DYNAMIC POSITIONING CONFERENCE
October 12-13, 2010

OPERATIONS SESSION

Effective Alarm Management for Dynamic and Vessel Control Systems

By Steve Savoy

Ensco Offshore Company

11 Oct 2010

1. Introduction

Marine control systems are always fitted with an alarming function. Most of the existing systems have tabular alarm displays that often do not provide operators with a meaningful interface. The existing alarm management guidelines mainly address applications for process control and aviation. These same techniques can be applied to marine control systems even as these systems normally do not have the large number of alarms that are associated with these processes. This paper will outline these same techniques showing how they can be used to improve operator interfaces for marine systems.

2. Alarm Management

An alarm is defined as "a mechanism for informing an operator of an abnormal process condition for which an operator action is required. The operator is alerted in order to prevent or mitigate process upsets and disturbances"[1] Alarms must be used for events that require operator action. The operator action is not just acknowledgement but also a response to the event. Alarms provide an indication of a system fault, required action, degraded system operation or compromised operating capabilities.

Alarm management is the "processes and practices for determining, documenting, designing, monitoring, and maintaining alarm messages"[1]. Good alarm management leads to more efficient operation, better operator situation awareness and mitigation of system faults. The process starts with a defined alarm philosophy.

3. Alarm History

Almost all major industrial accidents have had an alarm component as a contributing cause. Poor alarm management has been identified as one of the major causal factors.

The beginning of basic alarm management started during WWII. During this time period airplanes were rapidly evolving so that the pilots were faced with more instrumentation and less time to react in an abnormal situation. The military started to develop instrumentation and displays that provided better pilot situational awareness by the use of better displays.

In 1979 the Three Mile Island nuclear power plant accident had poor alarm displays as a contributing factor. The President's Commission said "The Control Panel is huge, with hundreds of alarms, and there are some key indicators placed in locations where the operator cannot see them"[2]. After this accident the nuclear power industry began to improve on operator displays and console layouts. This was a result of studying the human factors of plant operation. Factors such as maximum number of alarms that an operator can process, prioritizing and grouping of critical related alarms allow operators to better handle abnormal situations.

As a result of this and other catastrophic accidents, the process industry has developed guidelines and standards over the past 30+ years. The first alarm displays were lighted mimic panels where each lighted square indicated an alarm condition. In the 1960 the Instrument Society of America

(International Society of Automation) (ISA) released ISA_RP18 *Specifications and Guides for the Use of General Purpose Annunciators*. This was followed by ISA-18.1-1979 *Annunciator Sequences and Specifications*. The latest evolution of this document is ANSI/ISA-18.2-2009 *Management of Alarm Systems for the Process Industries*. Another revision of this document is planned to be released in October of 2010.

The Abnormal Situation Management Consortium was formed in 1994. The consortium's purpose was to study a number of plant incidents where alarms had been identified as a causal factor. The goal was to develop a better response to alarms. The Engineering Equipment and Materials Users Association issued Publication 191, *Alarm Systems: A Guide to Design, Management and Procurement*. This was one of the first comprehensive documents on alarm management.

4. Marine Regulatory

The marine regulatory documents give some guidance to alarm system implementation. The ABS *Guidance Notes on Ergonomic Design of Navigation Bridges 2003* has a section on alarms. It recommends that alarms be prioritized, grouped properly, nuisance ones avoided and ambiguities eliminated. The majority of the alarm references in the ship or MODU classification sections specify required equipment alarm but they provide little guidance on alarm management.

5. Alarm Management

There are formalized steps for implementing alarm management for any system. The process starts with a definition document. There are a number of common steps to implement an alarm management system.

4.1 Develop Alarm Philosophy

This process develops a guidance and specification document that defines overall design and implementation of an alarm management system. It should address alarm selection and justification. It serves as a design specification document. It defines operator interfaces and response, classes of alarms that are to be prioritized, and rationalization of all alarms with the alarm philosophy. Many of these alarms would be defined in the system design specifications.

4.2 Rationalization and Documentation

This step defines all alarms in detail. Each alarm should be examined for consistency and priority. System conditions that generate the alarm should be defined. This step would generate an alarm list or database with all information related to each alarm. There should also be FMEA information incorporated into the list.

4.3 Operating System Data Collection

This step collects historical data on the operating system. The data is analyzed for alarm frequency and volume. Any problem alarms e.g. nuisance or floods, should be identified. Possibly identify alarm dependencies that were not part of the rationalization and design process.

4.4 Audit and Monitor Performance

Periodically or in real time, monitor the alarm system performance. Historical Data-loggers are utilized to ensure that any abnormal alarm response is identified. These conditions can occur over the life of a control system due to maintenance, hardware degradation, software upgrades, etc.

4.5 Control and Maintain the System

Implement a management of change policy for changes in alarms. This would include changes due to system modifications, disabling due to equipment failure, or changes in the control process.

6. Alarm Analysis

The analysis phase collects data from an operational system over a period of time. Normally this should be a period of two to six months. The alarms are used to populate a database so that queries and reports can be generated. The data is normally analyzed for frequency of occurrence, floods, or alarms that remain for long periods of time.

6.1. Frequency

This analysis determines how many alarms occur within a day, hours or ten minute period. For process systems with thousands of alarms the ten minute period is a fairly standard benchmark[1]. Most marine systems have a relatively low frequency of alarms.

7. Poor Alarm System Characteristics

7.1. Stale Alarms

These are alarms that remain in alarm state for long periods of time. These are normally due to equipment failure.

7.2. Alarm Floods

These are time periods where there are multiple alarms in rapid succession. Dynamic positioning systems can have alarm floods during periods of position loss. A sensor jump can cause rapid thruster movement resulting in multiple compare errors both in power and azimuth. Additional sensor or position error alarms can occur simultaneously. This results in an alarm flood.

7.3. Nuisance Alarms

These are alarms that occur due to improper set-points, lack of alarm blocking during equipment start-up and shutdown. These alarms can occur with a change in operational mode. The operator acknowledges them then they re-occur in a short period of time.

7.4. Poor Definition

These are alarms that have confusing or unclear definitions. This leads to operator misunderstanding as to the meaning of the alarm.

An example of this would be the following alarm;

"Thruster 1 Rate Too Slow"

Does this indicate a serious problem? How slow is "too slow"? A better message may be;

"Thruster 1 Azimuth Rate Less that Nominal Value"

7.5. Alarm Floods

An operator can only effectively process a maximum rate of occurrence.   Industry guidelines give general rates[1]. A long term average of more than one alarm per minute is unacceptable whereas one in less than 10 minutes is considered acceptable.

7.6. Poor Operator Interface

These are some examples of poor alarm operator interfaces; A HMI presentation that has an alarm display area too small. There are too many or redundant alarms for the same event. Icons are not presented properly. There are improper icon colors or too many colors that do not allow the operator to effectively identify alarms. An alarm history that does not allow sorts based on time, type and priority.

8. Good Alarm System Characteristics

Obviously the goal of good alarm management would be to minimize the characteristics of a poor system.

8.1. Alarm Description

The system documentation should have complete and accurate descriptions of all alarms. This should include the cause of the alarm and relationship to the FMECA. The recommended operator action should be included as well as the exact source.

8.2. Frequency

Through the rationalization and description process, parameters should be chosen that minimize alarm frequency. Operational limits should be defined that minimize alarms.

8.3. Prioritization

There should be a prioritization or hierarchy that lends itself to grouping. This will give the operator a good display so critical alarms can be identified separately from less serious ones.

8.4. Minimize Nuisance

A good rationalization process should be able to minimize these types of alarms. Good equipment maintenance or set points will keep measured parameters correct so that these alarms are not generated.

8.5. Minimize Floods

This is more difficult to control since system upsets can cause other valid alarms. An example would be thruster alarms generated in response to a faulty thruster. A properly functioning thruster can generate alarms due to the fact that it cannot azimuth or meet power requirements causing compare alarms.

9. Dynamic Positioning and VMS Alarm Systems

Presently most systems have one alarm list presented in time sequence. Normally alarm displays are a small portion of the the overall operator HMI displays. Most systems have an alarm history page(s) that can display all events for over a day or more. Data Loggers can display events for longer time periods but these are not fully utilized for alarm management.

Alarms can be due to an actual event e.g. a motor temperature or the failure of a portion of the control system in which multiple alarms are generated.

9.1. General DP alarm groups

Dynamic positioning systems lend themselves to natural groupings according to function. The groups can be classed as follows;

Power -All alarms relate to power generation and power management functions.

Thrusters

Hardware failure - Alarms related to the hardware control system failures e.g. azimuth or power drive systems.

Operational limits - Alarms that alert the operator of azimuth or a power compare parameter that may be out of bounds.

Sensors - Alarms generated by sensor systems including hardware failures, control parameter limits or median test.

Consequence - Alarms generated by the system consequence analysis function. These types warn of improper power configuration, insufficient power in the event of a failure, etc.

Control - Alarms related to the control system function. These would include position parameter limit alarms.

Hardware - These are alarms related to a hardware failure of a device e.g. loss of power or invalid data from a sensor.

Network Data Communications - Alarms generated by communication errors or controller failures.

9.2. Analysis of DP System Alarms

A typical system alarm list can be analyzed for the number of percentages of alarms in each of the general groups. This may give guidance as to possible grouping for HMI displays. By segregating the system alarms into two or more groups for display will give the operator better differentiation of alarm displays.   A typical system has the following percentages of alarm groups;

|	
Consequence	*2%*
Control	*12%*
Hardware	*20%*
Power	*6%*
Sensors	*42%*
Thrusters	*20%*

If the above alarms are ranked by severity of 1 to 3, with 1 being most critical then the following numbers are generated;

|	
Priority 1	12%
Priority 2	70%
Priority 3	18%

In this case only 12% of the alarms are ranked as critical e.g. position excursion, exceeding watch circles or insufficient power available. Normally these would occur after multiple priority 2 alarms occur.

9.3 Alarm Frequency Data

 The following graph shows the number of alarms in different groups over a period of one month on an operational rig.
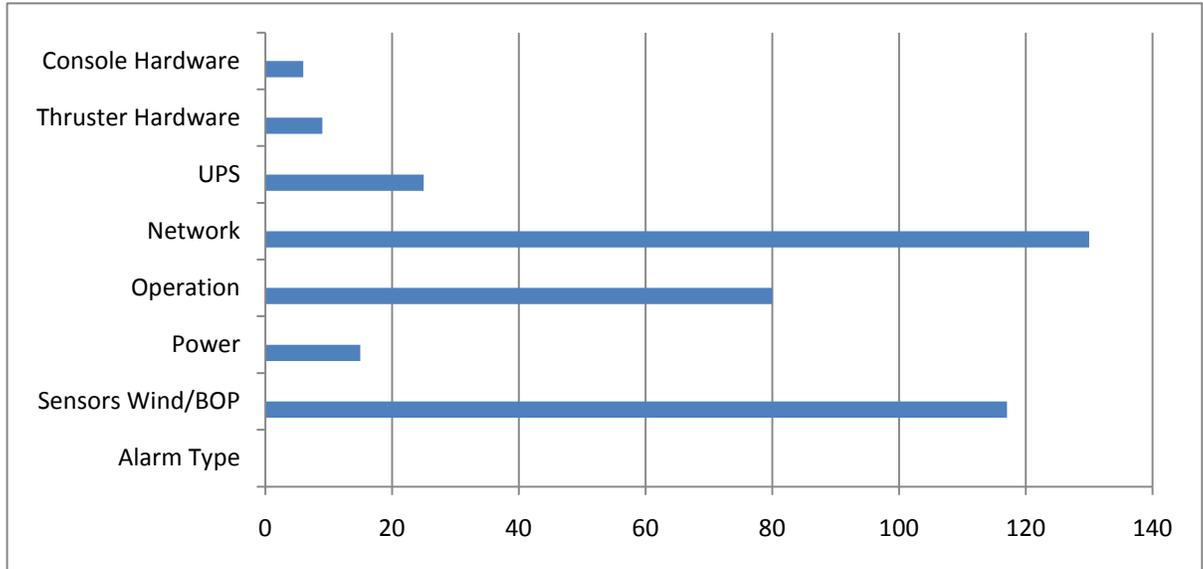
The following graph shows the number of alarms per day over one month. The large spike during the 20-June-10 date is due to a rig move where the acoustics system was being setup as well as additional equipment testing.
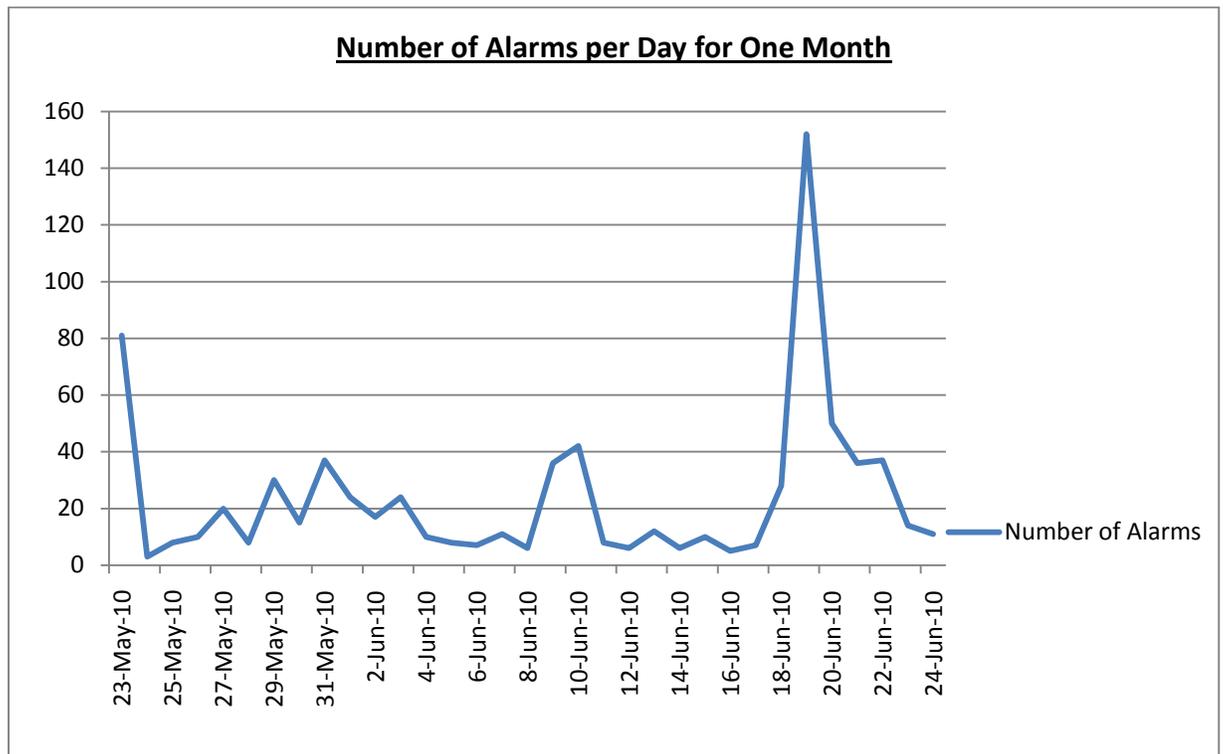
9.4 Thruster Faults

There are a number of common problem events that occur with DP systems relating to thrusters. These are normally one of the simulator scenarios that are given to DP operators during training. The two common types of problems are; 1) unresponsive operation to thrust or 2) azimuth commands. In these instances the DP system will command a thrust level or azimuth but the thruster will not respond. The other online thrusters will try to compensate for this incorrect vector force in the Thruster Allocation Logic. This most often results in multiple compare errors for both thrust and azimuth on the normally operating units. This is particularly true for a thruster that ramps up to 100% power and remains at that level. The remaining thrusters will ramp-up in power and change azimuth to compensate for this force. This usually leads to a flood of thruster power and azimuth alarms. The rapid demand in thruster power will can cause power generation and limit alarms as well. This can easily lead to DPO confusion if the offending thruster cannot be readily identified.

The following alarm sequence was the result of a thruster 4 that would not respond to azimuth commands. The following table shows this alarm sequence. The event starts with a thruster four azimuth compare alarm. Within ten seconds there were both heading and position excursions. At approximately one minute there was a power alarm. At this point the operator put on thruster 1. After 01:47 minutes a second azimuth compare alarm occurred on thruster four. The operator continued operating with thruster 4 online until +03:04 minutes after the start of the event when the unit was taken offline. During this three minute period there were approximately twelve alarms with twenty five alarms and status events reported. This is about one per seven seconds. It took the operator about three minutes to determine that thruster 4 was not responding.

After the thruster was taken offline, this caused an upset with power levels reaching alarm limits, due to the re-allocation of power. The operator then put on thrusters 8 and 4 online. This may have been done to try and determine if there was really a problem with thruster 4. It was left online for 10 seconds but during this time it caused enough of a system upset that the rig moved out of the Yellow watch circle.

Good alarm management could help in this situation. With a good description of the azimuth compare alarm and defining some of the causes may better prepare the operator when this type of fault occurs. If this sequence were studied along with good alarm definitions, it could help the operator recognize this type of failure earlier.

00:00	T4 Azimuth Compare	*First thruster alarm in sequence*
00:04	Heading Excursion	*Within two seconds the unresponsive thruster caused a heading excursion*
00:13	Position Excursion	*a position excursion occurred where the rig moved more than 2 meters.*
00:53	Heading Excursion Alarm - Cleared	
00:53	Bus Power Exceeding Limit	*a main power bus alarm occurred*
00:55	Bus Power Exceeding Limit Alarm - Cleared	
01:16	T1 Online in Auto Control	*T1 placed online by the operator*
01:49	T4 Azimuth Compare Alarm	*a second T4 azimuth alarm occurred*
03:06	T4 Offline	*operator takes T4 Offline.*
03:09	Generator at High Load Level	*Subsequent alarms show multiple thruster and power alarms*
03:18	T1 High Power Level	
03:18	T3 High Power Level	
03:18	T3 Thruster Power Level Compare	
03:29	T3 Thrust Compare	
03:41	T4 Online in Auto Control	*Operator put T4 as well as T8 back Online*
03:41	T8 Online in Auto Control	
04:01	T4 Azimuth Alarm	*Second T4 azimuth alarm*
04:12	T4 Offline	*Operator takes T4 back offline- Probably decided that T4 was not working properly at this time.*
04:17	Generator at High Load	
04:55	Heading Excursion	
05:17	Position Excursion	
05:29	Heading Excursion - Cleared	
06:35	Yellow Alarm Condition	*Rig moved out of Yellow watch circle (9m)*
07:38	Generator Put Online	*An additional generator was put online by the operator*

11 Oct 2010

| 09:11 | Yellow Alarm Condition – Cleared | *Rig moved back within Yellow watch circle* |

Table 1: Thruster Azimuth Failure Alarm Sequence

10. Conclusion

10.1. Present Situation

The vast majority of the marine control systems have very little to no alarm management functions implemented. The HMI alarm lists are generally continuous flat text files. The only thing that these systems have in common with more advanced ones is the use of Red as a standard alarm HMI color.

System documentation typically has poor alarm definition lists. There are systems without any alarm documentation. There are no alarm philosophy documents with most all of the systems.

A major component of system FMEAs are alarms resulting from failures. Competent DPOs should know all of the alarms and the appropriate response to the failure. This is dependent on good alarm definitions and rationalization. It is critical that alarms resulting from system failures give the operator as concise information as possible so that the correct mitigation can be done.

10.2 Future Improvements

A good first step would be detailed alarm lists with clear definitions, including the cause(s) in the description that would give operators more information. Better grouping of alarms on HMI displays with prioritization.

Ensure that all dynamic positioning system operators know all system alarms and their causes. This should be part of basic training but there is no formal structure for this purpose. This is dependent on individual motivation and experience.

An existing system would be difficult to modify in terms of software for alarm data reduction and advanced analysis. Data Loggers could be used for analysis and advance reporting since these are normally databases. Standard database analysis could be used to enhance alarm reporting. Alarm sequences based on FMEA failure modes could be identified to assist the operator. Assuming that the system data collection is fast enough this could be done in real time.

It is important that the level of awareness be raised because alarms are indication of a system's state. They are the first indication of failure or a possible emergency situation. Proper operator response is critical to preventing the escalation of a failure event to a possible serious operational one. Existing system's documentation needs a lot of improvement in the area of alarm management. Even a minimal implementation of basic alarm management could have a major impact on losses incurred through drift/drive-offs or other serious events.

References

[1] Alarm Management: Seven Effective Methods for Optimum Performance
        Bill R. Hollifield and Eddie Habibi

[2] Report of The President's Commission On THE ACCIDENT AT THREE MILE ISLAND

ABS *Guidance Notes on Ergonomic Design of Navigation Bridges 2003*

ANSI/ISA-18.2-2009 *Management of Alarm Systems for the Process Industries*.