Dr. Angela Summers
President
SIS-TECH

- *2009 ISA Fellow*
- *2005 ISA Albert F Sperry Award*
- *Technical writer, CCPS Guidelines for Safe and Reliable Instrumented Protective Systems*
- *1 of 5 US Experts to the IEC 61508/IEC 61511 committee*
- *Working Group Chair, TR84.00.02 (SIL Verification) and TR84.00.04 (Guidance on ISA 84.00.01-2004)*
- *Member of more than 20 industrial committees and forums*
- *Ph.D., Centennial and Engineering Fellow, The University of Alabama*
- *Licensed Professional Engineer in the State of Texas*

SIS TECH

What's up with SIS?

Angela E. Summers, PhD, PE
President
SIS-TECH Solutions, LP

SIS TECH

Presentation Scope and Disclaimer

3

- Scope
  - ISA 91.01
  - ISA TR84.00.??
    - .02 .03 .04
  - IEC 61511 or ANSI/ISA 84.00.01
- Disclaimer
  - Represents my personal opinion
  - May not represent the opinions of everyone on the committee

SIS TECH

ISA 84 – instrumentation and control in process safety applications

4

- The ISA 84 and 91 committees merged in 2007
- ISA 91 - **Criticality Ranking for Instrumentation**
  - Identification of the instruments that are classified as emergency shutdown systems and safety critical controls
  - Establishes requirements for testing and documenting the test results of these systems
- ISA 84 - **Electrical/Electronic/Programmable Electronic Systems (E/E/PES) for Use in Process Safety Applications**
  - Develops standards and technical reports for use in applying Electrical/Electronic/Programmable Electronic Systems (E/E/PES) for use in process safety applications.

SIS TECH

5

ISA 91.01

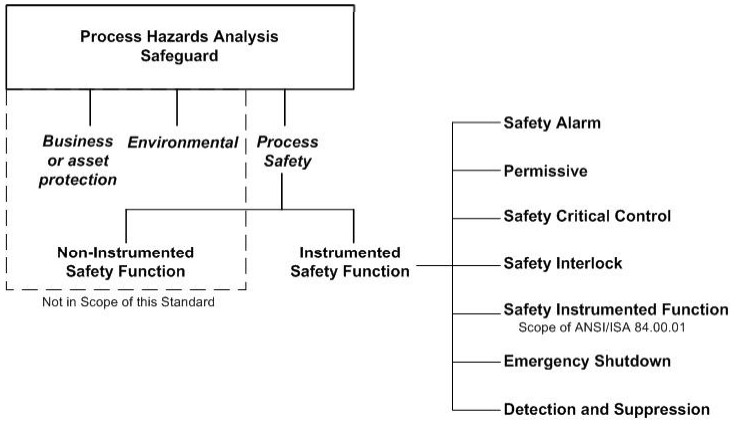
- New number: ISA 84.91.01 replaces ISA 91.01
- New title: **Identification and Mechanical Integrity of Instrumented Safety Functions in the Process Industry**
- Defines what must be covered by mechanical integrity
- Uses new term – Instrumented safety function
  - Process safety safeguard implemented with instrumentation and controls, used to achieve or maintain a safe state for a process, and required to provide risk reduction with respect to a specific hazardous event.

SIS TECH

6

Relationship between ISF and SIF

- Safety instrumented functions (SIF) are one of many types of ISF used to maintain safe operation.



Draft ISA 84.91.01

SIS TECH

ANSI/ISA 84.00.01-2004

7

- Title: **Functional Safety: Safety Instrumented Systems for the Process Industry Sector**
  - Next revision number: ANSI/ISA 61511
- Plan to adopt revised IEC 61511 when available
- Maintain "grandfather clause" for existing safety instrumented systems (SIS) - Part 1 Clause 1 y:

For existing SIS designed and constructed in accordance with codes, standards, or practices prior to the issuance of this standard (e.g. ANSI/ISA 84.01-1996), the owner/operator shall determine that the equipment is designed, maintained, inspected, tested, and operating in a safe manner.

SIS TECH

Complimentary ISA Technical Reports

8

- Updating 3 technical reports as a complimentary series
  - TR84.00.02
  - TR84.00.03
  - TR84.00.04
- Provide informative guidance related to specific phases of the SIS lifecycle
- Practical examples of implementation on various topics and applications
- TR updates include topics to be addressed in IEC 61511 update

SIS TECH

9

ISA TR84.00.02 - 2002

- **Safety Integrity Level (SIL) Verification of Safety Instrumented Functions** - Next revision late 2012
  - Reorganizing into 1 part with annexes
- Overview – Quantitative Analysis
  - assessing random and systematic failures, failure modes and failure rates
  - understanding the impact of diagnostics and mechanical integrity (MI) activities on the SIL and reliability
  - identifying sources of common cause, common mode and systematic failures
  - using quantitative methodologies to verify the SIL and spurious trip rate

SIS TECH

10

ISA TR84.00.03 - 2002

- New title - Mechanical Integrity of Safety Instrumented Systems (SIS) - Next revision 2011
  - Reorganizing in 1 part with annexes
- Overview – Testing and Maintenance
  - identification of personnel roles and responsibilities when establishing an MI plan
  - important considerations in establishing an effective MI program
  - detailed examples to illustrate user work processes supporting various activities of the MI program

SIS TECH

11

ISA TR84.00.04 - 2011

- Guidelines for the Implementation of ANSI/ISA 84.00.01-2004 – Already balloted
  - Same organization – 2 parts with multiple annexes
- Overview – The lifecycle
  - "grandfathering" existing SISs (Clause 3/Annex A)
  - operator initiated functions (Annex B)
  - separation of the BPCS and SIS (Annex F)
  - field device and logic solver selection (Annex L)
  - manual shutdown considerations (Annex P)
  - design/installation considerations (Annex N)

SIS TECH

12

ISA TR84.00.04 - 2005

- The big changes:
  - Annex C Management of Functional Safety
    - Including Clause 5 quality assurance requirements
  - Annex L Device Selection
    - Enhancing user approval approach with example method
  - Annex P Response to Detection of a Dangerous Fault
    - More considerations for fault detection strategy
  - New Annex Q Setpoint Guidance
  - New Annex R Key Performance Indicators

SIS TECH

Three new efforts

13

- ISA TR84.00.04 – Revision 3
  - Updating safety alarm guidance (Annex B)
- ISA TR84 – Wireless WG8
  - Considerations for implementation of wireless of SIS applications
- ISA TR84 – Security WG9
  - Consideration for ensuring safety and security of SIS applications

SIS TECH

Summary

14

- Practices are on a regular revision cycle
  - Most are on 5 year cycle, but often take longer
- During recent revision cycle, more focus on
  - Gathering prior use information
  - Understanding operating environment impact
  - Addressing common cause in hardware, software, and procedures
  - Estimating and accounting for systematic errors

SIS TECH

15

IEC 61511 Revision

- 100s of comments submitted by national committees
  - Changes to standard are limited to these comments
- Many changes intended to improve clarity
- Adding guidance on many lifecycle activities
- Presentation is limited to top 5 user impacting subject areas

SIS TECH

16

Top 5

- SIL 4
- Credit in the BPCS
- Hardware Fault Tolerance
- Prior Use
- Safety Manual

SIS TECH

17

1. SIL 4 - Problem

- Typical industry practices considered insufficient to achieve a single function SIL 4
- Some applications require 4 orders of magnitude risk reduction from instrumented systems (includes BPCS, SIS, Fire and Gas, etc.)
  - Inherently safer design is often not an option
  - Difficult to implement **multiple independent** instrumented safety systems
  - Dependency is not adequately addressed through division into multiple functions

SIS TECH

18

1. SIL 4 - Proposed Solution

- Supplemental analysis for single or multiple instrumented functions providing SIL 4 equivalent risk reduction:
  - Assess common cause between SIS and the cause of demand.
  - Assess common cause with other systems providing risk reduction
  - Assess any dependencies introduced by common proof test people, procedures and timing
  - Recommend quantitative method to estimate the hazardous event frequency
- Limit single function SIL 4 to non-PE logic solvers

SIS TECH

19

2. Credit in the BPCS - Problem

- No clear definition on what using the BPCS as a layer means
  - Can include both normally operating as well as state control functions
- Guidance in Part 2 Clause 9.3
  - Illustrates 2 separate systems to achieve 2 credits – 1 initiating cause and 1 safety function
- CCPS LOPA book allowed 2 credits in the BPCS
  - When BPCS is not initiating cause (2 safety functions)
  - Independence in sensors, final elements, and I/O modules
  - Requires security and MOC
  - Demonstrated performance (prior use)

SIS TECH

20

2. Credit in the BPCS - Proposed Solution

- Claim no more than 2 separate and independent instrumented functions (that are not designed per IEC 61511) for same event.
- Justify claimed risk reduction.
  - Design analysis and prior use
  - Fault detection and response
  - Mechanical integrity
  - Access and Management of Change (including manual/bypass controls)
- Aligns with ISA 84.91.01

SIS TECH

21

3. Hardware Fault Tolerance - Problem

- Logic solver HFT based on SFF
  - SFF has fallen out of favor of most users
  - How does less reliable translate to safer product?
- Field device HFT uses complicated method
  - Use of Add 1 or Subtract 1 rules are not clear
  - Misapplied by many people – too much or too little
- New IEC 61508 method (Route 2H)
  - No consideration of SFF
  - Focuses on prior use

SIS TECH

22

3. Hardware Fault Tolerance - Proposed Solution

- Remove current add/subtract HFT method
- Revise new IEC 61508 method (Route 2H) for user application
  - SIL 1 (0), SIL 2 (0), and SIL 3 (1) for demand mode
  - Minimum diagnostic coverage for PE devices (>60%)
  - Prior use history to ensure random and systematic issues are understood
  - For field devices and non-PE logic solvers only, allows lowering HFT if the:
    - risk assessment demonstrates that the overall risk is increased by adding complexity to achieve the minimum HFT

      AND
    - verification shows the SIS meets the SIL

SIS TECH

23

4. Prior Use - Problem

- Use of IEC 61508 compliant field devices with no field experience is considered "unwise" by Users
  - Operating environment significantly impacts performance
  - User implementation may improve or degrade performance from theoretical
- Field devices should be selected based on prior use and any available manufacturer data (including safety manual)
  - Continued use of any product requires "prior use" information (Clause 5)

SIS TECH

24

4. Prior Use - Proposed Solution

- Introduce guidance similar to ISA TR84.00.04 Annex L - User Approval
- Prior Use Process
  - Demonstrated in-service performance
  - Understand and account for application environment impact in installation and mechanical integrity plan
  - Establish feedback process to remove devices/technologies that do not perform as required
  - Document user manual to ensure that "learnings" are retained and communicated

SIS TECH

25

5. Safety Manual - Problem

- The term "safety manual" is also used in IEC 61508
  - Leads some to believe that the previous requirements can be satisfied by the manufacturer
- Manufacturer cannot provide constraints for operation, maintenance, fault detection for the intended operational profiles
  - Provide products to a wide variety of industry applications
  - Limited/no knowledge of hazardous events or process
  - Limited/no knowledge of how equipment fits within overall functional safety plan

SIS TECH

26

5. Safety Manual - Proposed Solution

- Define ***User*** safety manual
- Clarify user safety manual requirements
  - Per manufacturer model #
  - Use limitations – operating environment
  - Failure modes - how to detect and correct
  - Special - installation or configuration requirements
  - Mechanical integrity - operation and maintenance manuals

SIS TECH

27

Conclusion - Common Themes

- More emphasis on justifying performance claims
  - "Real-world" data - Process and human impact
  - Claims for any/all instrumented functions, including BPCS
- Holistic approach needed
  - Division into functions can obscure interrelationships and interconnections
  - Multiple instrumented functions with separate claims
- Recognize impact of systematic failures
  - Common cause
  - Human impact

SIS TECH