

# Functional safety digitalization to improve MOC and HAZOP Revalidation



SMART  
SAFETY.

Dordrecht, May 14<sup>th</sup>, 2025

Marco Turdo

HIMA Paul Hildebrandt  
GmbH

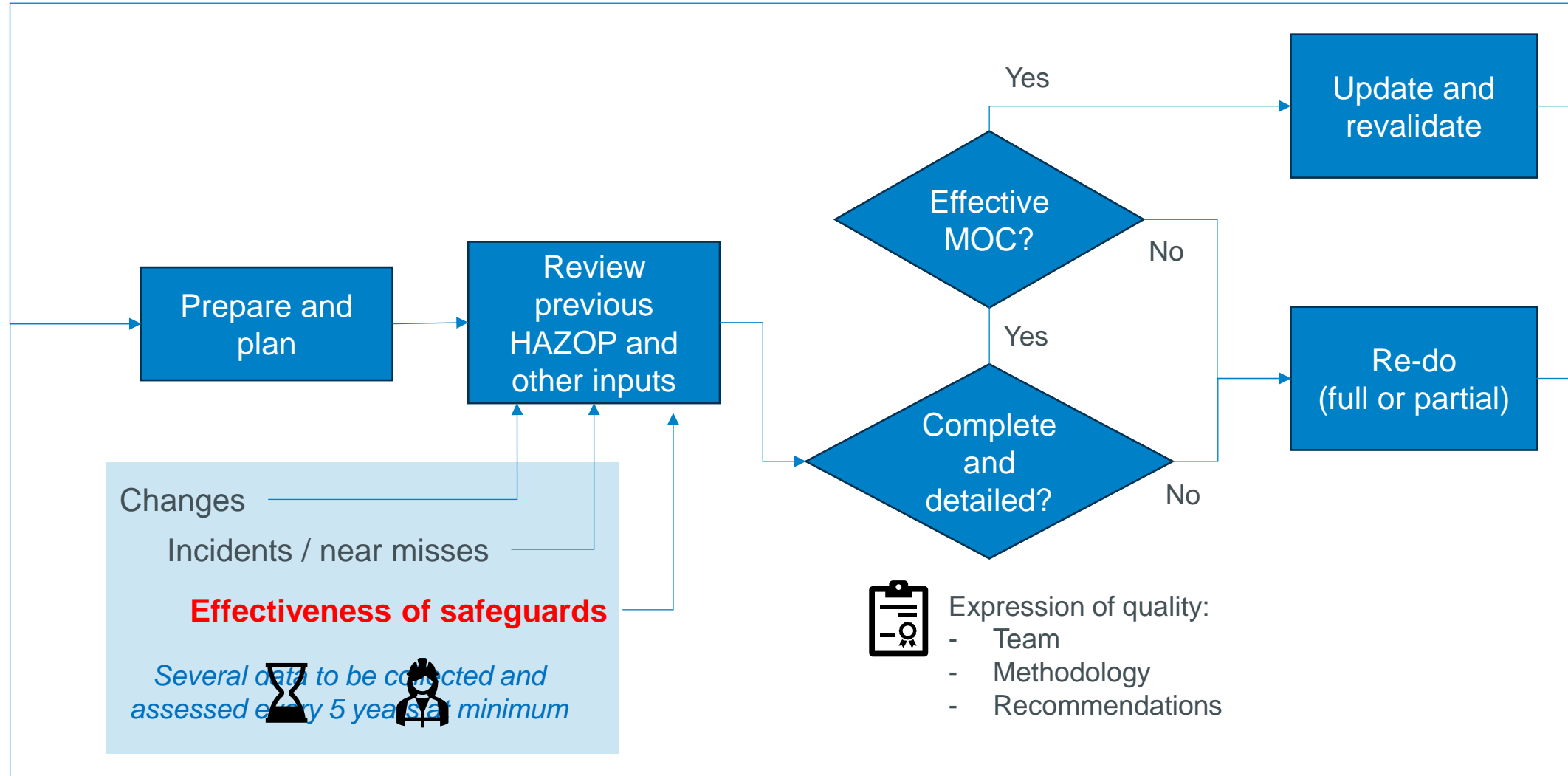
#safetygoesdigital



# HAZOP Revalidation Process

Regular common process (simplified)

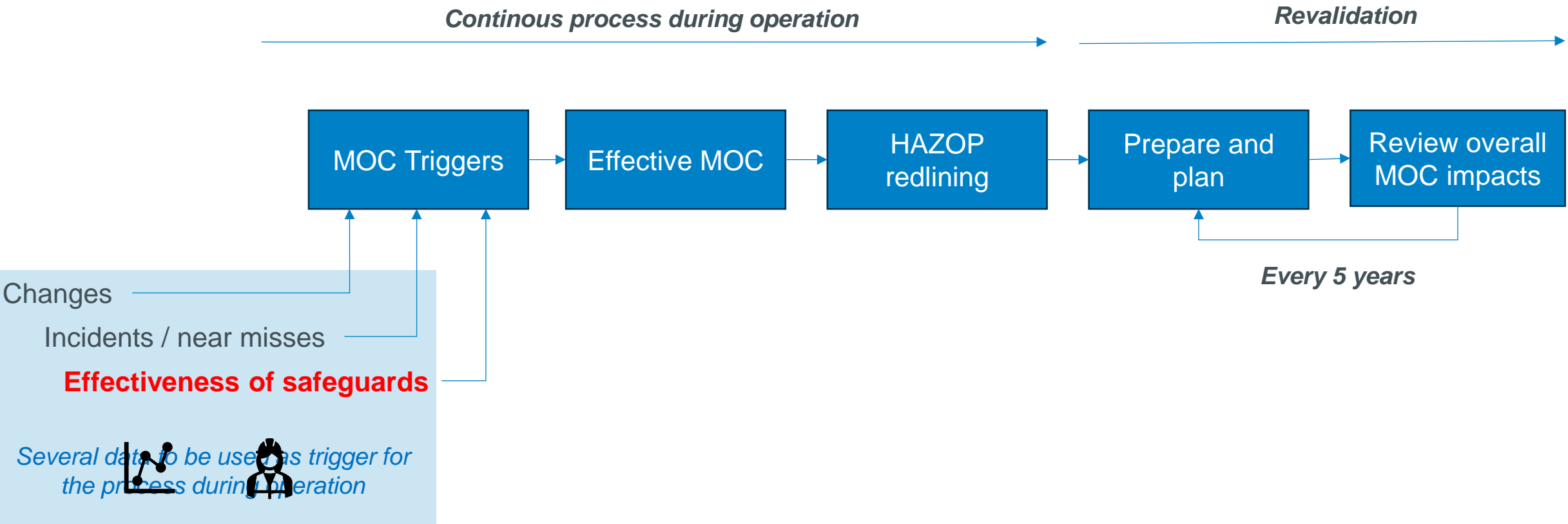
Every 5 years



# HAZOP Revalidation Process



Evergreen process (simplified)



# HAZOP Revalidation Process

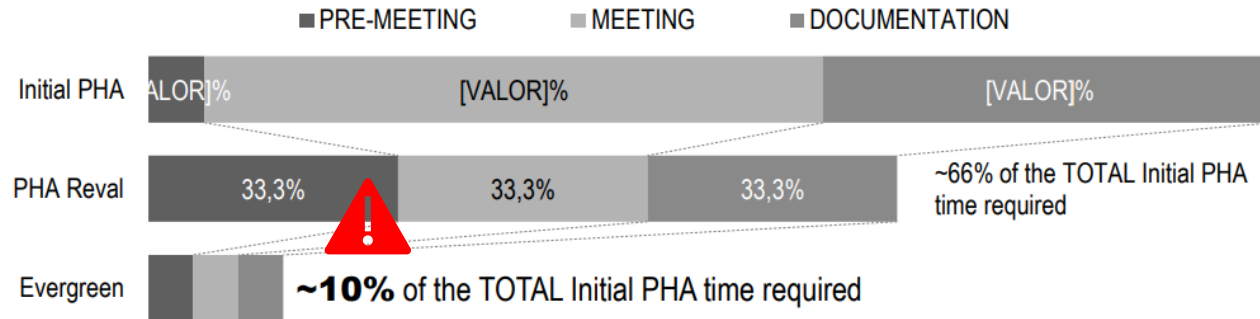


Figure 6. Time requirements comparison. Initial PHA vs. PHA Revalidation.

Bridges, W.G. Tew, R. Masello, M.A. (2018), *Best Practices for PHA Revalidations*, 14th Global Congress on Process Safety (2018), 18 AIChE Spring Meeting

Interesting to note:

- In the revalidation, preparation time is one third of the overall time
- In Evergreen process, it is key to capture easily triggering event

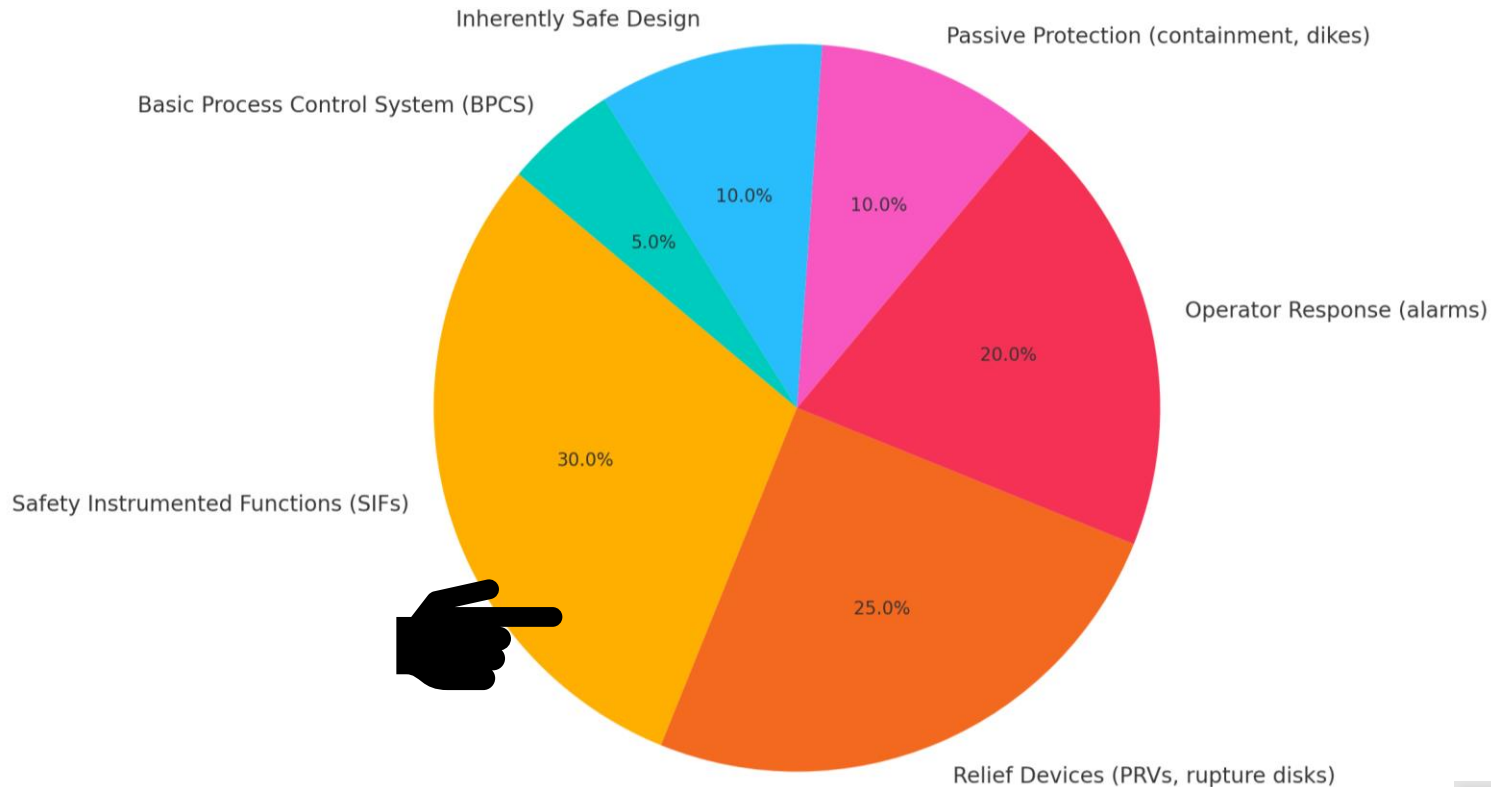


Let's focus on the efforts for evaluating safeguard effectiveness



# HAZOP Revalidation Process

Let's take the most popular and complex safeguard



SIF are increasingly becoming the most applied safeguard; what to monitor in a SIF?

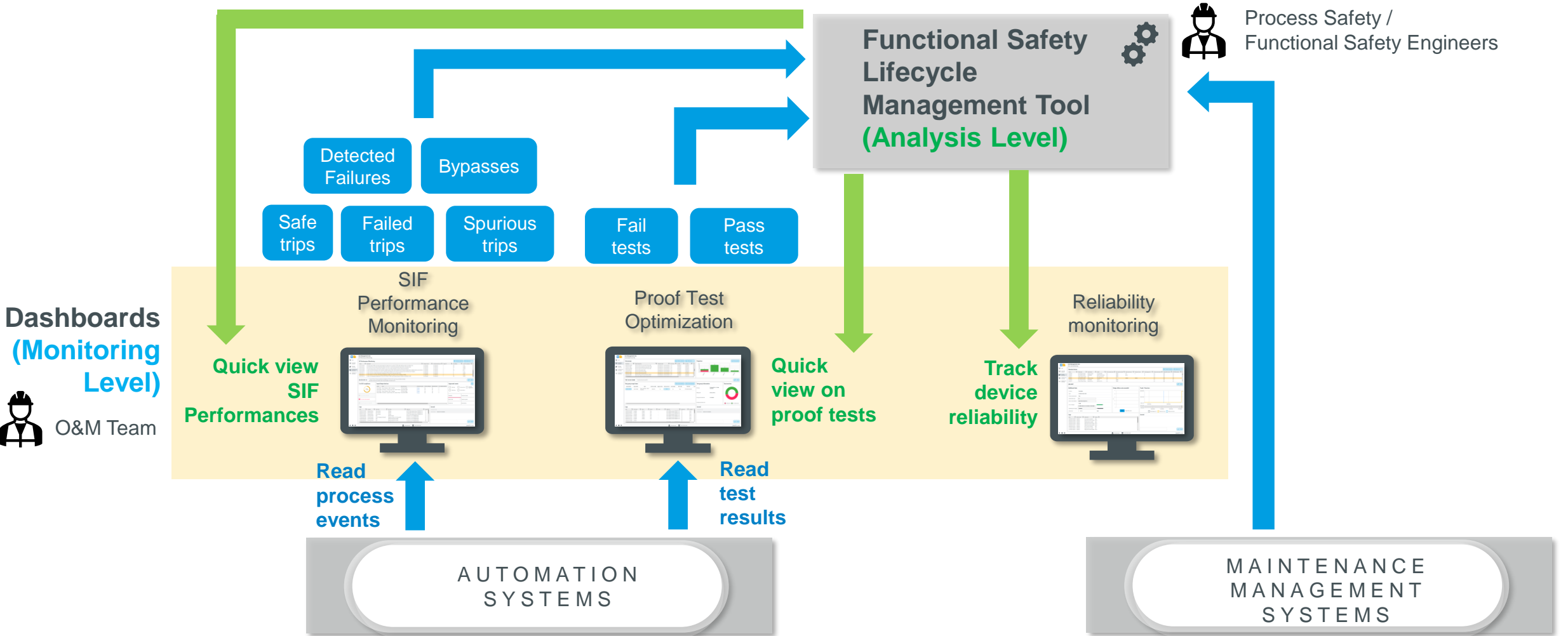
- Demand rate
- Spurious rate
- Fail to operate rate
- Failure rates of devices
- Achieved SIL



How should it be ideally done?


# Why digitalization?

Converting Data into Metrics allows to reduce the preparation time and the generation of automated triggers



# Why digitalization? Example of SIF Monitoring

Where can I see the performances of the SIFs?



SLD-Management view

SIF Performance Monitoring

Main

Automated Proof Test

Prior Use Monitoring

SIF Performance Monitoring

Operational SIL Monitoring

Active

Archive

Refresh selected

Refresh all

Print

Export

Name

Description

Demand mode

Actual demand mode

Target SIL

Trip setting

% of SIF compliance

60-CSC-SIF-08	SIF closes the gas valves XV-001A/B and XV-002A/B in case of loss of flame detected by the flame detectors BZS-001A/B	Low Demand	Low demand	3	LL	85.71
60-CSC-SIF-09	In case of HH pressure detected in the combustion chamber by the PZT-001, the SIF shutdowns the valve gas XV-001A/B and XV-002A/B and the trip the	Low Demand	Low demand	2	HH	85.71
60-CSC-SIF-10	TEST_In case of LL flow in the combustion air system is detected by FZT-002A/B, the SIF shutdowns all the gas valves XV-001A/B and XV-002A/B.	Low Demand	Low demand	3	Status	71.43
60-CSC-SIF-11	In case of LL flow in the demi water feed line detected by FZT-003, the SIF closes the valve XV-003.	Low Demand	Low demand	2	LL	71.43
60-CSC-SIF-12	In case of HH flow in the demi water feed line detected by FZT-004, the SIF closes the valve XV-004A & XV-004B .	Low Demand	Low demand	2	LL	85.71
60-CSC-SIF-14	In case of HH flow in the feed line detected by FZT-005, the SIF closes the valve XV-005A & XV-005B .	Low Demand	Low demand	1	LL	100.00
60-CSC-SIF-15	In case of HH temperature detected by TZT-001 & TZT-002 & TZT-003, the SIF closes the valve XV-005A & XV-005B & XV-005C.	Low Demand	High demand	3	HH	14.29
60-CSC-SIF-16	In case of LL flow in the demi water feed line detected by FZT-003, the SIF closes the valve XV-003.	Low Demand	Low demand	3	LL	85.71

60-CSC-SIF-15

In case of HH temperature detected by TZT-001 & TZT-002 & TZT-003, the SIF closes the valve XV-005A & XV-005B & XV-005C.  
An explosion generated by uncontrolled temperature in the flue gas system

% of SIF compliance

14%

Device failure detected!

Proof test delay detected!

Excessive bypass time detected!

Input/Output devices

Name	Type	Main test group	Change test group	Proof test delay
60-XV-101B	Valve and Actuator - Ball Valve with Spring Return Piston Actuator - Generic ball valve assembly	N/A	Change	No
60-PZT-102	Transmitter - Pressure Transmitter - /	TEST_60-PZT-002	Change	Yes
60-PZT-101	Transmitter - Pressure Transmitter - /	N/A	Change	No
60-XV-101A	Valve - Ball - Generic ball valve assembly	N/A	Change	No
60-TZT-102	Transmitter - Temperature Transmitter - Rosemount	N/A	Change	No
60-XV-010	Valve - Ball - /	TEST_60-XV-003	Change	Yes
60-TZT-101	Detector - Uv/IR Detector - Rosemount	N/A	Change	No
60-XV-201A	Valve - Ball - FlowServe	N/A	Change	No
60-TZT-103	Transmitter - Temperature Transmitter - Rosemount	N/A	Change	No
60-XV-101C	Valve and Actuator - Ball Valve with Spring Return Piston Actuator - Generic ball valve assembly	N/A	Change	No

Approved events

20 Safe trips

6 Spurious trips

15 Excessive bypass time

4 Failed trips

3 Device failure

Availability

Spurious trip rate

Demand rate

Failed to operate

Fail test rate

RRF achieved

Logs

Time	Trip Type	Trip Result	Trip Note	Object ID
26.03.2025 11:58:27	Process Demand	Pass	Failed Device(s): -	60-CSC-SIF-15-trip-2025
26.03.2025 11:54:56	Process Demand	Fail with dangerous failure(s)	Failed Device(s): 60-XV-101B, 60-XV-101A, 60-XV-101C, 60-XV-010, 60-XV-201B, 60-XV-201A	60-CSC-SIF-15-trip-2025
26.03.2025 11:51:26	Process Demand	Fail with dangerous failure(s)	Failed Device(s): 60-XV-101C, 60-XV-201B	60-CSC-SIF-15-trip-2025
26.03.2025 11:47:56	Process Demand	Fail with dangerous failure(s)	Failed Device(s): 60-XV-101B, 60-XV-010, 60-XV-201A	60-CSC-SIF-15-trip-2025
26.03.2025 11:33:11	Process Demand	Fail with dangerous failure(s)	Failed Device(s): 60-XV-101C, 60-XV-201B	60-CSC-SIF-15-trip-2025
26.03.2025 11:29:42	Process Demand	Fail with dangerous failure(s)	Failed Device(s): 60-XV-101B, 60-XV-010, 60-XV-201A	60-CSC-SIF-15-trip-2025
26.03.2025 11:26:13	Process Demand	Fail with dangerous failure(s)	Failed Device(s): 60-XV-101A	60-CSC-SIF-15-trip-2025

Journal

10.02.2025 15:48:42

Hima

Still Simulating events

10.02.2025 14:00:16

Hima

Testing the Journal

Status of compliance

Status of compliance

Alarms on metrics

Automatic log of events

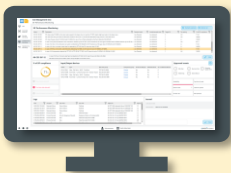
© HIMA Group 2025

8

# Why digitalization? Example of SIF Analysis

From Metrics to workable Inputs for HAZOP Revalidations / Evergreen process

Automated  
screening  
mechanism



Alarm

Example: SIF001  
does not meet the  
performance  
requirements

- MOC starting point
- Trigger for evergreen

## Evaluating impact on risk assessments

Not effective barrier indicated in red

Independent Protection Layers (Barriers)										<div><div></div><div></div></div> <div>Add Barrier</div> <div><div></div><div></div></div> UnLink Barrier <div><div></div><div></div></div> Export to Excel <div></div>	
		Barrier ID ( * )	Barrier Cate...	Type	HAZOP Comments	Short Description	Long Description IPL	Assumed PF...	Relat...		
<div><div></div><div></div></div>	<div><div></div><div></div></div>	<div><div></div><div></div></div> <div>50-CSC-SIF-04</div>	Instrumented	SIF SIL				0.01		<div>50-CSC-SIF-04-FSH</div>	
<div><div></div><div></div></div>	<div><div></div><div></div></div>	<div><div></div><div></div></div> <div>50-CSC-ALARM-01</div>	Instrumented	Alarm w/ Operator Response		BPCS Alarm on high flow		0.1		<div>50-CSC-ALARM-01</div>	

Non effective barrier is not considered in the risk reduction; hence gap is shown

Initiating Causes

Add LOPA Initiating Cause

Custom Actions

Export to PDF

	LOPA Initiating Cause				LOPA Results without Recommendations																							
	Short Descript... <div></div>	Cause Source <div></div>	Cause Type <div></div>	IEF <div></div>	Applicable IPLs <div></div>	MEF <div></div>			MEF w/CMs <div></div>		LOPA Gap <div></div>																	
<div><div></div><div></div></div>	Operator accidentally opens fully the control valve during the start up sequence when the controller is in manual.	Human Error (Probability)	Operator well trained with stress	0.1/yr	<table><tr><td>50-CSC-ALARM-01</td><td>Yes</td><td>1</td><td>0.1</td></tr><tr><td>50-CSC-SIF-04</td><td>Yes</td><td>2</td><td>0.01</td></tr></table>	50-CSC-ALARM-01	Yes	1	0.1	50-CSC-SIF-04	Yes	2	0.01	<table><tr><td>SA</td><td>1E-3</td></tr><tr><td>EN</td><td>1E-3</td></tr><tr><td>CM</td><td>1E-3</td></tr></table>	SA	1E-3	EN	1E-3	CM	1E-3	<table><tr><td>SA</td><td>1E-4</td></tr><tr><td>EN</td><td>1E-4</td></tr><tr><td>CM</td><td>1E-4</td></tr></table>	SA	1E-4	EN	1E-4	CM	1E-4	10
50-CSC-ALARM-01	Yes	1	0.1																									
50-CSC-SIF-04	Yes	2	0.01																									
SA	1E-3																											
EN	1E-3																											
CM	1E-3																											
SA	1E-4																											
EN	1E-4																											
CM	1E-4																											



# Why digitalization?

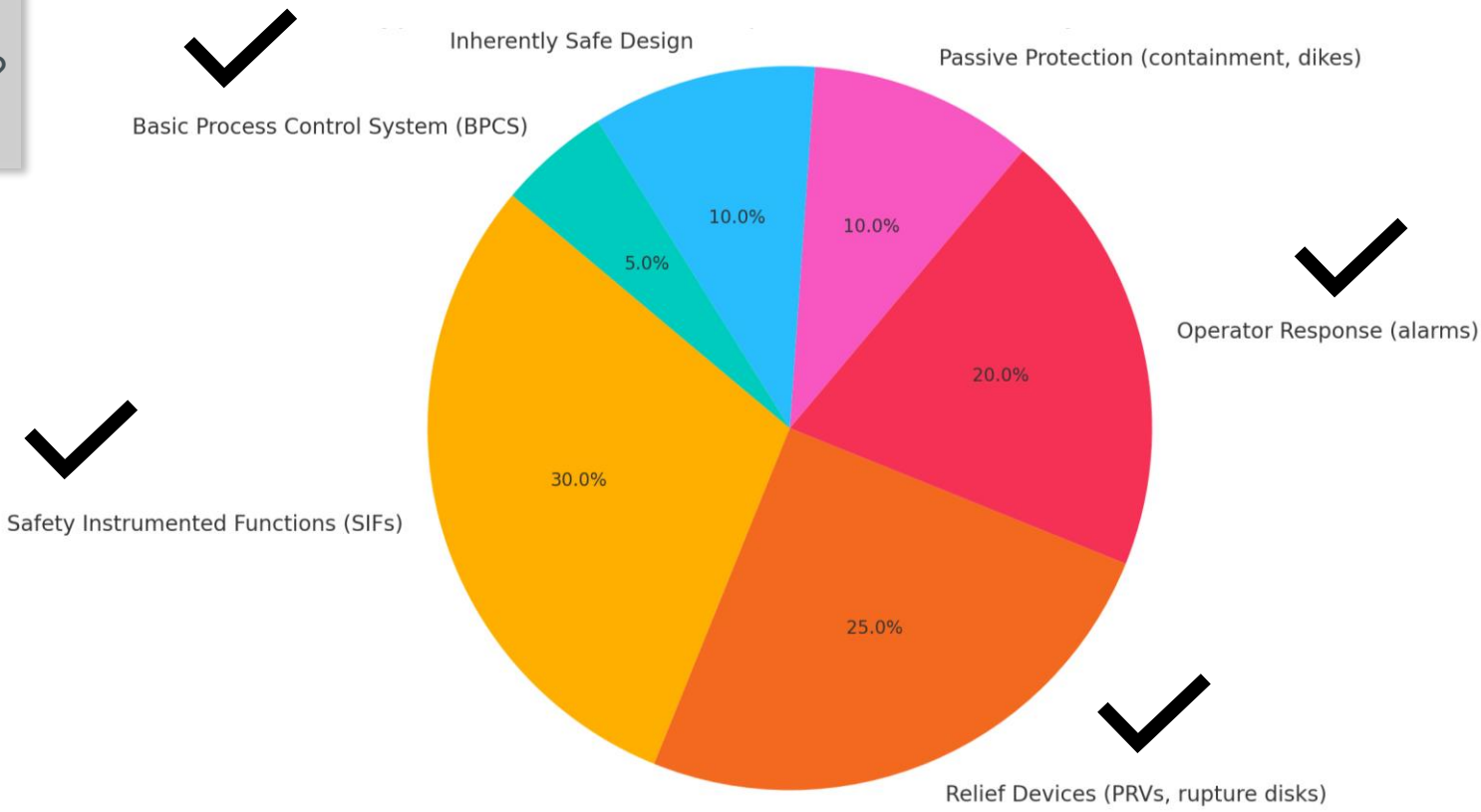
One integrated system to cope with more safeguards



Only SIF? What about other safeguards?



80% of safeguards can be covered in the same solution



# Summary



Digitalization of functional safety lifecycle can also improve your revalidation and evergreen process



Go for a solution that can bridge risk assessment and operation



Make sure data become a resource and not a problem



Take digitalization of functional safety lifecycle as a multidisciplinary task

# Contact



Global Lead Consultant in Digital Safety

M +49 1624686231

[marco.turdo@hima.com](mailto:marco.turdo@hima.com)

[www.hima.com](http://www.hima.com)