Improving Safety Systems with better risk assessment and digital tool

HIMA SMART SAFETY.

#safetygoesdigital

Arnoldi Davide

Principal Safety Consultant

About Me

Davide Arnoldi

Principal Safety Consultant

- 17 years of experience in Functional Safety
- Certification as FSEngineer TUV Rheinland and Expert by UL
- Facilitator for H&R STUDIES (HAZID/HAZOP/C-HAZOP/FTA)
- Facilitator for SIL determination (LOPA/Risk Graph)
- Expert in SIS design in various fields (Oil & Gas, Petrochemical, Power, Pharma, etc.)
- Trainer for Functional Safety courses

HIMA Group Today

HIMA CONSULTING

Independent
Family Business
in 4th Generation

1050
Employees

Global footprint
20 Country units with
local sales, Engineering and
Service

Safety DNA
Technology Leader
Functional Safety

Protection from
People, Assets and Environment

Qua
Ma n
G many

Customers
Process Industry
Industry

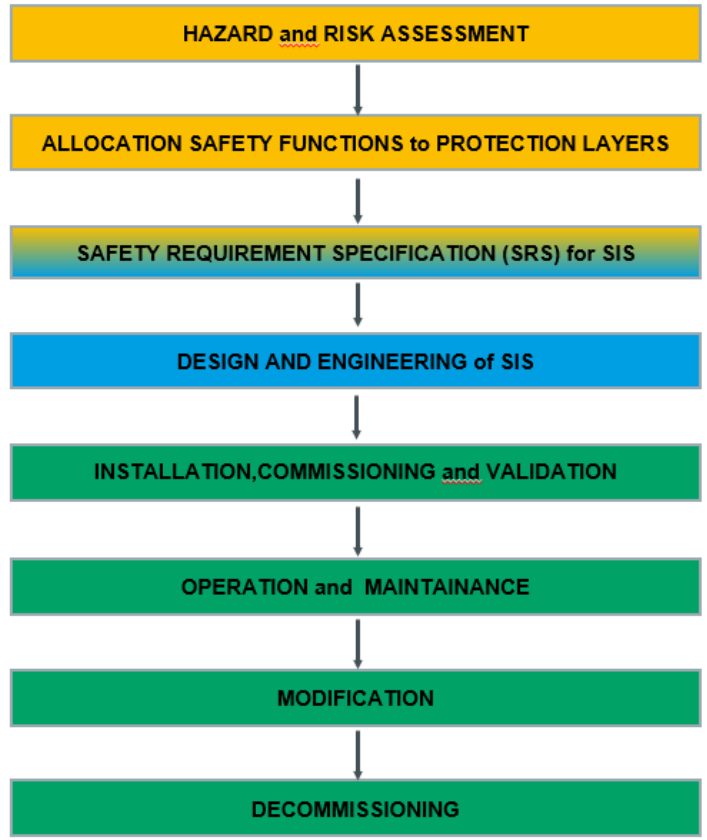
50,000 systems
installed worldwide
(SIL 3 / SIL 4)

EUR
Sale

Agenda

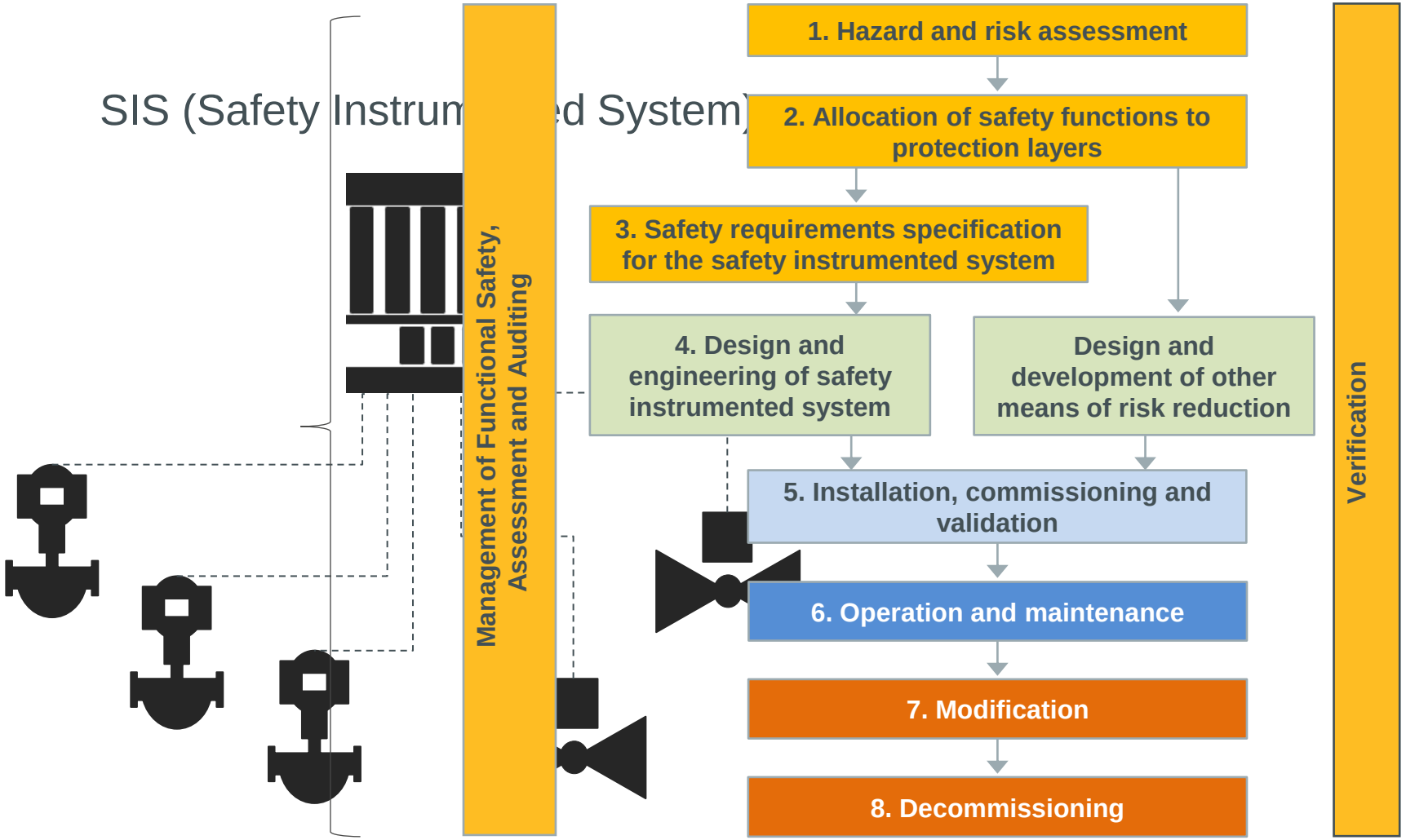
HIMA CONSULTING

1. Importance of H&R and SIL determination
2. Experience teaches... Real cases
3. Information management, the HIMA digital revolution
4. Conclusions



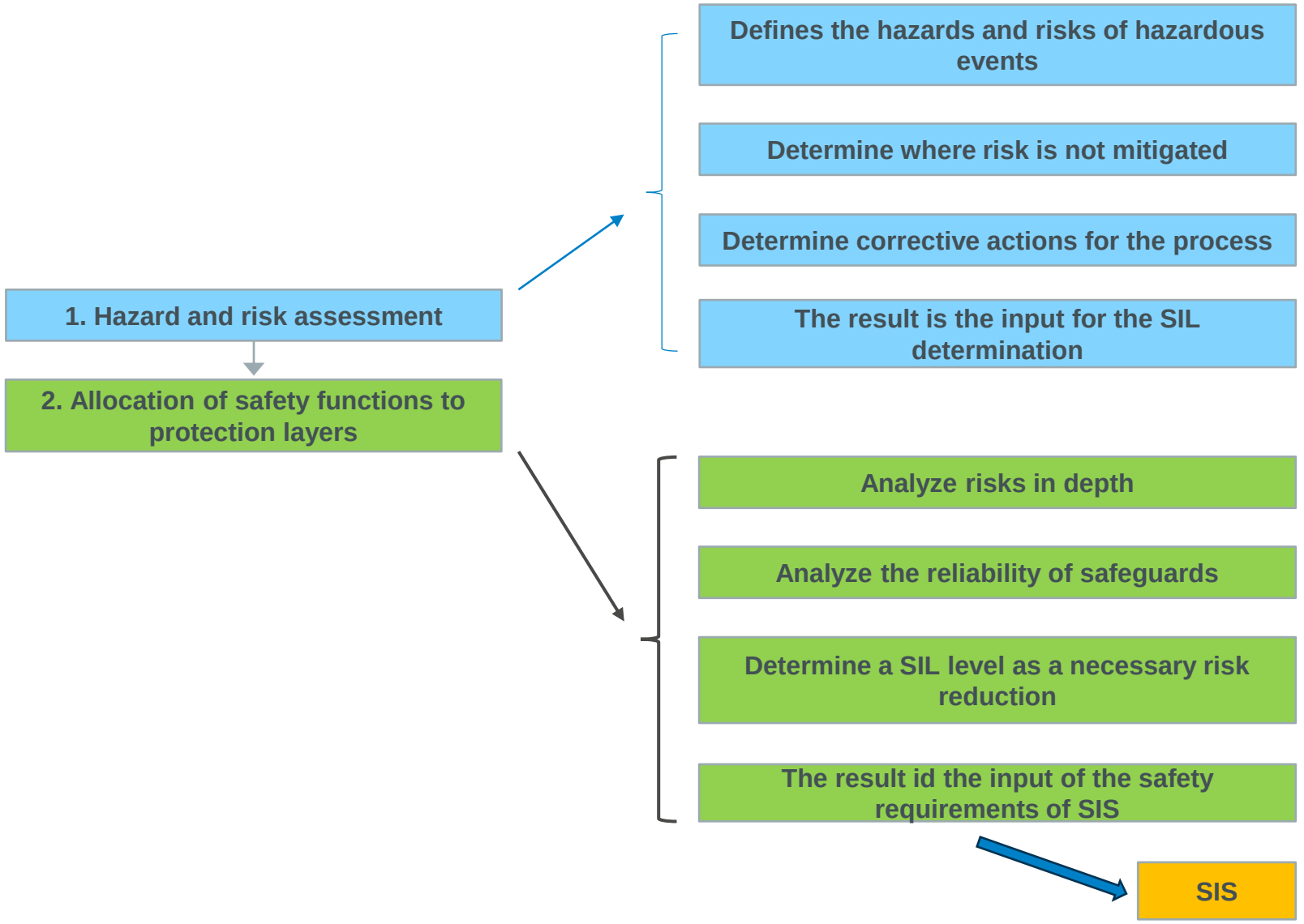
Importance of H&R and SIL determination

IEC61511 target

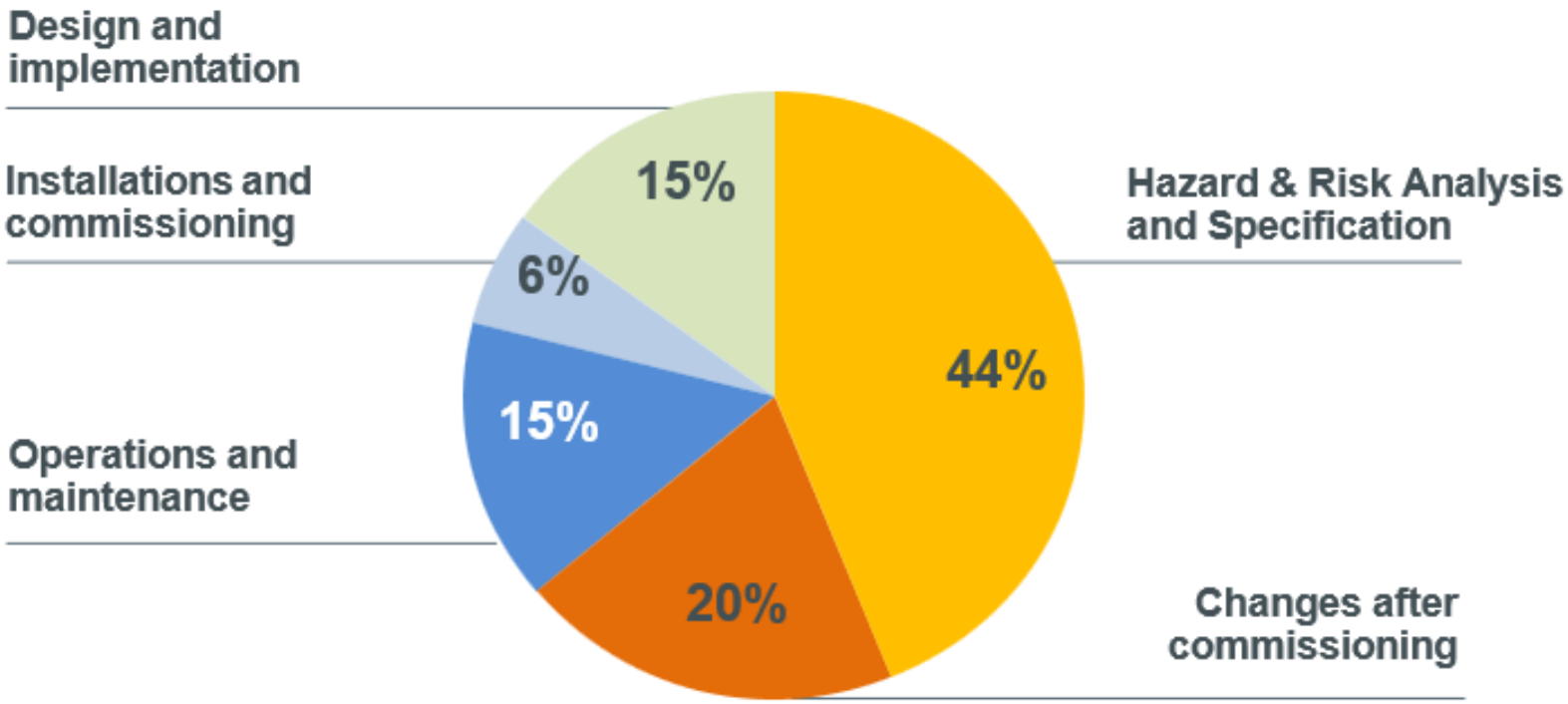


SIS Lifecycle, IEC 61511

H&R and SIL determination



Causes of major accidents



Out of control: Why control systems go wrong and how to prevent failure?
(2nd edition, source: © Health & Safety Executive HSE - UK)

Experiences teaches... real cases

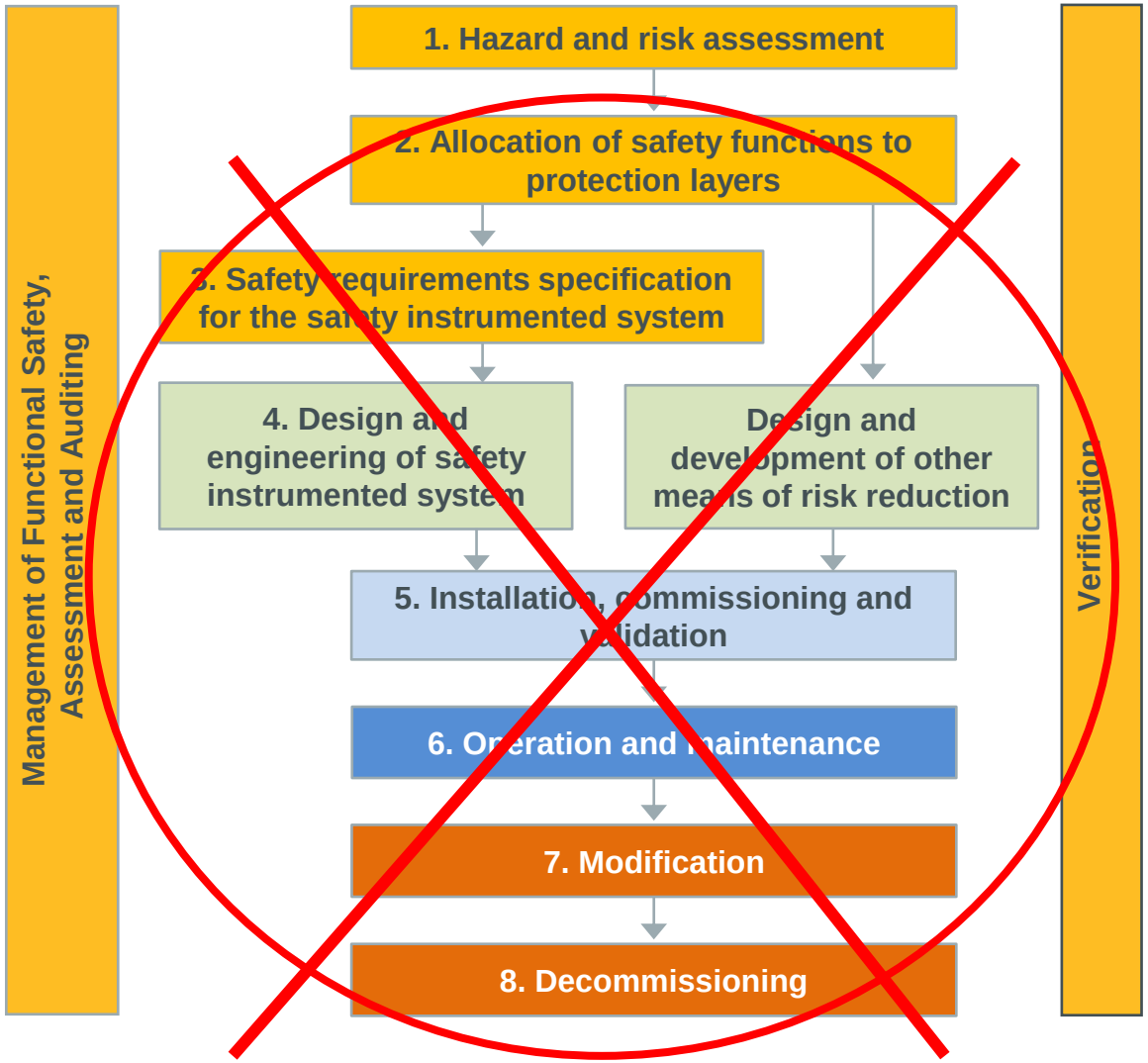
HAZOP "evergreen"

HIMA CONSULTING

DEVIATION	CAUSES	EFFECTS	S	F	Risk	PROTECTIONS	S	F	Risk
Less pressure	Failure pump P92 functioning ?	No water flow to SR91. Reduction in SR91 cooling efficiency. SR91 meltdown	4	4	H	LSL 90703 detects low level in steam drum (SD91) and initiates shutdown FIT 90602 detects low flow with operator intervention, low low flow initiates shutdown	1	2	L
	Manual valve HV 90609 in pump P92 suction closed	No water flow to SR91. Reduction in SR91 cooling efficiency. SR91 meltdown	4	4	H	LSL 90703 detects low level in steam drum (SD91) and initiates shutdown FIT 90602 detects low flow with operator intervention, low low flow initiates shutdown	1	2	L
	Manual valve HV 90613 in pump P92 discharged closed or automatic valve XV90603 closed by error ?	No water flow to SR91. Reduction in SR91 cooling efficiency. SR91 meltdown	4	4	H	LSL 90703 detects low level in steam drum (SD91) and initiates shutdown FIT 90602 detects low flow with operator intervention, low low flow initiates shutdown	1	2	L
	PCV 90701 failure (totally opened), reduced pressure in steam drum	Steam drum depressurization, the evaporation is at 100 °C, losses of water, pressure and thermal stress of the coil in the steam generator with possible damage	4	4	H	1. PIT 90701 on steam drum initiates SD for LL alarm TIT 90702 on steam drum LSL 90703	1	2	L

- Incomplete information in the definitions of causes and effects
- Incorrect assessment of risk reduction
- The risk is always mitigated but incorrectly
- HAZOP development on Excell sheet – stand alone data

HAZOP "evergreen" - result



As per HAZOP no SIS required!!

(but in reality, the risk remains!)

LOPA

Initiator Event	Event Frequency	Conditioning modifier	Prob.	Naked risk	TF	IPL	PFD	Freq reached	SIL
Failure of P-0130	0.1	Only 10% of the time an operator is present	0.04	0.004	0.01	when flow at FIT-30101 is less than set point stop reactor using the emergency shutdown (SD This is a SIL-1 interlock.	0.1	0.0004	1

- Incorrect LOPA methodology
- SIF not defined
- LOPA development on Excell sheet – stand alone data

LOPA (restudied)

Let's see the result without considering the SIF inserted.

Initiator Event	Event Frequency	Conditioning modifier	Prob.	Naked risk	TF	IPL	PFD	Freq reached	SIL
Failure of P-0130	0.1	Only 10% of the time an operator is present	0.04	0.004	0.001	NO	0	0.004	NO

In this case the SIF was not necessary and therefore:

- We could have saved on engineering hours;
- We could save on the quantities and characteristics of the devices to be purchased;
- We could save on installation, commissioning, maintenance and test;

The result of the Hazard & Risk and SIL determination assessments defines the size of the SIS.

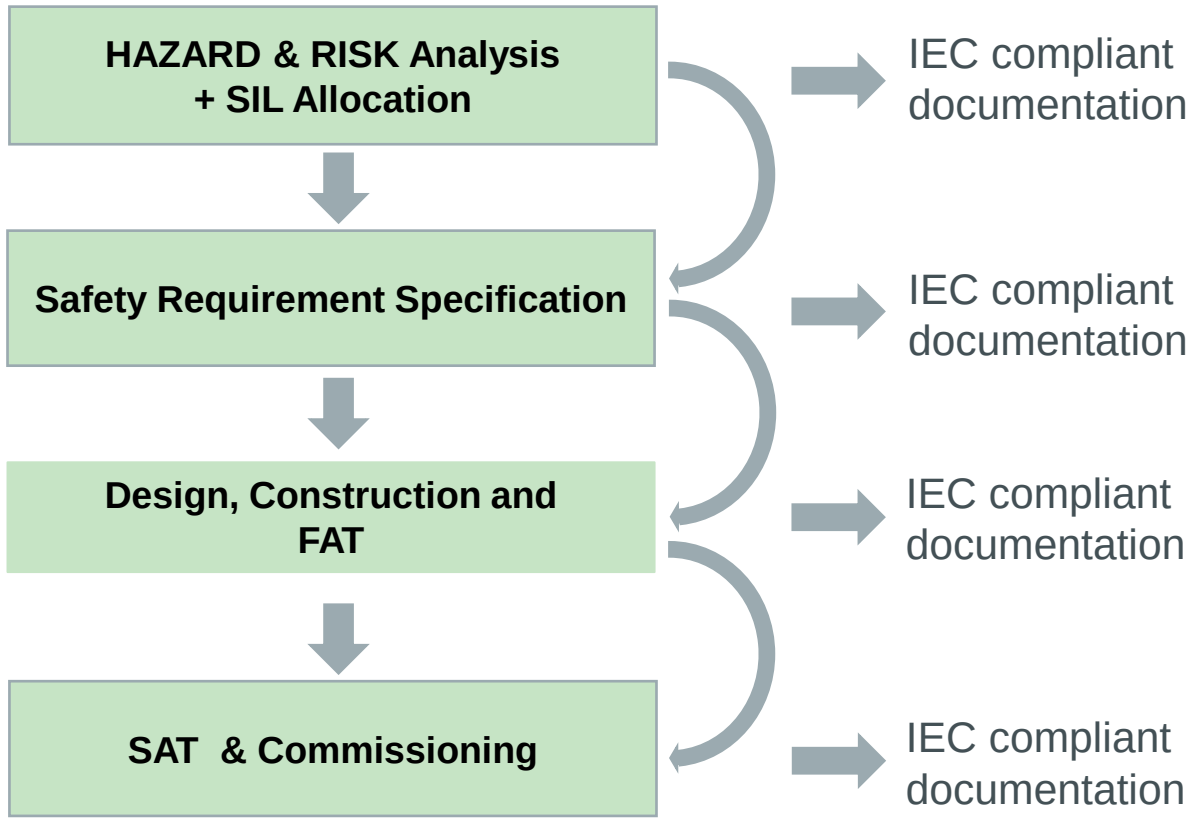
From this point it is always difficult to go back!

Information management, the HIMA digital revolution

Application Lifecycle IEC61511

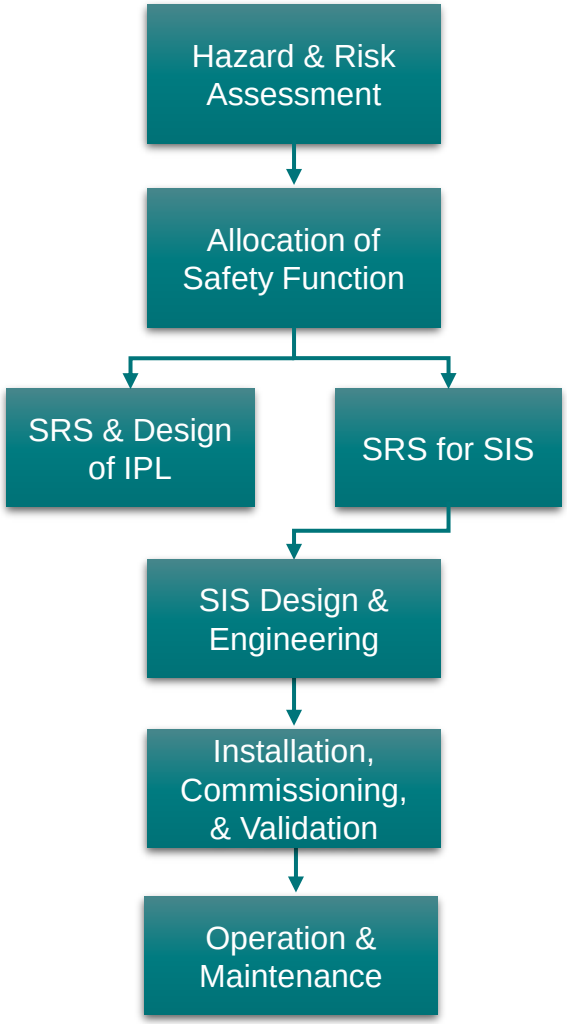
IEC 61511 emphasizes that information as Input and Output in all steps of the life cycle must be:

- **Free from any ambiguity**
- **Clear**
- **Traceable**
- **Precise**
- **Verifiable**



Setting a FS Management System is Complex

HIMA CONSULTING

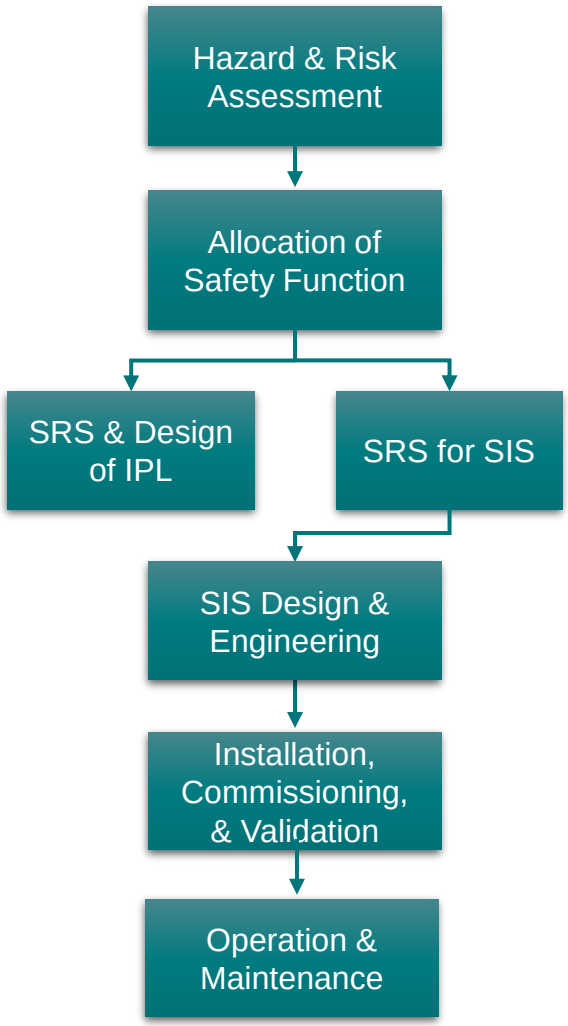


Activity	Responsible Today	Data Management Today
HAZOP, LOPA, Safety Case	Customer / EPC Contractors / HIMA / Free-lancers	Excel, PHA Pro, ExSILentia
		LOPA Spreadsheet Excel,SIFPRO
SRS development, SIL Compliance, Hardware/ Software design, FAT	Engineering Companies/ Free-lancers	Design Documents, Specification sheets, Drawing Manual, Comos
	System Integrators, SIS vendors, HIMA	Excel, Paper Documentation, SharePoint
SAT, Functional Safety Assessment, Proof Tests	System Integrators, HIMA	
	Customer‘s Personal	Oracle, SAP, Access, Automation Level

16

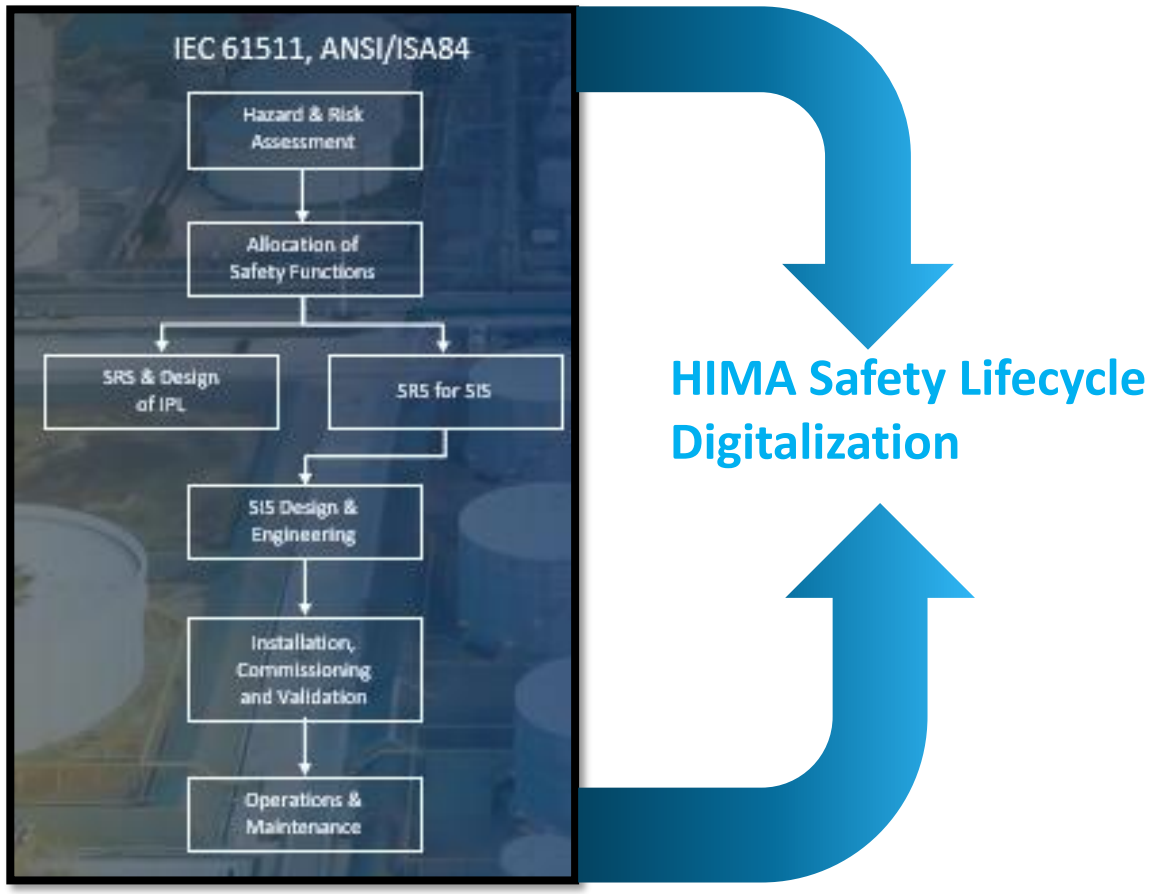
Complexity increases the gap...

HIMA CONSULTING



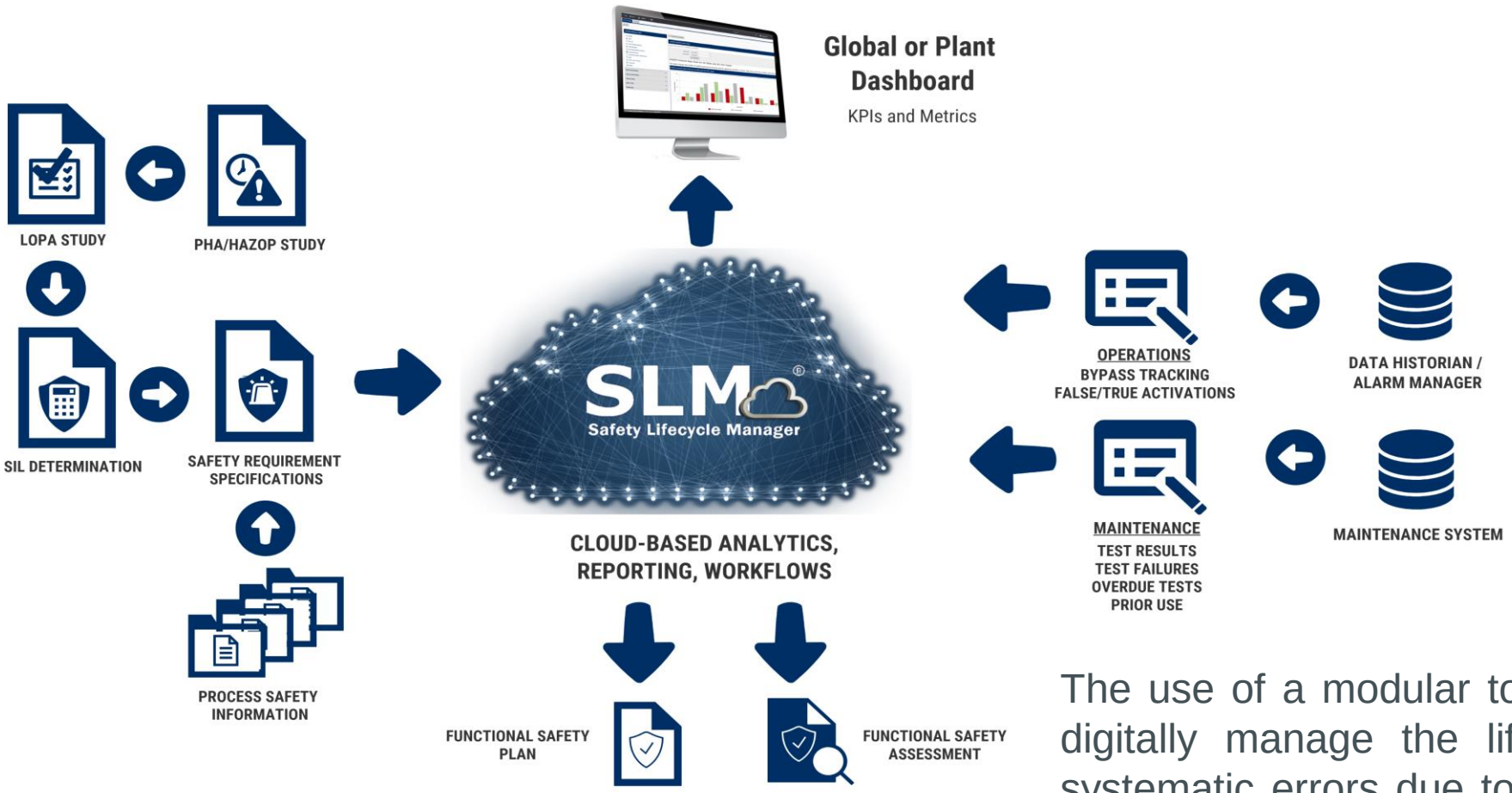
17

Digitalization = simplify



HIMA Safety Lifecycle Digitalization

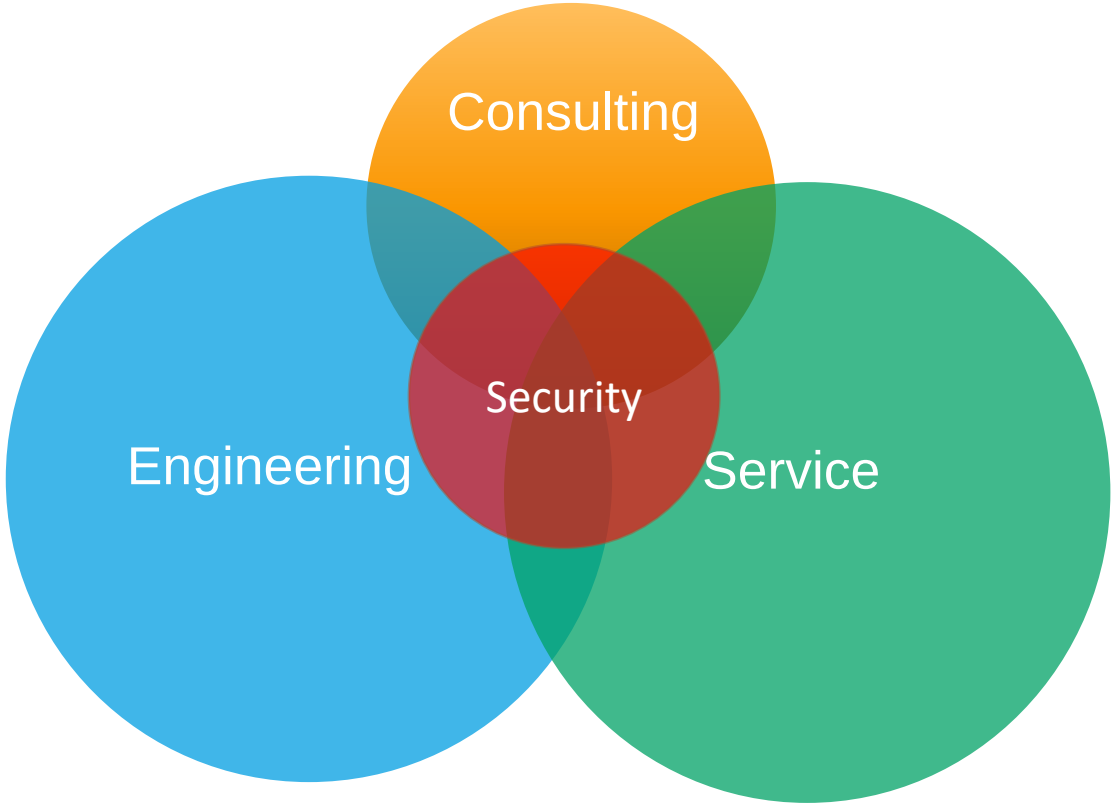
SLM: "The Only Source of Truth"

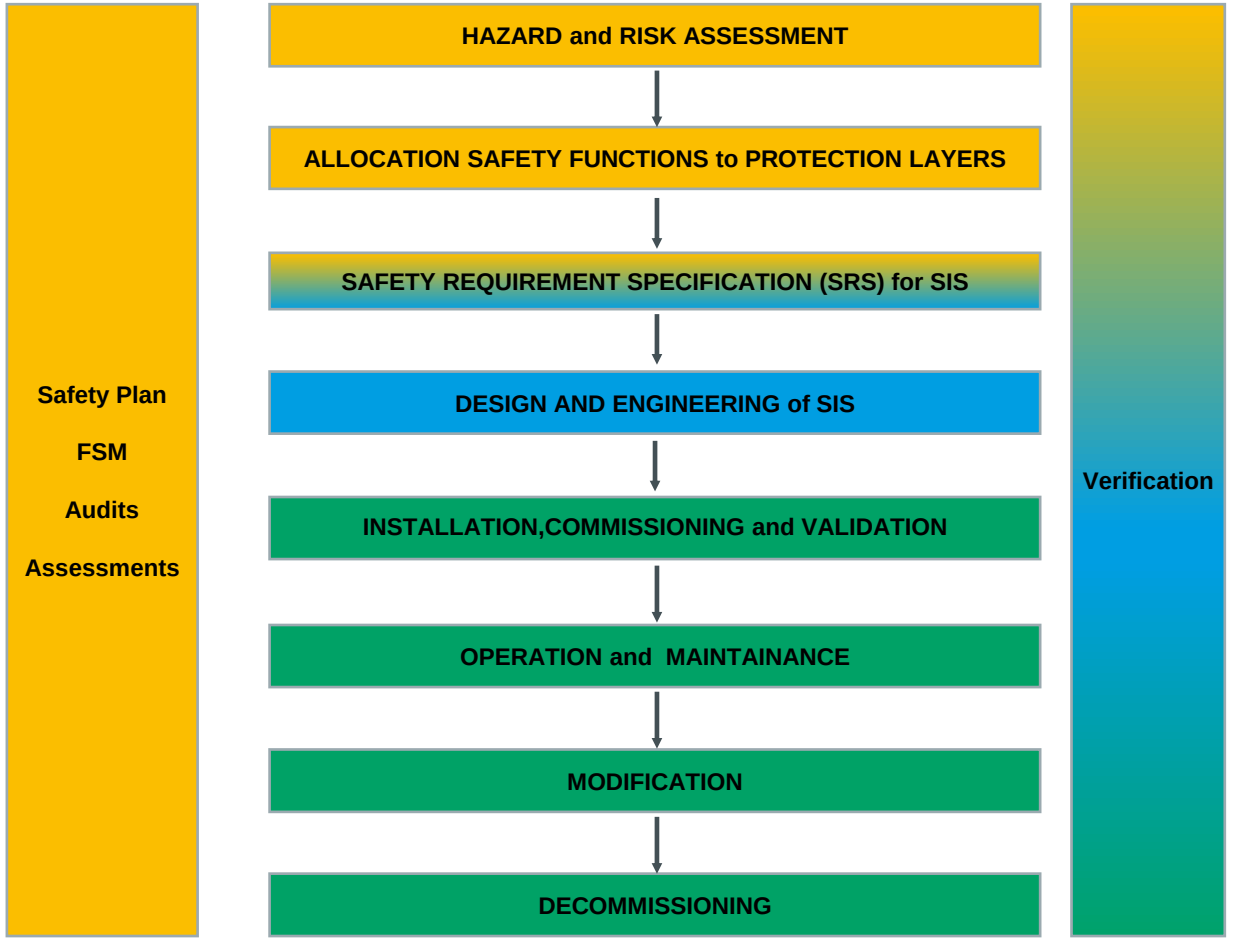


The use of a modular tool such as SLM allows you to digitally manage the life cycle of the FS, reducing systematic errors due to information transfers between the various steps.

In this way, SIFs requirements are always traceable and available over time!

Consulting & Service & Engineering Activities





Source: overall IEC 61511 lifecylce model

Conclusions

HIMA CONSULTING

- H&R and SIL determination are two fundamental steps for SIS design
- Performing H&R and SIL determination correctly allows you to define SIFs appropriately for the associated risk
- Using a digital tool such as SLM allows you to track the life of the SIF, always keeping the requirements available
- HIMA consulting as a single point of reference for the development of SIS projects including digitalization of the FS mmanagement

Contacts

HIMA CONSULTING

Davide Arnoldi
Principal Safety Consultant

M +39 366 574 7985
davide.arnoldi@hima.com
www.hima.com

HIMA SMART SAFETY.