Additions and Revisions to IEC61511

• Angela E. Summers, President
• Eloise Roche, Senior SCAI Consultant
Eloise Roche  
Senior SCAI Consultant  
SIS-TECH Solutions

- 24 years Chemical Industry background, largely in automation and functional safety management
- Specializes in Safety Controls, Alarms, and Interlocks (SCAI)
- Member of ISA-84 committee and multiple working groups
- Subcommittee Member for revision of “Guidelines for Safe Automation of Chemical Processes”
- Certified Functional Safety Expert
Dr. Angela Summers
President
SIS-TECH Solutions

- Specializes in control and process safety applications
- Active participant in many CCPS books
- Member of many industrial committees and forums
- ISA Fellow, AICHE Fellow, CCPS Fellow
- Ph.D. and Engineering Fellow, The University of Alabama
- Licensed Professional Engineer in the State of Texas
Additions and Revisions to IEC61511

• Angela E. Summers, President
• Eloise Roche, Senior SCAI Consultant
Revision Status

- Final Draft International Standard (FDIS)
  - Voting and strictly editorial comments

- Publication
  - Expected 1H2016
There are a lot of changes…

The following are changes the **international committee** of end users, vendors, service providers, etc. and the **national voting delegates** agreed to accept.
Broad Change Themes for Edition 2.0

• Boundaries on Hazard and Risk Analysis (H&RA)
• Data Quality
• Performance Metrics
• Hardware Fault Tolerance and Compensating Measures
• Grandfathering and Change Management
• (Cyber) Security for SIS
Boundaries on Hazard and Risk Analysis (H&RA)

Penning in the PHA

Limits for LOPA

Reality Check on Risk Graph

These requirements apply regardless of the H&RA methodology used
IEC 61511 Ed. 2.0 clarifies limits on

- Frequency claimed for BPCS (i.e., process control) failure as an initiating cause
- Risk Reduction claimed for BPCS protection layers
- Total risk reduction for all SIS and BPCS protection layers allocated for a demand cause
Frequency limit for BPCS failure as initiating cause

- BPCS includes all of the devices necessary to operate the process and its associated equipment in the desired manner, but does not perform SIFs

  N.B.: This includes alarm systems as well as systems performing other process control functions such as control loops, interlocking, process state management, etc.

- Average frequency of dangerous failures of BPCS as an initiating source \( \geq 10^{-5} \) per hour

  LOPA Tip: Approximately 1/10 years

- Failure of the BPCS may be caused by anything responsible for correct BPCS operation, such as the sensor, valve, operator error, or logic solver
Limits on BPCS protection layer credits

• BPCS protection layer risk reduction $\leq 10$
  – To claim a risk reduction $> 10$ for an instrumented protection layer in the BPCS, the BPCS (i.e., all the devices necessary to operate the process) must conform to IEC-61511

• If it is not intended that the BPCS conform to this standard:
  – One BPCS protection layer when the initiating source of the demand is BPCS
    • BPCS IC and BPCS protection layer
  – Two BPCS protection layers when the BPCS is not the initiating source of the demand
However...

• Each BPCS protection layer must be **sufficiently independent**
  – From the demand cause
  – From the other BPCS protection layer

• Consider sensors, logic solvers, final elements etc., in the evaluation of sufficient independence.
  – Standard specifically notes that a hot backup controller is not sufficiently independent from the primary controller

---

For BPCS IC + BPCS IPL or for 2 BPCS IPLs either need 2 separate controllers or a SIL-2 equivalent logic solver
Risk reduction >10 000 in instrumented layers

- The application (i.e., process and protection strategy) shall be reconsidered if the protection layer allocation results in a risk reduction requirement of more than 10,000 (i.e., SIL-4 equivalent) to be achieved by
  - 1 SIS
  - Multiple SIS
  - Combination of SIS and BPCS protection layer(s)

Add up the risk reduction (or average frequency of dangerous failures) of all instrumented protections for the hazard cause/consequence
Risk reduction >10 000 in instrumented layers also applies to average frequency of failure < 1/10 000 years

- Lack of independence shall be assessed and shown to be sufficiently low compared to the risk reduction requirements

- Assessment must consider:
  - Common cause of demand and SIS failure
  - Common cause failure of protection layers providing risk reduction
  - Any dependencies that may be introduced by common operations, maintenance, inspection or test activities or by common proof test procedures and proof test times
QUANTITATIVE Assessment

• Use a quantitative methodology to confirm that the safety integrity requirements are achieved

• Take into account the common cause and dependency between the layers

If you need risk reduction > 10,000 from instrumentation and controls, you need QRA.
Boundaries on Hazard and Risk Analysis (H&RA)

Questions or comments?
Allocation, Specification and Design Data

• During the allocation, specification, and design processes, there may be many values assumed or estimated:

  - Device failure rates (prior use or certification report)
  - Diagnostic coverage
  - SIS demand rates
  - Device response times
  - Proof test coverage
  - Repair/bypass duration
  - Timely operator response to alarm
  - Test interval
  - Common cause %

• IEC61511 Ed. 2.0 includes new and updated requirements regarding the justification and reliability of this data
SUITABLE for the APPLICATION

• All SIS devices must be suitable for the operating environment
  – Manufacturer’s documentation
  – Constraints from SRS
  – Assumed reliability parameters

If a sensor is too inaccurate or a valve too slow for a given SIF, that SIF will NEVER WORK, regardless of what the SIL calculation says.
Prior Use (NOT Proven In Use)

- Documented assessment based on *previous operating experience* in *similar operating environments*
  - User documents that the *device* has achieved satisfactory performance in a *similar operating environment*
  - Meets the required functional and safety integrity requirements
  - Identify and control sources of dangerous systematic faults and hardware failures
Prior Use

- Understanding *how the equipment behaves in the operating environment* is necessary to achieve a *high degree of certainty* that the *planned design, inspection, testing, maintenance, and operational practices are sufficient*.
Data Quality and Source

• Shall be credible, traceable, documented and justified
• Shall be based on the field feedback existing on similar devices used in a similar operating environment
• Engineering judgement can be used to assess missing reliability data or evaluate the impact on reliability data collected in a different operating environment

Certification report failure rates can be a starting point, but are usually not sufficient in and of themselves.
Reliability Data Uncertainty

• The reliability data uncertainties shall be assessed and taken into account when calculating the failure measure.
  – NOTE 1 Less field feedback results in more uncertainty. Published standards (IEC 60605-4), Bayesian approaches, engineering judgement, etc. may be used to estimate the reliability data uncertainties.

• Reliability data must have an upper bound statistical confidence limit of at least 70%
Other than random failure reliability numbers?

• Persons responsible for operation and maintenance shall review and confirm validity of assumptions made during H&RA, allocation, specification and design

• Examples:
  – Corrosion protection
  – Building occupancy
  – Operator/Maintenance occupancy in unit
  – Flammability parameters
  – Time needed for response to alarm
  – Alarm management effectiveness
Allocation, Specification and Design Data

Questions or comments?
Performance Metrics

• Collecting the data that would be used in a prior use justification, and periodically verifying that the performance remains consistent with the values used in the allocation and design becomes explicitly required in Edition 2.0
Procedures for Lifecycle Assurance

Required procedure content includes requirements to:

– Monitor and assess whether *reliability parameters* of the SIS are in accordance with those assumed during the design

– Define the necessary corrective action to be taken if the *reliability parameters* are different than what was assumed during design
Procedures for Performance Monitoring

• Procedures to ensure quality and consistency of testing and to ensure adequate validation after device replacement

• Procedures for collecting data related to the demand rate and SIS reliability parameters

• Methods and procedures that are used to test the diagnostics
Prove It...

- Periodically assess that requirements within IEC61511 for safety management and verification are being met throughout the lifecycle and that maintenance and operations are being carried out as assumed in design.

Stage 4 Functional Safety Assessment (FSA) becomes mandatory, and recurring
Fix it when actual ≠ expected

Discrepancies must be analyzed and (if necessary) modification made to maintain safety:

- Demand rate and spurious trip rate on each SIF
- Actions taken following a demand
- Cause of demands and spurious trips
- Failures and failure modes of SIS devices
- Failure of equipment forming part of any compensating measures
Performance Metrics

Questions or comments?
Hardware Fault Tolerance and Compensating Measures

• Edition 2.0 simplifies the basic requirements for hardware fault tolerance and for maintaining safety in the presence of a detected fault (compensating measures), but still allows for choosing more complicated paths...
But First...

- Hardware fault tolerance is a separate design requirement in addition to SIL PFD/FPH

- Hardware Fault Tolerance limits were created to mitigate some of the more common design and implementation systematic failures:
  - Using overly optimistic reliability parameter assumptions
  - Maintenance error such as leaving a root valve closed or a bypass jumper in place
Hardware Fault Tolerance (HFT) – One Table

<table>
<thead>
<tr>
<th>SIL</th>
<th>Minimum required HFT</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 (any mode)</td>
<td>0</td>
</tr>
<tr>
<td>2 (low demand mode)</td>
<td>0</td>
</tr>
<tr>
<td>2 (high demand/continuous mode)</td>
<td>1</td>
</tr>
<tr>
<td>3 (any mode)</td>
<td>1</td>
</tr>
<tr>
<td>4 (any mode)</td>
<td>2</td>
</tr>
</tbody>
</table>

- HFT requirement applies to each SIF
- HFT can be evaluated at each independent SIS sub-system
- DC for FVL or LVL programmable devices shall not be less than 60%

11.4.1, 11.4.2, 11.4.5 and 11.4.8
HFT- more complicated alternatives

• If not using FVL or LVL programmable devices, the minimum HFT can be reduced based on justification that designing per the table results in decreased safety
  – If the reduction would make HFT=0, must provide evidence that the likelihood of the excluded faults are very low relative to the SIL requirements

• If not following the HFT rules in IEC-61511, must follow either route 1H or route 2H from IEC 61508-2:2010
Detecting a fault does not make process safe

- The maximum time the SIS is allowed to be in bypass (repair or testing) while safe operation of the process is continued shall be defined.

- Compensating measures that ensure continued safe operation shall be provided when the SIS is in bypass (repair or testing).

Define maximum bypass time and have compensating measures to protect against the risk as necessary.
Compensating Measures – must be real

• **Temporary implementation of planned and documented methods for managing risks during any period of maintenance or process operation when it is known that the performance of the SIS is degraded**

• Hazard analysis is required to ensure compensating measures provide adequate risk reduction

• Dangerous fault alarms are subject to proof testing and change management
  – If the compensating measure depends on response to the alarm, the alarm is part of the SIS
Written Procedures with Correct Content

• Compensating measures that ensure continued safety while the SIS is disabled or degraded due to bypass (repair or testing) shall be applied with the associated operation limits (duration, process parameters, etc.)

• The operator shall be provided with information on
  – procedures to be applied before and during bypass
  – what should be done before the removal of the bypass
  – the maximum time allowed to be in the bypass state

• The compensating measure information must be regularly reviewed
Hardware Fault Tolerance and Compensating Measures

Questions or comments?
Grandfathering and Change Management

• ANSI/ISA84.00.01-2004 Part 1 (IEC61511-1 Mod) was virtually identical to IEC61511 Ed. 1.0
• The exception was the addition of one item to the scope that addressed SIS designed and constructed prior to the publication of that version of ISA84.00.01
• IEC61511 Ed. 2.0 will now address this issue in a clause within Section 5: Management of functional safety
Existing Systems

- For existing SIS designed and constructed in accordance with codes, standards, or practices prior to the issue of this standard the user shall determine that the equipment is ______ in a safe manner:
  - Designed
  - Maintained
  - Inspected
  - Tested and
  - Operating
SIS Change Management

- Changes affecting requirements on the SIS require change management

- Prior to modifying a SIS, evaluate whether modification could impact safety. If yes, enter safety lifecycle at appropriate phase.

- Create safety plan for modification and re-verification and ensure documentation is updated.

- When change triggers an FSA: Confirm that the modification work performed is in compliance with the requirements of IEC 61511.

Modification work affecting existing SIS specification, design, or implementation must be in compliance with IEC 61511.
Grandfathering and Change Management

Questions or comments?
(Cyber) Security for SIS

• With continued occurrences of successful cyber security attacks to control systems throughout the industrial world, HIGH LEVEL security requirements have been added to Edition 2.0
Security Risk Management

Security Risk Assessment is required:

- Description of identified threats and potential consequences
- Description of the measures taken to reduce or remove the threats
- Determination of requirements for additional risk reduction

• SIS design shall provide the necessary resilience against the identified security risks
Refers out to other standards and guidance

**ISO/IEC 27001:2013**
“Information security management”

**ISA/IEC-62443 Parts 1-3**
“Security for industrial automation and control systems” - Suite of 13 documents addressing IACS cyber security

**ISA TR84.00.09**
“Security Countermeasures Related to SIS” – Merging material from IEC-61508, IEC-61511 and IEC-62443 standards to provide guidance for cyber security for SIS and associated IACS
(Cyber) Security for SIS

Questions or comments?
Summary

IEC 61511 Ed. 2.0 provides focused updates on

- Initiating cause frequency and protective risk reduction claim limits for instrumented systems other than SIS (aka BPCS)
- Additional requirements for claiming 10,000 or more risk reduction for instrumented protections
- Requirements for justification and ongoing performance monitoring for data used in SIS design
- Designing for and managing risk in the presence of SIS faults
- Grandfathering and Change Management
- (Cyber) Security

How significant (i.e., “major” or “minor”) these changes are to each user will depend on their company’s current functional safety program
Questions?
Some Other Changes

• If the allocation for a hazardous event includes multiple SIFs on one SIS, the SIS must be suitable for the overall risk reduction

• A safety manual must be created for the SIS
  – Intended device configuration
  – Intended operating environment
  – Operation
  – Maintenance
  – Fault detection
  – Constraints
Some Other Changes

• Communication used to implement a SIF must use technique appropriate for safety applications at the required SIL

• Specified revision number required for prior use approved devices. Device change must be managed by MOC, at which point the continued validity of the prior use evidence is evaluated
Some Other Changes

- Functional definition of the SIF from the recorded allocation process must include:
  - Actions to be taken
  - Setpoint(s) for the measurement(s)
  - SIF response time requirements
  - Intended activation delays
  - How the SIF should react to detected faults
  - Valve closure requirements (i.e., tightness)

- Procedure to manage competence of everyone involved in SIS life cycle, including periodic assessment of competence of individuals against the (SIS lifecycle) activities they perform
A Few of the Other Changes

Questions or comments?