THE LASER MEGAJOULE FACILITY PERSONNEL SECURITY AND SAFETY INTERLOCKS

Jean-Claude Chapuis, Jean-Paul Arnoul, Alain Hurst,
Mathieu Manson, CEA/CESTA, Le Barp 33114 France

Abstract

The French CEA (Commissariat à l'Énergie Atomique) is currently building the LMJ (Laser Mégajoule), at the CEA Laboratory CESTA near Bordeaux. The LMJ is designed to deliver about 1.4 MJ of 0.35 µm light to targets for high energy density physics experiments. Such an installation entails specific hazards related to the presence of intense laser beams, and high voltage power laser amplifiers. Furthermore, the thermonuclear fusion reactions induced by the experiment also produce different radiations and neutrons burst, and also activate various materials in the chamber environment. All these hazards could be lethal. The SSP (Personnel Safety System) was designed to prevent accidents and protect personnel working in the LMJ.

DESIGN METHODOLOGY

Saftey Studies

For each type of hazard generated by the LMJ process (laser, high voltage, radiations), scenarios of accidents are identified and qualified in terms of gravity and frequency.

Table 1: Gravity v.s. Frequency

Gravity →	Lethal	Impor-tant	Impor-tant	Major	Major
	Major injury	Signi-ficant	Signi-ficant	Impor-tant	Major
	Minor injury	Minor	Signi-ficant	Signi-ficant	Impor-tant
	Incon-fort	Minor	Minor	Minor	Signi-ficant
		Rarely (< 2 times / year)	Some-times (< 20 times / year)	Often (< 200 times / year)	Perma-nent (> 200 times / year)
		Frequency of exposure →			

The table 1 is then used to determine the risk level (i.e. the importance of the potential accident) that is used in the table 2 that indicates the number ant the type of the associated protection barriers necessary to mitigate the risk at an acceptable level.

The CEA security methodological guide defines 2 types of barriers:

- The technical barriers (TB), that are any technical device used to protect the workers, such as access control or safety interlocks,
- The procedural barriers (PB) that involve a human action, that are used in complement of the TB to increase the protection level when necessary.

It also specifies the number of required barriers versus the identified risk level, with 2 options: desirable or acceptable. The choice between those options is generally technical, but it is often also cost driven.

Table 2: Risk Level v.s. Number of Barriers

Risk Level	**Number of barriers**	
	Desirable	Acceptable
Major	3 TB's	2 TB's + 1 PB
Important	2 TB's	1 TB + 1 PB
Significant	1 TB	2 PB's
Minor	2 PB's	1 PB

Functional Analysis

The objective of the Personnel Safety System is to prevent transitions from a safe state to a forbidden state**.**
The safe states are:

- Presence of hazard requiring the absence of personnel,
- Presence of hazard AND all the persons are qualified to work in presence of the hazard,
- Absence of hazard.

The forbidden states are:

- Presence of hazard requiring the absence of personnel AND presence of personnel,
- Presence of hazard AND a person is not qualified to work in presence of this hazard.

So the transitions that must be prevented with adapted barriers are the following:

- Entrance of a person when a hazard requires the absence of personnel,
- Entrance of a person not qualified for a present hazard,
- Occurrence of a hazard requiring the absence of personnel in presence of personnel,
- Occurrence of a new hazard in presence of unqualified personnel.

Two different kinds of safety systems are required to prevent these transitions:

- Access control to the building and to its different areas, that involves doors switches, safety locks and associated hardware.
- Risk management that involves safety interlocks, in relation with the potentially hazardous equipments. These equipments have to wait for permissive before generating any hazard, and have to acknowledge when the hazard is present.

FUNCTIONNAL ARCHITECTURE DESIGN

Design Principles

To satisfy at the lowest cost the requirements of safety regulations and those of the operation management, the choice was made to implement a functional architecture built around two independent technological barriers when required by the risk level.

The combination of these two independent technological barriers allows managing the dynamic evolution of the compromise between hazard presence and worker presence in the rooms, throughout the various scenarios identified in the safety studies.

Each technical barrier is composed of two subsets, one dedicated to hazard sources management, and the other one dedicated to worker presence management.

The two completely independent barriers, even at the sensor or actuator level, are designed with different technologies adapted to the required Safety Integrity Level (SIL 2 or SIL 3). The combination of these 2 barriers is equivalent to a unique barrier with a rate of dangerous failure of ~10^{-6} per year.

IEC 61508 Standard

The **IEC** (International Electrotechnical Commission) 61508 standard specifies a set of requirements for functional safety of electrical / electronic / programmable electronic safety-related systems.

It defines 4 levels of requirements or « SIL » that must be respected according to the acceptable failure objective of a safety function, either in continuous operation mode, or in low demand operation.

These levels are used to specify the safety requirement of each device or software involve in the SSP.

Table 3: SIL v.s. Average Failure Probability

Safety Integrity Level	Average probability of Failure on Demand per year
SIL 4	$\geq 10^{-5}$ à $< 10^{-4}$
SIL 3	$\geq 10^{-4}$ à $< 10^{-3}$
SIL 2	$\geq 10^{-3}$ à $< 10^{-2}$
SIL 1	$\geq 10^{-2}$ à $< 10^{-1}$

FUNCTIONAL DESCRIPTION OF SUBSETS

The SSP is composed of 3 main subsystems:

- The first technical barrier (TB #1),
- The second technical barrier (TB #2) totally independent from the first one,
- The SSP supervisory system that present different GUIs to the operator.

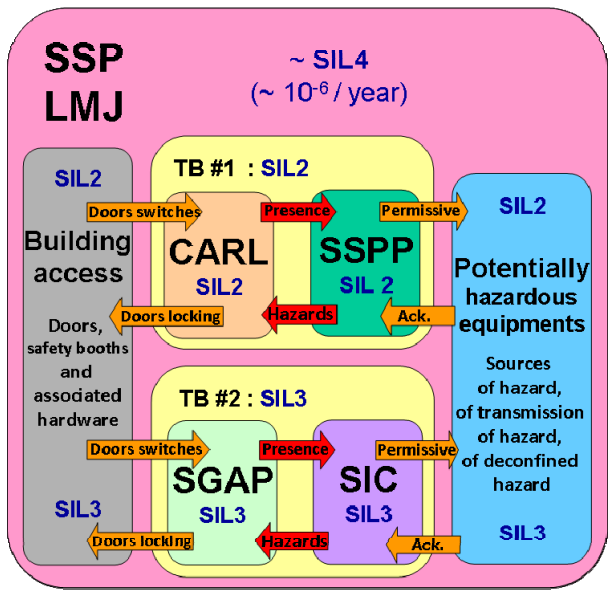

Figure 1: General SSP architecture.

First Technical Barrier

The first barrier designed in SIL 2 is based on a programmable technology (safety PLC). It is itself composed of two functional subsets:

- The "CALR" (Contrôle d'Accès des Locaux à Risques) ensuring access control to the areas that present hazards, by using contactless personal badges (RFID technology) and safety locks.
- The "SSPP" (Système pour la Sécurité du Personnel Programmé) controlling both the presence of hazards and their authorizations (permissive) at the equipment level.

The probability of a dangerous failure of the first barrier is between 10^{-2} and 10^{-3} per year.

Second Technical Barrier

The second barrier designed in SIL 3 is based on a non programmable technology (safety relays or equivalent). It is itself also composed of two functional subsets:

- The "SGAP" (Système de Garantie d'Absence de Personnel) whose objective is to ensure the absence of workers in the target bay during a powerful laser shot, thus preventing the risk of death due to a neutron flash. Access management to the rooms is done using access keys provided by a guard.

- The "SIC" (Système d'Interverrouillage Centralisé) that ensures, with key based safety interlocks, that the laser beams and the power conditioning system cannot be activated unexpectedly during a maintenance period.

The probability of a dangerous failure of this barrier is between 10^{-3} and 10^{-4} per year.

SSP Supervisory Software

Dedicated GUIs are provided to the operators in charge of the LMJ safety.

The main GUI presents the status of all the LMJ SSP. It has an alarm zone and an event log to allow alarm managing, and different control zones with push buttons to deliver risks authorization. Other GUIs present to the operator a general view of risks, a general view of the process state and a general view of the building security. Detail views are dedicated to hazardous equipments such as laser bundles, power conditioning devices, and Laser sources.

This software layer is designed with Panorama E^2 (the CODRA Company SCADA product) under Windows 7. It is independent from the safety loops which are controlled at the lowest level by PLC.

REFERENCES

[1] IEC 61508 international standard (International Electrotechnical Commission, 3, rue de Varembé Geneva, Switzerland)

[2] The Laser Megajoule facility: control system status report, ICALEPCS 2007, by J.P. Arnoul, F. Signol CEA/CESTA, Le Barp, 33114 France, P. Bétrémieux, J.J. Dupas, J. Nicoloso CEA/DIF, Bruyères le Châtel, 91680 France

[3] The Laser Megajoule facility: control system status report, ICALEPCS 2009, by J.J. Dupas, J. Nicoloso CEA/DIF, Bruyères le Châtel, 91680 France