Dynamic Alarm Management on an Ethylene Plant

Leslie D. Jensen, P.E.
ProSys GmbH
Postfach 1125
D-84479 Burghausen

Tel: +49-8677-911642
or +1-225-291-9591
Fax: +49-8677-911643
or +1-225-291-9594

Abstract

The process alarm interface has become one of the most important features of process control systems. During shutdown, startup, or a significant process failure, a shower of unnecessary alarms can hinder the operator in understanding and reacting to a significant process upset.

The ÖMV-Deutschland ethylene plant provides a representative example of this problem. The product separation units, which are highly flow and heat integrated, require several critical compressors. This paper discusses a dynamic alarm management system that has been installed to insure that only meaningful alarms are annunciated. Using **D**ynamic **C**onfiguration **S**oftware™, the unnecessary alarms are disabled or inhibited when the shutdown of a particular section of the plant is detected. Alarms are enabled when operation has returned to normal. In selected shutdown or startup cases, alarm trip points are changed and then restored after normal operation has been established.

Prior to the installation of dynamic alarm management, a refrigeration shutdown could generate more than 1450 alarms in a single area during a seven hour period, rendering the alarm summary useless. With **D**ynamic **C**onfiguration **S**oftware™, the alarm summary is able to provide a meaningful source of critical operator information in all circumstances. An analysis of a planned shutdown and startup using this dynamic alarm management system is included.

Preface

The proliferation of alarm conditions over the last twenty years is astounding. The cause is rooted in the capabilities of digital based control systems, in which Honeywell became an early leader. It is now possible to alarm literally every process input signal without any additional hardware cost. Additionally, alarms can be generated by higher level control functions.

The process operators' responsibility to monitor and react to alarms is normally a reasonable task. During normal operating conditions, the operator has time to respond to the occasional alarm that warns him of a more serious situation or off-spec material if corrective action is not taken. However, when a significant failure in the process occurs, the occasional alarm can become a flood of alarms that causes the operator stress and anxiety. At best, such a situation leads to annoyance, confusion, frustration, and fatigue. At worst, it can lead to disaster. This is contrary to the basic objectives of an alarm-driven interface.

ProSys has long recognized this problem and, through its own initiative, developed the first successful dynamic alarm management applications in 1990. To its credit, ÖMV had similar opinions and became the first to benefit from this alarm management philosophy and technology. Since then many advances have been made.

This paper is intended to document the post installation analysis of an application of the most recent generation of dynamic alarm management technology on an Ethylene Plant. The general goals, as will be shown, were fairly simple.

Project Objectives

The specific objective of the operations department was to "do something" about the alarm flood that accompanies major process incidents. The operators were simply being overwhelmed. The resulting project objective was defined as:

- Safely mitigate the annunciation consequences of major process incidents by
    - Dynamic suppression of unnecessary alarms during the incidents,
    - Dynamic activation of necessary alarms during incident recovery;

The system design also required that the process operators be able to comprehend and interact with the system.

Project Solution

The decision was made to install the alarm management capabilities of **D**ynamic **C**onfiguration **S**oftware™, or **DCS**, on all areas of the ethylene plant available on TDC 3000. These three areas are Warm Fractionation (Area A), Cold Fractionation (Area B), and Miscellaneous Units (Area C). The remainder of the ethylene plant is currently on TDC 2000 data highways.

The focus of the project centered around the ethylene plant compressors. Major process incidents in the areas covered by this project usually involve one of the compressors. While failures are infrequent, they result in massive broad-reaching consequences throughout the plant. The resultant loss of process flow and/or refrigeration in associated equipment triggers an avalanche of alarms.

Specific attention was to be given to the operator interface as an integral part of the solution. Operator displays were required to show which alarm points would be affected by the system and under what conditions the alarm enable states would be changed. The operator interface was also required to provide complete manual intervention to override the systems.

As the project progressed and the **DCS** system design philosophy emerged, it became apparent that additional benefits could be achieved. The **DCS** applications being developed to handle compressor incidents also provided an appropriate system for managing alarm annunciation during startups and shutdowns. Thus, the operator could be relieved of meaningless alarms during these situations as well. As a result of the ultimate system design philosophy, plant shutdowns and startups were also encompassed by the project.

Introduction to Results

The project was completed prior to a planned plant shutdown. As a result, it was possible to gather actual data showing the affect of the **DCS** alarm management applications.   The following trend graph shows the impact that the **DCS** alarm management systems had on Areas A and B combined.

Area A&B Shutdown - Cumulative Alarm Comparison
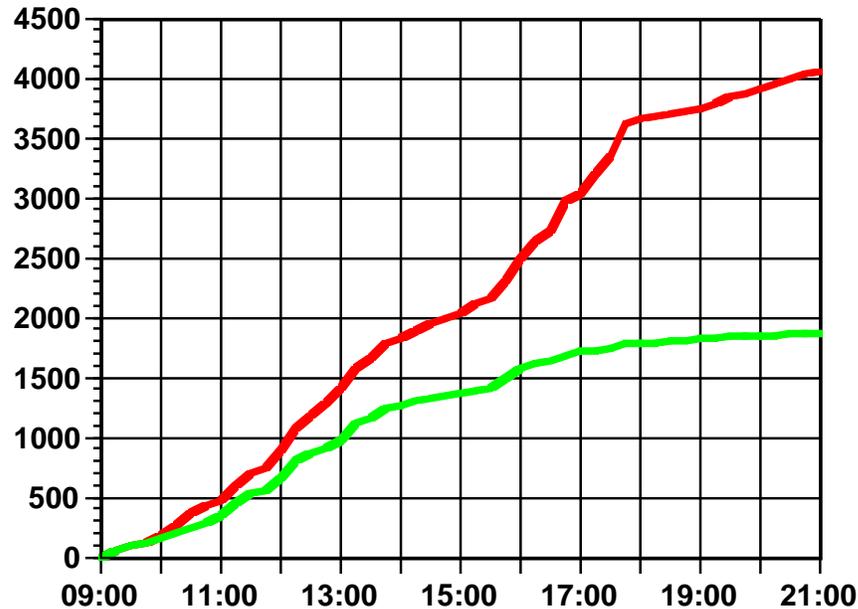
The vertical scale represents the cumulative number of annunciated alarms.   The horizontal scale is the twelve hour period beginning 9:00 AM on the morning of shutdown. The upper trend line shows the annunciated alarm count without any alarm management systems active. The lower trend line shows the annunciated alarm count with the installed **DCS** alarm management systems active. In other words, the difference between the two lines represents the annunciated alarm count which the operator never saw because of alarm management.

At the end of the 12 hours, the console operators of these two areas were spared more than 2000 alarms that would have otherwise been annunciated. Those were unnecessary alarms which the operator never had to deal with.

These results were accomplished with only 40% of all possible alarm points included under the **DCS** alarm management systems.   Therein lie both the wonder and the disappointment of the project, i.e., the results were very impressive, but they could have been much better!

Alarm Management Concepts

The fundamental purpose of alarm annunciation is to alert the operator to deviations from normal operating conditions, i.e. abnormal operating situations. The ultimate objective is to prevent, or at least minimize, physical and economic loss through operator intervention in response to the condition that was alarmed. For most digital control system users, losses can result from situations that threaten environmental safety, personnel safety, equipment integrity, economy of operation, and product quality control as well as plant throughput. A key factor in operator response effectiveness is the speed and accuracy with which the operator can identify the alarms that require immediate action.

By default, the assignment of alarm trip points and alarm priorities constitute basic alarm management. Each individual alarm is designed to provide an alert when that process indication deviates from normal. The main problem with basic alarm management is that these features are static. The resultant alarm annunciation does not respond to changes in the mode of operation or the operating conditions.

When a major piece of process equipment like a charge pump, compressor, or fired heater shuts down, many alarms become unnecessary. These alarms are no longer independent exceptions from normal operation. They indicate, in that situation, secondary, non-critical effects and no longer provide the operator with important information. Similarly, during startup or shutdown of a process unit, many alarms are not meaningful. This is often the case because the static alarm conditions conflict with the required operating criteria for startup and shutdown.

In all cases of major equipment failure, startups, and shutdowns, the operator must search alarm annunciation displays and analyze which alarms are significant. This wastes valuable time when the operator needs to make important operating decisions and take swift action. If the resultant flood of alarms becomes to great for the operator to comprehend, then the basic alarm management system has failed as a system that allows the operator to respond quickly and accurately to the alarms that require immediate action. In such cases, the operator has virtually no chance to minimize, let alone prevent, a significant loss.

In short, one needs to extend the objectives of alarm management beyond the basic level. It is not sufficient to utilize multiple priority levels because priority itself is often dynamic. Likewise, alarm disabling based on unit association or suppressing audible annunciation based on priority do not provide dynamic, selective alarm annunciation. The solution must be an alarm management system that can dynamically filter the process alarms based on the current plant operation and conditions so that only the currently significant alarms are annunciated.

The fundamental purpose of dynamic alarm annunciation is to alert the operator to <u>relevant</u> abnormal operating situations. They include situations that have a necessary or possible operator response to insure:
- Personnel and Environmental Safety,
- Equipment Integrity,
- Product Quality Control.

The ultimate objectives are no different than the previous basic alarm annunciation management objectives. Dynamic alarm annunciation management focuses the operator's attention by eliminating extraneous alarms, providing better recognition of critical problems, and insuring swifter, more accurate operator response. This project demonstrates the practical benefits provided by an effective dynamic alarm management system.

Process Incident Analysis

The following graph shows two relationships involving the impact of process incidents. The solid black curve shows the characteristic relationship between the impact of incidents and their frequency of occurrence. The gray shaded curve shows the characteristic relationship between the impact of incidents and the complexity of the associated alarm management analysis.

Incident Spectrum
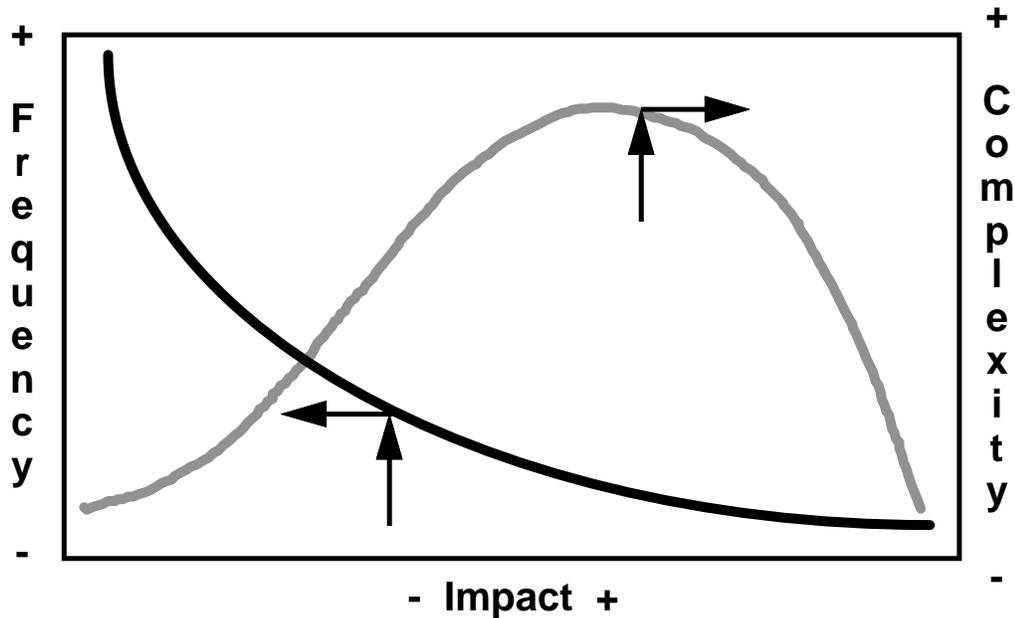
Impact can be defined in many different ways, such as operator stress level, lost production, maintenance costs, equipment damage, etc. However, the characteristic relationships remain the same.

The frequency - impact curve is based on the following observations. Alarms that are generally considered to be annoying or nuisance alarms tend to be the ones that occur when greater frequency. They are "tolerated" by operators because they have little or no impact on the process operation. Therefore, they require little or no response. Examples of low impact - high frequency incidents include such things as a low pump discharge pressure alarm each time a pump motor is stopped. Since the vast majority of pump stops are intentional, there is no response required of the operator and the alarm has no significance.

At the high impact - low frequency end of the spectrum, one finds compressor, blower, reactor, and fired-heater shutdowns. The loss of all feed pumps would also be a low frequency though high impact incident. These are the incidents that lead to secondary effect alarms. Hopefully, they occur very infrequently. When they do occur, the impact on the operator can be tremendous.

In the middle of the spectrum, one finds such events as reflux or pumparound pump shutdowns, as well as valve or instrumentation failures. These incidents alone may be minor, but they often can cascade and combine into more significant incidents.

The complexity - impact curve shows that both low impact and high impact incidents have a relatively lower analysis complexity than incidents in the middle of the spectrum. By way of the previous examples, the low-impact nuisance alarm from the pump discharge pressure is easy to analyze. When the pump is not running the operator doesn't need the alarm.

The analysis of high-impact major incidents is also easier than it may at first seem. When the refrigeration compressor fails, there will be **many** obvious alarm conditions which provide the operator no essential safety or product quality information. The analysis is pretty obvious and the reaction procedures have probably been established long ago.

However, the failure of a distillation column reflux pump can be more difficult to analyze. The alarm management reactions will probably depend on the length of time the pump is out of service. It will also depend on how many and which derivative consequences appear. Combinations of relatively minor incidents are the most difficult to analyze.

Limited Dynamic Options

If one looks for dynamic alarm management tools and parameters within the TDC 3000 system, several options appear. These options may be applicable to low-impact incidents which require a speedy response, such as the annoying pump discharge pressure alarm. Unfortunately, they are generally limited due to rigid configuration, scope of points that can be affected, or both.

- Contact Cutout - provides an alarm suppression scheme that is fixed by point configuration rather than operating conditions and does not have any operator override.
- Logic Points, Device Controllers, and APM/CL Programs - all provide discretionary logic functions. However, APM resource availability may restrict the number of points that can be managed and their practical overall scope is limited to points in the same APM.
- Unit Alarm Disable and Priority-based Audible Suppression - are very non-selective alarm suppression options that require operator action.

While these options represent steps in the right direction, they still have limitations, and because of that, these options are not widely usable. In addition, because of their "horsepower" demands, they may not be practical.

On a broader scope, disabling all of the points in a unit can only be done safely after that unit is shutdown. Further dividing a unit into sub-units just to give the operator the opportunity to disable part of his alarms has additional implications to be considered. Point unit assignment is fixed by configuration and changes impact many other area database files, displays, history groups, programs, etc. Suppressing the audible annunciation does not remove alarms from the alarm summary displays. These options also put the burden on the operator to decide when it is reasonable to take such an action.

Effective Dynamic Options

Effective dynamic alarm management requires more than rigid configuration or APM/CL programs, all of which have limited practical scope. Adjusting and fine tuning the alarm summary display and audible annunciation belies the problems but does not address the major issues and objectives of dynamic alarm management.

Effective dynamic alarm management requires an expert system that is flexible and reliable. It must empower operations supervision and process engineers to truly filter the

alarms by designing applications that determine which alarms should be managed and when they need to annunciate. It must also give operators easy access to and control of the system, along with an understanding of what it does.

Dynamic Configuration Software

With a sufficiently powerful system, one can attack the high-impact incidents that give every process operator and engineer nightmares.

The **DCS** system employed at ÖMV-D has many of the desirable characteristics. It is the result of development efforts that began over 5 years ago with the installation of a predecessor alarm suppression system. **DCS** has the general features listed below.
- The software modules are generic Application Module CL programs.
- The applications are highly flexible, easily modified and maintained.
- The applications can access any point on the LCN.
- The system design has proven to be highly reliable.

The software is area specific and, thereby, has area access protection to prevent access from any other area. Not even an engineer key can override this protection.

The system also utilizes standardized subpictures and overlays for operator as well as engineer access. All engineer configuration changes can be done from schematics.

DCS Modules

The software consists of three compatible modules: the case selector, the alarm block, and the configuration block. The case selector module is central to all applications. It contains any optional case logic to control which alarm and configuration blocks need to be activated. The case selector provides the following features.
- Default Safe Case Definition - establishes the base alarm annunciation status for all managed points when no other case can be safely determined.
- Area Security and Keylock Protection - insure integrity of alarm management applications by restricting operator access to stations loaded with the assigned area database.
- Manual, Semi-, Automatic Modes - allow operator complete control of the alarm management system. In manual mode, the operator determines and activates the currently effective case. In semi-automatic mode, the operator must confirm the case selection before it becomes active. In automatic mode, the selector will determine and activate the current case without any operator intervention.
- User-written Case Logic - provides customized logic for automating the case selection process.
- Inputs - accept operator input of manually selected cases.
- Outputs - activate the associated Alarm and/or Configuration Blocks.

The case selector execution is scheduled and can also be executed by event-initiated-processing (EIP). A minimum of either one alarm or configuration block is required for each logical case. Any number of blocks may be combined to achieve the objectives.

The alarm block module is case specific. It can handle definitions of the initial and time-delayed final alarm enable state parameter (ALENBST) for up to 20 alarm points. The alarm block provides the following features.

- Inputs - accept user specified definitions of the alarm points to be managed, along with the corresponding initial ALENBST, the final ALENBST with optional time-delay, and an optional intelligent ENABLE state definition for the final ALENBST.
- Outputs - set the ALENBST parameter to the appropriate state for each alarm point and activate any associated Alarm and/or Configuration Blocks.

The configuration block module is case specific and provides the following features.
- Sequential List Processing - allows sequence of operation definition for all specified parameter manipulations.
- Parameter Read/Write - provides the ability to read and/or write any parameter accessible to the Application Module.
- Inputs - accepts user specified definitions for parameter reads and writes.
- Outputs - write the appropriate parameter value as defined for each point and activate any associated Alarm and/or Configuration Blocks.

The implementation of the **DCS** alarm management systems conforms to a simple philosophy. All selector modules have a safe case defined. All points manipulated in any case definition are included by all cases within that selector. The operator interface provides the operator with easy access to the selector modules. The operator has easy access to displays that show the logic and structure of each case.

# ÖMV-D Project

Project Organization

The project organization included representatives from the ÖMV-D Operations and Engineering Departments to work with ProSys personnel. ProSys was responsible for the development, installation, and implementation of all standard and custom software packages and interface displays. ProSys was also responsible for the design and implementation of all **DCS** systems.

The engineering department was involved throughout the project. Engineering personnel participated in the systems design and review activities. They also provided project coordination between ProSys and ÖMV-D. The engineering personnel have the residual responsibility to maintain and expand the **DCS** system.

Operations personnel had very limited availability during the 4 month duration of the project due to a scheduled plant shutdown. The scope and conservative nature of the project systems were impacted by the limited availability of Operations personnel to review the systems design.

Systems Definition

For dynamic alarm management, the process is divided up into logically related sub-units which will be affected by their own set of logic conditions (referred to herein as a system). This does not preclude dependencies or overlap between systems. In fact that is a very important part of the analysis. The logic must define the possible modes of operations to be considered. Each mode then becomes a case. The following hypothetical process flow diagram illustrates this analytical procedure.
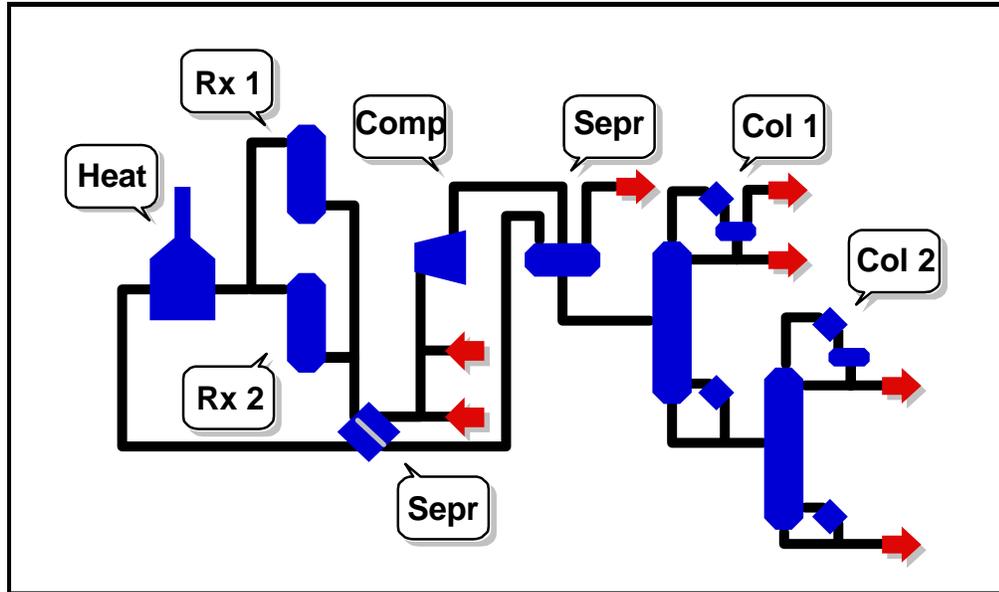
This process of sub-unit definition is much the same as defining units for alarming. However, there is no necessary relationship between point unit assignment and dynamic alarm management system assignment. Once the sub-units are identified, the systems and cases can be defined. The following diagram illustrates the applied **DCS** structure.
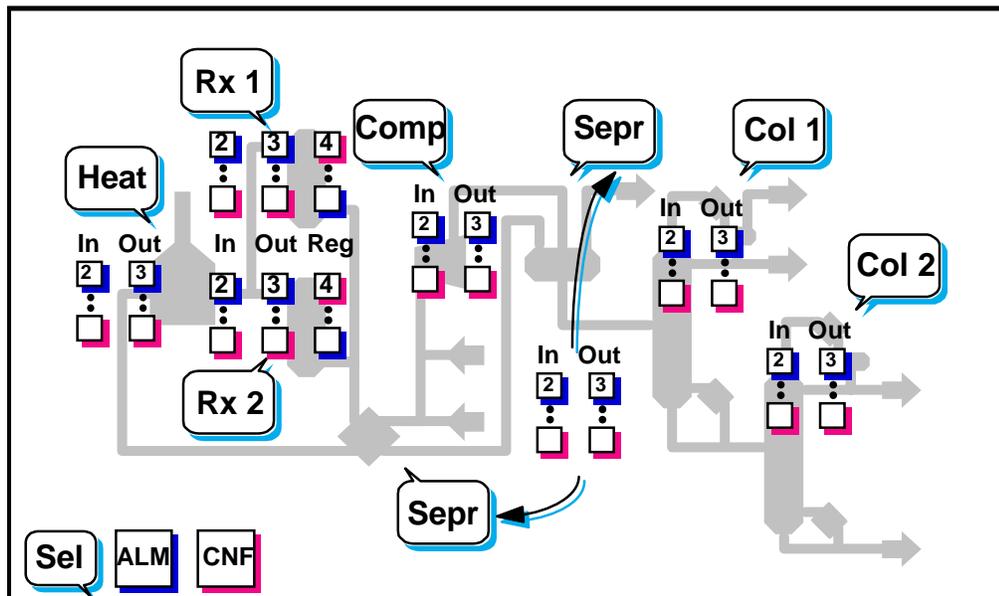
For this project, the system definition began with identifying the types of sub-units to be covered. The plant was then sub-divided into compressors, reactors, and columns. After defining the boundaries of the systems, individual alarm points were selected to be included in the appropriate sub-units. The case logic was defined based on digital, analog and other system case inputs. The logic was designed to be redundant such that, in most cases, an individual input did not determine the case.

It was determined that three standardized cases for each system would be sufficient to achieve the project objectives. These cases were identified as :

- Safe Case - all alarms are enabled immediately,
- Normal Operation Case - point ALENBST parameters are enabled after the alarm has cleared or after a specified time delay has expired,
- Shutdown - all alarms are disabled immediately.

Points were included in the systems based on selection criteria that were extremely conservative. Points falling into any one of the following categories were excluded:

- Pressure Controllers to Flare
- Nearly All Analog and Digital Levels
- Digital Pressures, Equipment Failures, Flame Detectors, Vibrations
- Motor Amps and Temperatures
- Utility/Auxiliary Systems (steam, MEA, caustic)

If there was any doubt about the possible consequence of including an individual point in a system, it was excluded. All other alarm points were included.

These criteria were extremely conservative because it would have required serious and lengthy discussions between operations and engineering to expand the scope of the systems. However, the availability of the necessary personnel during this project prohibited a more encompassing selection.

The resulting number of **DCS** alarm management systems, their content and structure are shown below by process area.

- Area A - Warm Fractionation
  - 198 of 584 Alarm Points (34%)
  - 9 Selectors, 42 Alarm Blocks
- Area B - Cold Fractionation
  - 227 of 477 Alarm Points (48%)
  - 11 Selectors, 51 Alarm Blocks
- Area C - Miscellaneous Units
  - 249 of 681 Alarm Points (37%)
  - 17 Selectors, 66 Alarm Blocks

What is most important to recognize is the limited percentage of points included in the systems. In no area did the percentage of alarm points included in the **DCS** systems exceed 50%. In total, only 40% percent of the available alarm points were selected for alarm management.

Project Results

In the following series of graphs, show the impact that dynamic alarm management had on the alarm annunciation in Areas A and B during a recent planned shutdown and startup. The alarm point data are accumulated and plotted at 15 minute intervals for the 10 and 12 hour graphs and at 5 minute intervals for the 2 hour graphs. On all graphs, the upper trend line shows the annunciated alarm count without any alarm management systems active. The lower trend line shows the annunciated alarm count with the installed **DCS** alarm management systems active.
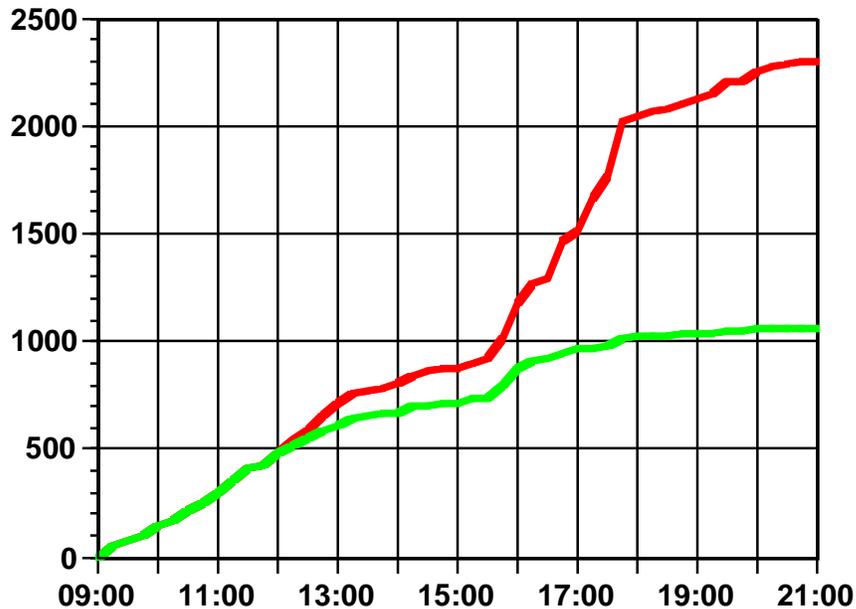
Area A Shutdown - Summary Display Analysis
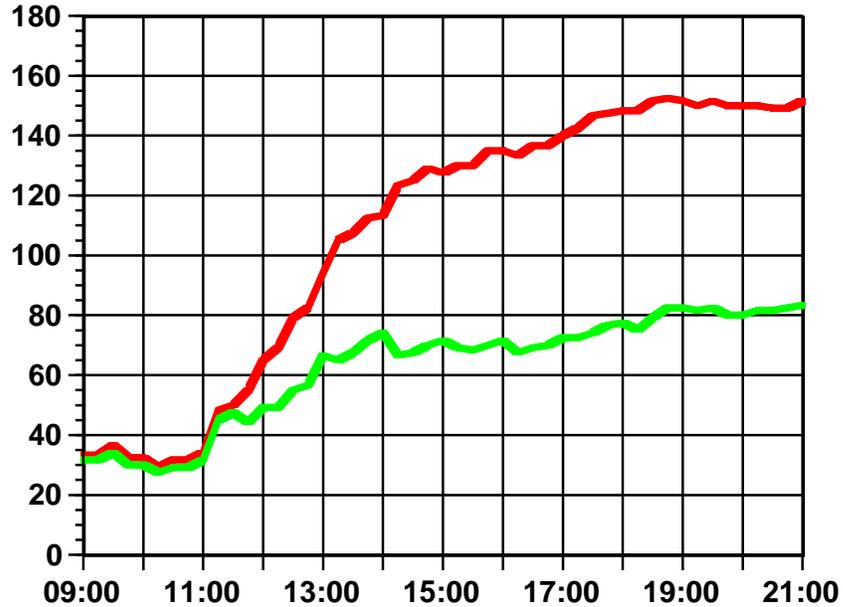
This graph shows the total active alarms on the area A alarm summary display as a function of time. The alarm counts start out equal, but as time passes and various sub-systems in the plant are shut down, the dynamic alarm management systems suppress unnecessary alarms.
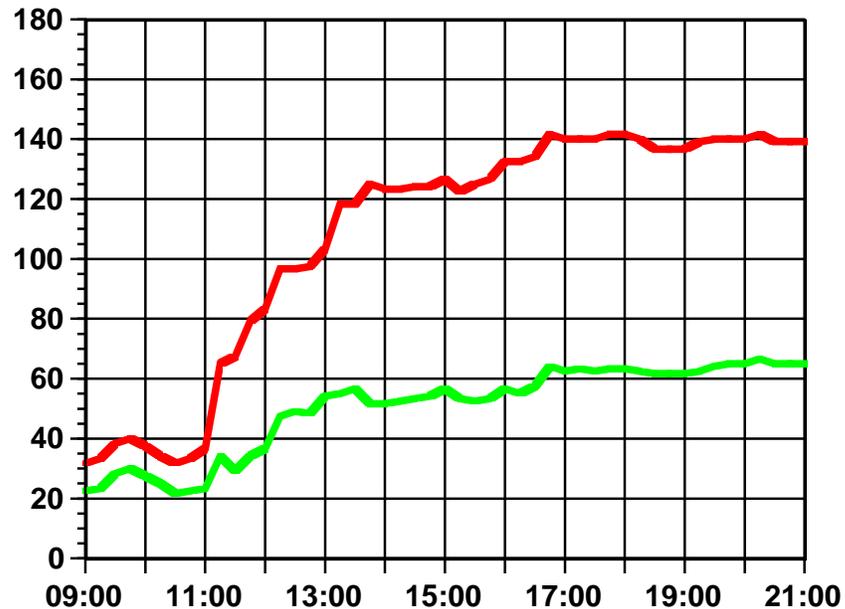
A key point to note is that without dynamic alarm management, the total alarms exceeded the 95-100 alarm limit which can be displayed on the area alarm summary. However, this was not true with dynamic alarm suppression.

Area A Shutdown - Total Annunciated Alarms

This graph shows the total annunciated alarms on area A as a function of time. The initial slope indicates oscillating alarms when considered in conjunction with the previous graph. The final alarm counts after 12 hours show that the operator was spared approximately 1200 alarms because they were suppressed.
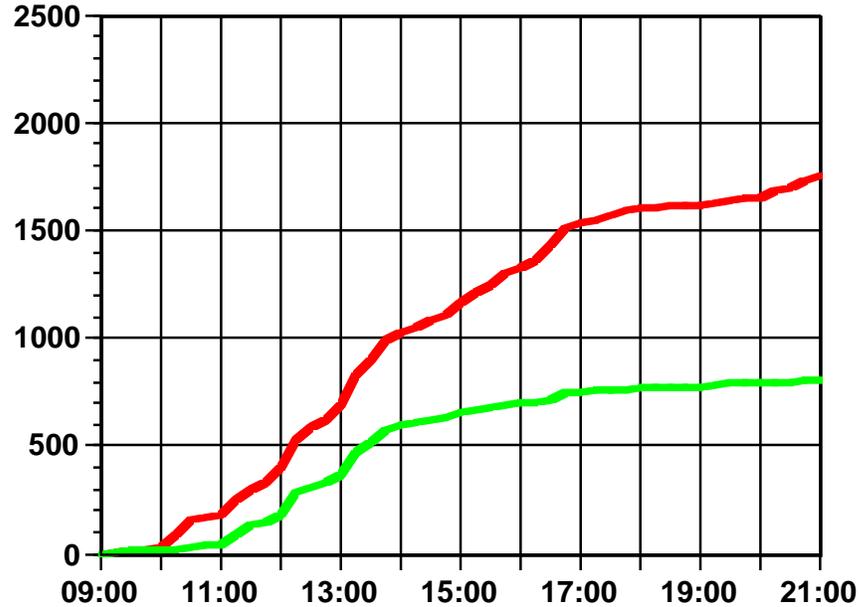
Area B Shutdown - Summary Display Analysis

This graph shows the total active alarms on the area B alarm summary as a function of time. The alarm counts start out equal one-half hour prior to the start of this graph. At that time the first dynamic alarm management systems suppressed a number of alarms. Again as time passes and additional sub-systems in the plant are shutdown, the dynamic alarm management systems suppress more unnecessary alarms.
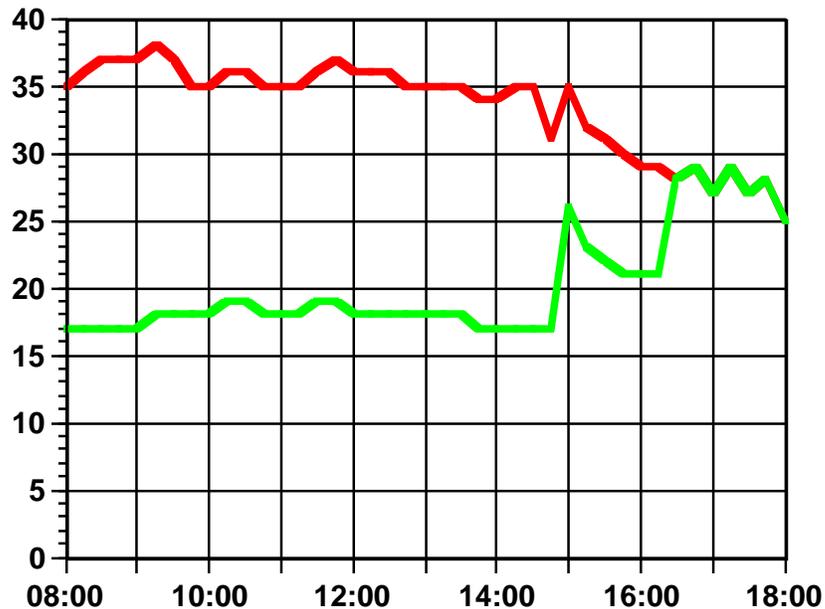
Once more, without dynamic alarm management, the total alarms exceeded the 95-100 alarm limit which can be displayed on the area alarm summary. However, this was not true with dynamic alarm suppression.

Area B Shutdown - Total Annunciated Alarms

This graph shows the total annunciated alarms on area B as a function of time. A combination of this slide and the corresponding slide for area A was shown at the beginning of the paper. The final alarm counts after 12 hours show that the operator was spared approximately 900 alarms because they were suppressed.

**Area A' Startup - Summary Display Analysis**

This graph shows the total active alarms on the area A alarm summary for the quench column, gas compressor and wash column/dryer systems as a function of time. Without dynamic alarm management, the total alarms for most of the startup period would have been nearly double those with dynamic alarm suppression.

Just prior to 3:00 PM, the quench column case logic chose the normal operation case. At this point all system alarm points which were not in alarm condition were enabled. As other alarm points cleared their alarm condition they too were enabled. However, after 5 minutes all remaining alarms were enabled. The sharp increase in alarms followed by a decrease as the column lined out at normal conditions indicates that the case definition was extremely conservative. This analysis supports a less conservative delay time for this system.

At about 4:30 PM both the compressor and wash column logic decided that the compressor was in service and alarms should be enabled. Therefore, the alarm count ends up equal at the end of this period.
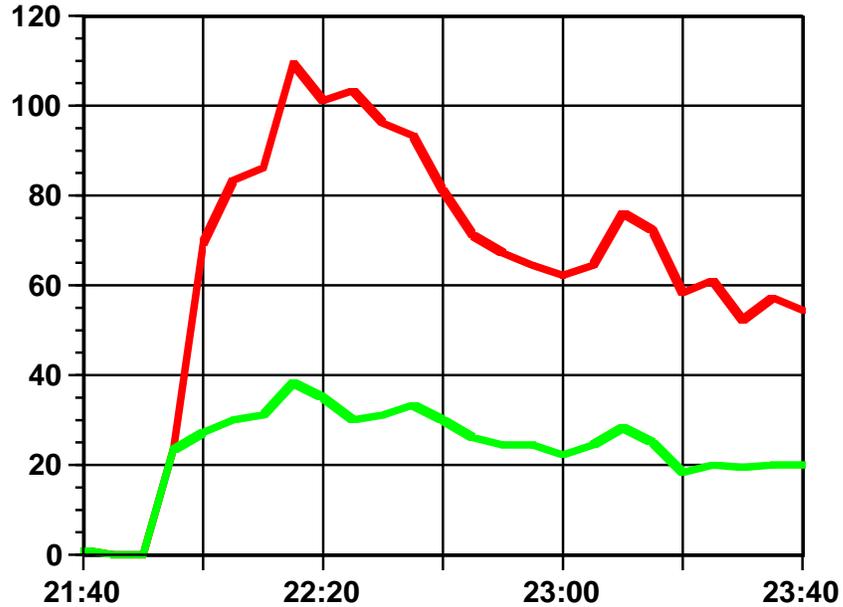
Area A' Startup - Total Annunciated Alarms
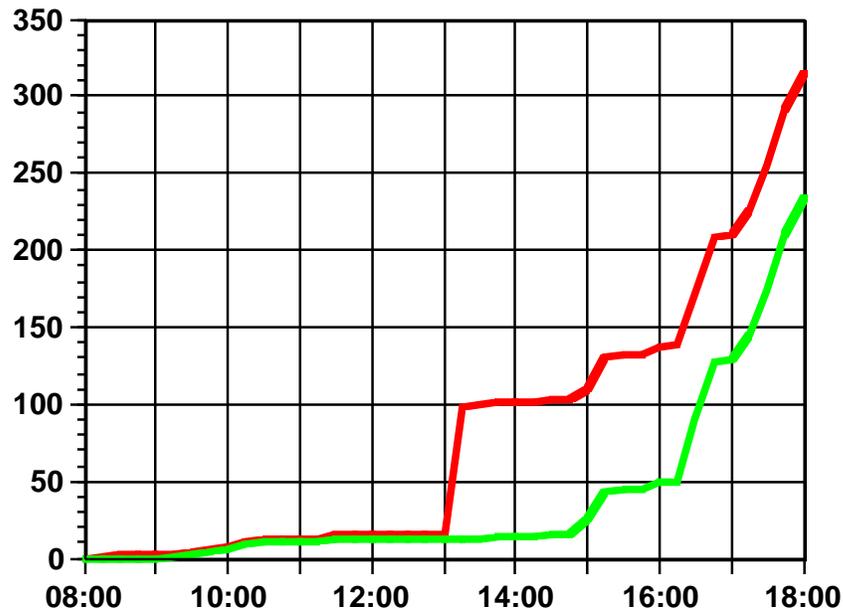
This graph shows the total annunciated alarms on area A for the same 3 selected systems as a function of time. The final alarm counts after 10 hours show that the operator was spared approximately 70 alarms because they were suppressed. Nearly all of these alarms occurred during one 15 minute period 2 hours prior to the 3:00 PM quench column startup. The slope at the end indicates that some points may have been prematurely enabled and/or there again were some oscillating alarms.

The following graphs present a retrospective analysis of a lightning-induced incident which occurred prior to the installation of dynamic alarm management. The event has been analyzed for the simulated affects which would have been seen if the current systems had been in affect at that time. For these graphs, the alarm point data are accumulated and plotted at 5 minute intervals.

Area B Retrospective - Alarm Summary Analysis

This graph shows the total active alarms on the area B alarm summary as a function of time. As time passes and sub-systems in the plant shut down, the dynamic alarm management systems would have suppressed unnecessary alarms.

Once more, without dynamic alarm management, the total alarms exceeded the 95-100 alarm limit which can be displayed on the area alarm summary. However, this would not have occurred with dynamic alarm suppression.

Area B Retrospective - Total Annunciated Alarms
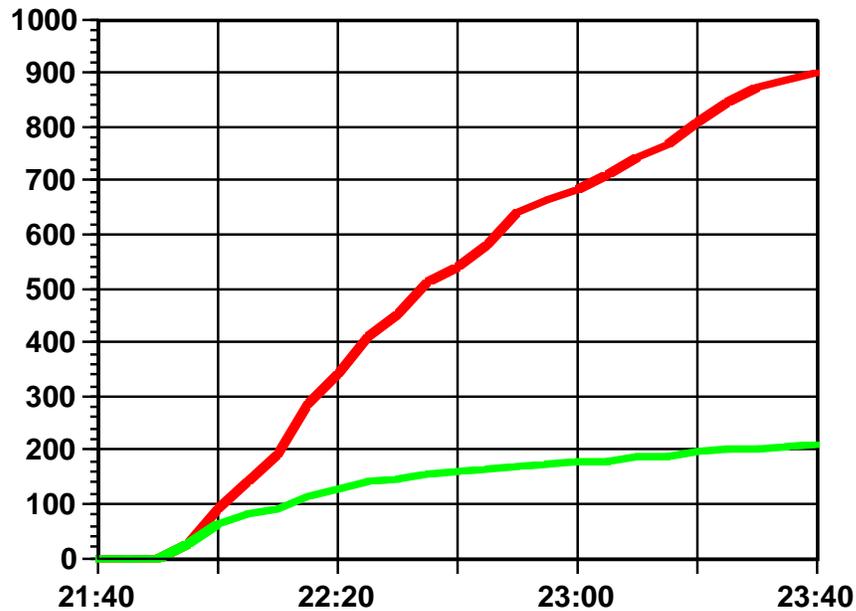
This graph shows the total annunciated alarms on area B as a function of time. The final alarm counts after 2 hours show that the operator would have been spared approximately 700 alarms because they would have been suppressed.

It is important to understand that the compressors were restarted within this period and that as a result, some alarm management systems may have returned to the normal operation case. In that case, alarms would have been enabled. This would reduce the indicated difference if they would have been prematurely enabled. Unfortunately, both digital and analog historical values are necessary to simulate the restart effects on individual systems and that information was not available. Nonetheless, within the first 3/4 hour, it is nearly certain that the operator would have been spared several hundred unnecessary alarms.

SUMMARY

The benefits of this investment depend upon improved operator performance and a corresponding reduction of incident losses. The operators are required to analyze and diagnose problems and failures and to respond in an appropriate and swift manner. Sometimes, they are expected to perform their jobs under the most unbelievable stress at the most unexpected times. Operator response to process incidents will be speedier and more accurate, with reduced stress, using dynamic alarm management systems.

When the operators' response performance is enhanced, the losses arising from poor product quality, equipment damage, personnel injury, and environmental damage will also be reduced.

Future Developments

Future developments in the areas of international language and generic selector logic are envisioned to enhance the capabilities of dynamic alarm management on TDC 3000. Additionally, AxM applications are being developed to provide a solution for high complexity alarm management applications.

Appreciation

In closing, the author would like to recognize those people who played significant roles in this project.
- ÖMV Deutschland
    - Dr. J. Seifert
    - Herr U. Nagel
    - Herr A. Rummert
- ProSys
    - Dr. R. Prinz
    - Dr. W. H. Beaver
    - Mr. J. R. Griffiths