A Practical Approach to Alarm Management
Part Two: Rationalization Based on Need and Risk

In Part One of this white paper series, *Crawling into Alarm Management*, we discussed simple and straightforward nuisance alarm reduction. That methodology - while not satisfying the rationalization criteria of the alarm management purists - is a common sense approach to resolving nuisance alarm issues. Its institution should make you a local hero in the control room, and may give you management support to take further steps.

Following a nuisance reduction, you will have some of the pieces in place that make it possible to consider a more formal rationalization. You've actually begun going through the motions of a formal rationalization during the nuisance reduction. Perhaps it is time to take the next step.

Understanding the Risk Related to Alarm Management

In a HAZOPS-style approach to alarm management – you call your best friends into a room and beat up the alarm configuration until it is properly designed for the way the plant runs. This takes a lot of time and resources, including personnel from various departments. Sometimes this type of rationalization can be justified - especially after you have already demonstrated the value of nuisance alarm reduction. Or you may find that the costs are not warranted when measured against the anticipated risk reduction.

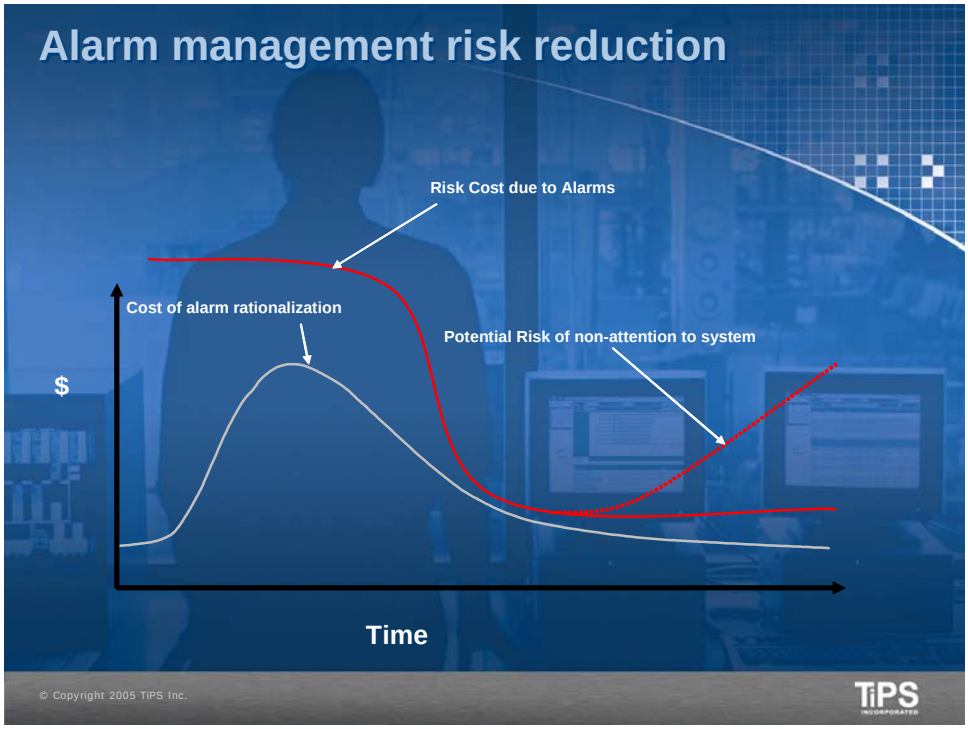

Figure 1 - Alarm risk reduction

After performing a HAZOPS-style alarm rationalization you have attained a state of lowest amount of investment at risk due to alarm management problems (within the constraints of the technology available to you). The risk will creep back up if you simply do an alarm management PROJECT, and do not embrace the activity of alarm management as a continuous PROCESS.

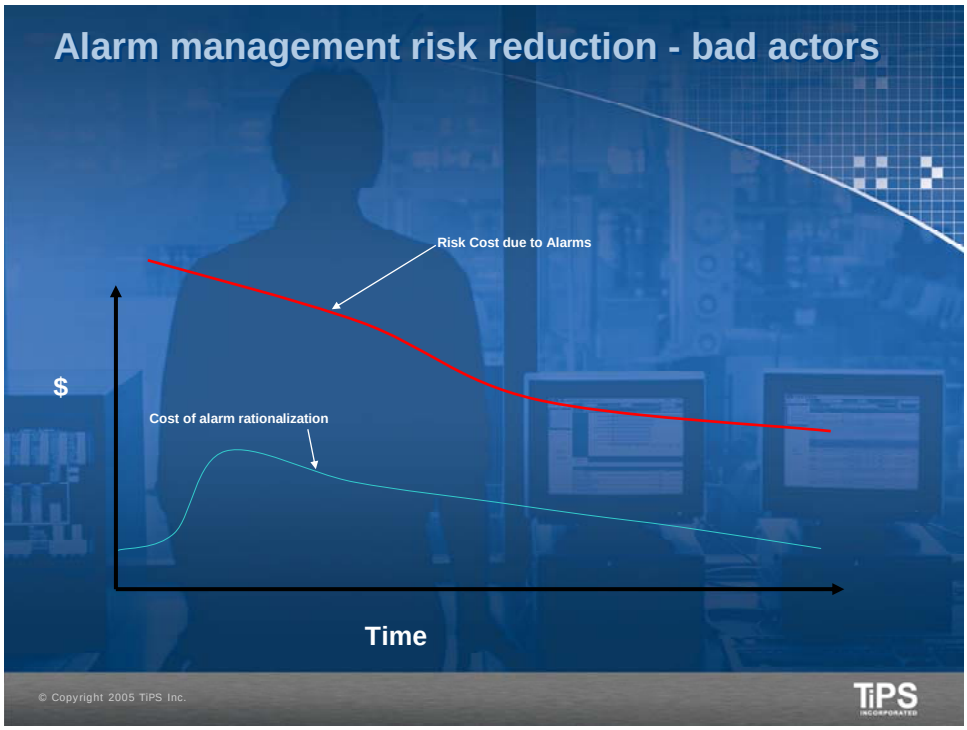

Figure 2 - Alarm risk reduction using bad actor approach

If you limit alarm management to assessing only nuisance alarms, and continue to use that approach, the risk is not reduced as rapidly as in a HAZOPS-style project, and the total risk reduction opportunity is more limited. However, a nuisance focused approach has the added value that since it is continuous, alarm-related risk is consistently being reduced. Also, the short-term impact on risk may actually be more aggressive than a HAZOPS-style approach because you are initially attacking the alarms that are causing blatant problems as opposed to waiting for the results of the completed project.

Industry feedback suggests that both methods eventually arrive at the same result in about the same time due to the difficulties in stabilizing operating team reactions to the radically changed environment following a HAZOPS-style rationalization. Changes to the alarm settings and how the system operates sometimes make for a new operating paradigm. That paradigm shift must be transferred to operators for them to understand how they must deal with the changes. This is why we normally advocate that this problem is best handled within operations, with their oversight, and control.

Evaluate the risk

Having proven to yourself and your management that alarm management can produce results, it may be time to propose a more serious approach. Begin by analyzing which units in your process carry the most risk should they suffer an alarm flood - or other operating disruption. It is possible to establish a risk matrix which can help you to understand the order of importance of plant units by risk. This matrix can then be used to establish the level of alarm management which you might apply to each unit.

Figure 3- Needs assessed by risk

1. Every unit deserves at least nuisance alarm elimination and some kind of continuous nuisance management.
2. Some units deserve additional treatment for safety or other areas of high risk.
3. Some units deserve a full rationalization of all tags and alarms due to the physical qualities of operation, safety or regulatory issues, or other reasons (even political).
4. Some units become prime targets for dynamic alarm handling if they have alarms that cannot be handled with static alarm activation points. Dynamic alarm handling can be simple or difficult depending on your infrastructure, needs, and the complexity of the process.

What this type of matrix creates is a template which establishes the levels of alarm management you intend to do within each unit and why. It also establishes expectations, which justifies additional expense based on the stated returns.

Using this type of matrix design you get rid of bad actors, and you implement a program of preventing problems in the units that carry the highest risk. The takeway is that it would not make sense to do a HAZOPS-style rationalization at a cost of $100k if the total risk is lost production of a value of $10k if the unit shuts down.

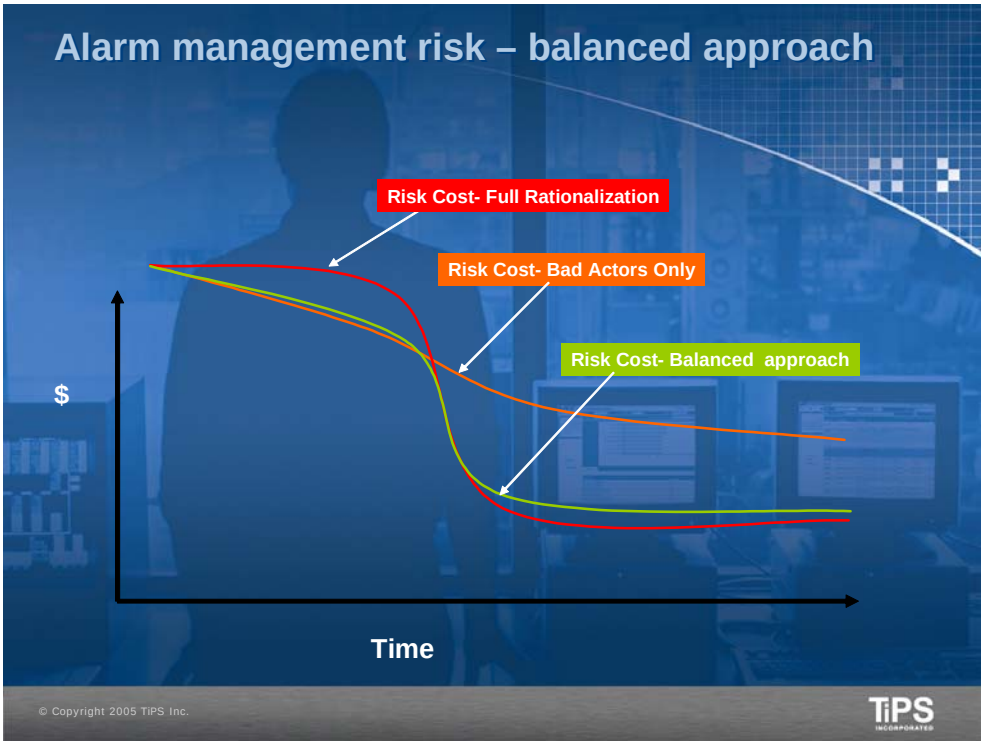

Figure 4- Difference in Risk-based approach

A unit with a risk profile that exceeds the anticipated cost of a HAZOPS-style rationalization, qualifies for that depth of project. This is the only way to protect the unit from the risk of alarms which have not activated recently, or at all.

Consider other Issues

Before you jump right in and enact this plan, consider the possible underlying causes of your alarms. What this usually leads to is the discovery that you simply cannot correct some alarm issues due to restrictions within the technology available to operate the plant. Consider other tools and technologies that may be necessary to properly implement a fully HAZOPS-style alarm design.

We often say “Every Alarm Exists for a Reason”. What this means is that once you get past the obvious bad actors, there is a good reason for every alarm. Is it due to poor graphics? Is it due to shortcomings in operator communications? Is it a maintenance issue? You get the picture. In industry, this “holistic” look at alarm design is known as “Situation Awareness”. Ian Nimmo’s company, UCDS specializes in helping with these issues. Study the papers that deal with situation awareness and you’ll find that two top related issues are graphics design and loop tuning. Loop tuning tools are generally easy to

justify based on ROI, and show remarkable improvements in alarm reduction from their first inception.

A fair assessment of your capabilities in this area may diminish the number of alarms you can redesign. However, it may also prevent a future incident due to over-zealous alarm reduction without attention to the needs of operations.

Make a Plan

Now you have the makings of a plan. Put it together, and prepare to act. Sometimes that means you need to get buy-in at a high level, especially if the efforts you have outlined imply significant investment. A pragmatic and realistic approach has a better chance of success.

So, put the plan in writing and put it in motion. Lacking buy-in, you STILL have things you can attack and improve in the system. You now have the tools, and you can create regular reports that keep you apprised of the system's needs. There's really nothing that can stop you from at least making things better. We've seen that happen over and over in lieu of a major effort. Sometimes it's better to fly below the radar.

Remember at this point to set in place the proper procedures to maintain your gains through integration with plant Management of Change (MOC) procedures. Make it difficult to change alarm configurations without overview by proper authorities.

Set expectations using achievable goals. Avoid a "best practices" trap. EEMUA 191 benchmarks may not be reachable until you have all the pieces in place to attain those performance targets while supplying all the information that operations needs in order to properly control the plant. This may entail operator graphics changes, instrumentation upgrades, advanced maintenance programs, or even DCS upgrades. Just be certain you don't try to oversell what you are trying to get done. Set reachable goals, and hit them.

Summary

We recommend you employ a balanced rationalization approach that includes nuisance reduction and formal rationalization. Examine both of these methods, and use the parts of each that are able to be accomplished knowing your current management disposition, personnel availability, budget, and risk. The formal approach allows you to anticipate bad actors in advance of potential upsets or incidents, so it should not be ignored. **However, it is statistically possible that you can work your way into a rationalized system by continually nibbling away at the bad actors.** There is a higher level of risk associated with a gradual approach, but it beats what you are dealing with now.

Be certain your approach embodies four elements:

Involvement and training of the operators. The operators must understand the new environment you are creating. If you make them part of the process of rationalization, then that training is inherent to the process. If you let them own the process, then it is theirs to resolve and maintain. *"Tell me and I forget, teach me and I remember, involve me and I learn." – Benjamin Franklin*

Consider all the aspects of the control system that give you a cause for creating an alarm. The alarm system can be compared to the trash bin of the control system - it's where we resolve every issue we either couldn't resolve with automation techniques or elected not to for whatever reason. Alarms are a symptom, not the problem themselves.

Create procedures that will take the place of previous practices that let the alarm system get into its current condition. The most important are a Philosophy and Management of Change procedures that overarch alteration of alarm configurations and alarm changes at the console (i.e. those which don't change the configuration - but do alter local settings).

Develop KPI's (key performance indicators) or other tools to track both the condition of the alarm system, and issues that can make it perform poorly (i.e. operator changes).

Expect results:

- Quieter control room
- Better Flood control/ avoidance
- Maintenance savings
  - Industry feedback indicates approximately 5% +/-
- Plant uptime 5-8%
- Avoidance of unplanned outages
- Better use of assets (one plant outage can delete the planned gains from a year of process improvements)
  - Regulatory control
  - Advanced control
  - Optimization