HUG knowledge 2017 Honeywell Users Group

Dan Poston
6-21-2017

SAFETY REQUIREMENTS SPECIFICATION

For safety Instrumented Systems

Honeywell
THE POWER OF CONNECTED

A Little about myself

- 28 years' experience in instrumentation, analytical systems, safety instrumented and basic process control systems. Currently, In the Global Project & Engineering group at Lyondellbasell as a Capital Project I&C lead and Corporate SME for SIS.

- Hold a Masters and Bachelor degree in Electrical Engineering from Purdue University. Advanced academic studies include control systems and probabilistic methods.

daniel.poston@lyb.com

Industry Consensus Standards

- *IEC 61511-2003 / ISA 84.00.01-2004*

  Functional Safety – Safety Instrumented Systems for the Process Industry Sector
- OSHA recognizes IEC 61511 / ISA-84-00.01 as a generally accepted good engineering practice for SIS
- The standard defines minimum requirements that shall be specified to properly design and document a SIS
- The standard identifies 42 requirements
  - The method and format for documenting these requirements is not described

Good SIS Documentation

- Compliant Safety Requirements Specification (SRS) documentation provides enough detail to **design** a SIF that meets its SIL requirement
  - Tailored specifically to the SIF application
  - Ties a SIF design to a given hazardous process scenario
- The SRS provides the criteria by which the performance of a SIF is **validated** while operating and during calibrations, inspections, & proof tests,

Project Impacts

- SRS development drives scope definition & engineering costs:
  - What process variable(s) detect the hazard condition?
  - What are the final element actions needed to mitigate the hazard?
  - How will plant operating personnel interact with the SIF logic and field devices?
  - What does plant operating personnel need to transition the SIF from a trip state, to startup state, to normal run mode?
  - What is needed to monitor the health, maintain, test, and troubleshoot the SIF?
  - What is needed to review the performance of the SIF during normal and abnormal process events?
  - Considerations for redundancy, partial stroke valve testing, self-diagnostics, online testing, and common mode failures

- Create a PLAN
  - Part of Functional Safety Management

SRS Plan

	The job functions assigned to each requirement are guidelines. All requirements should be reviewed by the core team responsible for defining and specifying the functionality of the Safety Instrumented Functions. **X - Consult**	*Process Engineering*	*Operation Representative*	*IEA Reliability*	*Control System Engineering*	*SIS Engineering*		
Item	**IEC61511 Edition 2.0 2016-02 Requirement**						**Controlled Documents (GoBy CCO SRS 4_7_2016)**	**When the activity is completed**
1	a description of all the SIF's necessary to achieve the required functional safety (e.g., a cause and effect diagram, logic narrative);	x	x	x	x	x	Cause & Effect Diagrams/Narratives *(Annex D)*	FEED
2	a list of the plant input and output devices related to each SIF which is clearly identified by the plant means of equipment identification (e.g., field tag list);	x	x	x	x	x	SIF List *(Annex A)* *ExSILentia (Annex A)*	FEED Detailed Engineering
3	requirements to identify and take account of common cause failures;	x	x	x	x	x	SRS General Requirements *(5.16)*	FEED
4	a definition of the safe state of the process for each identified SIF, such that a stable state has been achieved and the specified hazardous event has been avoided or sufficiently mitigated;	x	x				SIF List *(Annex A)*	FEED
5	a definition of any individually safe process states which, when occurring concurrently, create a separate hazard (e.g., overload of emergency storage, multiple relief to flare system);	x	x				Process Unit PHA/LOPA *(Annex B)*	FEED

SRS Plan

6	the assumed sources of demand and demand rate on each SIF;	x	x			x	Process Unit PHA/LOPA *(Annex B)*	FEED
7	requirements relating to proof-test intervals;		x	x		x	SRS General Requirements *(5.17)* SIL Verification tools *(Annex A)*	FEED Detailed Engineering
8	requirements relating to proof test implementation;			x	x	x	SAT/Proof Test Procedures *(Annex G)*	Detailed Engineering
9	response time requirements for each SIF to bring the process to a safe state within the process safety time;	x	x				General Requirements *(5.8)* SIF List *(Annex A)*	FEED Detailed Engineering
10	the required SIL and mode of operation (demand/continuous) for each SIF;	x	x			x	SIF List *(Annex A);* General Requirements *(5.3)* ExSILentia *(Annex A)*	FEED Detailed Engineering
11	a description of SIS process measurements, range, accuracy and their trip points;	x	x			x	*Instrument Data Sheets; Company Standards (Accuracy)* *Narratives (Trip Setpoints)*	Detailed Engineering
12	a description of SIF process output actions and the criteria for successful operation, e.g., leakage rate for valves;	x	x			x	SIF List *(Annex A)* ExSILentia *(Annex A)*	FEED Detailed Engineering
13	the functional relationship between process inputs and outputs, including logic, mathematical functions and any required permissives for each SIF;	x	x		x	x	Cause & Effect Diagrams/Narratives *(Annex D)*	FEED
14	requirements for manual shutdown or each SIF;	x	x				SRS General Requirements (5.10) Cause & Effect Diagrams/Narratives *(Annex D)*	FEED
15	requirements relating to energize or de-energize to trip for each SIF;	x			x	x	SRS General Requirements *(5.10)* SRS Specific Notes *(6.4, 6.4)* SIF List *(Annex A)*	FEED Detailed Engineering
16	requirements for resetting each SIF after a shutdown (e.g., requirements for manual, semi-automatic, or automatic final element resets after trips);	x	x		x	x	SRS General Requirements *(5.9)* Cause & Effect Diagrams/Narratives *(Annex D)*	FEED

SRS Plan

17	maximum allowable spurious trip rate for each SIF;	x	x			x	SRS General Requirements *(5.5.2)*	FEED
18	failure modes for each SIF and desired response of the SIS (e.g., alarms, automatic shut-down);	x	x		x	x	SRS General Requirements *(5.8, 5.12)* Cause & Effect Diagrams/Narratives (Annex D)	FEED
19	any specific requirements related to the procedures for starting up and restarting the SIS;	x	x				SRS General Requirements *(6.5)* Cause & Effect Diagrams/Narratives (Annex D) Process Unit Operating Procedures	FEED Detailed Engineering
20	all interfaces between the SIS and any other system (including the BPCS and operators);	x	x		x	x	SRS General Requirements *(5.12)*	FEED
21	a description of the modes of operation of the plant and requirements relating to SIF operation within each mode;	x	x				Process Unit PHA/LOPA *(Annex D)* *SRS Specific Notes (6.5)*	FEED
	the application program safety requirements as listed in 10.3.5;							
22	the SIFs supported by the application program and their SIL;				x	x	Cause & Effect Diagrams/Narratives (Annex D)	FEED
23	real time performance parameter such as, CPU capacity, network bandwidth, acceptable real time performance in the presence of faults, and all trip signals are received within a specified time period;				x	x	SRS General Requirements *(5.2, 5.6, 5.7, 5.12)*	FEED
24	program sequencing and time delays if applicable;				x	x	SRS General Requirements *(5.2)* Cause & Effect Diagrams/Narratives *(Annex D)*	Detailed Engineering
25	equipment and operator interfaces and their operability;				x	x	SRS General Requirements *(5.7, 5.12, 5.15)* SIS HMI Specification	FEED Detailed Engineering

Honeywell
THE POWER OF CONNECTED

SRS Plan

26	all relevant modes of operation of the process as specified in the SRS;				x	x	SRS General Requirements *(6.5)*	FEED
27	action to be taken on bad process variable such as sensor value out of range, excessive range of change, frozen value, detected open circuit, detected short circuit;				x	x	SRS General Requirements *(5.7)*	Detailed Engineering
28	functions enabling proof testing and automated diagnostics tests of external devices (e.g., sensors and final elements) performed in the application;				x	x	SRS General Requirements *(5.17)*	Detailed Engineering
29	application program self-monitoring (e.g., application driven watch-dogs and data range validation);				x	x	SRS General Requirements *(5.7)*	Detailed Engineering
30	monitoring of other devices within the SIS (e.g., sensors and final elements);				x	x	Cause & Effect Diagrams/Narratives *(Annex D)*	FEED
31	any requirements related to periodic testing of SIF when the process is operational;				x	x	ExSILentia (Annex A) Safety Manuals (*Annex E)* Proof Test Procedures *(Annex G)*	Detailed Engineering
32	references to the input documents (e.g., specification of the SIF, configuration or architecture of the SIS, hardware safety integrity requirements of the SIS);				x	x	SIS Hardware Specification *(Annex H)* SIS Software Specification *(Annex H)* SIS Supplier Functional Design Specification *(Annex H)*	FEED Detailed Engineering
33	the requirements for communication interfaces, including measures to limit their use and the validity of data and commands both received and transmitted;				x	x	SRS General Requirements (5.2)	Detailed Engineering

Honeywell
THE POWER OF CONNECTED

SRS Plan

34	process dangerous states (for example closure of two isolation gas valves at the same time that could lead to pressure fluctuations thus leading to a dangerous state) generated by the application program shall be identified and avoided;				x	x	Process Unit PHA/LOPA *(Annex B)*	FEED
35	definitions of process variable validation criteria for each SIF;				x	x	SRS General Requirements *(5.7)*	Detailed Engineering
36	requirements for bypasses including written procedures to be applied during the bypassed state which describe how the bypasses will be administratively controlled and then subsequently cleared;	x	x			x	SRS General Requirements *(5.15)* Site Risk Management procedure	FEED Detailed Engineering
37	the specification of any action necessary to achieve or maintain a safe state of the process in the event of fault(s) being detected in the SIS, taking into account of all relevant human factors;	x	x			x	SRS General Requirements (*5.10)* Cause & Effect Diagrams/Narratives *(Annex D)*	FEED
38	the mean time to repair which is feasible for the SIS, taking into account the travel time, location, spares holding, service contracts, environmental constraints;			x			SRS General Requirements *(5.11)* ExSILentia *(Annex A)*	FEED Detailed Engineering
39	identification of the dangerous combinations of output states of the SIS that need to be avoided;	x	x				Process Unit PHA/LOPA *(Annex D)* SRS General Requirements *(6.6)*	FEED Detailed Engineering
40	identification of the extremes of all environment conditions that are likely to be encountered by the SIS during shipping, storage, installation and operation. This may require consideration of the following: temperature, humidity, contaminants, grounding, electromagnetic interference/radio frequency interference (EMI/RFI), shock/vibration, electrostatic discharge, electrical area classification, flooding, lightning, and other related factors;			x	x	x	SIS Hardware & Instrumentation Design Specifications Supplier Functional design Specification Instrument Datasheets	FEED Detailed Engineering
41	identification of normal and abnormal modes for both the plant as a whole (for example, plant start-up) and individual plant operational procedures (for example, equipment maintenance, sensor calibration and/or repair). Additional safety instrumented functions may be required to support these process operating modes;	x	x	x			Process Unit PHA/LOPA (*Annex D)* SRS General Requirements (*6.7)*	FEED Detailed Engineering
42	definition of the requirements for any safety instrumented function necessary to survive a major accident event, for example, time required for a valve to remain operational in the event of a fire.	x	x				SIS Hardware & Instrumentation Design Specifications SRS General Requirements *(5.2)* ExSILentia (Annex A)	FEED Detailed Engineering

SRS Plan

- Project FEED Stage
  - Define 33 out of the 42 Requirement
    - Completed PHA/LOPA
      - 6 Requirements
    - Cause and Effects/Narratives
      - 9 Requirements
    - SIF List
      - 4 Requirements
    - General Requirements
      - 18 Requirements

SRS Plan

- Project Detailed Engineering Stage
  - Remaining 9 out of the 42
    - SIL Verification (ExSILentia)
      - 6 requirements from FEED used and now documented in the tool
      - 1 new Detailed Engineering requirement
    - Device Safety Manuals
      - 1 Requirement
    - Proof Test/ Risk Management/Operating Procedures
      - 4 requirements
    - Hardware/Software/HMI Specification
      - 4 Requirements
    - Device Datasheets
      - 1 Requirement

Application SRS 10.3.3

- 10.3.3 The application program safety requirements shall be derived from the SRS and chosen architecture (arrangement and internal structure) of the SIS. The application program SRS may be part of the SRS or in a separate document. The input to the application program safety requirements for each SIS subsystem shall include:
  - the specified safety requirements of each SIF, including sensor voting etc.;
  - the requirements resulting from the SIS architecture and the safety manual such as limitations and constraints of the hardware and embedded software;
  - any requirements of safety planning arising from 5.2.4.

Application SRS Continued

- 10.3.4 The application program safety requirements shall be specified for each programmable SIS device necessary to implement the required SIF consistent with the architecture of the SIS.

- 10.3.5 The application program safety requirements shall be sufficiently detailed to allow the design and implementation to achieve the required functionality and safety integrity and to allow a functional assessment to be carried out. The following shall be considered:

Application SRS 10.3.5 Continued

- the SIFs supported by the application program and their SIL;

LEGEND
X = CLOSE
O = OPEN
SD = SHUTDOWN
A =ACTIVATE
SCI-xx = SAFETY CRITICAL INSTRUCTION
NO. xx

					ACTION	XV-102		
					FAIL POSITION	FC		
			CLASSIFICATION					
					SERVICE	DEMETH BTMS FROM E-1719 TO C-1724A		
					RESET NOTES	A		
				NOTES				
ITEM	INPUT	TAG NUMBER			P&ID	123-456	DCS ALARM	BYPASS SWITCH
1	HI-HI LEVEL IN DEMETH BTMS VAPORIZER NO.2 C-1724A	LT-101A LT-101B LT-101C		1,2,3	123-456	X(3 SEC DELAY)	LZH-101	HZI-101A HZI-101B HZI-101C

Application SRS 10.3.5 Continued

- real time performance parameter such as, CPU capacity, network bandwidth, acceptable real time performance in the presence of faults, and all trip signals are received within a specified time period;
  - System loading
    - Processor scan time
    - Memory requirements
    - Network
  - How are LS hardware faults addresses
    - Are there any faults that need to fail safe the outputs?
    - AI channel fault a vote to trip?
    - Is there enough sensor redundancy that a fault on a input channel will degrade a SIF?
    - Consider MTTR used in calculations and determine action on faults.

- program sequencing and time delays if applicable;
  - Input conditioning (EU Range, validation, filter timer (time delay)
  - Voting
  - FO

Application SRS 10.3.5 Continued

- equipment and operator interfaces and their operability;
  - General Requirements – FEED; SIS HMI Specification – DE
    - The following requirements for human-machine interface shall be met for all protective functions, unless otherwise specified. Human-machine interface functions shall be implemented in the SIS HMI and the Operational Interface. The SIS HMI or the Operational Interface shall include but not be limited to the following for each function: See the SIS HMI Specification for further detail.
      - » Input values or status
      - » Set Points and process measurement values for trip action and pre-trip alarms
      - » Output state(s)
      - » SIF shutdown First Out status
      - » Override/Bypass and Inhibit status
      - » SIS logic solver communication status

- all relevant modes of operation of the process as specified in the SRS;
  - List all modes that affect the SIS General Requirements and C&E/Narratives
    - Normal
    - Startup/Shutdown
    - Regen

Application SRS 10.3.5 Continued

- action to be taken on bad process variable such as sensor value out of range, excessive range of change, frozen value, detected open circuit, detected short circuit;

Voting Condition	1oo2 Voted Transmitters		Trip Status
2 Healthy Sensors Normal 1oo2 Voting	OK	OK	OK
	OK	TRIP	TRIP
	TRIP	TRIP	TRIP
Bypass Conditions	BYPASS	OK	OK
	BYPASS	TRIP	TRIP
	BYPASS	BYPASS	NOT ALLOWED
Bad PV Conditions	BAD PV	OK	OK
	BAD PV	TRIP	TRIP
	BAD PV	BAD PV	TRIP
Bypass / Bad PV Conditions	BYPASS	BAD PV	TRIP

Application SRS 10.3.5 Continued

- functions enabling proof testing and automated diagnostics tests of external devices (e.g., sensors and final elements) performed in the application;
  - SRS General Requirements (Functional Testing)
    - Are there any automated testing performed by the application? Provide a list
  - C&E/Narrative
    - Define how the logic functions
    - Pass/fail criteria
- application program self-monitoring (e.g., application driven watch-dogs and data range validation); monitoring of other devices within the SIS (e.g., sensors and final elements);
  - SRS General Requirements (Diagnostics)
    - Sensor Deviations
    - Sensor faults (out of range Low/High) ma requirement
- any requirements related to periodic testing of SIF when the process is operational;
  - SRS Annex
    - Safety Manuals
    - SIL Verification Tools
    - Proof Test Procedures

Application SRS 10.3.5 Continued

- references to the input documents (e.g., specification of the SIF, configuration or architecture of the SIS, hardware safety integrity requirements of the SIS);
  - SIS Hardware/Application Spec
- the requirements for communication interfaces, including measures to limit their use and the validity of data and commands both received and transmitted;
  - SRS General Requirements, what is permitted
    - Peer to Peer, Ethernet, Modbus, Fieldbus, Profibus, HART
- process dangerous states (for example closure of two isolation gas valves at the same time that could lead to pressure fluctuations thus leading to a dangerous state) generated by the application program shall be identified and avoided;
  - PHA/LOPA
    - Hazard being mitigated may have many secondary FE actions.
    - Consider grouping all of the action into one C&E
- definitions of process variable validation criteria for each SIF.
  - Contextual (Low pump flow trip active only if pump is running)
  - Sensor alarm/fault, Voting tables
  - Sensor Ranges (Datasheets)

Application SRS 10.3.6

- 10.3.6 The application program safety requirements shall be expressed and structured in such a way that they:
  - describe the intent and approach underpinning the application program safety requirements;
  - are clear and understandable to those who will utilize the document at any phase of the SIS safety life-cycle; this includes the use of terminology and descriptions which are unambiguous and understood by all users (e.g., plant operators, maintenance personnel, application programmers);
  - are verifiable, testable, modifiable;
  - are traceable back through all deliverables including the detailed design documents, the SRS and the H&RA that identifies the required SIF and SIL.

Knowledge check

- The Safety Requirements Specification is a collection of documents that fully describe the functionality and performance requirements of a Safety Instrumented Function
- The SIS industry standard breaks down the SRS into 42 requirements covering all aspects of SIS design & engineering
- Development of the SRS requires collaboration among Process Engineering, Operations, and I&C Engineering
- 33 out of the 42 requirements are defined during/after the PHA/LOPA is complete.
- Application programming requirements added

SIS Application Development

- The objective of Clause 12 is to define the requirements for the development of the application program.
  - Programmer understand requirement
    - Programmer provides Function Design Specification
  - Justification for suitability of previously developed program library
  - Written procedures for developing, testing, and modifying during testing
  - Competencies
  - Define documents including versions used to develop application
  - LS safety manual constraints

Main Objective

- Minimize faults in application during development and testing
- Have evidence of the quality of the application