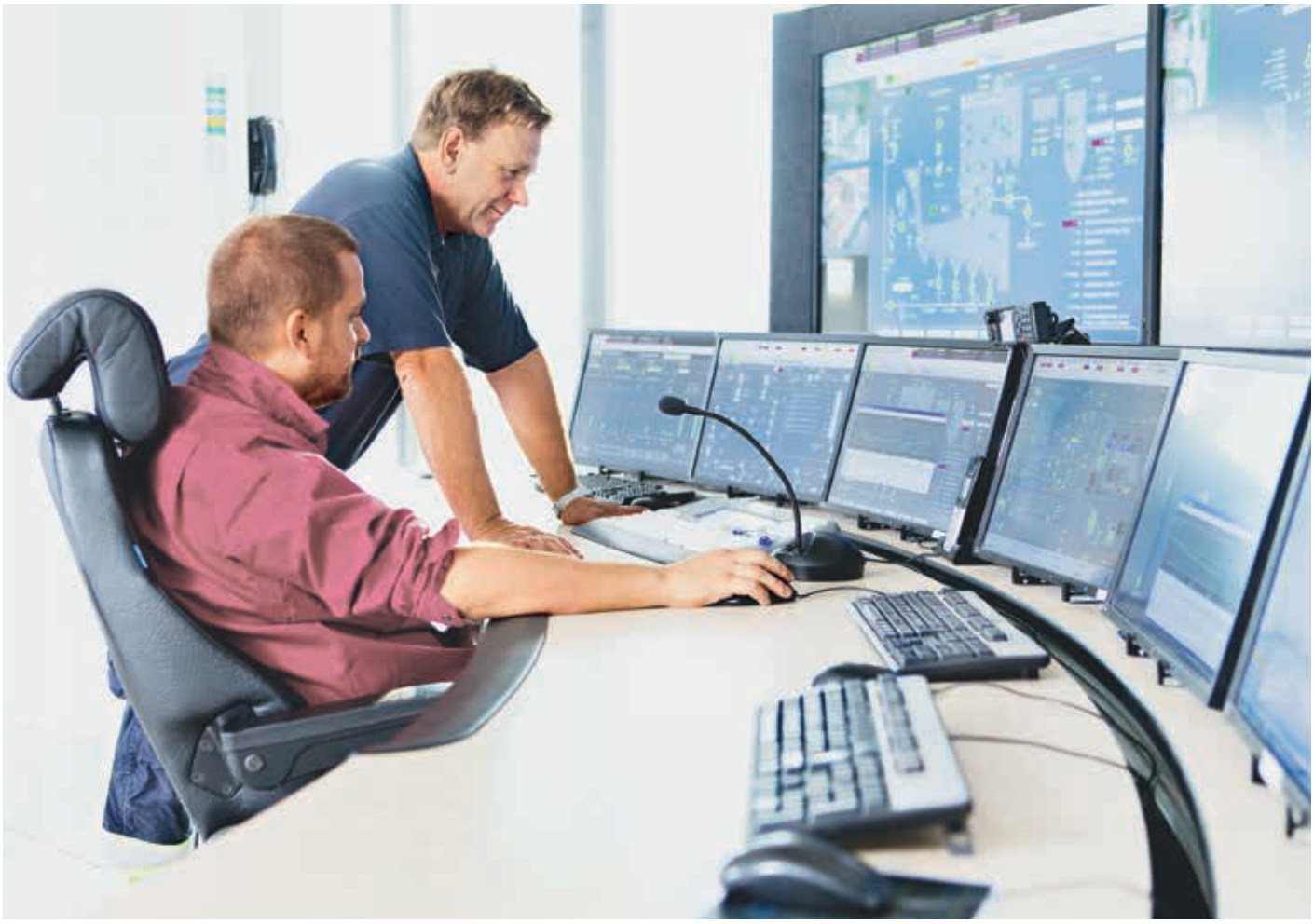


Alarming discoveries

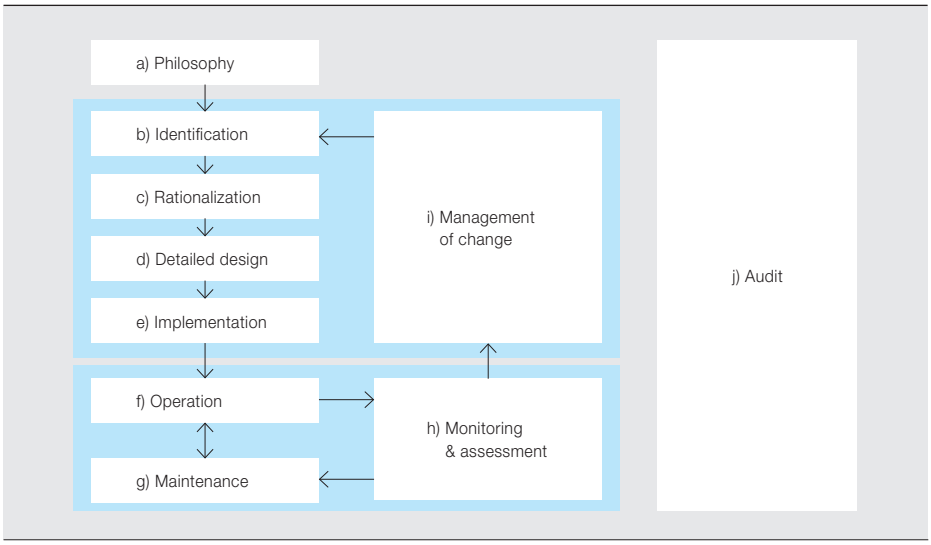
Improving operator effectiveness through alarm life-cycle support

MARTIN HOLLENDER, JOAN EVANS, THOMAS-CHRISTIAN SKOVHOLT, ROY TANNER – Ahead of a recent simulation exercise at Star City in Moscow, British astronaut Tim Peak was asked what the greatest challenges are during the simulation. He replied, “The most difficult thing to deal with is multiple failures” [1]. Likewise for industrial facilities using distributed control systems, alarm “floods” remain one of the biggest challenges. To get alarm floods under control, alarm-related design knowledge from early life-cycle phases needs to be easily accessible in the operational phase when additional information becomes available, so that decisions about advanced alarming methods like alarm suppression can be made with confidence. Having good management-of-change and life-cycle support in place makes it possible to keep the alarm system consistent with the changing reality in the plant and allows continuous improvement. To help, alarm management standards such as IEC 62682 and ISA 18.2 emphasize the importance of life-cycle support in alarm management.

1 Life-cycle thinking in functional safety and alarm management

	Functional safety		Alarm management
1996	ANSI/ISA 84.01	2009	ANSI/ISA 18.02
2003	IEC 61511	2014	IEC 62682

2 Life-cycle of IEC 62682



Although the need for effective alarm management is now generally recognized, accidents like the one in 2010 in the DuPont plant in Belle, West Virginia [2] show that even well-known safety leaders like DuPont still have deficiencies. Since software-configurable distributed control systems (DCSs) came into the mainstream, multiple alarms could be added at little or no cost to the end user. Unfortunately this has led to control systems that include a low alarm-system quality due to too many alarms being configured. A classic example is the explosion in the Texaco Milford Haven refinery in 1994 [3], where the two operators received 275 alarms in the last 11 minutes before the explosion. This is now seen as a characteristic of an overloaded alarm system, which makes it impossible for an operator to be properly aware of a situation and to diagnose and correct it. These types of alarm systems are neither useful nor acceptable and resulted in the development of systematic alarm management approaches first documented in the EEMUA 191 guideline published in 1999.

Title picture
Advanced alarm methods provide critical support for operators running modern plants.

Ten years later the ISA 18.2 standard added a life-cycle approach to alarm management similar to the life-cycle approach already well established in the safety community with ISA 84 and IEC 61511. Simply put: Ensuring safe operation and useful alarms needs ongoing efforts.

The new IEC standard 62682 (published in 2014) [4] – the first international standard for alarm management – is based on ISA 18.2 → 1. It emphasizes the importance of systematic life-cycle management. IEC 62682 requires, for example, that all information used to design alarms (safety studies, equipment specifications, etc.) should be systematically captured and documented. Later, during plant operations, additional information can supplement or revise the original design decisions. Such a revision requires that all information upon which the original decision was based is available and fully understood, to deter any potentially hazardous side effects from the changes.

→ 2 captures the essence of IEC 62682 and can be used to develop and maintain an alarm system compliant with the requirements of IEC 62682 and good industry practice.

A classic example of an overloaded alarm system is the explosion in the Texaco Milford Haven refinery, where the two operators received 275 alarms in the last 11 minutes before the explosion.

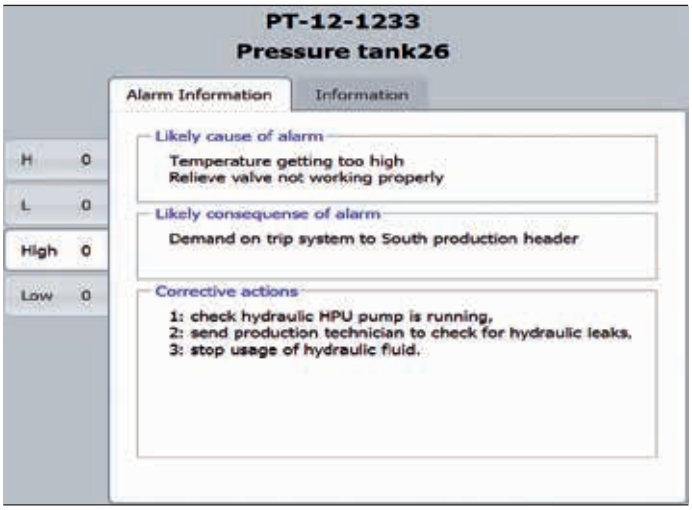
Alarm philosophy

The first step in the project life-cycle is the alarm philosophy. The alarm philosophy is the plan for how alarms are to be managed for the site. It defines:

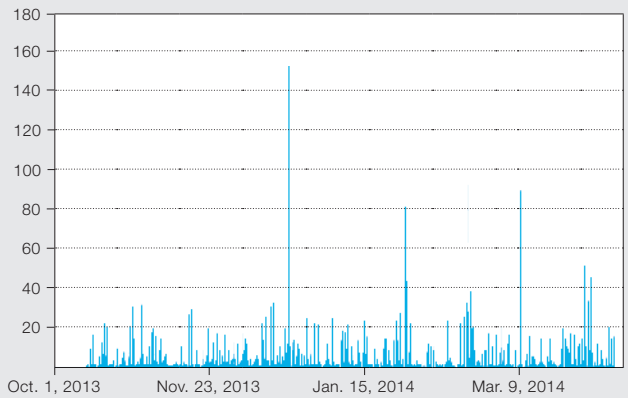
- Roles and responsibilities
- Alarm requirements
- Work processes and procedures to deliver agreed requirements

IEC 62682, among others, provides useful guidance on the content and structure of an appropriate alarm philosophy.

3 Alarm Helper



4 Alarm rate (per 10 minutes) during six months



Alarm management principles have to be translated into concrete project activities.

In ABB's experience, the challenge is not in the authoring of the document, but in its application to the project life-cycle. ABB consultancy support for this activity therefore focuses on the translation of alarm management principles into concrete project activities and deliverables while communicating the impact of alarm requirements to the extended project team.

This is crucial in ensuring that the purpose and design intent of alarms are identified and documented during project reviews such as hazard and operability studies (HAZOP), layer of protection analysis (LOPA) and piping and instrumentation diagram (P&ID) reviews.

As this alarm design information becomes available, the project continues by deciding how and where alarm-related data will be stored and managed. For this purpose IEC 62682 has confirmed the concept of having a master alarm database, which is defined as "an authorized list of rationalized alarms and associated attributes." ABB's implementation of this is called Alarm Rationalization Tool (ART) and offers many important advantages:

– Full database functionality for capturing and fast navigation of all alarm-related configuration and design data.
– Input forms that show all configuration settings related to an alarm on a single screen and are designed to support efficient alarm rationalization meetings.
– Controlled copy facilities that allow the reuse of existing configurations for similar cases.

Rationalization

IEC 62682 [5] reminds us that in the rationalization phase of the alarm life-cycle, the following need to be indentified for every alarm:

– Recommended operator action
– Consequence of inaction or incorrect action
– Probable cause of alarm

Having this information available during operation leads to more consistent operator actions and helps inexperienced operators build up their knowledge base and confidence. Where existing facilities are being revamped, operations staff are the most reliable source of this information. For new plants the full definition of required alarms is more challenging, relying heavily on design and vendor

As alarm design information becomes available, the project continues by deciding how and where alarm-related data will be stored and managed.

5 AlarmInsight tool for alarm rationalization

data to define the required alarm configuration.

As well as capturing alarm requirements and design data, a key feature of ABB's ART is the ability to export operator response data to ABB's online Alarm Helper facility ➔ 3. The Alarm Helper provides all of this information in Extended Automation System 800xA's operator workplace. Both Alarm Helper and ART are parts of ABB's comprehensive alarm management package called AlarmInsight. AlarmInsight is a full featured alarm management toolset developed and tested to work with System 800xA today and in the future.

Ready access to this online help facility is seen as particularly important for critical (in IEC terms highly managed [6]) alarms and is increasingly expected by safety regulators. Plants already using Alarm Helper also report that it is a very popular and effective operator support tool.

Continuous efforts

Moving into the operations phase, lifecycle management is a central part of IEC 62682 and ISA 18.2 and has also been integrated in to the third edition of EEMUA 191. Alarm management requires continuous efforts to maintain good practice and ensure consistency.

Today, many plants have their average alarm rate well under control with low average alarm rates during normal operation. However, alarm floods are frequently still a challenge.

➔ 4 shows the alarm rate of a petrochemical plant over half a year. Although the average alarm rate is below one alarm every 10 minutes and is therefore well under control, sometimes floods of more than 100 alarms every 10 minutes exist and smaller floods of about 20 alarms every 10 minutes occur quite regularly.

> Alarm floods cannot be avoided just by choosing good configuration values for limits, hysteresis or delay timers.

Unfortunately these floods often occur during the most demanding phases when operators most need support (eg, during startup or shutdown). Alarm flood scenarios include:

- Alarms floods generated because process sections are shut down (eg, low flow alarms after pump stops), operating in different operating modes (eg, cleaning), or instruments being calibrated. These alarms can become a problem if they occur together with a process problem and important alarms are buried inside a flood of unnecessary alarms.
- Alarm floods along the causal chain following a process upset. A single root cause can generate lots of consequential alarms. The first alarm in the alarm list might not be the alarm closest to the root cause – depending on the process dynamics and how thresholds are configured, secondary and misleading alarms might show up first.

Such alarm floods cannot be avoided just by choosing good configuration values for limits, hysteresis or delay timers. Advanced alarming techniques like hiding (called suppression-by-design in IEC 62682) and grouping come into play. ABB's System 800xA provides a powerful toolbox for advanced alarming on controller, server and workstation levels, and include alarm grouping, hiding (dynamic suppression) and alarm shelving (time-limited operator-driven suppression).

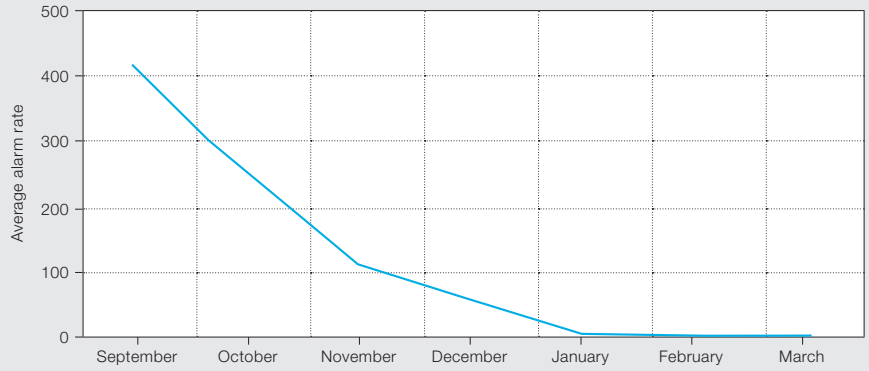
Balanced risk

When addressing alarm floods, the challenge is to strike a balance between the potential risks associated with suppressing an alarm during a particular scenario, versus the need to address peaks in the alarm rate during abnormal conditions. These risks are best mitigated via a combination of a proven, comprehensive toolsets such as ABB's AlarmInsight ➔ 5 and a robust management of change (MOC) process to include the appropriate level of review and approval.

Initial (prospective) rationalization reviews may have identified candidates for basic alarm suppression such as alarm grouping for alarms to be masked when equipment is out of service. Later alarm flood studies during the operations phase will seek to go further and draw on

ABB was able to reduce the average alarm rate in a Rashpecto offshore gas production plant, reducing plant trips from 25 to six per year.

6 Reducing the alarm rate at the Rashpetco offshore gas plant using ABB's AlarmInsight



the full portfolio of AlarmInsight functionality:
- Operator comments on alarm responses stored and presented in Alarm Helper
- Detailed alarm analysis data via Expert Tool and Alarm Analysis
- Current alarm attributes from the ART database

This combined toolset facilitates the identification of potential alarm suppression scenarios based on analysis of actual plant data. With the need for manual "ad hoc" analysis removed, the potential for human error in deducing cause and effect is greatly reduced and conclusions can be based on much larger data sets – extending over several years if appropriate. Once a particular scenario has been identified, reviewed and confirmed, the toolset can then be used to explore whether there are other instances in which the same logic can be applied. The product integration between ABB's System 800xA and AlarmInsight enables continuous alarm optimization, enforcement and monitoring over time.

This approach has been of proven value in a number of cases, including:
- Identification of consequential alarms following a particular shutdown
- Critical event analysis, highlighting event triggers with potential for early operator response (intervention) and mitigation of equipment shutdown/ plant upset

The main benefits are achieved through a life-cycle toolset providing a framework for continuous improvement, and include:
- Reduced production trips
- Reduced legislative risk – safer, more environmentally robust operations
- Improved operator effectiveness

→ 6 shows how ABB was able to reduce the average alarm rate in a Rashid Petroleum Company (Rashpetco) offshore gas production plant. This resulted in a reduction of plant trips from 25 down to six per year. As each trip is associated with significant costs, the overall savings are substantial.

Insight achieved

Alarm management is an area of increasing concern to regulators, other public bodies and the public at large who are pushing for evidence of a life-cycle approach and continuous improvement, resulting in safer plant operations. With IEC 62682 the best practice in alarm management is finally available as an international standard. ABB delivers alarm management improvements with a comprehensive toolset, delivering documented bottom-line savings, which are accepted by regulatory authorities as good practice.

Martin Hollender
ABB Corporate Research
Ladenburg, Germany
martin.hollender@de.abb.com

Joan Evans
ABB Process Automation, Oil, Gas & Chemicals
Billingham, United Kingdom
joan.evans@gb.abb.com

Thomas-Christian Skovholt
ABB Process Automation, Oil, Gas & Chemicals
Oslo, Norway
thomas-christian.skovholt@no.abb.com

Roy Tanner
ABB Process Automation, Control Technologies
Wickliffe, OH, United States
roy.tanner@us.abb.com

References

[1] D. Shukman. (2015, November 11). *Tim Peake: British astronaut's training nears end.* Available: http://www.bbc.com/news/science-environment-34788169
[2] S. Smith, "Did DuPont Prioritize Cost Over Safety at Belle, W.Va., Facilities? Chemical Safety Board Investigation Indicates It Did," *EHS Today*, July 2011.
[3] "The explosion and fires at the Texaco Refinery, Milford Haven, 24 July 1994," Health and Safety Executive, Norwich, 1997.
[4] *Management of Alarm Systems for the Process Industries*, IEC 62682, 2014.
[5] *Required and Recommended Alarm Philosophy Content*, IEC 62682, section 6.2.1, Table 3, p. 36.
[6] *Highly Managed Alarms*, IEC 62682, section 6.2.9, p. 38.