CCS
Consejo Colombiano de Seguridad

An AIChE Technology Alliance
CCPS
Center for Chemical Process Safety

10ª CONFERENCIA LATINOAMERICANA DE SEGURIDAD DE PROCESOS DEL CCPS

18 / 19 / 20
SEPT

Barranquilla
2024 Colombia

An AIChE Technology Alliance
CCPS Center for Chemical Process Safety

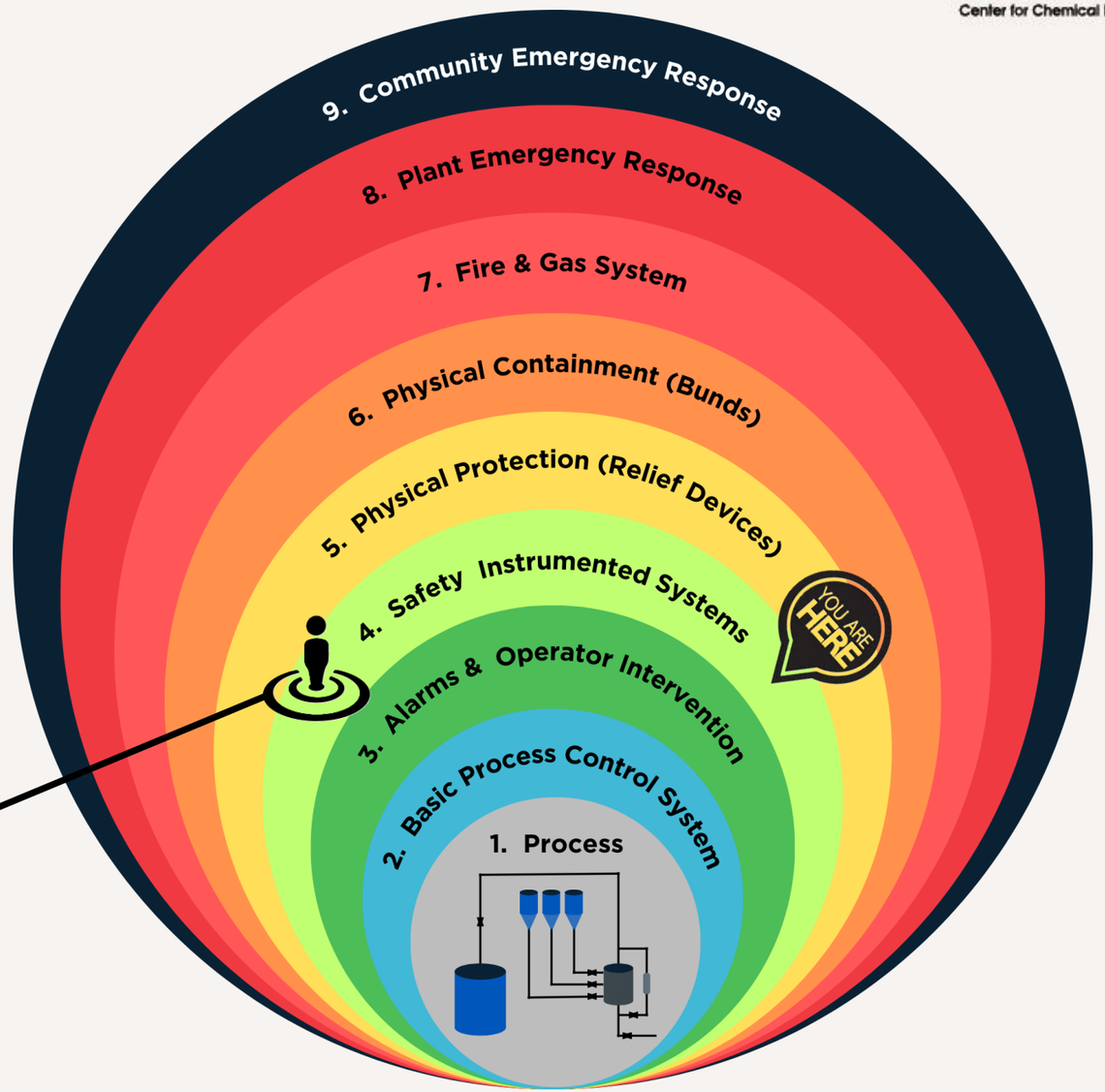
CCS Consejo Colombiano de Seguridad

UNCOVERING HIDDEN RISKS: IDENTIFYING & ADDRESSING SYSTEMATIC FAILURES IN SAFETY SYSTEMS

CHARLIE SOUZA PE, CAP, TUV FS ENG
ACUTECH GROUP, INC.

10ª CONFERENCIA LATINOAMERICANA DE SEGURIDAD DE PROCESOS DEL CCPS

THE PROCESS SAFETY ONION DIAGRAM



SIS
SAFETY INSTRUMENTED SYSTEMS

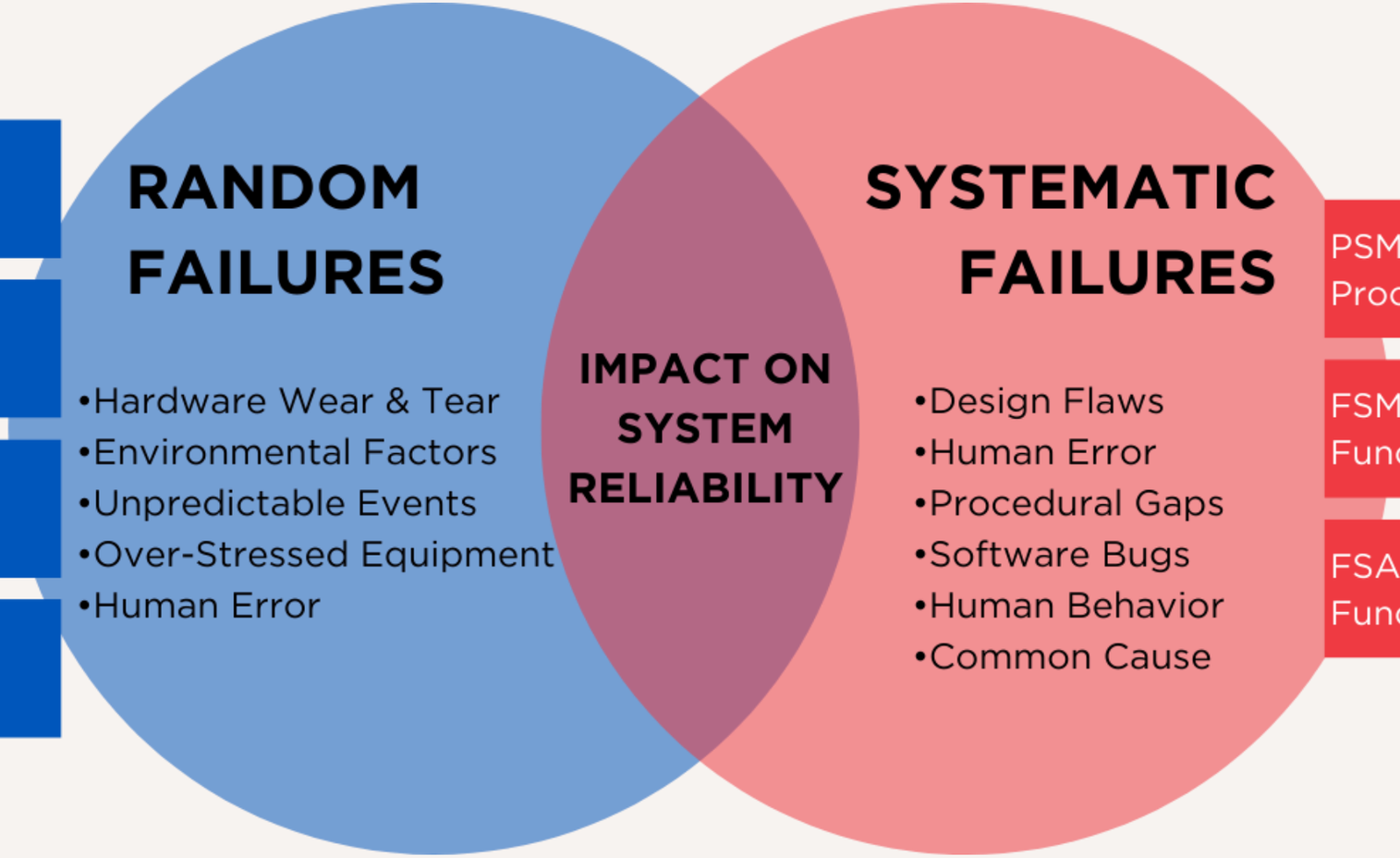
FAILURE TYPES

SIL
Safety Integrity Level

HFT
Hardware Fault Tolerance

SC
Systematic Capability

PTP
Proof Test Procedures



PSM
Process Safety Management

FSM
Functional Safety Management

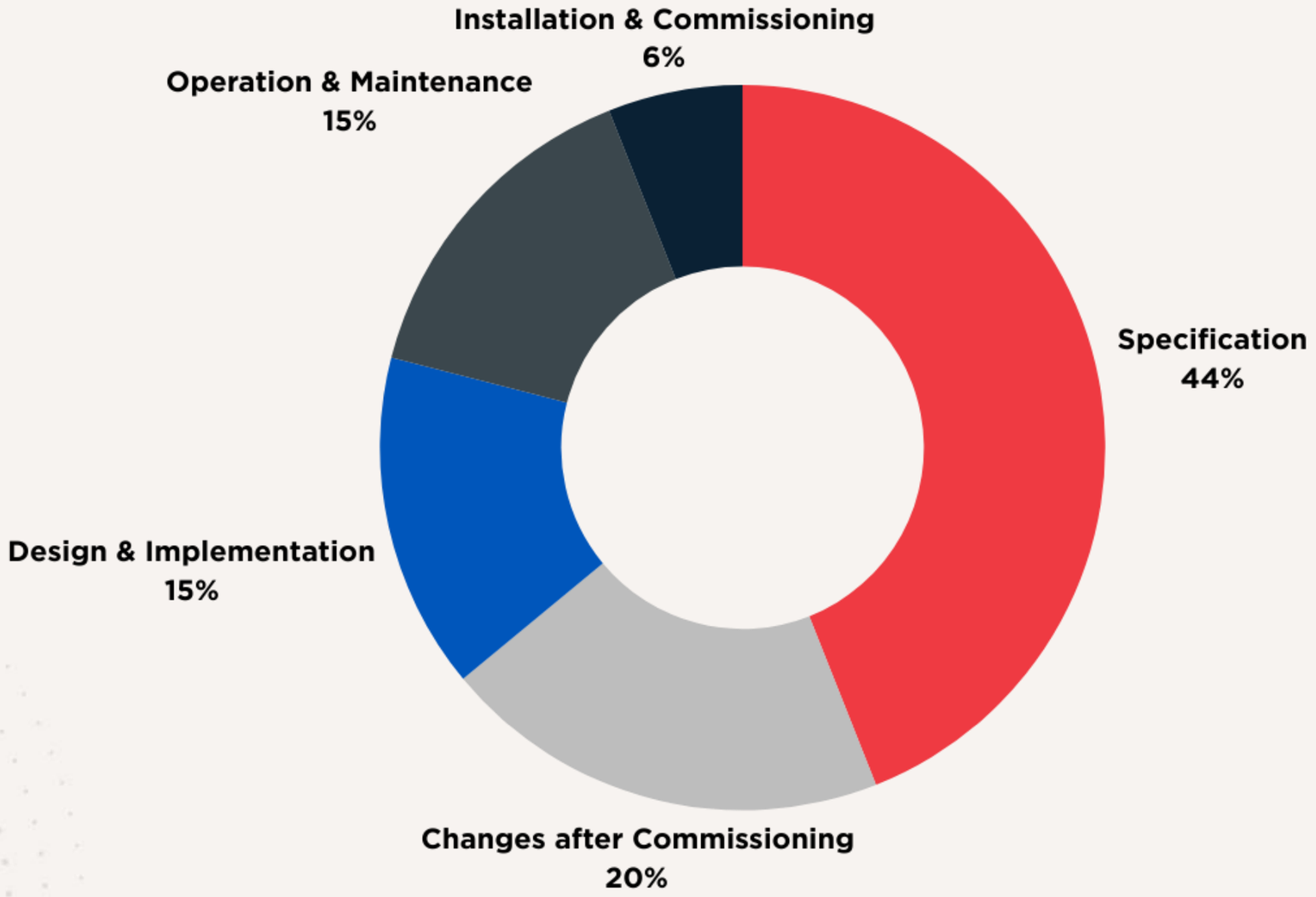
FSA
Functional Safety Assessments

RANDOM FAILURES VS. SYSTEMATIC FAILURES

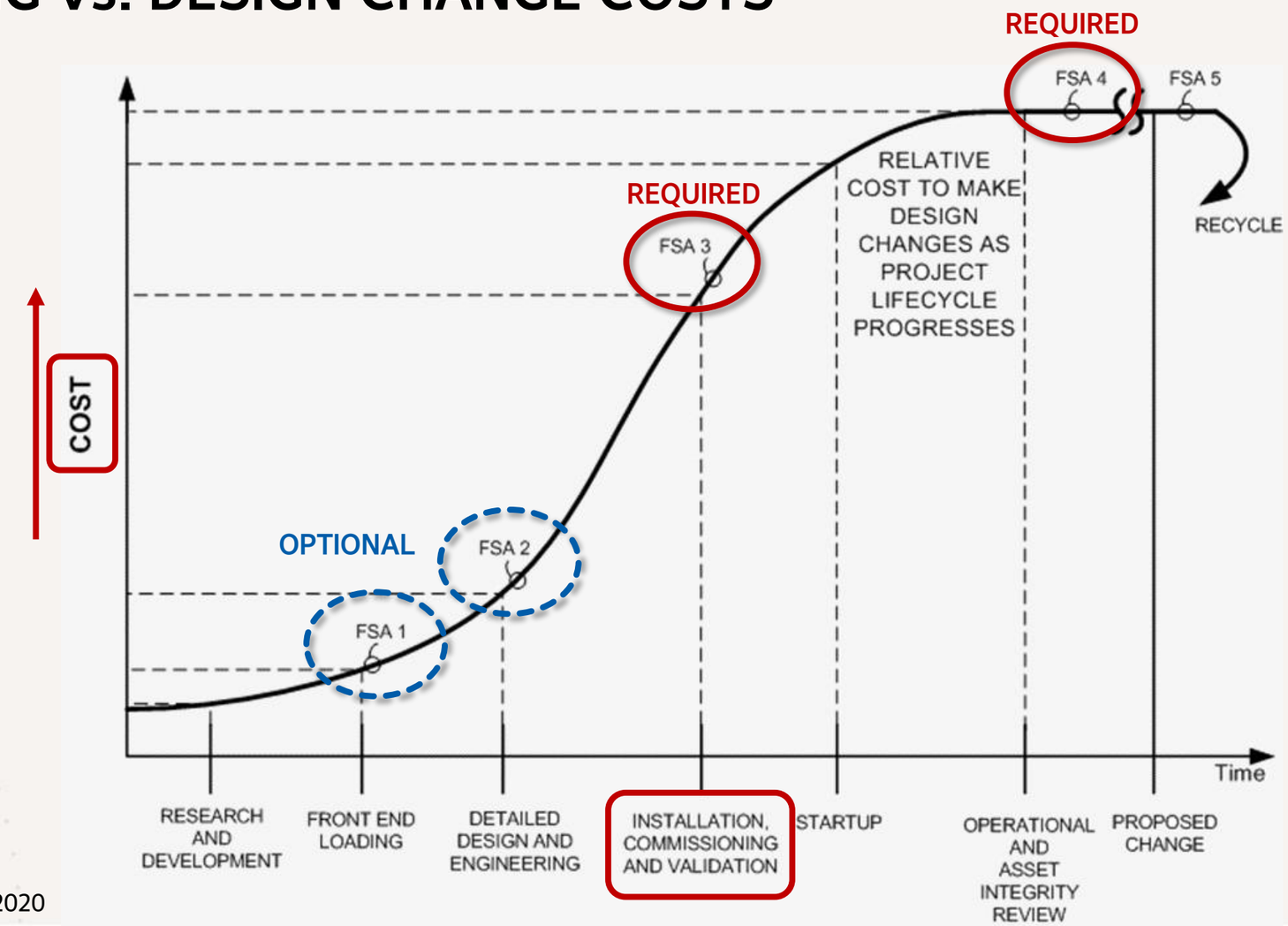
SYSTEMATIC:
FEWER BUT WITH A MORE SIGNIFICANT IMPACT

RANDOM:
NUMEROUS BUT GENERALLY LOWER IN IMPACT

HSE PRIMARY CAUSE BY PHASE



FSA TIMING vs. DESIGN CHANGE COSTS



SOURCE: ISA-TR84.00.04-2020

FSA REQUIREMENTS AT EACH STAGE

FSA 1 Checklist: Hazard and Risk Analysis Independence and Risk Reduction Limits Review

Item No	Item
1.1	The value assumed in the H&RA for the frequency of dangerous process control (a.k.a., BPCS) failures as the initiating source of a hazardous event is consistent with the limits in clause 8
1.2	The as
1.3	Use of
1.4	Hazard
1.5	The fu • s • l • f • s • t • r • f fun *A sub
1.6	Each i the los OR Co mitiga
1.7	Total a within
1.8	SRS ar • p • i
1.9	P&ID (
1.10	Functi • c • r
1.11	Initial countermeasures hav

FSA 2 Checklist: Safety System Detailed Design Review

Item No	Item
2.1	Recommendations from FSA stage 1 have been satisfactorily addressed
2.2	Reliab audita
2.3	SRS is
2.4	Suffic confir
2.5	Quant depen
2.6	SIL ve a) b) c)
2.7	Desig interv
2.8	Specif
2.9	Opera
2.10	PSI do
2.11	Verifi docun
	Any d

FSA 3 Checklist: Functional safety portion of PSSR

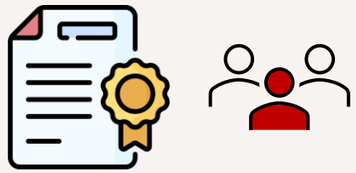
Item No	Item
3.1	Recommendations from FSA stages 1 and 2 are satisfactorily addressed
3.2	Verification of the safety system logic solver configuration, programming, and the functions therein (e.g., FAT) was completed and documented in alignment with clauses 12 and 13 requirements if not previously performed as input to FSA 2 (see above). Any defects found during verification have been corrected, or compensating measures have been put in place to address any decrease in estimated risk reduction
3.3	Verification of the safety system devices (e.g., logic solver, auxiliary system, and instrument loop commissioning) was completed and documented in alignment with clause 14 requirements Any defects found during verification have been corrected or compensating measures have been put in place to address any decrease in estimated risk reduction
3.4	Validation of the safety system(s) and the functions therein (e.g., SAT, end-to-end function testing) was completed and documented in alignment with clause 15 requirements. Any defects found during validation have been corrected or compensating measures have been put in place to address any decrease in estimated risk reduction
3.5	Specified security countermeasure verification was completed and documented All defects found during security countermeasure verification have been corrected
3.6	As-built updates have been made to H&RA, SRS, PSI documentation and procedures after correction of verification and validation defects
3.7	H&RA, SRS, and PSI documents with as-built updates remain consistent with each other and still adhere to the clause 8-12 requirements
3.8	Safety system operating procedures (e.g., bypass, alarm response, compensating measures) and other required documentation have been created
3.9	Safety system maintenance procedures (e.g., preventive maintenance, inspection, proof test, on-line repair upon diagnosed failure) have been created

*NOT REQUIRED

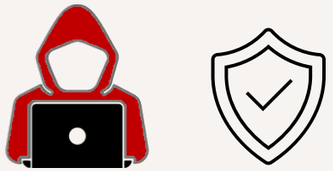
*REQUIRED

SOURCE: ISA-TR84.00.04-2020

FSA TEAM INDEPENDENCY & THE CYBERSECURITY CLAUSE



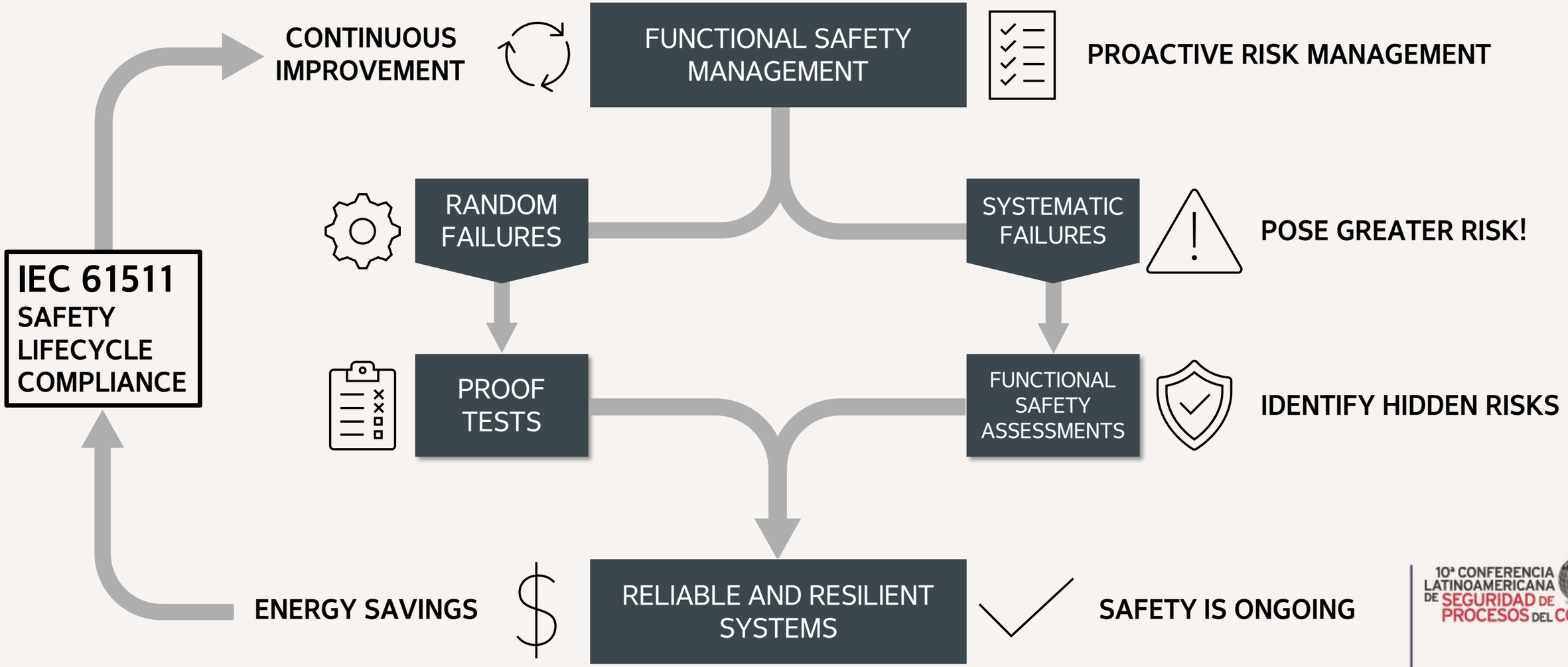
ANSI/ISA-61511-1:2018 Clause 5.2.6.1.2 requires at least one senior, competent, independent (from the work being assessed) person to take part in the FSA.



ANSI/ISA-61511-1:2018 Clause 8.2.4 A security risk assessment shall be carried out to identify the security vulnerabilities of the SIS.

SOURCE: ANSI/ISA-61511-1:2018

KEY TAKEAWAYS




An AIChE Technology Alliance
CCPS
Center for Chemical Process Safety
CCS
Consejo Colombiano
de Seguridad