

Desde gerenciar até otimizar alarmes

Deveria haver menos alarmes, mais alarmes ou apenas o número certo? Veja em ANSI/ISA-18.2

Por Richard Slaughaupt

Se você já fez muitas pesquisas sobre gerenciamento de alarmes ultimamente, você descobrirá que a maioria dos centros de discussão é na redução do número de alarmes, que operadores de sala de controle devem lidar em um dia normal, ou durante um distúrbio no processo. Esta tendência segue a sabedoria convencional, de que muitos alarmes são habilitados simplesmente, porque é tão fácil de fazê-lo em sistemas de automação de processos baseados em computador. Isso pressupõe que muitos alarmes são mal escolhidos, ou desencadeados com facilidade.

Como muitas vezes somos lembrados, acrescentar um alarme nos dias da pneumática e de painéis convencionais envolvia algum esforço e custo, então tinha de haver uma razão convincente. Como resultado, o processo de seleção foi em grande parte auto-regulado. Com o advento dos modernos sistemas de controle, foi muito mais fácil, talvez muito fácil, fazer alarmes para tudo.

Em seguida, os operadores passaram a enfrentar dezenas de alarmes durante um distúrbio, e muitas vezes não conseguiram determinar quais eram importantes e quais não eram (Figura 1). A indústria de gerenciamento de alarmes nasceu da necessidade de controlar esse problema. Os primeiros esforços geralmente assumiram que havia muitos alarmes, e precisavam ser avaliados um por um, eliminando aqueles que causavam mais problemas do que sua validade.

Com praticamente todos os principais fornecedores de automação no jogo, inúmeras aplicações foram desenvolvidas para domar o problema de alarmes. Estas geralmente seguem o mesmo objetivo principal, de reduzir a quantidade e a taxa de alarmes aos quais os operadores devem responder. No entanto, o foco nesses tópicos apenas aborda parte do objetivo. O objetivo final não é um número ótimo de alarmes, mas sim, criar um ambiente onde o sistema de alarmes forneça a informação mais crítica que os operadores precisam, em qualquer momento e em qualquer situação possível.



Figura 1. Operadores da sala de controle muitas vezes são confrontados com um número absurdo de alarmes, cortesia de sistemas de controle modernos.

Ajuda da Norma ANSI/ISA-18.2

Em 2003, a ISA começou a desenvolver uma norma para dar mais direção ao gerenciamento de alarmes. Após seis anos de trabalho, a norma ANSI / ISA-18.2-2009 de Gestão de Sistemas de Alarme para Indústrias de Processo foi lançada, e essa versão foi recentemente atualizada. Esta norma da ISA partiu da abordagem normal de porcas-e-parafusos, e focada em uma visão mais ampla dos processos de trabalho ao invés da mecânica. Reconheceu que a gestão de alarmes tem um componente significativamente humano. Embora sistemas e mecanismos estejam envolvidos, a maioria dos processos são conduzidos por pessoas.

Com base no trabalho anterior do "Abnormal Situation Management Consortium" (ASM), da "Engineering Equipment and Materials Users Association" (EEMUA) e da NAMUR, a indústria petroquímica vem usando este padrão há quase uma década. Ela foi recentemente recebendo uma tremenda força em outras indústrias, e deve ser necessária sua leitura para todos os profissionais de automação de processos. O padrão se concentra em alarmes encontrados em sistemas modernos de automação de processos, como em sistemas de controle distribuído (SDCD), em sistemas de aquisição de dados e de controle supervisão (SCADA), e em controladores lógicos programáveis (CLP). Seu escopo visa todas as variedades de processos de fabricação batch ou contínuo e tudo ao redor- por isso sua aplicação é universal.

Como a ANSI / ISA-18.2 é uma norma, e não apenas uma orientação ou sugestão, ela carrega o peso de ser "reconhecida e geralmente aceita como boa prática de engenharia". Isso significa que grupos como a "Occupational Safety and Health Administration", o "Chemical Safety Board" e o "American Petroleum Institute" usam isso como critério ao avaliar sistemas e investigar eventos.

Entendendo o ciclo de vida do alarme

Os métodos tradicionais e a ANSI / ISA-18.2 são semelhantes em alguns aspectos, uma vez que ambos são sobre a redução do número de alarmes. A primeira abordagem começa com muitos alarmes e, em seguida, reduzi-los para um número gerenciável, enquanto a última abordagem é construída desde o início com um senso elevado de seletividade. A ANSI / ISA-18.2 mudou o pensamento predominante ao estabelecer um padrão mais elevado para a implementação de um alarme, com base na noção de que, se mais atenção e cuidado for dado à seleção de alarmes em primeiro lugar, deve haver menos deles. Ela também esclareceu o processo de racionalização de alarme como apenas um passo de uma abordagem holística do ciclo de vida, começando com a idéia de apenas criar alarmes onde o processo e as considerações de segurança o exigem.

O ciclo de vida de 10 passos tem alguns pontos de partida, sendo que um dos mais comuns está em estabelecer uma filosofia fundacional, e continuar com todas as outras etapas necessárias para gerenciar os alarmes de forma adequada – desde a identificação até a manutenção (figura 2). Enquanto outros artigos sobre o tema podem fornecer detalhes mais amplos e uma descrição mais geral da ANSI / ISA-18.2, este artigo se concentrará no lado prático do gerenciamento de alarmes: projeto e implementação.

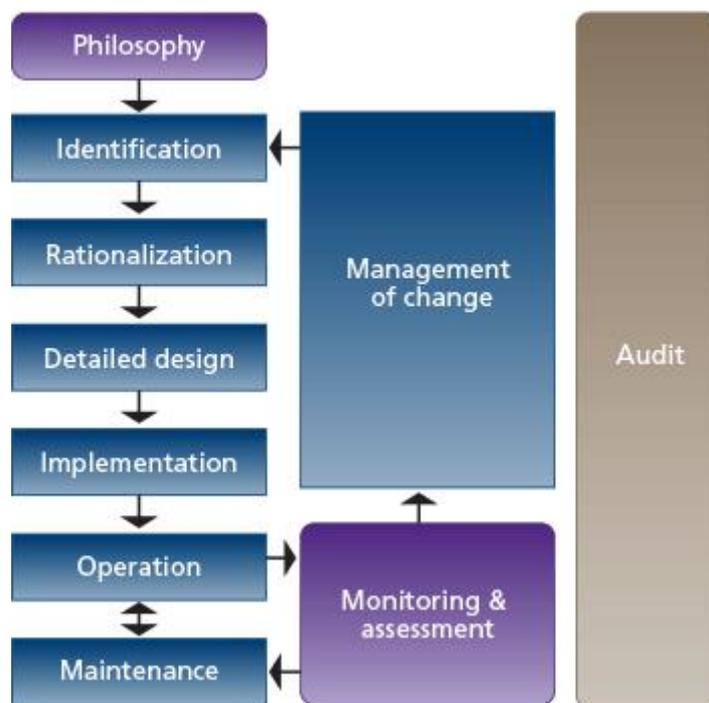


Figura 2. A ANSI/ISA-18.2 estabeleceu uma estrutura para desenvolver e trabalhar com alarmes usando uma abordagem sistemática.

Muito, pouco ou somente o necessário

O objetivo final para uma indústria de processo ou unidade individual não é ter um número específico, fixo de alarmes, mas sim o número certo para as circunstâncias atuais. O conceito é simples, mas a implementação é mais complexa. A preocupação subjacente sobre ter um número liberal de alarmes é que muitos ativarão ao mesmo tempo e confundirão os operadores. Durante esta "inundação de alarmes", eles não poderão discernir alarmes importantes de duplicados ou irrelevantes. Como resultado, a avaliação situacional estará comprometida, e os operadores poderão tomar decisões ruins ou mesmo ocasionar um incidente em vez de neutralizá-lo.

Contar com a idéia "menos-é-melhor" é a proliferação de novas ferramentas que resultam em mais alarmes. Muitos fornecedores fornecem bibliotecas de códigos que melhoram (aumentam) a geração de alarmes, através de recursos de diagnóstico incorporados. Muitos desses alarmes podem ser identificados como a causa raiz, de eventos de processo indesejáveis mais generalizados e, como tal, não devem apenas ser eliminados durante a racionalização. Em vez disso, esses avisos valiosos podem e devem ser adicionados ao conjunto de alarmes.

Esses alarmes podem ser avisos antecipados de início de condições críticas e, portanto, servir com um propósito valioso. Mas seu tempo também é indiscriminado, porque sua condição de disparo geralmente é limitada, como uma perda súbita de sinal relatada por uma instrução de entrada analógica usada para monitorar a vazão de resfriamento. Por este motivo, a aplicação adequada requer algum tipo de filtragem baseada em contexto, para restringir a ocorrência em circunstâncias erradas ou inúteis.

O uso de funções alarmantes de diagnóstico tem sido controverso há algum tempo. Se um transmissor de pressão estiver mostrando sinais de degradação em sua eletrônica, ele pode detectar o problema e enviar um aviso. Mas a quem? Os operadores da sala de controle? Pessoal da manutenção? Naturalmente, a resposta é: "Depende".

Uma das qualificações mais básicas de um alarme legítimo, é que o operador deve ser capaz de fazer algo para consertar ou mitigar a situação. Então, se esse transmissor de pressão está fornecendo uma

leitura muito crítica, provavelmente merece um alarme de sala de controle, mesmo que os operadores não sejam provavelmente os que estão lá para consertá-lo. Pode causar-lhes, no entanto, implementar uma solução de contorno, ou compensar a perda da informação, enquanto o dispositivo estiver sendo substituído pela manutenção.

Agora, multiplique esse cenário por todos os instrumentos inteligentes e atuadores na planta ou unidade de processo. Se cada um dos potencialmente centenas ou milhares de dispositivos que podem causar um alarme estiver configurado para fazê-lo, pode haver ramificações importantes. A solução fácil é direcionar essas mensagens de diagnóstico para a manutenção, mas esta solução é míope se algo for realmente crítico. Voltando ao nosso exemplo, digamos que o transmissor de pressão falhe. Pode resultar um processo de distúrbio, o que desencadeia outros alarmes, mas a situação teria avançado para uma situação crítica, onde poderia ter sido evitada por ação antecipada do operador.

Para complicar ainda mais a situação, o grau de criticidade do transmissor de pressão pode variar dependendo do que está acontecendo com o processo. Durante um procedimento ou tempo particularmente crítico em um processo em lote, a ameaça de dados perdidos ou questionáveis do dispositivo pode ser muito importante para os operadores. Em outras ocasiões, eles podem não importar tanto.

Alarme dinâmico

Isso nos leva a uma conclusão importante: muitos alarmes são mais úteis ou críticos em alguns momentos do que em outros. O objetivo é tornar esses alarmes críticos ativos nos momentos em que são mais necessários, e reprimidos quando não são.

Aqui está outro exemplo: um compressor fornece ar pressurizado para uma variedade de dispositivos em torno de uma unidade de processo, como atuadores de válvula (figura 3). Cada um desses dispositivos dependentes do ar verifica se o suprimento de ar é adequado, e irá falhar se o tubo estiver entupido ou alguém fechar inadvertidamente uma válvula. Agora suponha que o motor do compressor falhe. Ele tem seu próprio alarme para alertar os operadores e pessoal de manutenção, de que o suprimento de ar foi interrompido. Os operadores podem precisar abrir uma válvula, para redirecionar ar de outra parte da instalação, enquanto a manutenção soluciona o compressor.

Agora, com a causa raiz já detectada, a sala de controle precisa de uma dúzia ou mais de alarmes de todos esses dispositivos dependentes do ar, cada um relatando algum tipo de falha? Seguido por mais uma rodada de alarmes dos sistemas que usam esses dispositivos? Claramente não. Uma vez que a causa comum é anunciada aos operadores, os alarmes relacionados subseqüentes devem ser suprimidos, de modo a não distrair o operador do problema real.

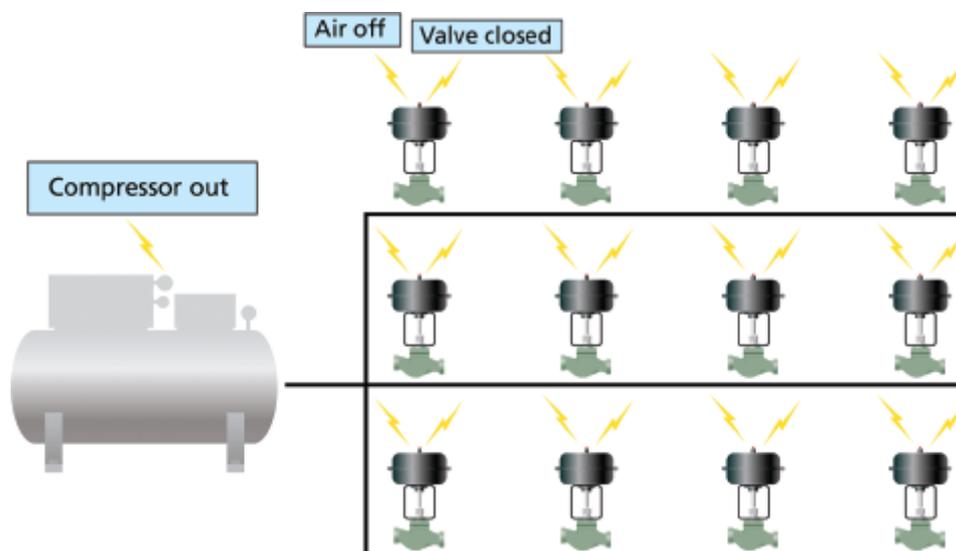


Figura 3. Um único evento pode se tornar uma causa comum, desencadeando uma inundação de alarmes individuais à medida que os resultados se agitam através de vários sistemas.

Tipos de supressão

A ANSI/ISA-18.2 define três formas de supressão de alarmes:

1. Shelving (engavetar), onde um operador suprime manualmente um alarme temporariamente.
2. Supressão pré-definida, onde o sistema de automação do processo suprime um alarme com base em um conjunto específico de condições.
3. Fora de serviço, onde um alarme foi suprimido porque uma parte do equipamento é desligada para manutenção ou algum outro motivo.

A supressão pré-definida é a mais interessante e desafiadora, e normalmente é dividida em duas categorias: supressão estática e dinâmica. A supressão estática baseia-se no estado do processo e do equipamento. Os alarmes específicos são ativados ou suprimidos durante procedimentos ou condições definidas. Por exemplo, alguns alarmes só podem ser ativados durante a inicialização da unidade. Esta técnica simples é a mais comumente implementada dos dois tipos de supressão.

A supressão dinâmica é projetada para evitar inundações de alarme durante distúrbios e outros cenários mais complicados. Dá ao sistema bastante "inteligência" para determinar os alarmes mais importantes sob as circunstâncias, assegurando-se de chegar aos operadores, enquanto que suprimindo alarmes desnecessários e irrelevantes.

A supressão dinâmica é a mais desafiadora, porque exige criar as regras que o sistema usa para determinar o que é importante e o que não é. E, como um sistema de segurança, deve ter os sensores corretos para detectar as condições em que essas regras se baseiam. Em alguns aspectos, pode ser ainda mais complexo do que uma função de segurança, porque centenas de alarmes podem ser afetados e muitos fatores podem entrar no processo de tomada de decisão.

Entendimento muito complexo

Como nos sistemas de segurança, o gerenciamento de alarmes requer especialistas experientes, particularmente quando se deslocam para áreas tão complexas quanto a supressão dinâmica de alarmes. Novas ferramentas emergiram no mercado para ajudar no projeto, implementação e manutenção de tais sistemas.

O abrandamento de um operador com muitos alarmes ao mesmo tempo é claramente prejudicial, mas o limite para o que constitui "muitos" depende da urgência, importância e complexidade da resposta necessária ao evento. O nível de habilidade e a experiência de operadores individuais também devem ser considerados.

As empresas podem investir no desenvolvimento de pessoal interno de gerenciamento de alarmes através de programas de treinamento, como os oferecidos pela ISA, ou utilizar consultores experientes e integradores de sistemas, que podem auxiliar com programas de gerenciamento de alarmes, fornecendo orientação e auxiliando as implementações, conforme a situação o requer. Desenvolver e manter pessoal interno é uma decisão de investimento a longo prazo que precisa ser feita conscientemente. O uso de consultores experientes e integradores de sistemas para ajudar a criar e manter programas de gerenciamento de alarmes, fornecendo orientação e assistência com as implementações conforme a situação requer, é outra opção de investimento a considerar.

Considerações

- A criação de alarmes efetivos não depende de tendo um número específico, mas de fazer as escolhas corretas.
- ANSI/ISA-18.2 é uma ferramenta muito útil se for aplicada adequadamente em pontos críticos no processo.
- Em última análise, os alarmes devem apoiar a avaliação situacional para que os operadores possam tomar boas decisões operacionais.

Sobre o Autor

Richard Slaughaupt é um consultor da empresa MAVERICK Technologies.

Artigo traduzido por Tomé Guerra para a ISA São Paulo Section e republicado com permissão da ISA, Copyright © 2017, todos os direitos reservados. Este artigo foi escrito pelos autores acima e publicado originalmente na revista InTech Online de Set-Out/2017 em <https://www.isa.org/intech/20171002/>. A ISA não se responsabiliza por erros de tradução neste artigo.