Combined Cybersecurity and SIS/SIL Design

MLM-020-A

Industry	– Process Industry
Principal Role	– All
Professional Role	– Control Engineer + Process Engineer
Enterprise Phase	– Master Planning

Turn on your audio and click start to begin video

START

Key Definitions

- **Safety**
  - Freedom from unacceptable risk.
  - [SOURCE: IEC 61508-4, 2010, 3.1.11 and IEC 62443-1-1, 2009, 3.2.94]
- **Functional Safety**
  - Part of the overall safety relating to the EuC and the EuC Control System that depends on the correct functioning of the E/E/PE safety-related systems and other risk reduction measures. [SOURCE: IEC 61508-4, 2010, 3.1.12]
- **Conflict between Safety and Security**
  - A situation where the system cannot achieve its required target performance because one or several safety measures and one or several security countermeasures are not coordinated.
- **Security**
  - Condition of system resources being free from unauthorized access and from unauthorized or accidental change, destruction, or loss [SOURCE IEC 62443-1-1]

Source Technical Specification Draft

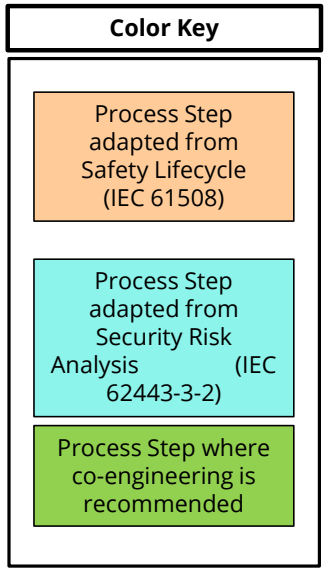
- This MLM is based on the current committee draft of IEC TS 63069 “Framework for Safety and Security” Annex D.
- The TS 63069 Technical Specification is intended to interface the two “horizontal” safety and security standards series, IEC 61508 and IEC 62443.
- This Technical Specification had an earlier existence as a Technical Report but has been heavily revised to better align with the recent ISA TR84.00.09 (based on IEC/ISA 61511, the process industry domain standard of 61508).
- Both IEC 61508 and IEC 62443 standards are currently under revision, so internal references are subject to change.
- The contents of the TS are currently purely informative and subject to revision.

Basis of Design

- The Project Scope Definition defines what the process is required to do, and constraints on acceptable methods of achieving those objectives.

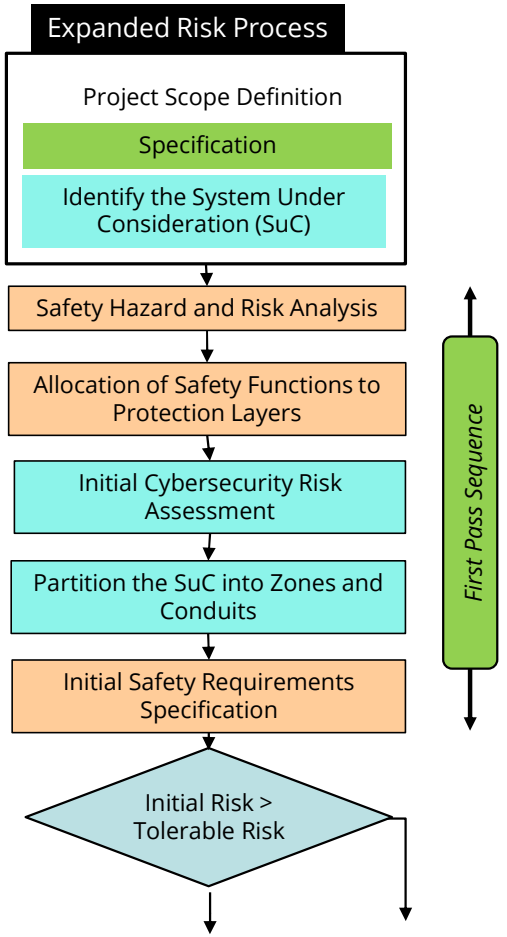
- It can happen that there are unrecognized incompatibilities in the specified requirements that will only become apparent as the design progresses.

General Process of Risk Assessment – Page 1

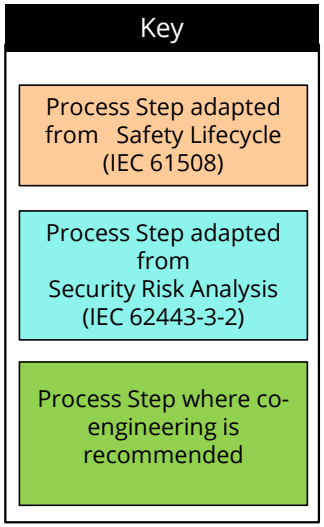


When:

- In the latter stages of Preliminary Engineering
- Before cost/time estimates are frozen

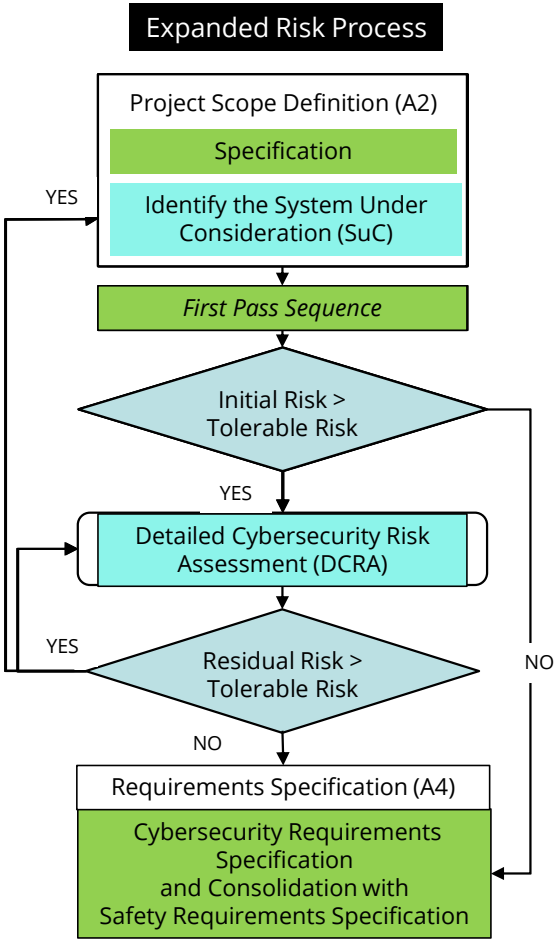


General Process of Risk Assessment – Page 2



By Whom:

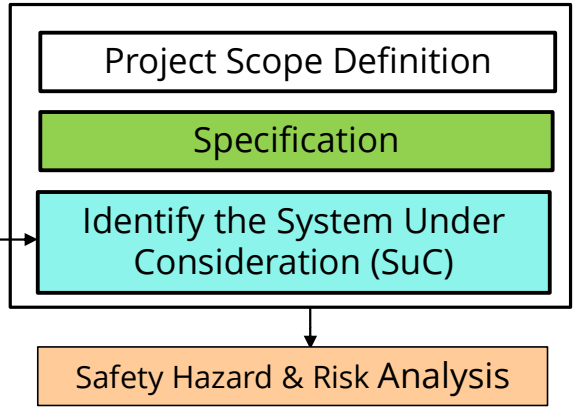
- Control System Engineer
- Functional Safety Engineer
- Cybersecurity Engineer
- Process and Operations Specialists



General Process of Risk Assessment - Initial

Inputs	Expanded Risk Process	Outputs

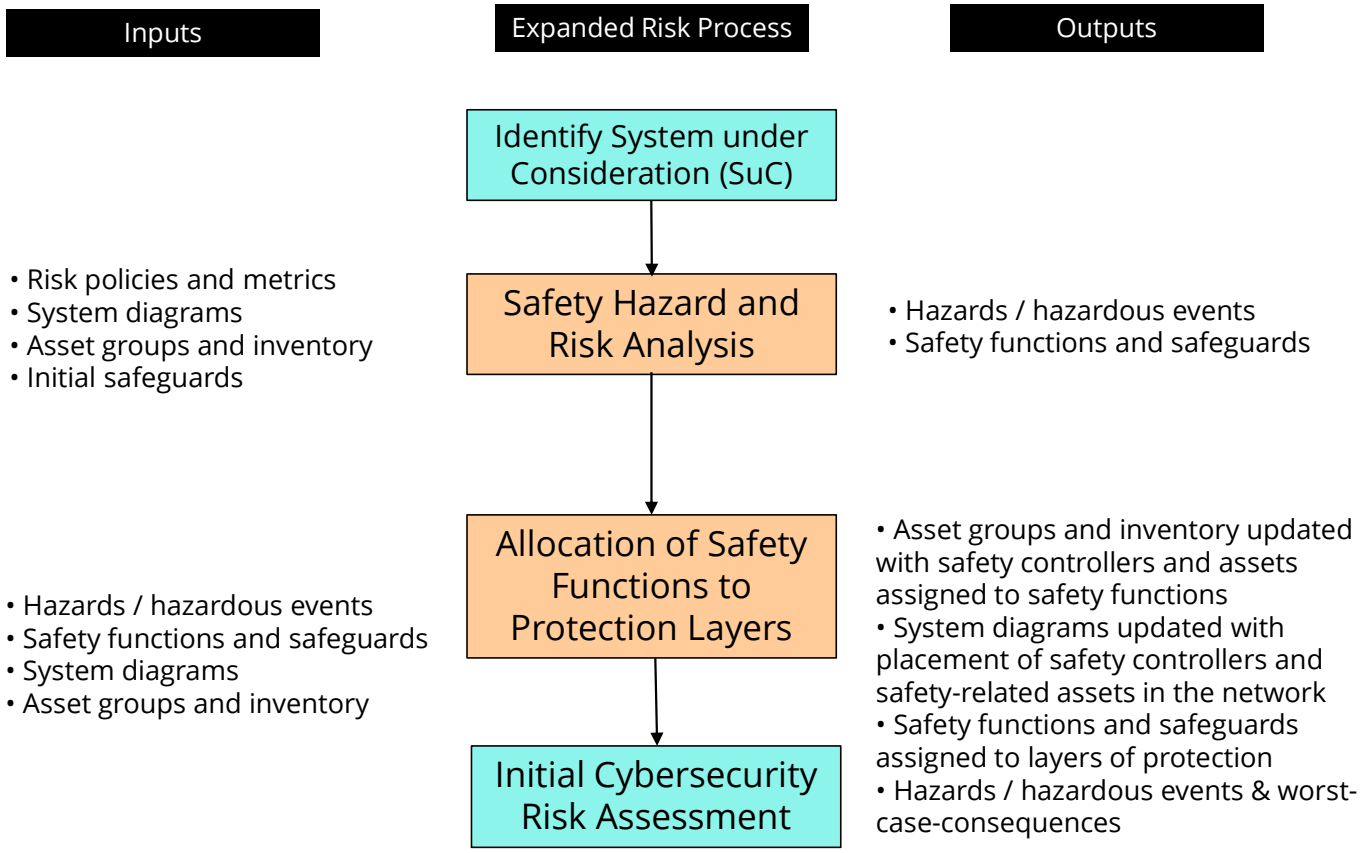
- Functional requirements
- Existing policies & procedures



- Project scope document
- Preliminary asset inventory
- Responsibilities for IT/OT
- Initial safeguards
- Initial cybersecurity measures

- If an acceptable solution cannot be achieved within specified policies and procedures, reconsider basic inputs.

General Process of Risk Assessment - Initial



General Process of Risk Assessment - Initial

Inputs	Expanded Risk Process	Outputs
	Allocation of Safety Functions to Protection Layers	
• Risk policies and metrics • Purpose & functionality of the SuC • Major hazards & worst-case consequences	Initial Cybersecurity Risk Assessment	• Operational functions & associated asset groups • System diagrams • Initial risk evaluation: worst-case unmitigated risk per operational function/asset group • Initial SPR-T for operational functions/asset groups (optional)
• Purpose/functionality of the SuC • Geographical location of assets • Initial risk evaluation	Partition the SuC into Zones and Conduits	• Updated Asset inventory with asset groups assigned to zones • Updated system diagram including zones & conduits • Data flow diagrams
	Initial Safety Requirements Specification	

General Process of Risk Assessment - Initial

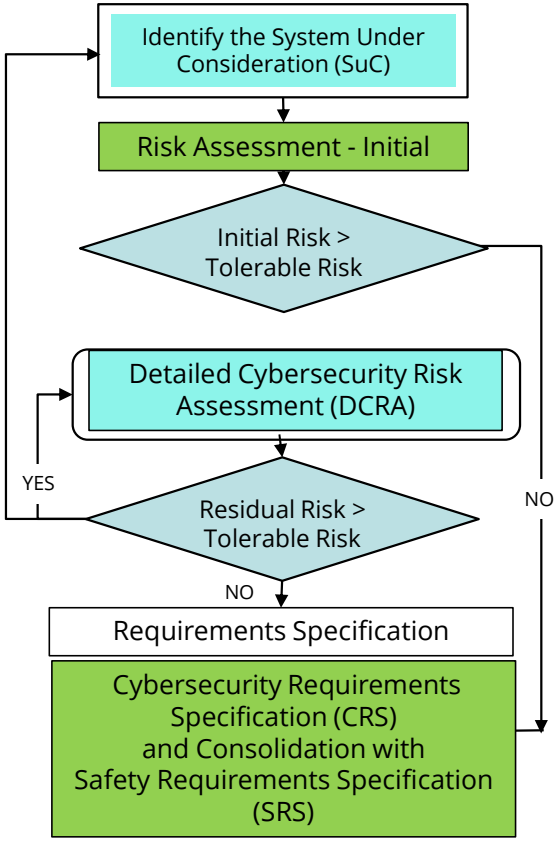
Inputs	Expanded Risk Process	Outputs
• System diagrams incl. zone and conduit diagrams • Safety functions and safeguards assigned to layers of protection	Partition the SuC into Zones and Conduits ↓ Initial Safety Requirements Specification ↓ Initial Risk > Tolerable Risk	• Updated system diagrams including safety-related systems and required data flow • Initial safety requirements

General Process of Risk Assessment – cont.

Inputs

- Purpose / functionality of the SuC: High level use case inc. data flow diagrams, architectural diagrams, zone and conduit diagrams
- Hazards and potential consequences
- Vulnerabilities and common threats for the SuC
- Risk policies and metrics
- Existing security measures for each zone and conduit
- Existing safety functions, safeguards, and initial safety requirements

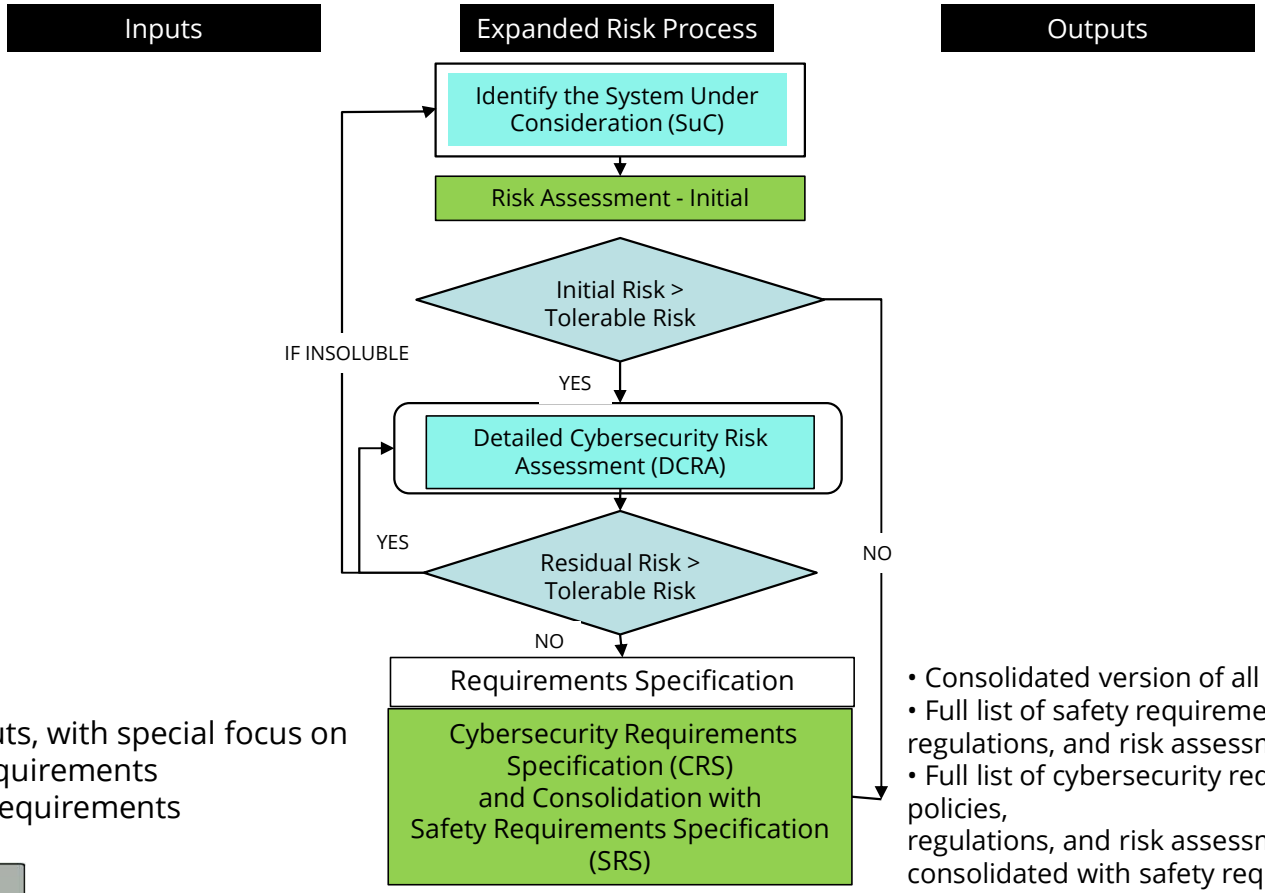
Expanded Risk Process



Outputs

- Cybersecurity risk scenarios
- Unmitigated risk and residual risk per risk scenario
- SPR-T for each zone or conduit, function, or system
- Cybersecurity requirements: Design approval or recommendations to further reduce risk

General Process of Risk Assessment – cont.



- All above outputs, with special focus on
- Initial safety requirements
- Cybersecurity requirements

- Consolidated version of all above outputs
- Full list of safety requirements from policies, regulations, and risk assessments
- Full list of cybersecurity requirements from policies,
regulations, and risk assessments and consolidated with safety requirements

Key Messages

The following are key messages in this MLM:

- Safety and Security are parallel requirements
  - But while Designed Safety can be validated and frozen, Security may deteriorate unless patched.
- Security improvement must not deteriorate safety requirements
- Just because there is no apparent reason why a system should be breached is no defense against an incautious attack on a different target.

Further Information

This MLM has been adapted from two IEC publicly available documents:

- *IEC PAS 63325 Ed1, 'Lifecycle Requirements for Functional Safety and Security for ACS' issued in 2020, and*
- *IEC TR 63069:2019, 'Industrial-process measurement, control and automation - Framework for functional safety and security*'.
- These are currently being combined to form an IEC Technical Specification *IEC TS 63069 'Framework for functional safety and security*'.

ISA TR84.00.09, 'Cybersecurity Related To The Functional Safety Lifecycle' covers the field in detail and is currently in revision as Ed3. but is limited to systems covered by IEC ISA 61511

Further Information

- **Related MLMs**
  - MLM-042-A, Cyberattacks on Ukraine's Power Grid - Part 1
  - MLM-042-B, Cyberattacks on Ukraine's Power Grid - Part 2
  - MLM-042-C, Cyber-attacks on Ukraine's Power Grid 2022 - Epilogue (Russian invasion of Ukraine 24 February 2022)
- **References**
  - ISA TR84.00.09-2017, 'Cybersecurity Related To The Functional Safety Lifecycle'
  - IEC PAS 63325 Ed1, 'Lifecycle Requirements for Functional Safety and Security for ACS'
  - IEC TR 63069:2019, 'Industrial-process measurement, control and automation - Framework for functional safety and security.

Please click here to provide feedback on this module

Author

Ian H. Gibson

Process, Control, and Safety Engineering Consultant

Industrial Chemist, Chemical Engineer, Instrument Engineer, and Functional Safety Engineer, Ian has designed, built, commissioned, operated, maintained, and debugged plants in mineral processing, polymers, oil & gas, and various other industries over the past 60-odd years. He is a Life Senior Member of ISA and Honorable Fellow of IICA (the affiliated Australian organization).

He has served as an Australian Expert on the IEC 61511 Maintenance Team for ten years and as secretary of ISA 99 WG13.

Translating engineering jargon between I&C, process, mechanical, electrical, structural, and piping specialists is his avocation.