Personnel Protection Systems

New control solutions for safety applications

KT – Innovation Day – 26th October 2018

F. Valentini (BE-ICS-CSE)

Personnel Protection Systems @ CERN

DEVELOPMENT PROCESS

1 2 3 4 5

Risk Assessment
All hazards are analyzed and all possible accident scenarios identified.

Safety Instrumented Functions
The system's automatic safety actions are translated into mathematical Boolean formulas.

TRIGGERING EVENT- RULES FOR VETO REMOVAL FROM LASER X COVERED BY HOOD X:

```
LSR_X_Offline=0 ∧ (MODE_OPER=1
                   V
                   Hood_X=1 ∧ (MODE_ACCE=1 V MODE_PATROL=1))

    OUTPUT → VETO_LSR_X = 1
ELSE
    OUTPUT → VETO_LSR_X = 0
```

System Architectural Design
All safety components and the logic controller are chosen and the detailed design is finalized.

PLC Code Development & Cabinets
The logic controller (PLC) is programmed and extensively tested. The electrical cabinet is mounted.

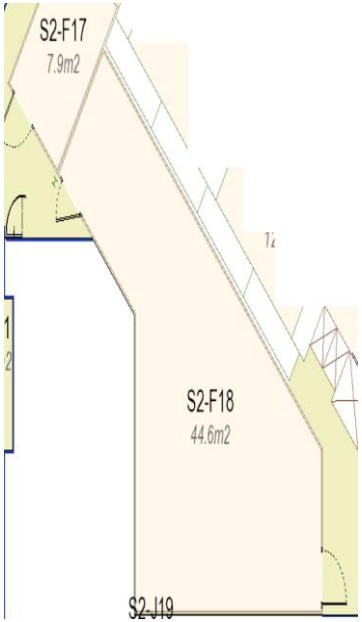
Site Installation & Commissioning
All mounting and cabling works on site are realized. The electrical cabinet is connected and final commissioning /DSO tests performed.

DOMAIN OF OUR PROPOSITION

Personnel Protection Systems @ CERN

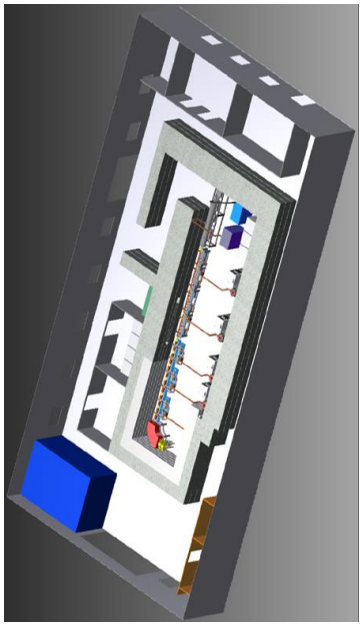
Small/Medium size
Safety Systems
Experimental Areas

Our proposition intends to help dealing more efficiently with this type of installations by reducing development and maintenance costs related to the logic controller part.



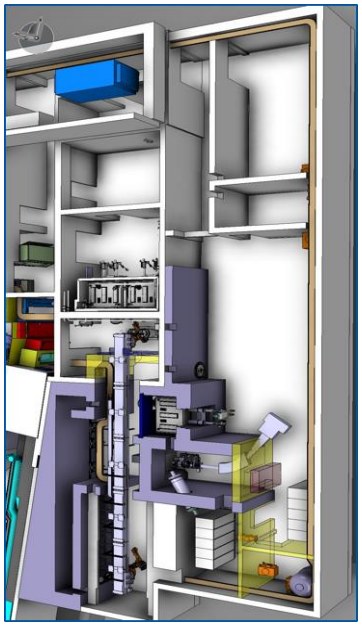
LASER ROOMS

Small rooms with 1 or 2 access doors and max 5 class-4 lasers.



ADAM-LIGHT

Small bunker with 1 only access door and few hazardous equipment inside.



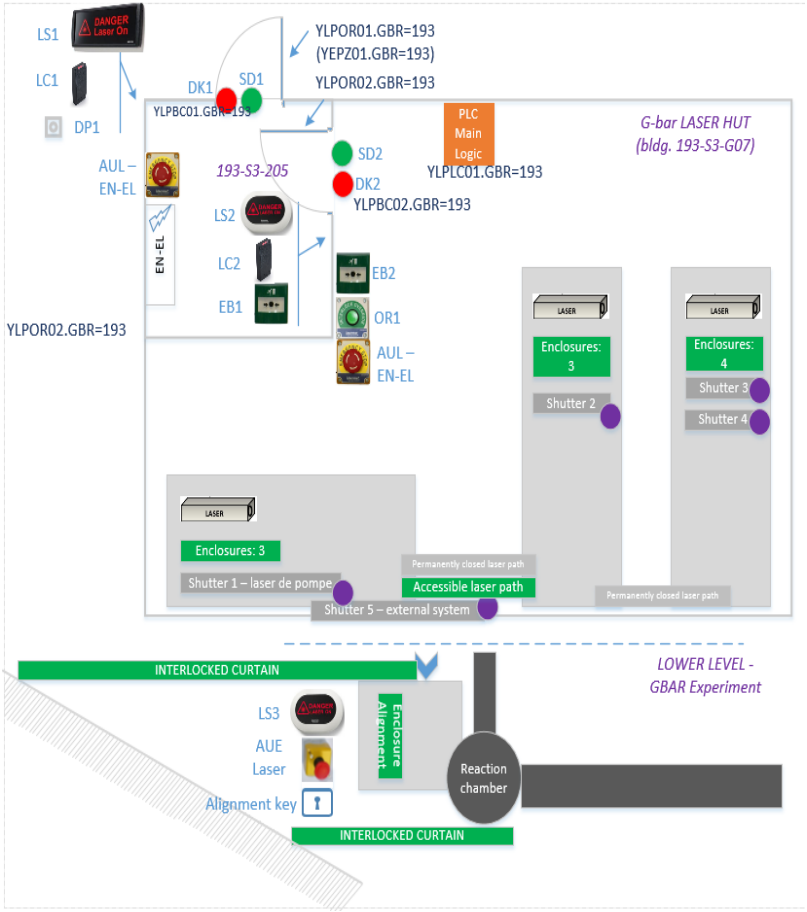
MEDICIS LAB

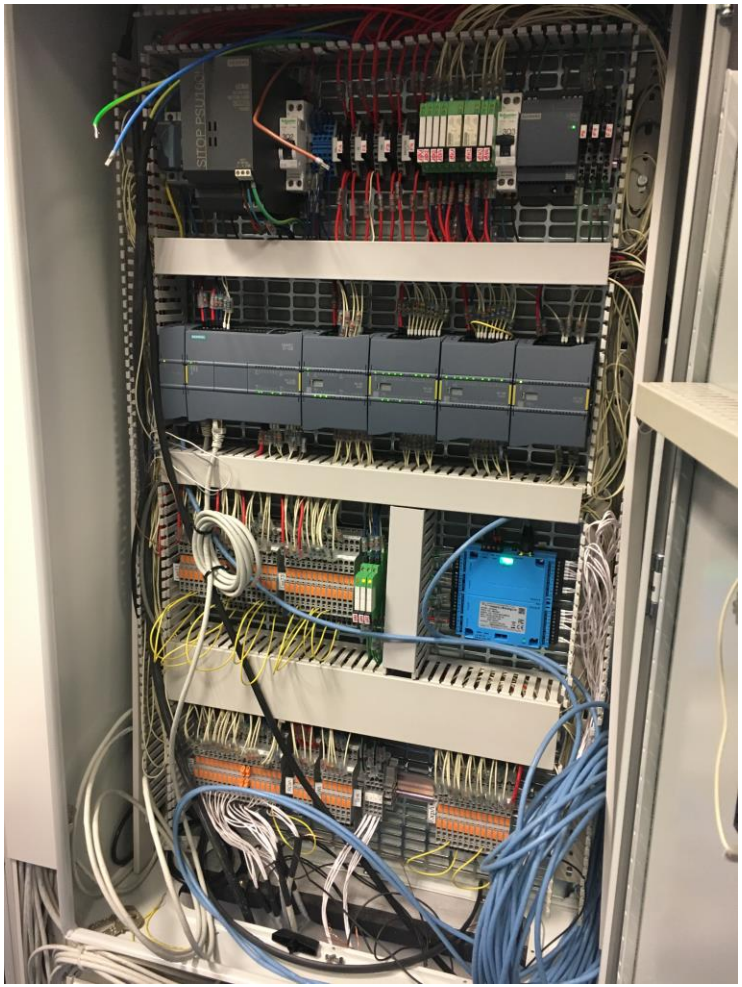
Few communicating rooms hosting radiological hazards.

TEN similar installations are expected per year !

Example: GBAR Laser Room Installation

Inputs: 21 **Outputs: 10**





Outsourcing cost for the cabinet: 30K CHF

Our Primary Objective

Make Affordable Safety

A safety system can effectively reduce damages to personnel operating in hazardous situations. The cost of the system shall be then considered as an investment that shall however remain reasonably proportional to the Value at Risk.

Reduce Costs for Material & Installations

The material costs for controllers and cabinets cabling are often prohibitive for small size experimental facilities funded by universities or other institutions.

Solution Compliant with SIL-2/3 Requirements

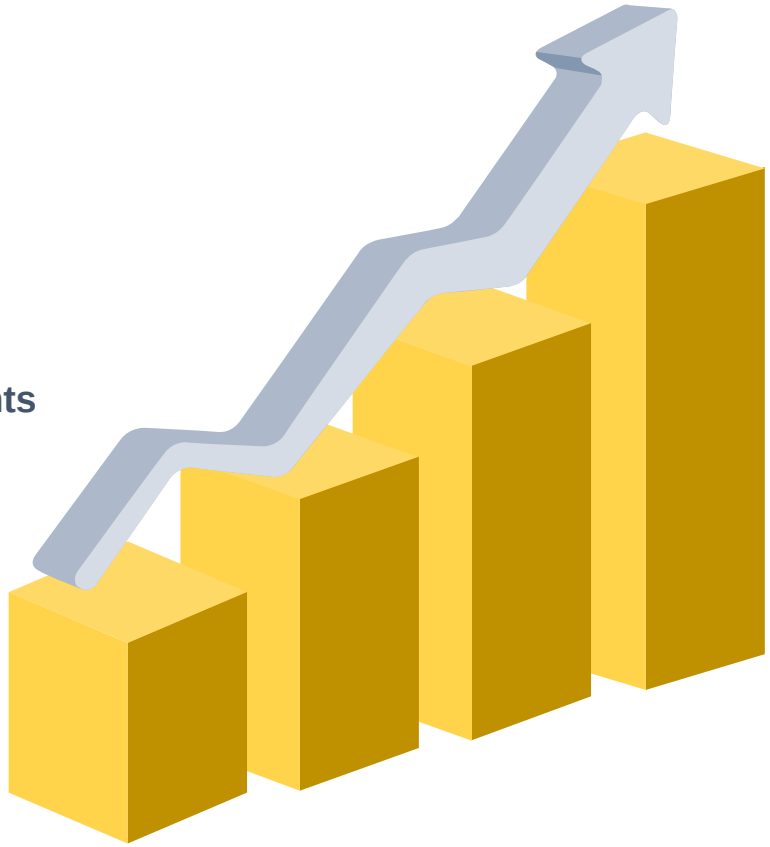
The conformity on any electrical / electromechanical device related to personnel safety shall be proven against the IEC-61508 standard.

No Specific Software Development

A model of development where any PPS installation has its own version of safety software can become unsustainable after few dozens of instances.

Minimal Maintenance

Minimize the decay of resources that, year after year, remain blocked into maintenance tasks.



Our Proposition

Acknowledgments:
University Federico II (Naples)

The R&D Activity: basic concept

TRIGGERING EVENT- RULES FOR VETO REMOVAL ON DOOR-1 DOOR:

(MODE_ACCE=1 V STOP_Int=0 V STOP_Ext=0 V Override_DOOR1=1)

OUTPUT → **VETO_DOOR1 = 0**

ELSE

OUTPUT → **VETO_DOOR1 = 1**

TRIGGERING EVENT- RULES FOR VETO REMOVAL ON DOOR-2 DOOR:

(MODE_ACCE=1 V STOP_Int=0 V STOP_Ext=0 V Override_DOOR2=1)

OUTPUT → **VETO_DOOR2 = 0**

ELSE

OUTPUT → **VETO_DOOR2 = 1**

TRIGGERING EVENT- CONDITIONS FOR SAFETY OVERRIDE OF DOOR 1:

(Int_PB1=1 V KeyPad1=1)

OUTPUT → **Override_DOOR1 = 1**

TRIGGERING EVENT- RULES FOR VETO REMOVAL FROM LASER X COVERED BY HOOD X:

LSR_X_Offline=0 ∧ (MODE_OPER=1

V

Hood_X=1 ∧ (MODE_ACCE=1 V MODE_PATROL=1))

OUTPUT → **VETO_LSR_X = 1**

ELSE

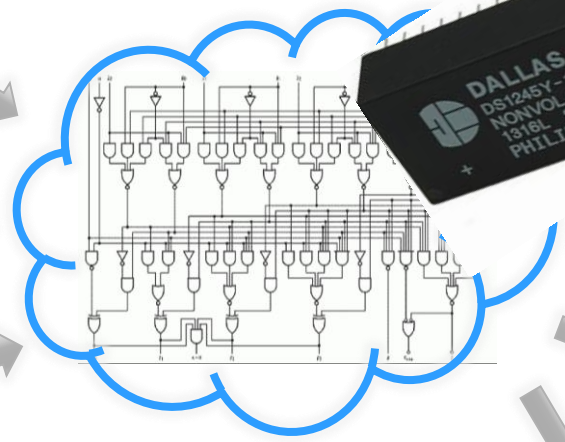
OUTPUT → **VETO_LSR_X = 0**

MTTF: 3'441 Years

10 Years data retention

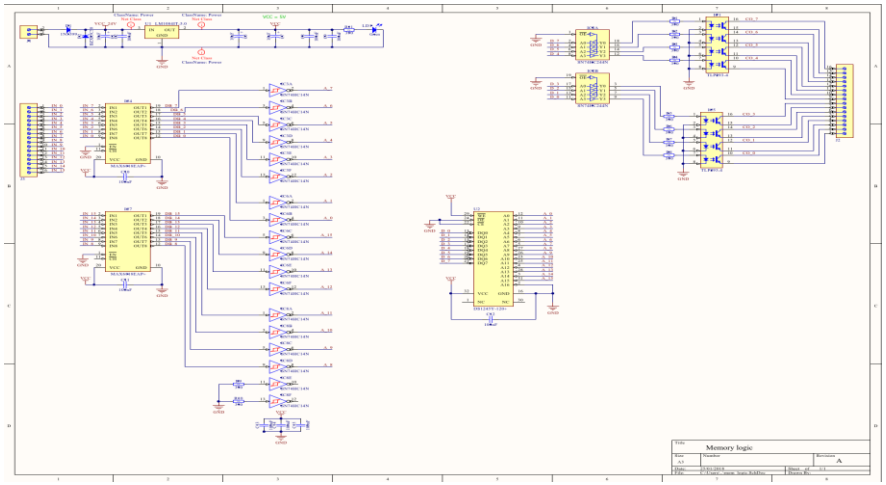
Very Simple Logic Solver

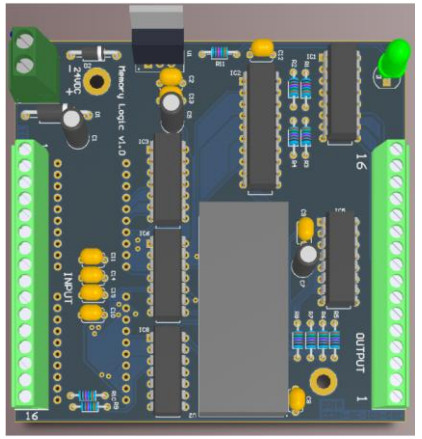
Lookup Table



Remote Monitoring

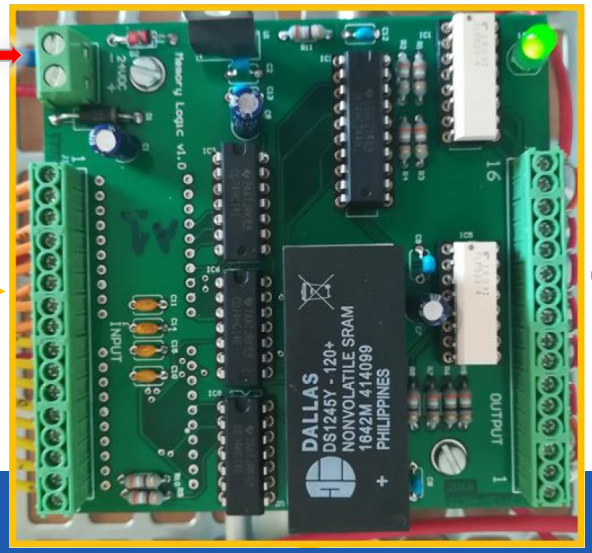
The R&D Activity: first prototype





24V

16 Digital Inputs



8 Digital Outputs

Development Milestones

I

Add new features: +GPIO, Network, local HMI, auto-diagnostic

II

Identify generic configurable interlock scenarios.

New design & prototyping phase.

III

2019

Reliability studies, tests & conformity certification

Pilot installation

SIL-3 certified

Conclusions

- **Our proposition allows to**:
  - Build compact boxes for mural fixation;
  - Eliminate costs for big cabinets design, cabling and PLC programming;
  - Reduce sensibly the maintenance works.

- **Fast return on investment after deployment of 2 small/medium size PPS.**

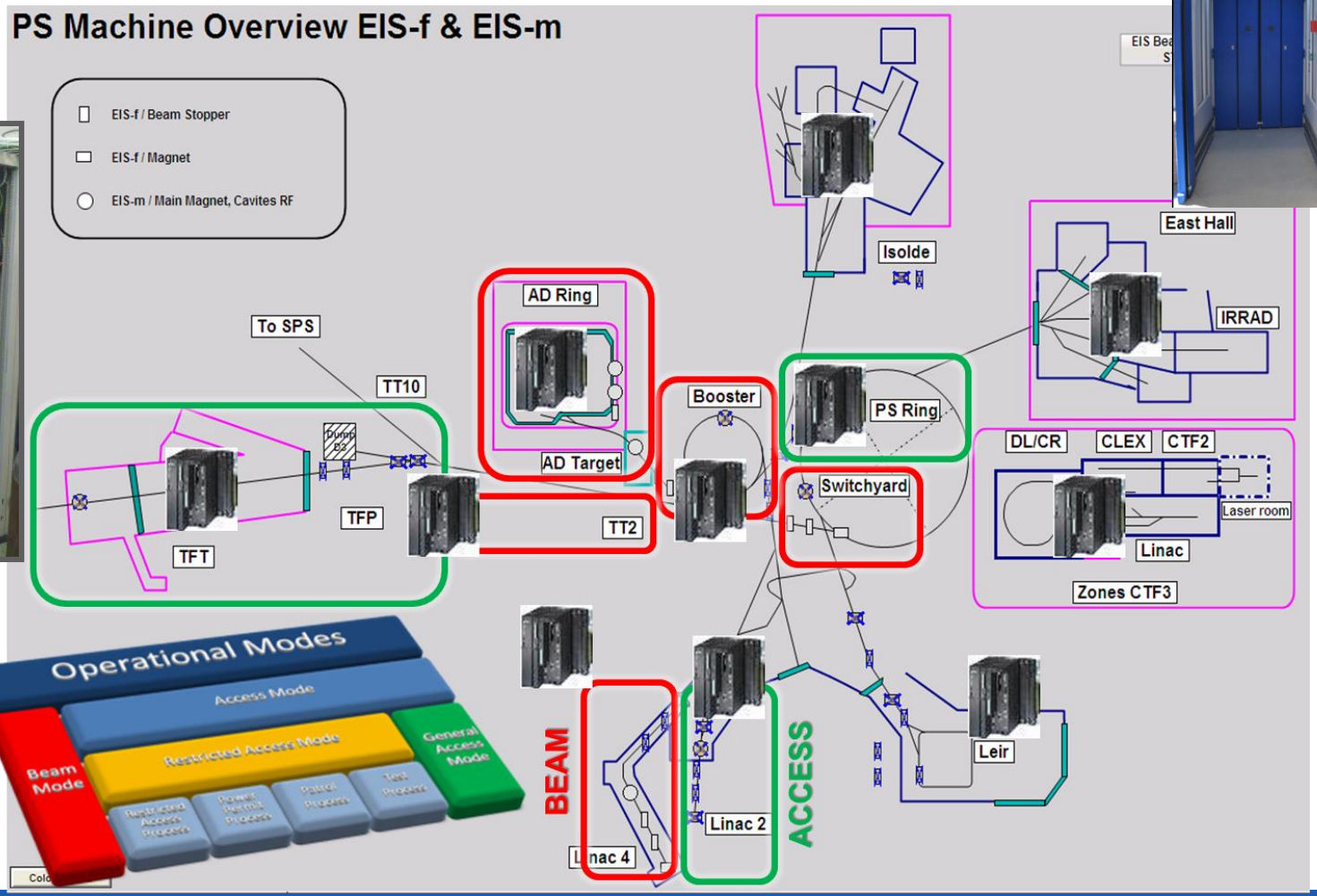
- **Potential applications for renovation of SPS North EXP Areas, 60 Laser rooms and other small facilities @ CERN.**

- **Other areas of application outside CERN**
  - Medical sector: interlock of radiological treatment rooms;
  - Other research laboratories: Alba, ITER, etc.
  - Industrial sector: interlock of hazardous machinery.

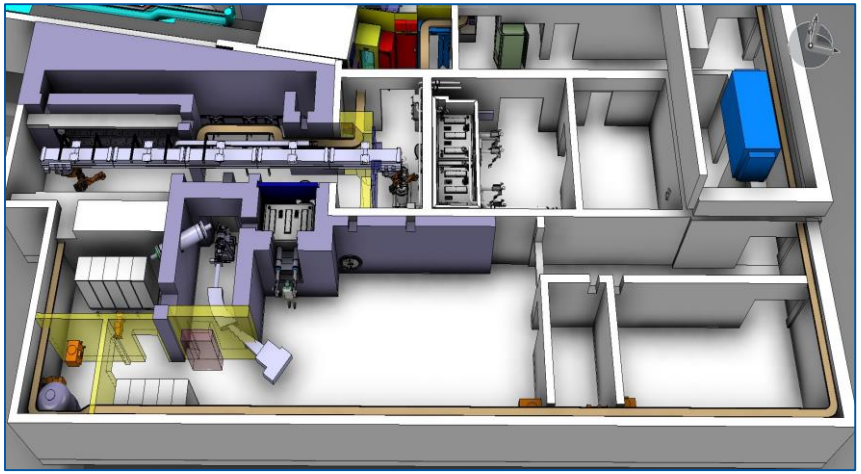

CERN

Personnel Protection Systems @ CERN

Large size accelerator Complexes (as LHC, PS, SPS)

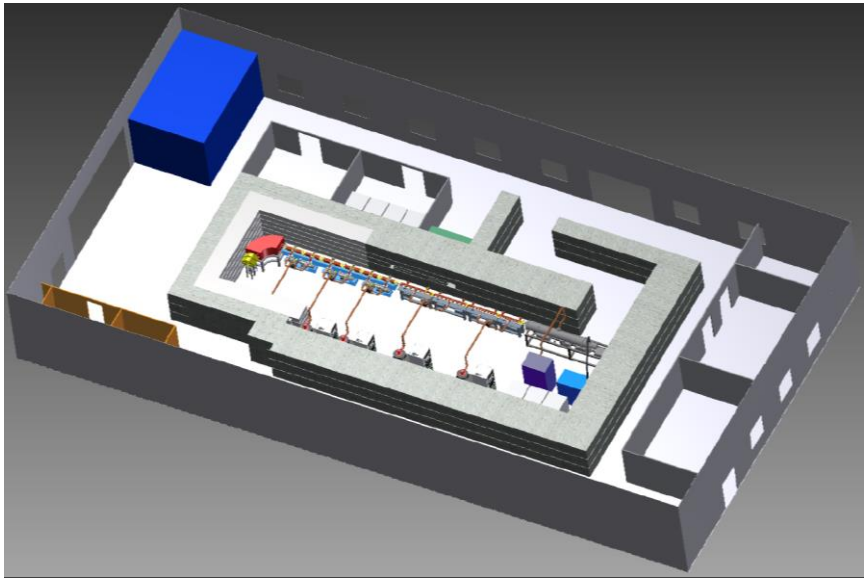


Small/Medium Size PPS (Experimental Areas)



MEDICIS LAB

ADAM-LIGHT Exp



TEN similar installations are requested per year to BE/ICS !

Main Limitations of PLC solutions

Most Basic PLC Configuration:

Siemens PLC 1200 Safety series

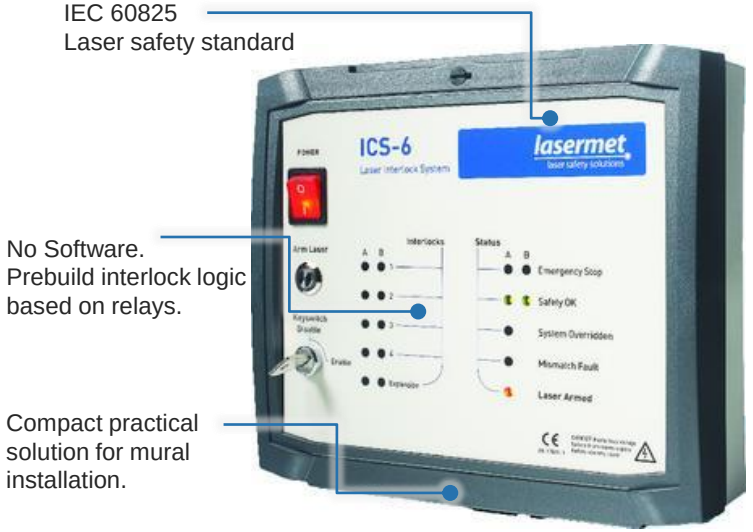
+

Siemens Simatic Panel

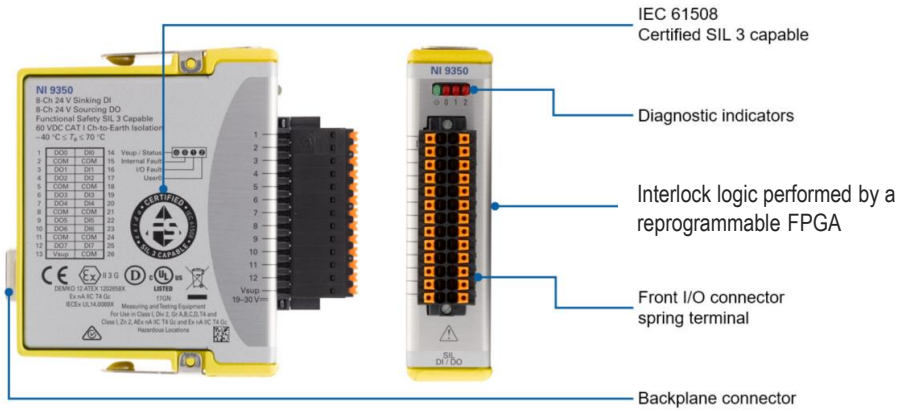
- **Cost of Material**: approx. 2’500 CHF for Siemens parts.
- **Production Time**: 1 staff engaged for *min* 2 weeks (1w cabinet mounting, 1w SW development & testing).
- **Maintenance Costs**: dozens of PLCs with different SW to be kept updated.
- **Siemens Update Policy**: annual new releases of PLC firmware and development software impacts on operation of the experiments.

Other available options: two products of interest

Lasermet ICS-6



National Instruments 9350

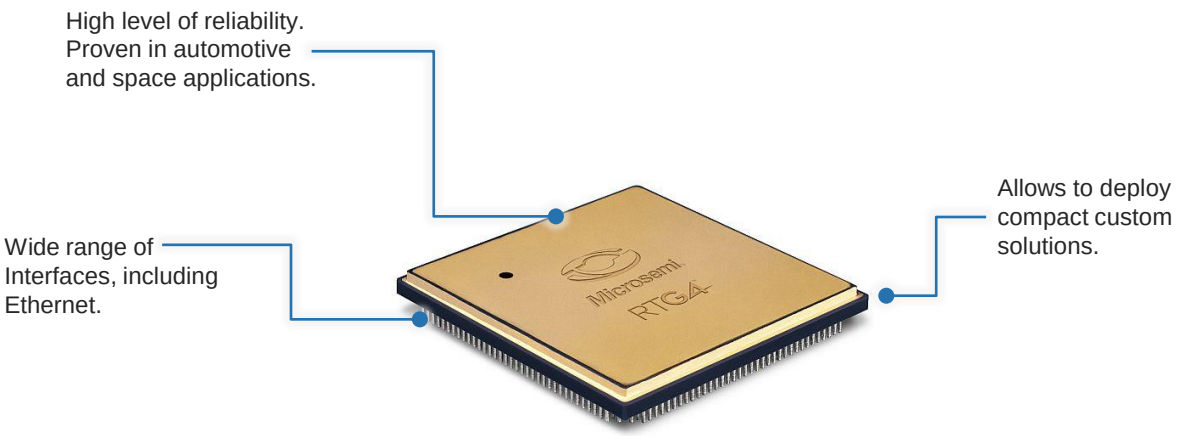


Disadvantages

- **Certified only against laser safety standard.**
- **Too limited prebuild interlock logic.**
- **Remote monitoring NOT possible.**
- **Very limited I/O space (8DI / 8DO) & no com between modules.**
- **Expensive: more than 1’000 usd.**
- **Remote monitoring only if integrated in a cRIO chassis.**

Other available options: FPGAs

Microsemi FPGA



Disadvantages

- **A certification against iec-61508 is not available.**
- **Specific techniques of redundant programming shall be adopted.**
- **Programming environment not certified against iec-61508.**
- **Integration in a custom PCB more complex: longer dev times.**

The R&D Activity: basic idea

MTTF: 3'441 Years

10 Years data retention

Lookup Table

16 INPUTS

- Each input combination address one specific cell.

MEMORY

Cell X: Rule1 Rule2 Rule3 Rule4 Rule5 Rule6 Rule7 Rule8

- 2^{16} cells to write;
- Each cell contains 8 bit;
- Each bit value represents a SIF result.

8 OUTPUTS

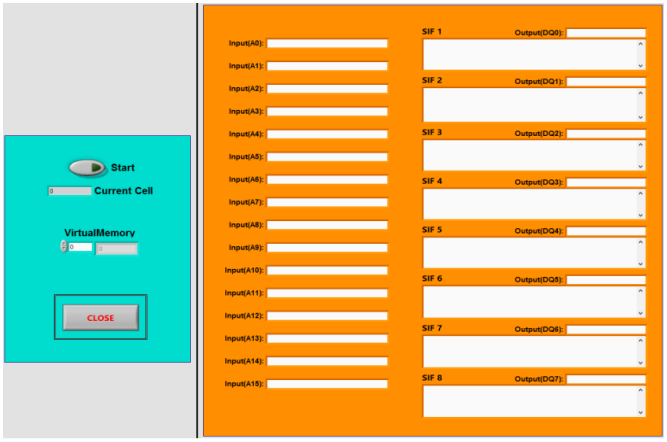
- Each output corresponds to one of the 8 bit contained in the addressed cell.

Simple Boolean Logic Computation

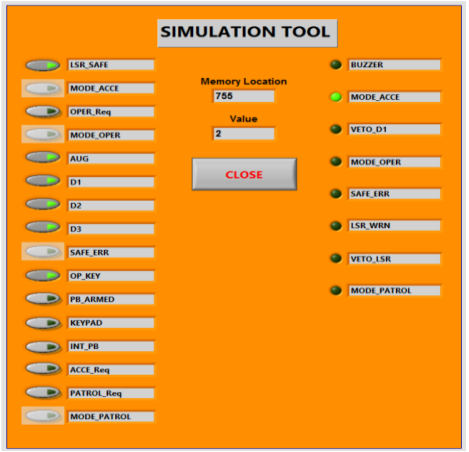
IF [*Premise*] **THEN** [*Action*]

The R&D Activity: software part

(1) Logic Specification



(2) Logic Simulation



(3) Memory Flashing

(4) Exhaustive Testing