graphical programming environments as well as bindings to conventional programming languages, like C. A schematic program is compiled into an array of gates on the circuit, which will realize the desired logic.

The great advantage of FPGAs over general-purpose computers and PLCs is speed. Response times of implemented functions can be in the nanosecond range, obviously depending on their complexity. Testing and modifying logic is as easy as reprogramming a PLC.

FPGAs are normally run within an integrated framework, such as National Instruments cRIO 903x series [8], where the FPGA is controlled by a real-time RT-Linux system, providing connectivity to network and peripherals similar to a normal PC. The FPGA connects directly to its own I/O modules, of which there are many available for different applications. Supervision of the system is easily implemented via the RT-Linux unit.

ISBN 978-3-95450-148-9

Table 1: Comparison of Some of the Most Important Metrics Between the Different Interlock 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

The most important drawbacks when considering FPGA-based solutions for safety systems is that they are usually not safety-related by design in the same way as safety PLC systems or HIMA logic cards. While calculations can be made based on the published MTBFs of individual system components, modules explicitly certified for use in SIL-rated systems have not been available. However, this is likely to change in the future, as vendors will be introducing safety-related modules for their systems.

At CERN, a pilot implementation of a small independent safety interlock using a National Instruments FPGA is being studied [9]. One of the aims of this project is to gain experience and confidence in the technology as well as to test the auxiliary functionality provided by the RT-Linux system in running related access control functions, badge readers, touch panels, etc. The test bench FPGA system of this project is shown in Figure 6.

Figure 6: National Instruments cRIO 9030 FPGA controller test bench. The RT-Linux unit is on the left with Ethernet, serial, USB, and video connections. The FPGA unit is on the right with four I/O modules, of which two connected. Each I/O module of this type hosts 32 digital signals.

CONCLUSIONS

We have compared four different technologies for constructing safety interlocks based on our return of experience over years in designing safety systems. The technologies compared were PLCs, relay-based logic, dedicated logic cards, and FPGAs. All of them have their pros and cons and, indeed, depending on the application, their proper place in the toolbox of an interlock builder: When strictly SIL-certified systems following norms IEC 61508 and 61511 are required, PLCs or dedicated logic cards remain the preferred choices. However, for building diverse and rendundant safety systems following norm IEC 61513, relay-based logic and FPGAs can also be very useful. Table 1 presents a synthesis of some of the most important performance metrics potentially affecting the choice of technology for a new interlock system.

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, ICALEPCS15, Melbourne, Australia (2015).

ISBN 978-3-95450-148-9