Alarm Audit and Enforcement: Automating the Integrity of Alarms for Manufacturing Systems

IOP Conf. Series: Materials Science and Engineering **521** (2019) 012008 doi:10.1088/1757-899X/521/1/012008

Alarm Audit and Enforcement: Automating the Integrity of Alarms for Manufacturing Systems

T. Ault

Automation Engineer & Alarm Advisor, Chevron & Colorado State University, 709 Lenox Ct. Paso Robles, CA, 93446, USA

L. Yang
Dept. of Electrical & Computer Engineering Colorado State University, 1373 Campus Delivery Fort Collins, CO 80523-1373

Abstract. This work details the development of a continuous monitoring system technology to track the compliance of alarms in a manufacturing environment. A problem arose due to having simultaneous capital projects and continual process optimization work at several production sites. With continual changes to the control systems, a project was developed to ensure that alarm adjustments never violated established safety thresholds for systems. A technique was used to rationalize alarms using a risk based objective analysis to establish safety thresholds for each alarm. Then a tool was developed that continually cross-referenced alarm safety server with process control network to immediately notify management and engineering of any adjustments that violated alarm and safety rules for the site. This work led both to improved site safety and to an improvement of alarm metrics due to greater confidence in adjusting alarms with this audit tool. One site saw a monthly reduction of the quantity alarms by 55% and the elimination of alarm floods.

1. Introduction

Several production sites in southern California were undergoing major capital upgrades, large amounts of maintenance work, and optimization projects concurrently. At any given time, there would be several programming contractors either installing a new vessel with associated controls, updating process control network (PCN) databases, or tuning control valves in an industrial setting. In the past, alarms were hardwired and required significant planning to remove or place new alarms. With the widespread use of distributed controls systems (DCS), the amount of alarms has increased at sites along with the ease to alter them [1]. Due to simultaneous operations with construction, operations, and maintenance, it was a required that an additional safety system was needed to alert engineering and management if any new alarms were added, deleted, or modified that would endanger the sites. It was determined to continually cross reference an alarm master database with process controllers to determine instantaneously if any unsafe conditions exist with regards to alarms. Alarm auditing the process control network (PCN) against an alarm master database has been utilized in industry and the lack of such a system has been attributed as a contributing factor to some process incidents [2]. Few examples were found for the use of a continual monitoring system for the alarms. The continual monitoring poised some technical and organization challenges in this project.

The general established method for alarm rationalization is based on American National Standards Institute (ANSI) and International society of automation (ISA) [3]. There are several modifications to this technique for alarm rationalization ranging from the very simple to the complex [4]. Alarm

rationalization is a systematic approach to evaluate every alarm tag in a facility to determine whether it is an alarm and if so document consequences, impact, corrective actions, response time, and priority. Inconsistent and undisciplined use of alarms can create a frustrating situation for operations and lead to ignored alarms. The goal of alarm rationalization is to review, validate, and justify alarms that meet the criteria of an alarm. The goals include the most efficient number of alarms to ensure the process system is safe, operators have sufficient time to respond, and operates in a safe process range. [5] One of most important parts of alarm management is considered alarm rationalization and the approach used will be a major element if the effort is successful or fails to manage alarms at a large site. [6] A risk-based approach was utilized to evaluate each proposed alarm and risks associated with it to determine key parameters of each alarm. The parameters to determine during the analysis included maximum time to respond (MTR), alarm priority, alarm type, cause, operator actions, and setpoint.
After the alarm rationalization was completed, a master alarm database was created with the results. From there an automated alarm audit and enforcement tool was created to cross reference the actual process control network alarm settings with the alarm rationalization in the master alarm database. While the continuous audit of online systems may seem easier due to process control and network surveillance being more common and continually improving, challenges always exists getting databases and software to communicate with each other. Varsahelyi et al discuss some of the historical evolution of continually monitoring large amounts of online data. [7] This paper reviews the unique approach used for alarm rationalization and the development of the automated alarm audit and enforcement tool. Results document the improvements in alarm metrics and related work that occurred because of the project.

2. Methodology

Management determined that the current state of alarm management should be improved to prevent the unauthorized changes of alarms which could violate the safety thresholds of the sites. This was a concern due to simultaneous programming projects occurring at facilities undergoing capital improvements by several programming contractors. The first step was to rationalize the alarm to determine the correct parameters. While data existed for some sites for the alarm tag, setting, priority, and other important data, it was requested to refresh the data at each site. It was agreed that for all new systems, modified systems, and systems with known problems a formal process will be undertaken to document and correct alarm rationalization issues. A systemic approach was developed to rationalize the alarms based on an objective analysis carried out by facilitator and key personnel. This approach was termed an alarm objective analysis (AOA). The following participants were considered key participants for the objective analysis: Facilitator, head operator, shift operator, process engineer, programmer, automation engineer. Engineering documentation is also required for the meeting which included (but not limited to) piping & instrumentation diagrams (P&IDs), process hazard analysis studies (PHA), cause and effect matrix, and list of alarm tags. With the key personnel and engineering data collected, the goals of the alarm analysis are:

- Identify, rationalize, and document alarms and alarm setpoints that are required for safe operations
- Select minimum number and proper type of alarms
- Define unique responses to alarms
- Assign alarm priorities based on the severity of the potential abnormal condition and the maximum time to respond (MTR)
- Develop database the defines the required alarms

To aid this, a spreadsheet was developed for each alarm where the initiating event could be recorded with the alarm to respond to the event. From there the maximum time to respond could be analysed to determine the priority of the alarm. The spreadsheet recorded alarm tags, causes to trigger alarm, maximum time to respond (MTR), setpoint, engineering units, and severity of cause. With this data captured, the team can utilize the simplified table shown (Table 1) to determine the proper alarm priority.

Table 1: Simplified table for alarm consequences

	Consequence			
MTR (minutes)	None	Minor	Major	Severe
>30	No Alarm	No Alarm	No Alarm	No Alarm
5-30	No Alarm	Low	Low	High
1-5	No Alarm	Low	High	High
<1	No Alarm	High	Urgent	Urgent

It should be pointed out that "no alarm" for this example means that the operator is still notified but it does not get elevated to an audible and high alert visual notification. Typically, an incident that has a high maximum time to respond and low consequence was re-engineered. This is due to if the incident is a slowly developing process, safety controls could be introduced to control the risk. Another example of alarm prioritization matrix is shown in table 2. These tables and risk tolerances all vary between industries, it is important only to have an agreed set of alarm priorities that are aligned with the risk to the site.

Table 2: More detailed table of alarm consequences

Alarm Priority Determination						
	Severity of Consequences					
Time Available	**Incidental**	**Minor**	**Moderate**	**Major**	**Severe**	**Catastrophic**
> 60 Min	NO ALARM	NO ALARM	NO ALARM	Re-Engineer	Re-Engineer	Re-Engineer
30 – 60 Min	NO ALARM	LOW	LOW	LOW	HIGH	HIGH
10 - 30 Min	NO ALARM	LOW	LOW	HIGH	HIGH	CRITICAL
< 10 Min	NO ALARM	LOW	HIGH	HIGH	CRITICAL	CRITICAL

Based on the results of the alarm objective analysis, the following set of process control network priorities were also developed to further assist operations organize and manage alarms (table 3). These are the priorities that will be used on the human machine interfaces (HMIs) to alert operators and list the current active alarms. The lowest number (more critical alarms) will be listed above other alarms that are current occurring. Table 3 below lists the relationship between alarm priorities from the alarm objective analysis and what was used in programming to further organize the alarms.

Table 3: Developed alarm priorities based on alarm consequences

Alarm Priority System	
Alarm Priority	Controller Alarm Priority
CATASTROPIC	1
CRITICAL	2 to 99
HIGH	100 to 199
LOW	200 to 499
JOURNAL ENTRY	500 to 799
DIAGNOSTIC	800 to 998
NO ALARM	999

The distribution of alarm priorities should be reviewed periodically to ensure that the risk profile of a site is not skewed to highly to urgent alarms or low priority alarms. To provide a suitable risk profile for the plant there should be a reasonable amount of urgent alarms to manage. In other words, too many high urgency alarms will lead to distraction and not capture the true risks to the site. Like other safety analyses, the distribution of alarms from catastrophic, to critical, to high, and then to low should resemble a pyramid. An example of this is given below in table 4 which was developed from one of

the upgraded sites. The middle column shows the current percent of each alarm priority along with what the project team thought the recommended alarm priority quantity should be for the sites.

Table 4: An example of the profile of alarm priorities for a sample site

Alarm Priority	Current	Recommended
Most Urgent	4%	2-10%
Medium	16%	10-25%
Least Urgent	80%	65-80%
Total	3201	

The below figure (figure 1) summarizes the steps of the alarm objective analysis (AOA). Due to either a new project being commissioned, lapse in time since last analysis, or other reason, an AOA would be conducted, and a spreadsheet developed (Step 1). The engineering data would be fed into the data and validated (Step 2). The meeting would occur and based on alarms and their event consequences priorities would be established (Step 3). The results would be reviewed and approved (Step 4). Finally, the documentation would be collected and uploaded into a master alarm database (Step 5). After this was completed each site had an approved alarm master database that included the critical data needed for the alarm audit and enforcement tool.

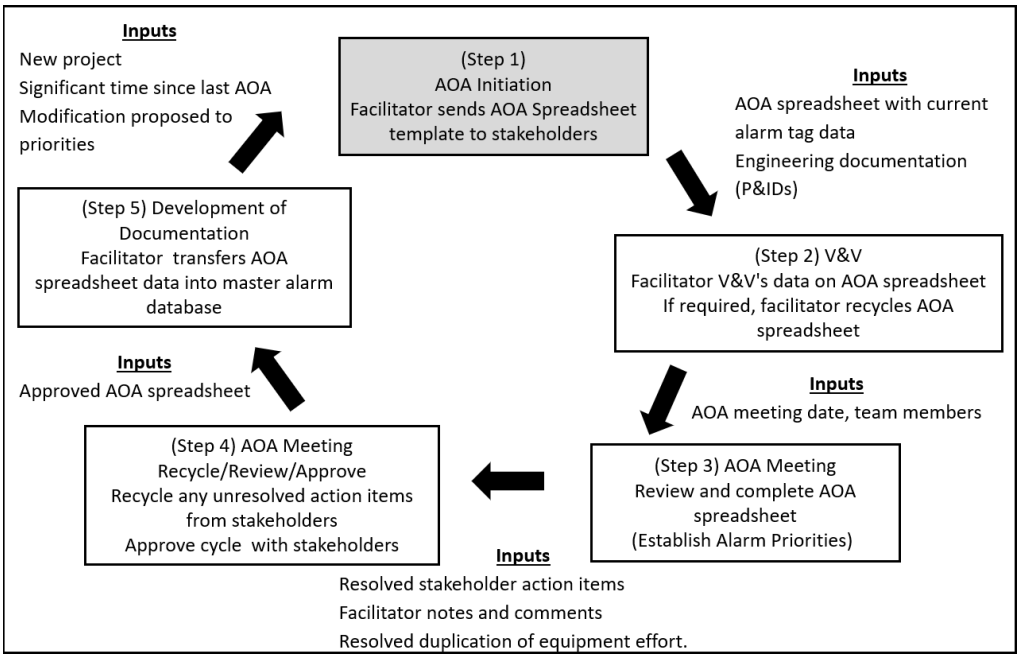

Figure 1: Flow chart of the alarm objective analysis (AOA)

The next stage of the project was to design the architecture to communicate between the process control network and the alarm master database (also termed the alarm safety server). The goal of the development was to provide an automated reconciliation audit and enforcement process to verify that alarm settings implemented in site's process control network (programmable logic controllers, human machine interfaces) matched the designed settings stored in the master alarm database. The process will run on a continual basis to identify changes made to alarm set points and priorities. It was also designed to determine if alarms were deleted or added at the process control network without update the master alarm database. If automated enforcement is enabled, discrepancies shall be rectified by changing the settings implemented in the process control network to match the master database settings. If automated enforcement is not enabled, discrepancies shall be rectified by changing the implemented settings to match the master database settings manually. System change audit logs will

be created by the reconciliation process to document the discrepancies found. The development to enable the communication between the HMIs, historian, and alarm safety server began with creation of alarm audit tag objects are created by the custom master alarm audit object during initial configuration, and become a static resource once deployed. Plant expansions may require that more objects be created; in that case the master alarm audit object must be reconfigured for the larger number of alarms. A custom master alarm audit object was created using Visual C# and tool kits provided by software used in process control network. These objects scan the system for alarm objects, and create, configure and deploy alarm audit Tag objects. The alarm audit Tag objects have attributes that will be bound to the set points, priority and mode of the alarm objects in the network. One alarm audit tag object will be created for every 20 alarms. Below figure 2 shows an overview of the architecture for the system:

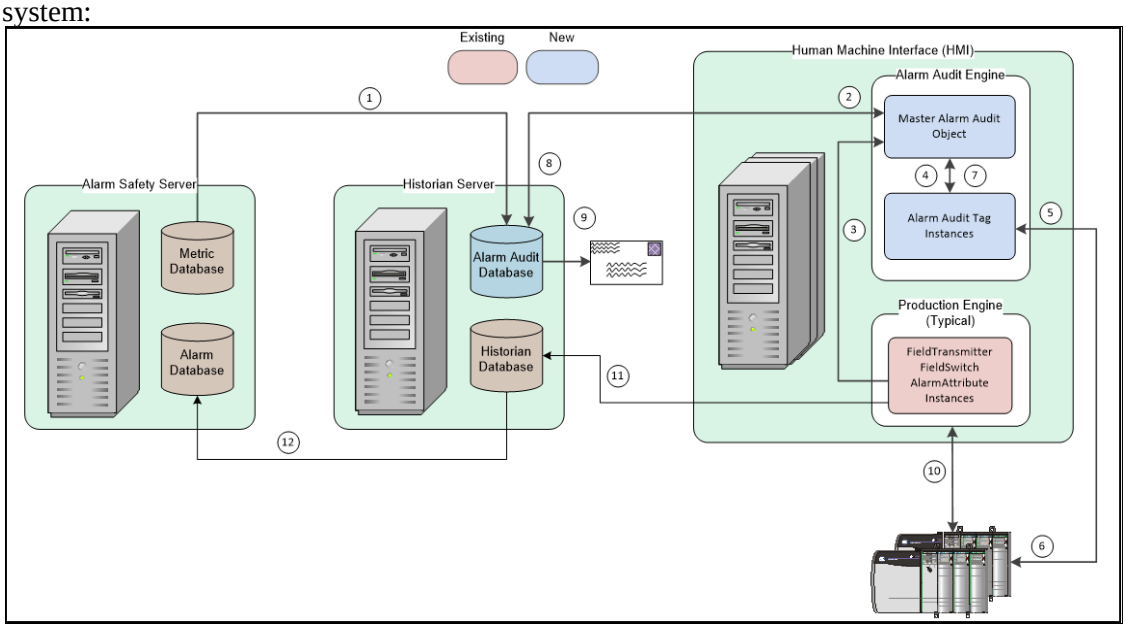

Figure 2: Overview of audit tool architecture

The overall process of the alarm audit and enforcement tool and its interacting with the existing system is listed below that further explains the details and workflow of figure 2:

1. Alarm objective analysis (AOA) info in the Alarm Audit Database is pulled from the metric database by a scheduled job running in Alarm Audit Database
2. AOA info is transferred to Master Alarm Audit Object in HMI
3. Alarm scanner iterates through production field transmitter, field switch, and alarm attributes objects on a regular basis and generates alarm audit tag instances to monitor alarm configuration.
4. Individual alarm configuration data is applied to alarm audit tag instances for comparison and correction.
5. Alarm audit tag instances monitor alarm configuration in HMIs/PLCs on a regular basis.
6. Alarm configuration discrepancies are corrected in PLC(s) when found
7. Alarm audit tag instances report alarm configuration enforcement actions to the Master Alarm Audit Object
8. Alarm configuration audit and enforcement information is transferred back to the Alarm Audit Database
9. A triggered job in the alarm audit database produces email-able reports.
10. Normal PLC-to-HMI SCADA dataflow
11. Normal alarm historization
12. Normal alarm history transfer to alarm database

The project began with little formal documentation for the alarm master database. By following an agreed upon process, the master alarm database was created. With master alarm database created and containing safety information about each alarm, an automated audit tool was created to cross reference field information with the safety information in the master database. After the system was created and following typical commissioning and start-up checks, the automated audit and enforcement tool went into service.

3. Results

Immediately after formal commissioning and correction of technical issues, the system began generating reports to engineering and management. Reports included any discrepancies between the master alarm database and the field. This included new alarms, deleted alarms, changes to setpoint, and changes to priority. With this management oversite, the concurrent engineering work that was making multiple changes to programming by different contractors was more supervised since there was an automated way to check for discrepancies. After the creation of reports began, alarm meetings also occurred to regularly review the alarm information. The meetings focused on any data found by alarm audit tool, suppression of alarms, and “bad actor” alarms (top alarms in terms of frequency). With this data, operations teams could agree on any needed changes to alarm system and initiate management of change which would lead to an update of the master alarm database. At this time, the system has been deployed to four large industrial sites with five more planned. One of the early adopters has utilized the data to reduce alarms by reclassifying them to a lower priority based on safety analysis. This site has reduced alarms from roughly 55% by utilizing the audit tool with the safety information in the alarm master database. All sites which have had the audit tool deployed have not suffered from any lost production or safety incidents due to multiple programming projects occurring at site.

4. Conclusions

Prior to project, a series of industrial production sites did not have an automated mechanism of reconciling and verifying if implemented alarm settings matched designed settings. Verification and validation is an important safety concept and it includes alarming. By implementing this audit tool, it allowed sites to continue to mature validation and verification of appropriate barriers and safeguards. Alarm configuration changes occur in alarm generating systems sometimes without corresponding changes in the master alarm database. Prior to work, there was no means of validating alarm master database with field alarm configuration systems on a periodic basis. This audit tool bridged this gap. This work led to development of an audit tool that checks for alarm setpoint, alarm priority and alarm HMI tag mismatch but also led to auxiliary improvement in safety. It also checked unauthorized changes to alarm settings. It allowed operations to continually verify if alarms were acting as a protection layer against hazardous events. Giving the operator a reliable alarm configuration information helps the operator maintain plant within safe operating limits and recognize a potentially hazardous condition early and take proper action. Some sites may not have a similar need due to less work activity or less frequent changes to alarms. Need for a similar alarm audit took can vary depending on industry, capital investment, and management controls already in place. There was a large design discussion on the need of continuous vs. batch reports as well. In other words, it was debated if the reports could be generated monthly by a batch scan of data versus instantaneously. This system utilized instantaneous audits, but the decision of how often the reports are generated will also vary based on each application. The result is a system that allows sites to continually verify and validate all facility alarm configurations are safe by use of an automated tool. Future work is looking at ways to further study high frequency alarms against the master alarm database to better rank alarms which need attention. This work is planning to leverage artificial intelligence technology to improve decision making and adding business value for alarm reporting.

5. References

[1] Koene, Johannes, and Hiranmayee Vedam. "Alarm management and rationalization." Third *International conference on loss prevention*. 2000.

[2] Shafer, Don, and Phillip A. Laplante. "The BP Oil Spill: Could software be a culprit?." *IT professional* **12.5** (2010): 6-9.
[3] ANSI-ISA, I. S. A. "18.2 Management of Alarm Systems for the Process Industries." (2009).
[4] Noda, Masaru, et al. "Event correlation analysis for alarm system rationalization." Asia‐Pacific *Journal of Chemical Engineering* **6.3** (2011): 497-502.
[5] Hollifield, Bill R., and Eddie Habibi. Alarm Management: *A Comprehensive Guide: Practical and Proven Methods to Optimize the Performance of Alarm Management Systems.* Isa, 2010.
[6] Beebe, Dustin, Steve Ferrer, and Darwin Logerot. "The connection of peak alarm rates to plant incidents and what you can do to minimize." *Process Safety Progress* **32.1** (2013): 72-77.
[7] Vasarhelyi, Miklos A., and Fern B. Halper. "The continuous audit of online systems." *Auditing: A* Journal *of Practice and Theory.* 1991