Removal of Hardware ESD, Independent of Safety Logic Solver

by Sam Roy

Executive summary

This is a discussion to remove independent hardware based Emergency Shutdown for Logic Solver as identified in ANSI/ISA-84.00.01-2004, IEC 61511-1 Section 11.2.8.
This is a discussion to remove independent hardware based Emergency Shutdown for logic Solver as identified in ANSI/ISA-84.00.01-2004, IEC 61511-1 Section 11.2.8

“Manual means (for example, emergency stop push button), independent of the logic solver, shall be provided to actuate the SIS final elements unless otherwise directed by the safety requirement specification”.

Premise for removal:
A. SIS is implemented per ANSI/ISA-84.00.01-2004, IEC 61511 performance based safety standards, in conjunction with owner’s SIS implementation guidelines.
B. The Logic Solver is designed with hardware fault tolerance and performance capabilities to meet/exceed the most stringent Safety Integrity Level (SIL) implemented in the Logic Solver.
C. The Logic Solver provides diagnostics alarms for hardware and software failure, allowing opportunity to take corrective steps and on-line repair to avoid Logic Solver inadvertent failure.
D. The Safety Requirement Specification (SRS) identifies the basis for removal of Emergency Shutdown (ESD) independent of the Logic Solver.

Given these as a starting point:

Is it practical to implement and maintain hardware Emergency Shutdown (ESD) switch/Master Trip Relay (MTR) setup that is more safely available than the Logic Solver, and can be used effectively?

Remove independent hardware ESD switch/MTR setup for safety Logic Solver.

ESD switch/MTR setup can be found in different styles. These are based on company standard and project requirements. Typical ESD switch/MTR setup may consist of:

Hardware:
A. Redundant ESD switches 2oo2 configuration, each switch with 1oo2 contacts, 120v AC power, energized to trip, actuates shunt trip breaker to remove redundant power supplies from Logic Solver CPU and all I/O modules.
B. Singled ESD switch, key lock, with 2oo2 contacts, 24v DC Power, de-energized to trip, actuate 2oo2 safety relays to remove power from required output boards.
C. ESD switch/MTR may affect multiple Logic Solvers within a process unit.
D. Some cases alarm and/or indications for circuit availability, relay failure, etc is included.

Notes:
A. Removal of redundant power supplies (pull the plug) on an operating Logic Solver is not recommended by the manufacturer. In general this function is not tested during Factory Acceptance Test (FAT) or during Site Acceptance Test (SAT).
B. Similarly argument applies for removal of redundant 24v DC power supplies from output boards.
C. Actuation of hardware ESD switches/MTR is based on operator judgment call; that places multiple SIF to Fail-Safe state concurrently; which by itself could cause additional safety hazard.

Removal of independent hardware based on ESD switch/MTR for Logic Solver is based on:
A. Functional Safety Management
B. Safety Instrumented Function (SIF) mode
C. Allocation of Logic Solver
D. Logic Solver hardware qualification
E. Application Program to address all operational modes
F. Avoidance of common cause, common mode failure
G. Logic Solver failure detection and Mean Time To Restore (MTTR)
H. MOC to maintain Logic Solver integrity
I. Logic Solver re-validation at Turn-a-Round

This discussion is focused on Logic Solver design and integration activities, Stage 2 deliverable (Figure 8, ANSI/ISA-84.00.01-2004, or IEC 61511-1) to meet above objective.

To remove hardware ESD switch/ MTR setup; the Logic Solver shall be selected, configured, Application Program developed, and integrated per ANSI/ISA-84.00.01-2004, IEC 61511-1 in conjunction with the owner SIS implementation guidelines.

This discussion includes items related to Triconex safety Logic Solvers. Similar items may be considered for other Logic Solvers. Individual projects may require additional items to be resolved.

**Functional Safety Management**

FSM for project implementation to include:

A. Personnel competency in Logic Solver selection, hardware / software design and integration, including ability to realize faults and common cause, common mode issues that may lead to inadvertent failure.

B. Independent Review to ensure Logic Solver configuration, Application Program development, Integration, Pre-FAT, FAT manual development and execution are in compliance with Sec. 11.0, 12.0 and 13.0, and meets project specific Safety Requirement Specification (SRS).

C. Based on complexity of the application the Independent Review may be internal to the project team, or independent reviewer as identified in project Safety Plan per Sec. 5.2.4, 5.2.6.1, 7.0.

**Hardware ESD Switch/MTR Removal Applicability**

Applicable for:
- Non-SIF items
- Low Demand mode SIF with:
  - Automatic diagnostics execution (sensor, final element) once per Logic Solver scan
  - Proof Test Interval (TI) is determined to meet SIL and TI is << Demand Interval (DI).
  - Hardware ESD Switch on Operator Station connected to Logic Solver I/O for each major process equipment such as furnace, compressor, reactor, drier, etc. Fault tolerant multiplexer has to be considered if Operator Station is away from process units.
  - Soft manual trip switch on operator screen for each SIF
- HIPP SIF designed based on Low Demand mode
  - Same as above requirements
  - Hardware ESD Switch through Logic Solver I/O for each HIPP
- High Demand SIF: (may be considered)
  - Automatic Diagnostics execution, and Dangerous Detect alarm is to initiate Fail-Safe state.
  - TI is determined to meet PFH or half the DI whichever is lower.
  - Hardware ESD Switch through Logic Solver I/O for each High Demand SIF
Logic Solver Allocation

Following items are to be considered:

A. Process oriented and redundant train separation.
B. Process sustainability / flare handling capability in case of any single Logic Solver inadvertent failure.
C. Each major turbo compressor Integrated Machinery Protection System (IMPS) implemented in independent Logic Solver.
D. Number of furnaces (or process heaters) integrated in a single Logic Solver to be based on flare handling capacity and/or sustainability of related compressor in case of Logic Solver inadvertent failure.
E. Within single Logic Solver I/O separation based on major process equipment
F. SIF I/O allocation per sub-system fault tolerance setup.
G. Process or sub-system functions not considered as SIS in PHA/LOPA work process shall not be included in Logic Solver Application Program.
H. Partial Stroke Test execution function and valve performance is to be part of DCS and Asset Management System.
I. Safety Function Prevention and Mitigation are in independent Logic Solver.
J. Fire / Gas detection is in independent Logic Solver.

Logic Solver Hardware Qualifications

Selections and implementation to include:

A. IEC 61508 compliant, SIL-3 (or worst case SIL) applicability.
B. Proven In Use, plant experience in similar application.
C. Logic Solver PFDavg calculation; provided by the manufacturer.
D. Mean Time To Fail Safe (MTTFS) calculation; provided by the manufacturer.
E. Logic Solver CPU hardware failure from designed features to degraded mode to be tolerated for fixed time (based on criticality of the application) after which placing equipment to Fail-Safe state shall be in effect.

F. Detected failures for Logic Solver hardware and software are to be restored within 24 hrs.

G. Logic Solver environmental alarm that could lead to multiple SIF attaining fail-safe state concurrently shall be resolved with appropriate priority.

Qualitative Steps for Application Program Development

Application Program development to include:

A. Follow Logic Solver manufacturer manual and Safety Application Guidelines.
B. Maintain KISS principle and include SIS functions only.
C. User comprehensible and configured for maintainability through the safety lifecycle of the SIS.
D. Organize program segments based on major process equipment and logical sequence as applicable.
E. Within each Application Program organized functions, with ample comments and functional description.
F. Develop Application Program with Function Blocks and sequences. Function Blocks (Proven In Use, New, Modified) are to be approved by the owner prior to Application Program development.
G. Modified or new Function Blocks are to be functionally tested prior to Application Program development.
H. SIF function shall not depend on non-SIF execution. Provide identifiable separation between SIF and non-SIF functions.
I. Where final element is shared by SIF and non-SIF functions; place final element in SIF section.
J. SIF to be programmed for de-energized to trip.
K. Follow Names, Tags, Descriptions, Annotation, Alias, etc. similar to existing programs in the plant.
L. Include time delays, deadband as applicable to avoid spurious trip or nuisance alarms, yet meet safety function requirements.
M. Include sensor diagnostics features and maintenance bypass for proof test and repair.
N. Include final element failure alarm; comparison between Logic Solver commands Vs final element status. Bypass for final element (if required) shall require specific evaluation for functional safety.
O. Include Trip First-out, Reset permissive and individual Reset for each final element.
P. Include required operator interface and alarm. Only value added operator interface shall be included.
Q. Operator interface command to Logic Solver shall be through momentary signal, Logic Solver to confirm command status.
R. Provide Watch Dog Timer for Application Program execution.

Logic Solver Integration

A. Follow manufacturer manual and safety guidelines for Logic Solver integration. Utilize Proven-In-Use methodology.
B. Provide EMI protection for Logic Solver cabinet internals.
C. Provide redundant 120v AC / 24V DC Power Supply units with on-line repairable setup.
D. Include appropriate fuse degradation for Field Termination Panels.
E. Provide hardware failure priority alarms:
   • CPU failure, I/O Module failure
   • Logic Solver common trouble
   • 120v AC, 24v DC Power loss to Logic Solver
   • Application Program Scan Time Exceed
   • Peer To Peer Communication failure
   • Logic Solver / Operator Station communication failure
   • Cabinet Fan failure, Cabinet Hi Temp

Avoidance of Environmental Stress Failure
Avoid extreme environmental conditions that could lead to multiple SIF activation concurrently. Include following features for RIE where SIS cabinetry are in operation.
   A. Location, elevation, cable entrance, lightning protection, AC high voltage transformer location, etc. are designed to maintain SIS integrity.
   C. Provide separation between SIS and DCS cabinets.
   D. Provide redundant 120v AC Uninterruptable Power Supply (UPS) for Logic Solver and cabinetry items.
   E. Provide Unclassified Electrical Zone with temperature and humidity controlled atmosphere to meet Logic Solver requirement.
   F. Provide RIE fire detection / protection
   G. Provide alarms for:
      • 120v AC Power sources failure
      • RIE pressurization loss
      • High Smoke
      • Loss of HVAC
      • Fire protection system failure or On
      • High RIE temperature

Others
   A. Logic Solver maintenance and MOC requirements are not addressed herein.
   B. Logic Solver Re-validation during Turn-a-Round is not included herein.

Project Safety Requirement Specification (SRS) shall include above items in details to support SIS implementation.
### Abbreviations

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td>Central Processing Unit</td>
</tr>
<tr>
<td>DCS</td>
<td>Distributed Control System</td>
</tr>
<tr>
<td>EMI</td>
<td>Electro Magnetic Interference</td>
</tr>
<tr>
<td>ESD</td>
<td>Emergency Shutdown</td>
</tr>
<tr>
<td>FAT</td>
<td>Factory Acceptance Test</td>
</tr>
<tr>
<td>Hi</td>
<td>High</td>
</tr>
<tr>
<td>HIPP</td>
<td>High Integrity Pressure Protection</td>
</tr>
<tr>
<td>HVAC</td>
<td>Heating Ventilation Air Conditioning</td>
</tr>
<tr>
<td>I/O</td>
<td>Input / Output</td>
</tr>
<tr>
<td>KISS</td>
<td>Keep It Simple and Straight</td>
</tr>
<tr>
<td>LOPA</td>
<td>Layer of Protection Analysis</td>
</tr>
<tr>
<td>LS</td>
<td>Logic Solver</td>
</tr>
<tr>
<td>MTTFS</td>
<td>Mean Time To Failure Spurious</td>
</tr>
<tr>
<td>MTTR</td>
<td>Mean Time To Restore</td>
</tr>
<tr>
<td>MTR</td>
<td>Master Trip Relay</td>
</tr>
<tr>
<td>PHA</td>
<td>Process Hazard Analysis</td>
</tr>
<tr>
<td>SIF</td>
<td>Safety Instrumented Function</td>
</tr>
<tr>
<td>SIL</td>
<td>Safety Integrity Level</td>
</tr>
<tr>
<td>SIS</td>
<td>Safety Instrumented System</td>
</tr>
<tr>
<td>SRS</td>
<td>Safety Requirement Specification</td>
</tr>
<tr>
<td>Temp.</td>
<td>Temperature</td>
</tr>
<tr>
<td>TI</td>
<td>Test Interval</td>
</tr>
<tr>
<td>TMR</td>
<td>Triple Modular Redundancy</td>
</tr>
<tr>
<td>UPS</td>
<td>Uninterrupted Power Supply</td>
</tr>
<tr>
<td>2oo3</td>
<td>Two out of Three</td>
</tr>
</tbody>
</table>

---

**About the author**

Sam Roy is a Consulting Application Engineer at Schneider Electric, Safety Lifecycle Engineering Group, Webster, Texas. Responsibilities include delivering Analysis phase of SIS Safety Lifecycle tasks. He has over 35 years of Process Controls, ESD and Automation experience. He worked at Union Carbide, subsidiary of Dow Chemical Company for 29 years. Since 1993, he has been involved in the development of SIS projects and SIS best practices. He is a Professional Engineer of Texas with TÜV Functional Safety Expert Certification.