ISBN: 978-3-95450-236-3 ISSN: 2673-5350 doi:10.18429/JACoW-IBIC2023-MOP011

SAFETY CONSIDERATIONS FOR SHIELD DOOR CONTROL SYSTEMS*

H.A. Watkins†, W. Barkley, C. Hatch, D. Martinez, D. Rai, E. Simakov
Los Alamos National Laboratory, Los Alamos, NM, USA

Abstract

The Accelerator Operations and Technology division is upgrading the control system for a 33-ton shield door that will be used when the Cathodes and RF Interactions in Extremes (CARIE) accelerator begins operations. The door was installed in the 1990's but safety standards such as ISO 13849-1 have since emerged which provide safety requirements and guidance on the principles for the design and integration of safety-related parts of a control system. Applying this standard, a safety controller, safety relays and a light curtain barrier have been added to eliminate injury and exposure of personnel to potential hazards during door operations.

OVERVIEW OF CARIE

Los Alamos National Lab (LANL) is starting construction of a new C-band (5.712 GHz) accelerator test facility for cathode, accelerator, and material science studies. The new facility is called Cathode and RF Interactions in Extremes (CARIE). This accelerator will reside in a radiation protection vault on the Los Alamos Neutron Science Center (LANSCE) mesa. This location will house a cryo-cooled copper RF photoinjector with a high quantum efficiency (QE) cathode and a high gradient accelerator section with beam power up to 20 kW [1].

SHIELD VAULT

CARIE will reside in a 12 by 25-foot interior vault that uses 4-foot-thick magnetite blocks to shield the exterior control and operations areas. The vault was originally designed for use with the Advanced Free Electron Laser (AFEL) project which is no longer in operation. A 33-ton moveable shield door separates the vault from the control room. When closed during CARIE operation, the door protects personnel from neutron and bremsstrahlung radiation, activated air, and ozone. The door is constructed of 12 magnetite concrete blocks welded together on their edges and welded to a reinforced concrete base. The door is mounted on four sets of Hilman rollers and guided by tracks on the floor, the door is opened and closed by a hydraulic piston [2]. The shield vault door will need to open and close multiple times a day to support experimentation within the vault. The original control system was decommissioned and removed in the early 2000's. However, the shield blocks, hydraulic piston and roll track system remain intact (see Fig. 1). Attempts to test the door mechanism and piston were successful and the door is operational from a mechanical perspective. The shield door and existing hydraulic system (see Fig 1).

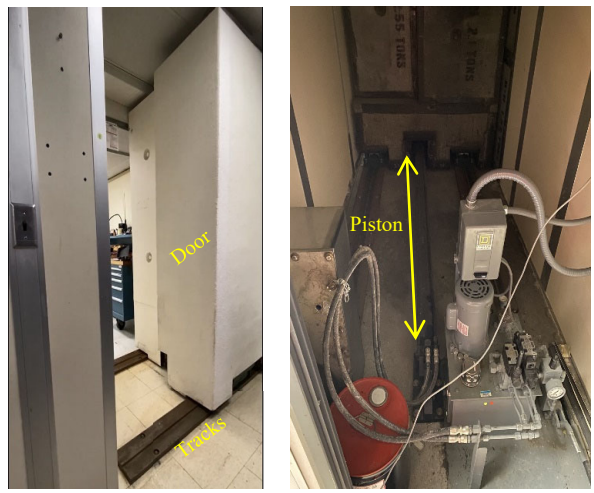

Figure 1: Shield door opening and hydraulic system.

FUNCTIONAL REQUIREMENTS

The purpose of the control system for the shield door is to allow scientists and engineers to easily access the interior vault when CARIE is not in operation and for the door to remain closed when operations commence. The control system requirements are very simple. Open and close buttons mounted exterior to the vault easily meet the functional requirements for operation. Investigation of the mounting points and legacy relay system indicate this is most likely what existed during its operation during the 1990's until decommissioning in early 2000's.

SAFETY REQUIREMENTS

The legacy requirements of safety for the shield door design focused on the radiation shielding that the door provided to the users when the original AFEL was in operation. However, safety of the control system e.g. door operations were not considered or evident in the initial design. ISO 13849-1 is the safety standard that now governs safety requirements for the operation of control systems. This safety standard provides safety requirements and guidance on the principles for the design and integration of safety-related parts of a control system. This standard defines the performance level (PL), which is the discrete level used to specify the ability of safety-related parts of control systems to perform a safety function under foreseeable conditions.

WHAT IS SAFETY? WHAT IS RISK?

Control system engineers must incorporate safety into designs to provide the protective measures needed to insure

* This work was supported by the U.S. Department of Energy through the Los Alamos National Laboratory. Los Alamos National Laboratory is operated by Triad National Security, LLC, for the National Nuclear Security Administration of U.S. Department of Energy (Contract No. 89233218CNA000001).
LA-UR-23-29961
† hwatkins@lanl.gov

ISBN: 978-3-95450-236-3 ISSN: 2673-5350 doi:10.18429/JACoW-IBIC2023-MOP011

safe operations. Control system safety can be defined as "freedom of the operator from unacceptable risk." This infers that there is minimal level of risk involved even when a system is considered safe. Risk is then defined as "a combination of the probability of the occurrence of harm and the severity of that harm" [3].

$$\text{Risk} = \text{Severity of harm} \times \text{Probability of the occurrence of harm} \quad (1)$$

RISK ASSESSMENT

Every time we rely upon a control system to reduce risk, we also need to consider the probability that the safety control system itself will fail. If a safety control system fails, it does not provide the risk reduction measure. This is the domain of functional safety and incorporates the PL as its basis to have the control system reliability exceed the needs of the risk reduction measure [4].

Control system engineers should begin with a risk assessment using the flow chart (see Fig. 2) to determine limits, hazards, risk, and the protective measures needed to mitigate exposure to the hazards. This risk assessment was completed for the shield door project and resulted in a design to minimize operator exposure to identified hazards.

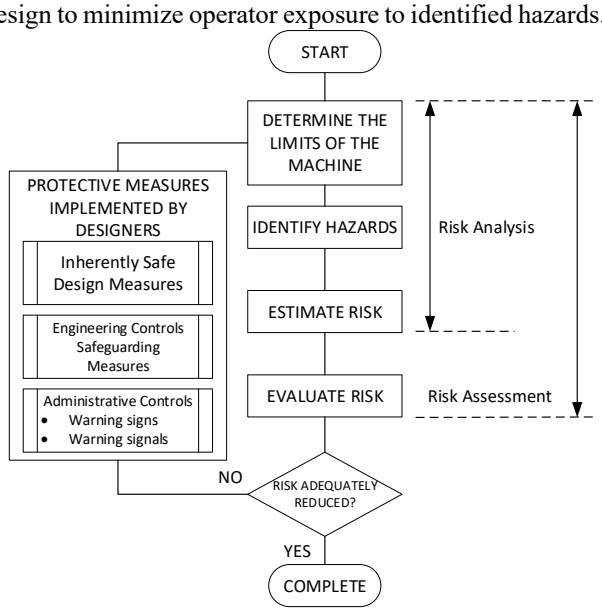

Figure 2: Risk assessment flow chart.

DETERMINE LIMITS

Assessing the operating limits of the machine in question is the first step of the flow chart. The shield door project determined that the limits of the shield door were based on the track structure and the stroke of the hydraulic cylinder. The door being fully opened occurs when the hydraulic cylinder is fully retracted. A leaf style limit switch is placed 1-inch inside of the fully retracted system to allow for an engineering limit. The other limit is full extension of the hydraulic cylinder where the pump is placing 300 psi of fluid pressure through the lines to close the door. The system can reach full closure and the hydraulic cylinder is still able to provide additional stroke of 1-inch. Another engineering limit is added at the door closure to disengage the pump and stop motion. Identifying these limits then allow for moving to the hazard identification step of the flowchart.

INDENTIFY HAZARDS

Mechanical hazards fall into six different categories.

- **Crushing**
- Shearing
- Cutting
- Entanglement
- Drawing-in or **trapping**
- Stabbing or puncture

The shield doors specific mechanical hazard was identified as crushing. The hydraulic piston when in operation can crush the human body and cause serious injury if the hydraulic pump remains engaged and an engineering limit has not been reached.

ESTIMATE RISK

Since a hazard has been identified the next step is to estimate the risk of the crushing hazard of the shield door. The risk estimation chart allows an engineer to determine the degree of risk as a performance level requirement (PLr) given the severity of injury, frequency of exposure to the hazard and the possibility of avoiding the hazard. Figure 3 shows the flow chart with the dashed line estimating risk for the shield door.

S = Severity of Injury
S1: Slight
S2: Serious ←
F = Frequency or exposure to hazard
F1: Seldom to less often ←
F2: Frequent to continuous
P = Possibility of avoiding hazard
P1: Possible under specific conditions ←
P2: Scarcely possible

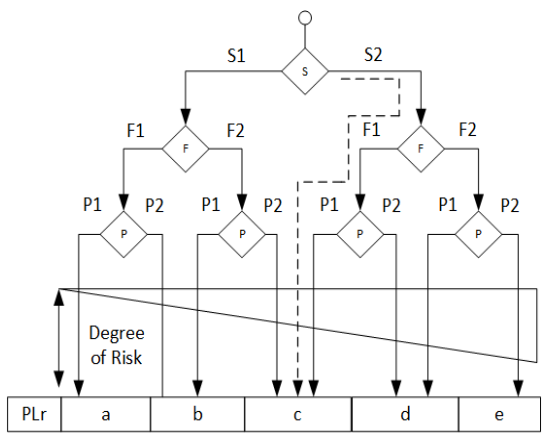

Figure 3: Risk estimation flow chart.

ISBN: 978-3-95450-236-3 ISSN: 2673-5350 doi:10.18429/JACoW-IBIC2023-MOP011

The determination of the required performance level was PLr = PLc. This allows the designer to evaluate the risk and the components needed to mitigate that risk. In the case of the shield door, components that will be selected to mitigate the crushing hazard must meet a minimum rating of PLc to ensure that the component reliability meets or exceeds the risk estimation requirement.

EVALUATE RISK

Now that the hazard and PLr have been identified, it is now possible to implement measures to reduce the exposure to the hazard in the form of protective measures. In the case of the shield door, it is not possible to make it inherently safe which should always be a designer's first evaluation method. The area where the shield door closes allows personnel access when the door is open so safeguarding measures or engineering controls must be implemented to reduce the likelihood of door movement during personnel entry but also provide full operations of the door.

PROTECTIVE MEASURES

Light Barrier

The protective measures chosen to reduce exposure to the crushing hazard of the door during operation was a light barrier system. The light barrier system uses a light array from a transmitter to beam light to a receiver section. When light becomes disrupted the safety programmable logic controller (PLC) senses the disruption and trips the safety relay. The PLC also has test equipment built-in to monitor the health of the light barrier and safety relay to ensure the equipment has not malfunctioned. This system can be mounted at the opening of the shield door to protect personnel trying to enter the vault when the door is in motion.

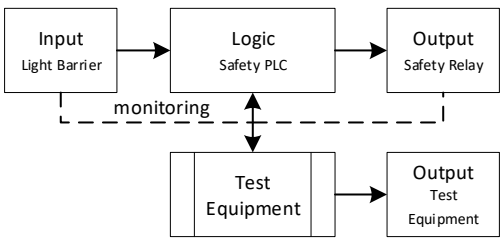

Figure 4: Safety diagram for light barrier.

Figure 4 shows the system as designed where the light barrier interfaces to a safety PLC with a safety relay. The PLC input is then programmed to latch open the output relay when the light barrier is triggered. The safety relay is then added in series to the control relays to disable motion of the door when latched. Latched systems also require a reset input, not pictured, to recover the system to normal operation if a safety event occurs. The test capability built into the safety PLC provides real time functional testing of the light barrier and safety outputs to ensure these systems will function correctly when needed. This improves the performance level rating of the system to PLc.

Status Indicators

Following the risk assessment flow chart and its iterative process it was determined the light barrier works to provide safety when very close to the door threshold however additional risk mitigation would be an administrative control to indicate to users further away that the door was in motion. Administrative controls were added to indicate to users the state of the door. Table 1 indicates the lights and sounds used as administrative controls for this project.

Table 1: Indications for Administrative Controls

Light Indicator	State
Green	Door Open
Orange	Door Closed
Red	Safety Stop
Blink Red	Door In-Motion
Siren	Door In-Motion

Emergency Exit

The important part of iterating through the risk assessment flow chart process is additional hazards may be identified. An additional hazard of trapping was identified during the assessment. The shield door could trap personnel inside if closed, no other exits exist to the vault. Risk estimation shows this is a PLa requirement due to slight risk of injury, seldom frequency and only possible under very specific circumstances. This simplifies the safety diagram where a simple exit override switch can be used interior to the vault and override the close command with an open command.

Emergency Stop

A similar emergency stop button was also provided for situations where operators external to the vault wish to stop all motion or lock out motion. This button did not meet the criteria for a safety requirement and is considered a design feature instead of a safety measure. However, it does provide a single control that allows all motion to be halted and overrides any motion commands of the control system.

PERFORMANCE LEVEL PARAMETER

Before the control system engineer dives into component selection, it's important to understand a manufacture's specification of performance level (PL). The PL must be determined for each safety component of the control system and/or the combination of components that performs a safety function. The following principal aspects are used to establish PL according to ISO 13849-1:

1) Category (Structure) – establishes the required safety function in case of a fault.
2) Diagnostic Coverage – is a measure of the effectiveness of the diagnostics to detect dangerous failures.

ISBN: 978-3-95450-236-3 ISSN: 2673-5350 doi:10.18429/JACoW-IBIC2023-MOP011

3) Mean Time to Dangerous Failure (MTTFd) – is the expectation of the safety component to provide failure free functionality.
4) Common Cause Failure – relates to the failure of different components resulting from a single event. [3]

Safety component manufactures will provide the PL ratings of their equipment, but it is the responsibility of the control engineer to implement the correct risk mitigation and testing to ensure those PL ratings meet or exceed the PLr requirements of the system. The PL ratings range alphabetically from a through e and will be called out on a vendor's datasheet as PLa – Ple. PLa would be the minimum level of safety performance and PLe would meet the highest level of safety performance.

COMPONENT SELECTION

Once safety measures have been designed the correct components must be selected to meet both the functional safety requirements and the performance level requirements for reliability. Several manufacturers make safety related equipment. The manufacturers Keyence, IDEC, Phoenix Contact and Schneider were all evaluated for safety related components for this project. Keyence was chosen as the supplier for all safety related components however the other three manufacturers were used for components for the operator control design which resides adjacent to the safety system. Keyence provided the clearest guidance on safety. The manufacturer calls out specifically the PLx ratings of their components, provided on-site engineering support for demonstration and discussed their safety technology in depth.

The Keyence GLR96H was chosen for the light barrier. This barrier has 96 beams and has a protection height of 1.9 m. The beam pitch is 20 mm which is capable of detecting hands, arms or legs. It uses 870 nm infrared LEDs for the light source and supports a detection distance of 15 m. Only 3.5 m distance is required for the door when fully opened. The PL safety rating for this device is PLe (see Fig. 5) which exceeds the PLc requirement determined during risk evaluation [5].

Approved standards	EMC	EMS	IEC61496-1, EN61496-1, UL61496-1
		EMI	EN55011 ClassA, FCC Part15B ClassA, ICES-003 ClassA
	Safety		IEC61496-1, EN61496-1, UL61496-1 (Type 4 ESPE) IEC61496-2, EN61496-2, UL61496-2 (Type 4 AOPD) IEC61508, EN61508 (SIL3), IEC62061, EN62061 (SIL CL3) EN ISO13849-1:2015 (Category 4, PLe) UL508 UL1998

Figure 5: Manufacturer's datasheet.

The Keyence GC-1000R is a safety PLC which also includes built in safety relay outputs. This controller provides the hardware control and safety logic programming necessary to implement the light curtain barrier, latch reset and the emergency stop switch. Included in this safety PLC is the capability to provide test equipment monitoring of the connected devices. This brings the PL safety rating of the controller to a PLe rating which exceeds the original PLc requirement needed to mitigate the crushing risk and the PLa requirement of the trapping risk discovered during risk assessment.

CONCLUSION

Safety considerations for control systems require a risk assessment to ensure that existing or new designs address risk exposure to operators. In the case of the shield door for the CARIE vault two hazards were identified. Engineered safety controls and administrative controls were implemented to reduce the risk of hazard exposure to a minimal level for operators. Los Alamos National Lab has instituted a new focus on disciplined operations. This focus reminds employees to use the safe conduct of research principals to cultivate a questioning attitude about safety and reminds all employees to maintain a healthy respect for what can go wrong. These principles don't just apply to the personnel operating devices such as the shield door but also to the control system engineers who are providing remote control capabilities for these devices.

REFERENCES

[1] E.I. Simakov *et al.,* "Update on the Status of C-Band Research and Facilities at LANL", in *Proc. 5th North American Particle Accel. Conf. (NAPAC'22)*, Albuquerque, New Mexico, USA, August 2022 pp. 855-858. doi:10.18429/JACoW-NAPAC2022-THY

[2] K. Meier, "Engineering Considerations of the Advanced Free Electron Laser Facility", presented at the 13th International Free-Electron Laser Conference, Santa Fe, NM, Aug 1991, paper, unpublished.

[3] *Safety Support Guide Book*, Keyence, Itasca, IL, USA, 2020.

[4] M. Tacchini, *Functional Safety of Machinery, How to Apply ISO13849-1 and IEC 62061*, Poncarale, Brescia, Italy: Wiley, 2023.

[5] GL-RH Data Sheet, Keyence, Itasca, IL, USA Dec 2022.