2015 Honeywell Users Group
Europe, Middle East and Africa

Safety Systems Alarms, Events and Sequence of Events (SOE)
Johan School, Honeywell
 Agenda

• Introduction, Definitions and Process Conditions
• Alarm Philosophy
• Safety application events & Examples
• Safety and Control networks supporting SOE and A&E
• Safety Manager Experion SCADA integration SOE and A&E
• Safety Manager Extended Experion integration SOE and A&E
• Time synchronization and sources
• SOE supported variables
• SOE and A&E best practices
• Conclusion
About your presenter

- Johan School
- 22 years with Honeywell
- Global Product Manager Safety Solutions
- Active member national and international Safety standard committees
- TÜV Functional Safety engineer
Introduction

• Event data collection is crucial in safety and critical control applications. Sequence of Events (SOE) solutions can capture both the first event and sequence of events that occur in your system during a shutdown or a trip sequence to help you document when events have occurred.

• Providing accurate detection, recording and storing of events and leveraging accurate time stamps, SOE solutions enable you to analyze when change of states occurred in your process and the precise order of occurrence.
Definitions

- SOE => Sequence of Events
- A&E => Alarm & Events
- Time Sync => Time synchronization
- Critical Limits => immediate action required
- Standard Limits => action required
- Target Limits => related to optimisation
- Safety Historian => Independent software for collecting events.
- SER => Sequence of Events Recorder
An abnormal situation can evolve from an operating upset that could potentially become a catastrophic event involving serious destruction and harm to the plant and/or the surrounding community.
Alarm Philosophy
Alarm philosophy

• Define and prioritize alarms

please note: Non-alarms that provide useful information for the operators (or documentation) are called notifications or user alerts.

They are not alarms, and during an abnormal operating condition or emergency, they can be silenced and ignored.
Alarm philosophy

• Set appropriate limits

– An alarm philosophy document should describe the difference between managed alarms and unmanaged alarms. The methodologies and maintenance of safety-related alarms (managed) should be described and the minimum requirements defined.

– For example, the methodology may call for layers of protection analysis (LOPA), clearly defining “safety layer” or “layers of protection,” their contribution to safety, how it's guaranteed through mean time between failure (MTBF) and mean time to repair (MTTR), and what testing is required to meet the standards.
Alarm philosophy

• Define clear procedures for managing alarms
  – Please note: Non-alarms that provide useful information for
    the operators are called notifications or user alerts. They are
    not alarms, and during an abnormal operating condition or
    emergency, they can be silenced and ignored.

• Rationalization procedure
  – Alarm management overview
  – Alarm management lifecycle
  – Alarm design principles
  – Alarm management rationalization methodology
Alarm philosophy

• Make alarms manageable

  – The objective of an alarm philosophy is to control daily alarms and to reduce the size and frequency of alarm floods.

  – When the system performs effectively, the operator workload is not burdened by the alarm system, and we can consider alarms to be within normal operations.
Alarm philosophy

• Provide tools for managing alarms, enforcing the philosophy and maintaining the system.

  - The important considerations when selecting an alarm management analysis tool are:
    - Can I get my historical data into it without too much difficulty?
    - Does it allow me to visualize and analyze my problems?
    - Is it easy to generate the daily, weekly, monthly, quarterly and annual reports I need based on my philosophy?
    - Is the software easy to maintain as my system evolves?

• Continue to have alarm review meetings with the operators for the life of the alarm
2015 Honeywell Users Group
Europe, Middle East and Africa

Safety application Events & examples
Safety application events

• Safety application events are very likely to create alarm floods so the number of alarms generated must be minimised.

• Typically, a single shutdown input will cause a number of outputs to trip. It is counter-productive for all of these to be alarmed to the operator. Also, the trips will usually create a major disturbance to the whole or a substantial part of the plant, generating a number of other alarms.

• Under such upset conditions, the operator needs to know:
  – What has tripped?
  – What caused it?
  – What are the consequences for the rest of the plant?
  – Will anything hazardous occur as a result?
Some examples of Alarms

• Critical Alarm:
  – BADPV (1oo1)
  – Final Element Discrepancy Alarm

• Standard Alarm
  – BADPV (1oo2 (from 2003))
  – Discrepancy Alarm (1003 in Alarm)
  – Motor Control Alarms

• Alert Alarm
  – Valve discrepancy alarms
So….

• What should be the notification level of a trip alarm?
  – Journal (just log the alarm)
  – Alert (Low Alarm)
  – Standard (High Alarm)
  – Critical (Urgent Alarm)

• Because the equipment or unit already has been put in a safe situation, a trip notification as such does not indicate an unsafe situation.

• That is why a trip alarm would by default have an ‘alert’ priority.

• Please note in case a trip can have a knock-on effect on other units, the notification is intended to prevent further escalation and subsequent uncontrolled shutdowns of other units.
More detailed Definition/recommendations

• Safety system application pre-alarms
  – Shall be considered as process alarms, typically used when DCS does not have a field measurement. In this case the Safety transmitter is used, notification only.

• Safety system application alarms
  – Trip status
  – First out detection
  – Non-voted transmitters
  – Voted transmitter
  – F&G related alarms
    • Detector failure
    • xx% LEL, yy% LEL (typically in a voting scheme)
More detailed Definition/recommendations

• Safety system application maintenance alarms
  – Bypass and override switches (as defined in the Safety application, good engineering practice !)
  – Forcing of field signals (as defined in the Safety system, not so good engineering practice for an operational safety application)

• Safety system diagnostic Alarms
  – Related to the health of the safety system
Alarm-flood following a trip

- Operators often find alarm systems difficult to manage following a trip. The stress of the situation makes matters even worse. A good performance indication for proper alarm management is the number of alarms in the first 10 min following a trip.

<table>
<thead>
<tr>
<th>Acceptability</th>
<th>More than 100</th>
<th>10 to 100</th>
<th>Less than 10</th>
</tr>
</thead>
<tbody>
<tr>
<td>Definitely excessive and very likely to lead to the operator abandoning use of the system</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hard to cope with</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Should be manageable</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- 80% of your alarms are low priority
- If it has no consequence or doesn't matter for more than 30 min’s why have an alarm?
More detailed Definition/recommendation

• **SOE => Sequence of Events**
  – Logging of alarms typically initiated by the safety solution.
  – Accurate
  – useful for analysis
  – Logging (e.g. MOS, FORCE activities)
  – Logging (e.g. PVST)
  – Logging demands
  – Diagnostic Alarms

• **A&E => Alarms & Events**
  – Logging of alarms and critical alarms initiated by the control solution and safety solution.
2015 Honeywell Users Group
Europe, Middle East and Africa

Safety & control networks supporting SOE and A&E
Typical safety network configuration

- C200
- C300 Controller
- Applications
- Experion Server
- Icon
- Safety Station
- FTE
- CF-9
- SM-C300 PCDI over FTE
- Safety Manager
- SafeNet P2P over segregated Network
- (S)NTP
- PTP
- (S)NTP
- PTP
- Modbus TCP
- Other device
- Safety Manager
- Remote I/O
- (S)NTP
- PTP
SOE collectors

• Experion Server
  – Collected and stored by the Experion server
  – Independent or merged view

• Safety Historian
  – Independent environment/SW package/machine

• Can also be used both
2015 Honeywell Users Group
Europe, Middle East and Africa

Safety Manager Experion SCADA integration SOE / A&E
• No special hardware or software needed, part of the Safety Manager architecture

• Key difference between SOE and A&E

  – SOE
    • time stamp locally done at Safety Manager
    • initiation/alarm level defined at Safety Manager (Safety Builder)
    • Collection/storage via Safety Historian and Experion

  – A&E
    • time stamp done at Experion Server
    • A&E initiation/alarm level defined at Experion Server (Quickbuilder)
    • Collection/storage via Experion
Safety Manager Experion SCADA integration SOE / A&E

- SOE (Sequence Of Event)
  - Configuration via Safety Builder
  - Time stamping done at Safety Manager Controller/IO
  - TAG including timestamp is communicated to SOE collecting device (Safety Historian or Experion)
Safety Manager Experion SCADA integration SOE / A&E

• (A&E) Alarms & Events)
  – Time stamping done at Experion Server
  – Configuration at Experion level (Quickbuilder)
  – Collection/storage via Experion (including all Experion features for alarm handling)
Configuration example with 2 SOE collectors

- Time synchronization is done via an external clock source
- SOE generation is enabled in the Controller properties
- Both Experion Server and Safety Historian are defined to be SOE collecting devices
SOE configuration DI

- Just tick the checkbox
- When the status changes, automatically
  - TAG will get a timestamp
  - Details made available in the SOE list

SOE configuration AI

- Just tick the checkbox
- Define the Alarm Limit
- When the Limit is exceeded, automatically
  - TAG will get a timestamp
  - Details made available in the SOE list
Configuration Safety Manager Experion SCADA integration SOE / A&E

A&E configuration (Configuration Studio/Quickbuilder)

- Point details
- Alarm TAB
  - Enable Alarm
  - Define and configure priority
  - Load in Experion Server

A&E configuration (Station)

- Need access/write credentials
- Point details
- Alarm TAB
  - Enable Alarm
  - Define and configure priority
• SOE information is stored at communication board level

• If 2 SOE collectors are required (e.g. Safety Historian and Experion) 2 communication modules will need to be configured

• The SOE information stored at the communication boards is 100% identical
2015 Honeywell Users Group
Europe, Middle East and Africa

Safety Manager Advanced Experion Integration SOE and A&E
Safety Manager Advanced Experion Integration

• **SOE**
  – time stamp locally done at Safety Manager
  – initiation/alarm level defined at Safety Manager (Safety Builder)

• **A&E**
  – time stamp done at Safety Manager
  – initiation/alarm level defined at Safety Manager (Safety Builder)

• **Collection/storage via Experion**
Advanced Experion integration SOE / A&E

- SOE and (A&E) Alarms & Events
  - Time stamping done at Safety Manager
  - Configuration at Safety Manager level (Safety Builder)
Advanced Experion integration configuration example

- Time synchronization is done via an external clock source
- SOE generation is enabled in the Controller properties
- Experion Server is defined to be the SOE collecting device
Advanced Experion integration SOE / A&E

**SOE configuration DI**

- Just tick the checkbox
- When the status changes, automatically
  - TAG will get a timestamp
  - Details made available in the SOE list

**Alarm & Event configuration DI**

- In the main tab:
  - Define and enter the State 0 and State 1 text
- In the Experion tab:
  - Select the “Normal State”
**Advanced Experion integration SOE / A&E**

**SOE configuration AI**
- Just tick the checkbox
- Define the Alarm Limit
- When the Limit is exceeded, automatically
  - TAG will get a timestamp
  - Details made available in the SOE list

**A&E configuration AI**
- Define the limit and Alarm Priority for the:
  - Low Low
  - Low
  - High
  - High High
Additional engineering and message location

• Is additional engineering or configuration required in Experion?
  – NO, due to the Extended Experion integration, a publication of the Safety Builder database will automatically make all these variables and settings available within the Experion environment.

• Where do these messages end up?
  – SOE will appear in the dedicated SOE messages overview of Experion
  – A&E will appear in the Alarms and Event Overview
  – Including all functions and features as supported by Experion (Assets, Alarm Shelving, Filtering, Suppression and many more)
2015 Honeywell Users Group
Europe, Middle East and Africa

Time synchronization and sources
The Safety controllers might be synchronized by the following sources:

- Experion (SCADA, Extended Experion Integration)
- DCS (Modbus RTU, Modbus TCP/IP)
- PTP (IEEE1588)
- (S)NTP
- Safety Station
- Safety Historian
Time synchronization

Honeywell

SafeNet

Safety station

PTP/(S)NTP Server

11:31:37:324

FTE

Experion Server

11:31:37:324

SAFENET

Safety station

11:31:37:324

11:31:37:324

11:31:37:324

11:31:37:324
Time synchronization

Safety station

Experion Server

FTE

SAFENET

PTP/(S)NTP Server

11:31:37:324

11:31:37:324

11:31:37:324

11:31:37:324
Time synchronization and sources

The Safety controllers can set time sync priority
- Configurable per Safety controller
- 3 levels

By default Clock Source Priority 1 will be used.

If Clock Source Priority 1 fails after the configurable time-out, Clock Source Priority 2 will be used, etc.

Only Safety Managers and devices that are logically connected to the selected SM Controller and that have the option Clock Source Allowed checked are available in these pop-up menus.
2015 Honeywell Users Group
Europe, Middle East and Africa

SOE supported variables
Time resolution SOE

• **Basic SOE**
  – Time stamp set by QPP
    - Chassis IO (Safety Manager & FSC)
    - Universal Safety IO
    - Solution cycle time

• **Low Latency SOE**
  – Time stamp set by IO module
    - Universal Safety IO and Universal Safety Logic Solver
    - 1msec

• Both can be used within the same IO module/solution
SOE capable variables

• The following variables are SOE configurable:

  – Digital inputs
    - SOE message generated on status change (0=>1…1=>0)
  – Analog inputs
    - SOE message on configured Alarm Limit e.g. (<10%....>90%)
  – Digital Outputs
    - SOE message generated on status change (0=>1…1=>0)
  – Analog Outputs
    - SOE message on configured Alarm Limit e.g. (<10%....>90%)
  – Digital Markers
    - SOE message generated on status change (0=>1…1=>0)
  – Digital inputs/outputs location COM (e.g. from DCS)
    - SOE message generated on status change (0=>1…1=>0)
  – Diagnostic Alarms (these are automatically generated)
2015 Honeywell Users Group
Europe, Middle East and Africa

SOE / A&E best practices
Typical mistakes while configuring SOE/A&E

Alarm Flooding

1. During the engineering phase, details on Alarm and SOE requirements are very often not known yet and the engineer configures everything to SOE “enabled”

At the first serious unwanted situation, the SOE collector is flooded with events making it challenging to define the initial cause of the problem

1. Want to make sure every process situation is captured, SOE enables all. See below, 3 tags on a FLD SOE enabled, will generate 3 identical events.

Again, the SOE collector will be flooded with events probably not relevant making it challenging to define the initial cause of the problem

2. Setting incorrect initiating limits, thus providing incorrect data

3. Incorrect alarm setting of Fast transient signals causing chatter
Typical mistakes while configuring SOE/A&E

• Incorrect “collector” choice (SOE or A&E*)
  – Time resolution might be incorrect (may depend on configured scan rate Experion server).
    ◦ Challenging analysis as times may be shifted between the journals

• Incorrect Alarm priorities/definitions
  – Operator response may be incorrect

• Incorrect filtering on SOE/ A&E collector
  – Incorrect asset selected
  – Incorrect log-on credential definitions
    ◦ Alarms / Events may not be seen/ no reaction

• Not evaluating logging of Safety Historian
  – As it separate, it might be forgotten,
  – only the Safety team has access to it,
  – Unfamiliar with the Safety Historian software package

* SCADA integration only
Conclusion
Benefits of correct implementation of SOE and A&E

- Accurate determination of "root cause" after a mission critical event
- Drives faster time to solution
- Improves accuracy of data
- No special modules required
- High rate of continuous event recording
- Configurable filters
- Historical data analysis
- Various time synchronization options
- Provides logging for proof-testing (and remember a demand is also a successful test !)