ACHIEVING A SUCCESSFUL ALARM MANAGEMENT DEPLOYMENT THE CLS EXPERIENCE*

E. Matias#, Mighty Oaks, Victoria, BC Canada
Tonia Batten, Jianwei (Mark) Li, Ward A Wurtz, Canadian Light Source, Saskatoon, SK Canada
Laurier Baribeau, McGill University, Montreal, Canada
Dylan Maxwell, Facility for Rare Isotope Beams, Michigan State University, East Lansing, MI U.S.A.

Abstract

Alarm management systems promise to improve situational awareness, aid operational staff in responding to accelerator problems and reduce downtime. Many facilities, including the Canadian Light Source (CLS), have been challenged in achieving this goal. At CLS past attempts focused on software features and capabilities. Our third attempt switched gears and instead focused on human factors engineering techniques and the associated response processes to the alarm. Aspects of ISA 18.2, EEMUA 191 and NREG-700 standards were used. CLS adopted the CSS BEAST alarm handler software. Work was also undertaken to identify bad actors and analyzing alarm system performance and to avoid alarm flooding. The BEAST deployment was augmented with a locally developed voice annunciation system for a small number of critical high impact alarms and auto diallers for shutdown periods when the control room is not staffed. This paper summaries our approach and lessons learned.

BACKGROUND

CLS operates both a third generation synchrotron light source and a smaller linac for experimental isotope production from a common control room. The synchrotron and associated beamlines are controlled using EPICS.

REGULATORY CONTEXT

The CLS is regulated by the Canadian Nuclear Safety Commission (CNSC). Of specific considering with respect to alarm handling is compliance with Canadian Human Factors Engineering Standards [1,2]. The CNSC has mandated compliance with NREG-700 human factors standards [3]. These impose specific requirements on the overall alarm management strategy.

In addition to the mandatory regulatory requirements CLS has also chosen to optionally make use of some of the guidance provided by ISA 18.2 [5]and EEMUA 191 [6] where it does not conflict with regulatory requirements and provides value to operational staff as well as building on operational experience in other facilities.

REQUIREMENTS

Industry Standards

More broadly industry standards have been developed in the process industry for alarm management and increasing are being viewed as reflective of best industry practice. Though there are differences between industrial process facilities and science facilities many common concepts can be applied. We have established the following requirements based on these standards:

a) Identification of alarms should be according to ISA 18.2 (3 criterions) to the extent practical. Not all notification are alarms and not all alarms are equal.

b) In the context of EPICS both Minor and Major alarms require operator immediate response. However, Major alarms are more urgent and shall be responded first if operator gets both Minor and Major alarms.

c) Specific guidance shall be provided on the expected response from the operator as well as guidance to the operator on an automated response programmed into the control system.

Initial Philosophy Applied at CLS

The experiences at the Spallation Neutron Source (SNS) [7] formed a starting point for the adoption of a new approach at CLS. Building on the SNS experience, existing operational cultures at CLS and the realities of operating an accelerator facility the following requirements were applied:

d) Only alarms that require a human response should annunciate in the control room.

e) Minor alarms (shown in yellow) indicate abnormal operation requiring action to avoid a future trip while Major alarms (shown in red) indicate a system trip or failure.

f) Specific guidance should be provided on the expected response.

g) Audio alarms (voice annunciation or horns) should only be used for alarms requiring urgent response.

h) Care should be taken to avoid alarm flooding.

i) Alarms requiring response even during shutdown periods should trigger auto-diallers.

*Research described in this paper was performed at the Canadian Light Source, which is funded by the Canadian Foundation for Innovation, the Sciences and Research Council of Canada, the National Research Council Canada, the Canadian Institute of Health Research, the Government of Saskatchewan, Western Economic Diversification Canada and the University of Saskatchewan.

#elder.matias@mightyoaks.com

ISBN 978-3-95450-139-7

Distributed Alarm Management

Responsibilities for responding to alarms are distributed across multiple groups within CLS. A common approach is required while still balancing the specific requirements of the accelerator operations, mechanical services, controls, experimental facilities and safety groups. This necessitates multiple alarm handles accessible in different areas of the building.

Shutdown Periods with the Control Room Unattended

During machine shutdowns the control room is not staffed, the alarm management strategy must make use of auto-diallers, e-mails and text messaging for critical alarms during these time periods.

Support for Unattended Experiment Operation

The capability should exist to generate alarms accessible by cell phones (e.g. text messaging) and the ability to generate alarms that are accessible to experimental staff and users over cell phones/e-mail.

SYSTEM ARCHITECTURE

The architecture that has been adopted is one that makes use of a combination of pre-existing software packages (e.g. CSS) and locally developed software.

Control System Studio

Within the Control System Studio (CSS) framework [8] CLS adopted the BEAST software package [9] for alarm management.

Conventional wisdom (ISA 18.2) is to only have a single alarm hander. However, to address operational realities within CLS multiple alarm handlers each dedicated to supporting a specific operational group have been deployed. We currently envision having the following CSS alarm handlers:

a) *Accelerator Alarm Handler* – primarily used by accelerator operations staff and provisioning alarms that have a direct and immediate impact on accelerator operations staff.

b) *Mechanical Services* – primarily monitored by technical services staff responsible for water cooling and ventilation systems.

c) *Health, Safety and Environment* – primarily monitoring conventional and radiological safety alarms.

d) *Control System Alarm Handler* – Predominately monitoring the health of control system services and IOCs in the field.

e) *Floor Coordinator Alarm Handler* – Predominately monitoring the health of the beamline systems.

Each of these is in various stages of deployment. Not all of the authors are in agreement the current strategy is for process variables that are of concern to more than one operational group, they appear in multiple alarm handlers with guidance on response appropriate for that group. For example, a radiation alarm may result in a control room operator taking immediate steps to remove the hazard while for a safety group it may launch an investigation and reporting activity.

Audio Alarm in the Control Room

Each of these is in various stages of development and deployment. For process variables that are of concern to more than one operational group, they appear in multiple alarm handlers.

Auto Diallers

Auto diallers have been in use at CLS since 2001. These predominately call cell-phones of on-call staff. This alarm method is predominately used for non-accelerator alarms that have a significant impact on the safe and secure operation of facility. Alarms include the fire protection systems, cryogenics system failures, critical cooling/heating systems, loss of building power, and failure of sump-pumps in lower levels of the facility.

Once CLS switched from construction to routine operation we switched to having these auto-diallers call the control room first and then only call the on-call cell phones if not acknowledged by the control room.

Control System Web

As we added additional beamlines we started to see increased demands for the ability to have alarms dispatched through SMS messages This Web based system, built on the twisted application framework, was adopted to support this function. This system makes use of a third-party SMS messaging system called Twilio for message dispatch. Figure 1 shows the structure of the Control System Web application.

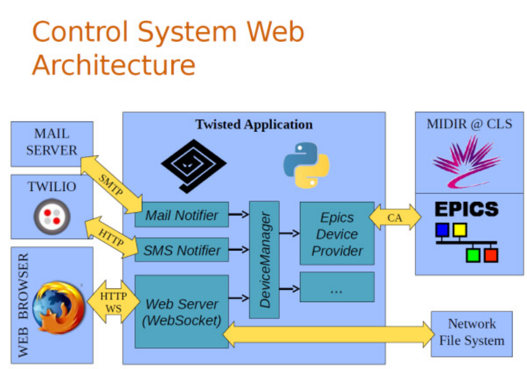

Figure 1: CS Web Architecture using Twilio.

OPERATIONAL CONSIDERATIONS

Alarm Rationalisation Is Critical

If a new alarm system is to be configured, it is highly recommended to go through the alarm rationalization process. This process requires inputs from different functional groups such as operation, engineering, controls, and safety. In this process, alarms will be identified and their priorities and guidance to operators will be determined and documented. We have taken such effort when we deploy the CSS alarm handler for some systems. It proves that this is the best way of reducing redundant alarms and maybe more importantly helping different groups understanding the alarms. This process works the best for a new alarm handler, but it also works great for the existing ones.

Empowering Operational Staff

As the alarm handler is more entrenched into routine operation day-to-day modifications of guidance and associated supporting information has been taken over by the relevant operational group that must respond to the given alarm. This provides for tighter integration into response procedures and timely changes. Operations staff have been trained in the use of configuration management software (PTC Integrity [10]) used for the rest of the control system.

VALIDATION

Staged Deployment

To ensure that the alarm handler was accepted by operational staff and found to be effective in minimizingdown time a staged approached was adopted where an initial deployment with a limited number of process variables (PVs) was installed into the control room. Through repetitive review with operational staff we were able to validate the correct mix of PV being used, the level and effectiveness of guidance and layout of the alarms.

Structured Review against NREG-700

Once the system was successfully deployed a systematic review was performed against the NREG-0700 standard to ensure compliance.

Safety System Horns

NREG-700 mandates that a signal level 10 dB(A) above average ambient background noise is generally considered adequate and such alarms should reliability capture the user's attention while not being unpleasant.

In xxx we encountered an incident where a radiation monitor in a very noisy RF area did not immediately vacate when local radiation monitoring went off. After completing a TapRooT™ investigation [11] and Human Factors Review it was determined that both the local horns and indicates were inadequate to gain the attention of staff. All radiation monitors in the facility were augmented with additional localised alarm annunciation.

In 2013 a review was made of the use of horns in the control room and we found that horns were set well above 10 dB(A) and negatively impacted operations and the ability of the staff to respond to the alarm. Changes are now underway to correct this problem.

Simulated Walkthroughs

Very early on during building the CLS and before having an operational accelerator simulated desktop walk through were performed for critical upsets. The use of this technique has been more limited once in operations. However we remain open to using this technique to validate alarms and guidance.

ALARM HANDLER OPTIMISATION

In terms of the operation of the alarm handler software it is possible to improve overall performance by a careful review of the alarm log and adjustment to alarm thresholds within the EPICS PV definition.

Alarm System Performance

Alarm system performance can be improved dramatically within a reasonable time period.

The CLS experiences show that for an existing alarm system, the performance can be improved dramatically within a reasonable time period. Figure 2 identifies the top chattering alarms, based on this work was undertaken to assess the field conditions around this process variables and adjust either field equipment or alarm thresholds.

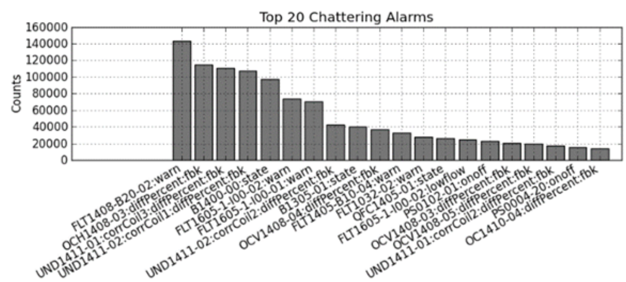

Figure 2: Top 20 chattering alarms in CSS Control Room Alarm Handler.

Also critical is the review of the number of alarms generated from transient events. It can be helpful to establish target levels and monitor the system so that when events do occur that exceed these thresholds a review can be undertaken on the alarm structure to determine an optimal level. Human Factors standards provide some rules of thumb on these levels. Figure 3 and 4 illustrate the trends observed at CLS.

ISBN 978-3-95450-139-7

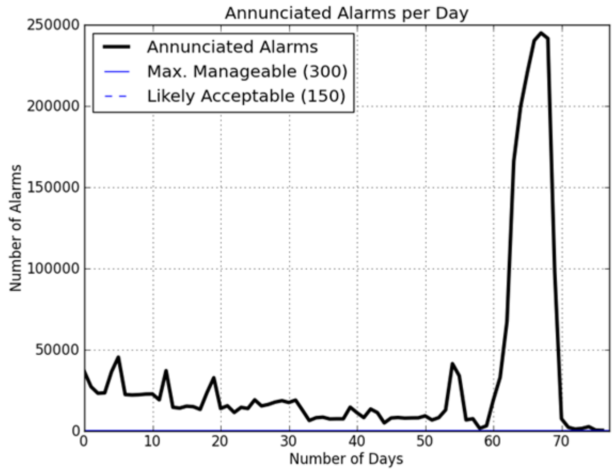

Figure 3: Performance of CSS Control Room Alarm System.

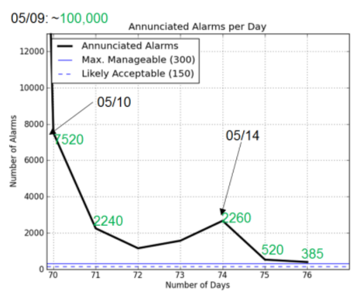

Figure 4: Scaled Fig. 3.

The performance of the CSS Control Room Alarm Handler over 76 days was analyzed. There are 241 chattering alarms and Fig. 2 shows the top 20 chattering alarms. Most of these chattering alarms may have been screened from the operator through strict filter settings, but they do flood the alarm journal and make the alarm history virtually useless as well as placing extra load on the relational database. Fig. 3 shows the number of alarms per day for 76 days (ending May 16, 2012). Fig. 4 is the scaled of Fig. 3 for the last 7 days. It is noticed that in the last 7 days the number of alarms dramatically drop to 385 per day from 100,000 per day. According to ISA 18.2, the recommended maximum threshold for allowable alarm per day is 300 and the CLS deployment of the CSS Control Room Alarm Handler was capable of approaching that level for a short time period. Such improvement was made by identifying these chattering alarms and then fixing them by various mechanisms. The details of troubleshooting chattering alarms are not documented in this paper. It is noted that the effort of troubleshooting and repairing of these chattering alarms had been undertaken over a few months.

CONCLUSION

The alarm management process at CLS is a work in progress, we have made major inroads over the past two years in developing a strategy that is both embraces human factors engineering principles and broader industry thinking on alarm management.

We have found that CSS is an effective tool, however it does not fully meet our needs and we have had to make use of other tools to augment CSS for notification outside of the main control room.

The success of the alarm management process is driven almost as much by careful analysis and configuration of the alarms as it is by the underlying software.

REFERENCES

[1] F. Harrison, "Human Factors in the Design of Accelerator Facilities", ARW2009, Vancouver, Canada.(2009). http://www.triumf.info/hosted/ARW/program.htm.

[2] CNSC, "Human Factors Engineering Program Plans", Canadian Nuclear Safety Commission. (2003). G-276.

[3] J. M. O'Hara, et al., "Human-System Interface Design Review Guidelines," US Nuclear Regulatory Commission,. NUREG-0700, Rev. 2. (2002).

[4] J. M. O'Hara, et al. "Human Factors Engineering Program Review Model", US Nuclear Regulatory Commission, NREG-0711 Rev. 3

[5] ISA, "Management of Alarm Systems for the Process Industries", ANSI/ISA 18.2 (2009).

[6] EEMUA, "Alarm Systems – A Guide to Deisng, Management and Procurement Second Edition", EEMUA, London. (2007) ISBN 0 85931 1455 4.

[7] X. Geng, K. Kaesmir, S. Hartman, "Alarm Rationalisation: Practical Experience Rationalising Alarm Configuration for an Accelerator Subsystem", ICALEPCS2009. Kobe, Japan, WEP109 p.606-608. (2009).

[8] M. Clausen, J. Hatki, J. Penning, "The CSS Story", PCaPAC2012, Kolkata, India. WEKA01 p.1-3. (2012).

[9] K. Kasemir, X. Chen, E. Danilova, "The Best Ever Alarm System Toolkit", ICALEPS2009 Kobe, Japan. TUA001, p. 46-48. (2009).

[10] PTC, *"PTC Integrity Software"*. www.ptc.com

[11] M. Paradies, and L. Unger. "*TapRooT – Changing the Way the World Solves Problems*". System Improvement Inc., Knoxville TN. (2008).

ISBN 978-3-95450-139-7