Safety Alarms – to SIL or Not to SIL

Dordrecht – Process Safety Congress 2026

Marco Turdo

HIMA

SMART SAFETY.

#safetygoesdigital

Let‘s start with some definition

Alarm (IEC 62682 edition 2)
audible and/or visible means of indicating to the operator an equipment malfunction, process deviation, or abnormal condition **requiring a timely response**

Good practice > 20 minutes

Safety-related alarm
Safety alarm (IEC 62682 edition 2)

an alarm that is classified as critical to process safety for the protection of human life or the environment

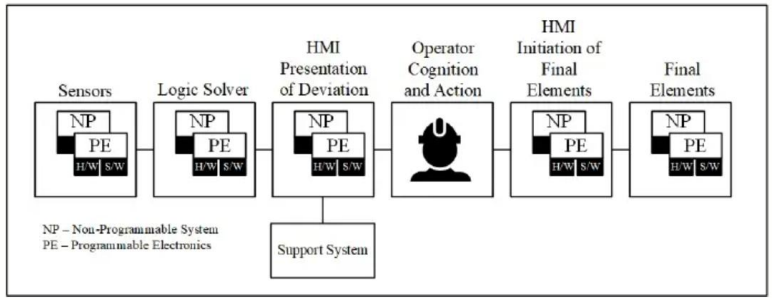


Figure B.1 – Example of safety alarm system architecture
Source: IEC 62682 rev2

Safety Instrumented System SIS (Extract from IEC61511 edition 2)
…
Note 3 to entry: A SIS may include human action as part of a SIF (see ISA TR84.00.04:2015, part 1).
…

So, in theory, we can have a SIL 3 Safety Alarm, right?

Easy correlations?

A risk reduction factor is assigned to it (e.g. RRF 100)

A safety alarm is a SIF that can have a SIL target

Safety Alarm as IPL

Safety Alarms are common IPLs identified during LOPA or other Allocation Methodologies

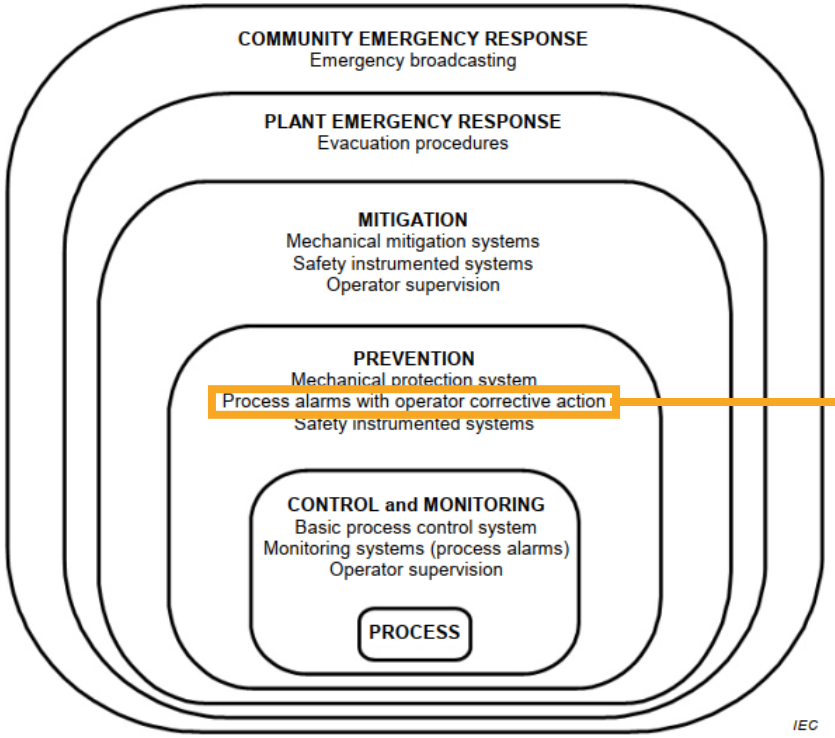
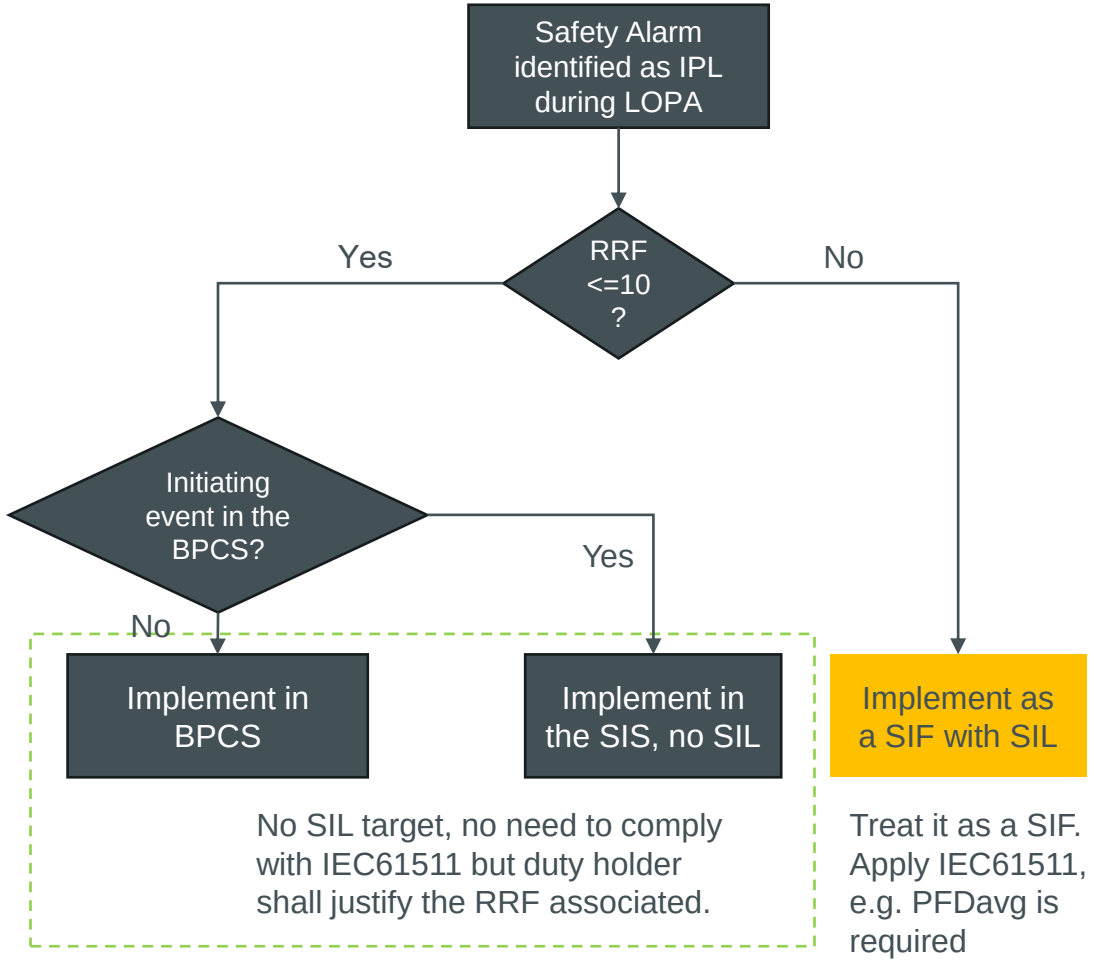


Figure 9 – Typical protection layers and risk reduction means

Source: IEC61511-1



…and now? It is too easy to give requirements

Is it only SIL or not SIL?

Building safety alarm justification

PST to be known

Alarm management system in place

Proof test on devices and audit program on alarm response

Adequate response time

Human factor of operator interface

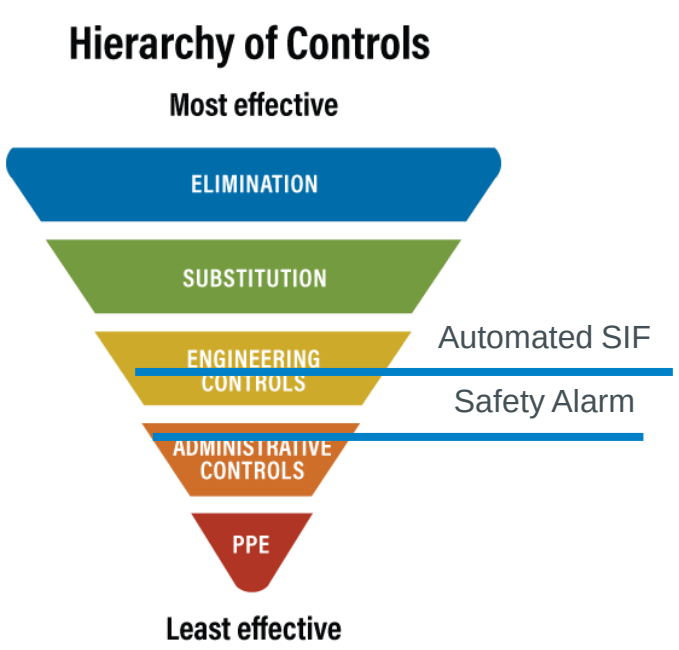
Standard operating procedure clear and accessible

Training and competence management

To SIL or not to SIL?

It is not the first question

1



Safety alarms are less effective than automated SIFs

2

Limit the Safety Alarm to RRF 10

Avoid to rely too heavily on Human Reliability

3

If a SIL target is needed, keep questioning the result like the UK HSE example

Reasonably Practicable to automate?

Operator Response within Instrumented Safety Functions in the Chemical, Oil & Gas, and Specialist Industries

Appendix 1: Process for Managing Instrumented Alarm Functions credited with risk reduction against MAH's

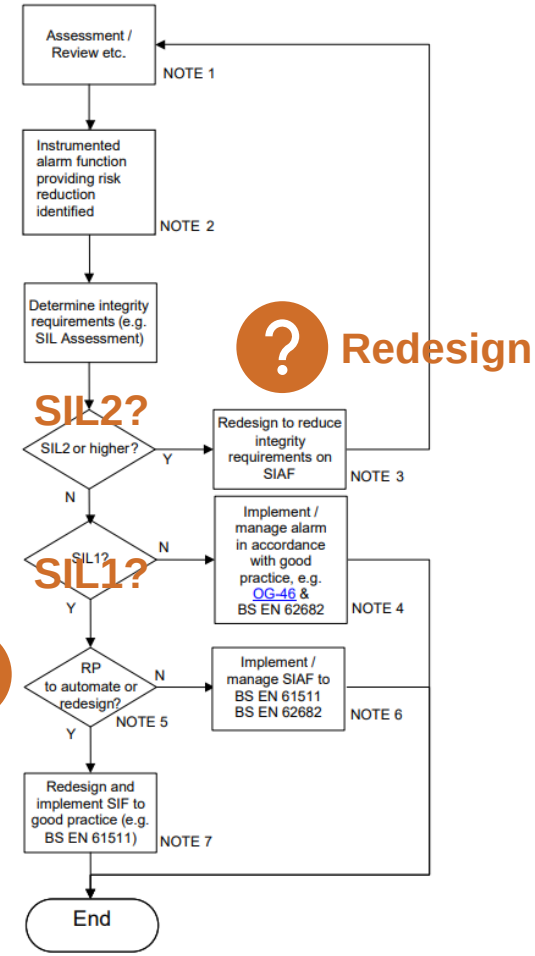
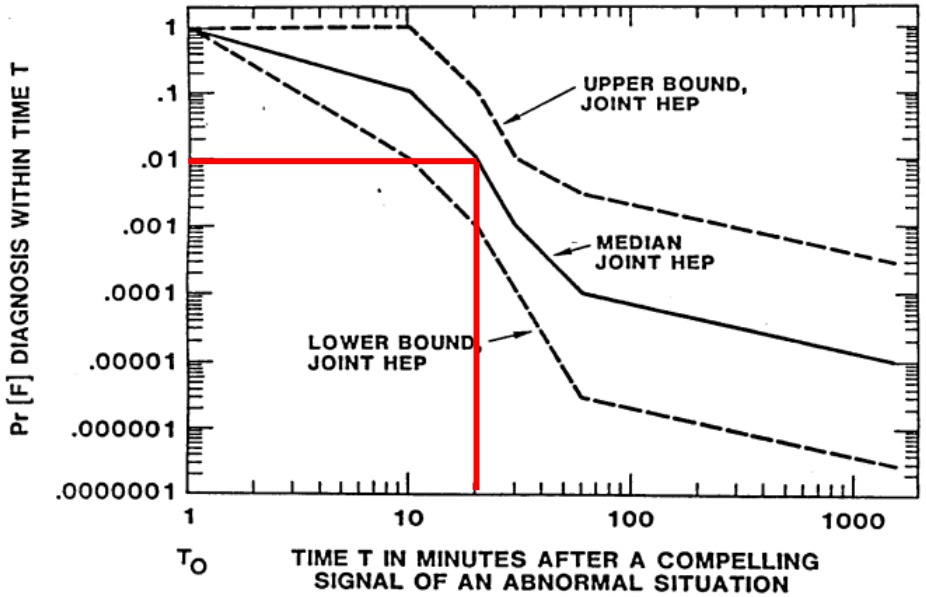


Figure 1: Process for the management of Instrumented Alarm Functions credited with risk reduction against MAH's

https://www.hse.gov.uk/foi/internalops/og/og-00047-appendix-1.pdf

Why SIL1 is considered the maximum?

Numerical response



NUREG/CR-1278 – The Human Reliability Handbook; guidelines from the US NRC on Human Reliability Analysis.

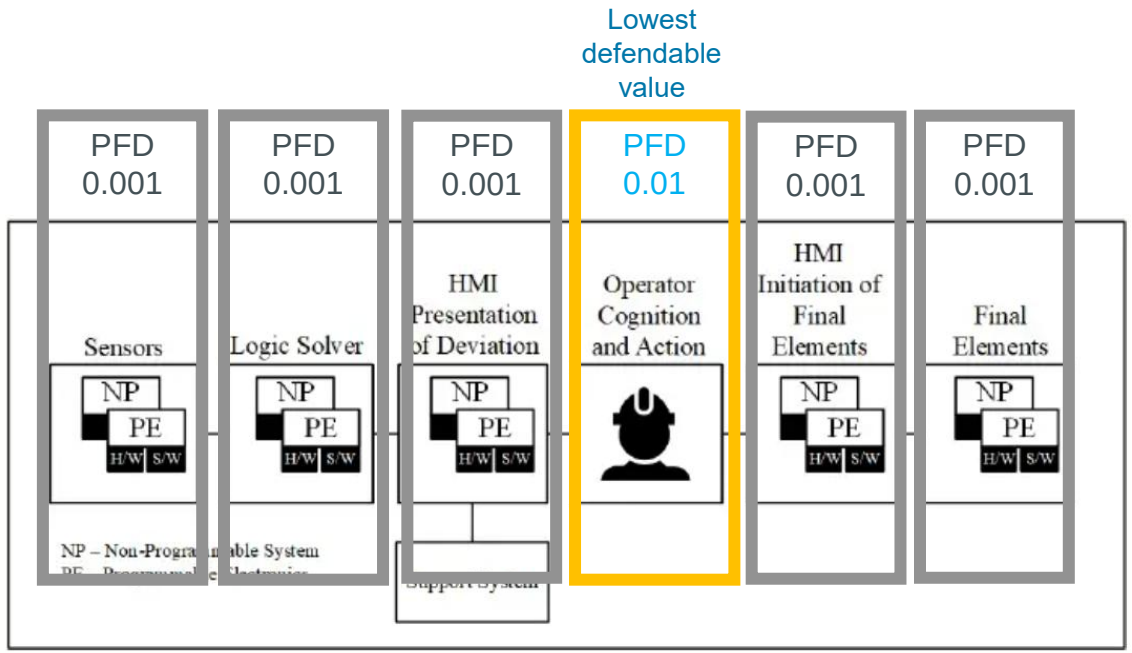


Figure B.1 – Example of safety alarm system architecture

Source: IEC 62682 rev2

Total PFD 0.015
=
RRF 66.7
=
SIL1

Not imagination, they are real

Quantifying human reliability

Can we trust quantification of Human Error Probability?

SIL means that we need to **quantify the human reliability** of an operator to respond to the alarm.

How do we quantify it?

Option 1

Table F.4 – Typical protection layers (prevention and mitigation) PFD_{avg}

Protection layer	PFD_{avg}
Control loop	$1{,}0 \times 10^{-1}$
Human performance (trained, no stress)	$1{,}0 \times 10^{-1}$ to $1{,}0 \times 10^{-2}$
Human performance (under stress)	0,5 to 1,0
Operator response to alarms	$1{,}0 \times 10^{-1}$
Vessel pressure rating above maximum challenge from internal and external pressure sources	10^{-4} or better, if vessel integrity is maintained (that is, corrosion is understood, inspections and maintenance is performed on schedule)

NOTE The figures in Table F.4 are illustrative of the range of values that could appear in assessments. These values cannot be taken as generic probabilities and used in specific assessments. Human error probabilities can be appropriately assessed on a case by case basis.

Source: IEC 61511-3:2016 Clause F.6 Table F.4

Option 2 **HEART** Human Error Assessment and Reduction Technique

Option 3 **THERP** Technique for Human Error Rate Prediction

Can results of HRA figure be considered static?

This number is influenced by those factors…are those factors static?

- Time Pressure
- Experience
- Mental Model
- Procedures
- Feedback
- HMI / Signals
- Workload
- Stress / Env.
- Checking
- Risk Perception

Source J. C. Williams (2015) Heart—A Proposed Method for Achieving High Reliability in Process Operation by Means of Human Factors Engineering Technology, Safety and Reliability, 35:3, 5-25

= Avoid safety alarms with RRF > 10 if you can and if you cannot, make them as reliable as possible

Can technology support the operator?

Let’s focus here on the alarm detection and operator support

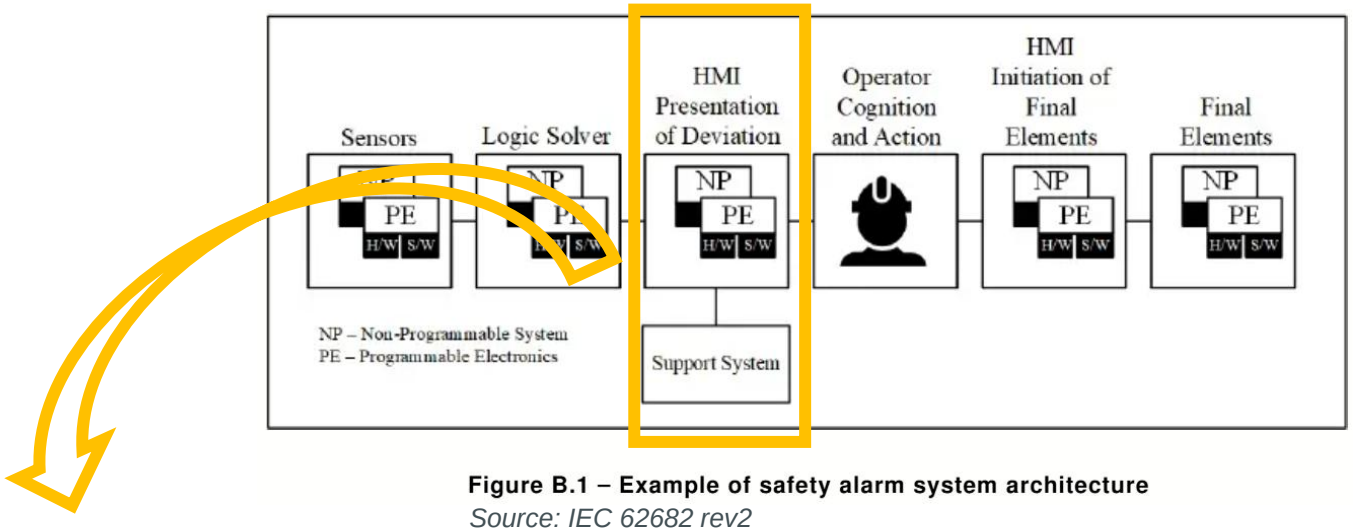
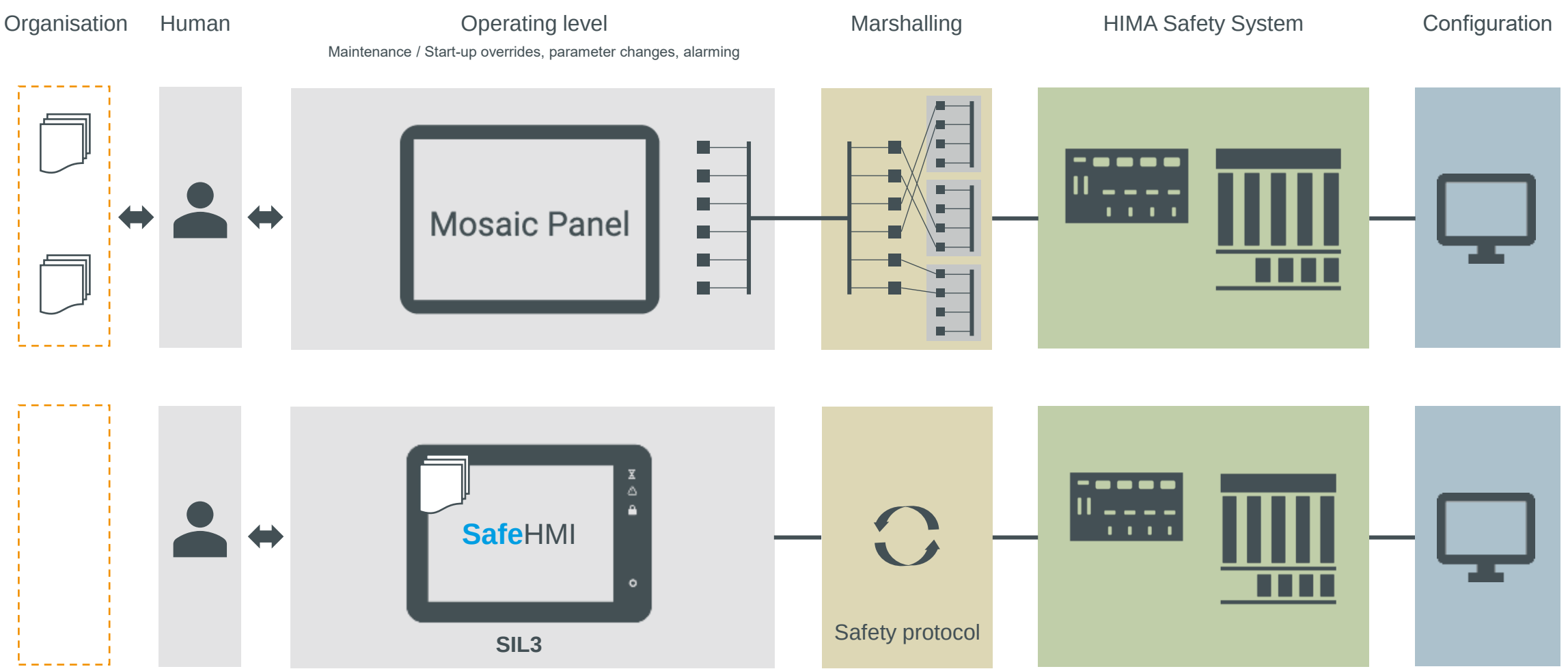


Figure B.1 – Example of safety alarm system architecture
Source: IEC 62682 rev2

Typical issues with alarm presentation:

- Alarm panels are not IEC61508 developed / certified
- Require frequent proof testing
- No contextual information or operator guidance (cause, consequence, required action)
- Lamp failure remain unnoticed until test (without specific line monitoring solution)
- Addition, deletion, or modification of alarms require hardware and/or software changes, increasing complexity and risk of errors

Reliable HMI and accessible SOPs



Conclusions

- Limiting Safety Alarms is the golden rule
- The criticalities around Safety Alarms go beyond the numbers
- Human factors are dominating the limitations of Safety Alarm reliability
- If a Safety Alarm gets a SIL target, justification is normally possible up to SIL1 only
- Improving the design of Safety Alarms is one of the key action to reduce human factors

Visit HIMA Stand to know more about the new SafeHMI.

Contact

Director of Safety Lifecycle Digitalization

marco.turdo@hima.com
www.hima.com