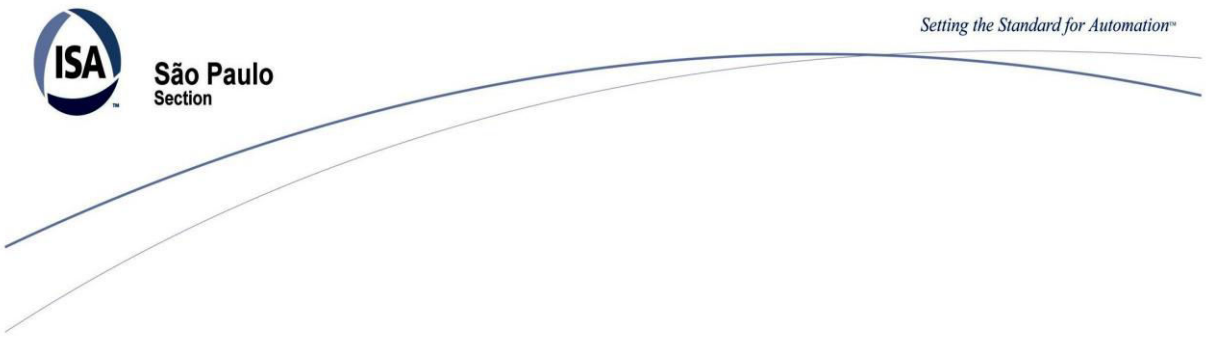
Novembro/10

Newsletter



Editorial

Esta é a quinta edição de 2010 do newsletter bimestral da ISA Seção São Paulo. Nesta edição, são apresentados dois artigos de empresas do segmento e um artigo técnico traduzido livremente a partir de uma publicação retirada de uma organização com foco em tecnologia. Apresentamos também um resumo do nosso último ETM (Encontro Técnico Mensal), realizado em São Paulo, na ABM, cujo tema foi Medição de Vazão. Além disso, destacamos a realização do Brazil Automation 2010, o maior evento de instrumentação, Sistema e Automação da América Latina e um dos mais importantes do mundo. Confira também o calendário de eventos de 2010 atualizado.

Gostaríamos de reforçar que aceitamos temas disponibilizados pelos sócios, desde que contenham informações de novas soluções tecnológicas ou assuntos de interesse, para publicarmos no nosso jornal.

A. Tomé Guerra – ISA Seção SP – Comitê de Publicações
B. Carlos Gury – ISA Seção SP – Comitê de Publicações

Visitem também o nosso site: www.isasp.org.br

Nesta Edição!

EVENTOS:

- **ETM sobre Aplicações e Tecnologias atuais de Medição de Vazão**
http://www.isasp.org.br/site/newsletter/Novembro_2010_pag_2

ARTIGOS TÉCNICOS:

- **Artigo Técnico da National Instruments sobre soluções para barramentos industriais**
http://www.isasp.org.br/site/newsletter/Novembro_2010_pag_3

- **Artigo Técnico da Yokogawa sobre um caso prático de gerenciamento de alarmes**
http://www.isasp.org.br/site/newsletter/Novembro_2010_pag_4

- **Artigo Técnico do site ControlDesign.com sobre a tecnologia PoE (Power over Ethernet)**
http://www.isasp.org.br/site/newsletter/Novembro_2010_pag_5

CALENDÁRIO:

- **Brazil Automation 2010**
http://www.isasp.org.br/site/newsletter/Novembro_2010_pag_6

- **Calendário oficial de eventos para o ano de 2010 atualizado**
http://www.isasp.org.br/site/newsletter/Novembro_2010_pag_7

- **Associe-se à ISA**
http://www.isasp.org.br/site/newsletter/Novembro_2010_pag_8

ISA SEÇÃO SÃO PAULO PROMOVE EVENTO COM PARTICIPAÇÃO DA PETROBRAS - 14-10-2010

A ISA Seção São Paulo realizou no ultimo dia 14 de Outubro, na sede da ABM (Associação Brasileira de Metalurgia, Materiais e Mineração) mais um de seus Eventos Técnicos. O Evento trouxe o tema Aplicações e Tecnologias Atuais para Medição de Vazão.

O Evento contou com a participação de mais de 90 pessoas, que juntas puderam ter acesso as mais recentes informações sobre o tema.

A abertura do evento foi feito por Roberto Magalhães, da empresa HIRSA, com o tema "Medição multivariável de vazão termal para gases e aplicações para dutos, flares e chaminés. A programação do Evento contou ainda com a apresentação de mais 02 palestras técnicas, ministradas por empresas detentoras da tecnologia em questão na seguinte seqüência.

• Uso de computadores de vazão, corretores de volume e transmissores multivariáveis e medição de gás: conceitos e diferenças operacionais – apresentada pela Emerson
• Tecnologias para medição de vazão fiscal de líquidos – apresentada pela KFW

Ao final das apresentações técnicas, o Sr. José Alberto Pinheiro, da Petrobras, fez uma importante palestra sobre Medição de vazão no Pré-Sal, trazendo ao público presente os desafios e necessidades que serão demandados pela Petrobras e pelo Brasil nesta nova realidade de exploração de petróleo.

Ao término das apresentaçòes, os participantes puderam participar de um sorteio, onde foram distribuídas duas filiações da Seção SP, além de outros prêmios. Após o sorteio, foi oferecido um coquetel de confraternização que foi servido nas dependências da ABM, o que acabou aproximando a todos e servindo de um excelente canal de networking.

O próximo Evento a ser realizado pela Seção SP acontecerá no mês de Novembro, em Santo André, na Unidade da Braskem e que terá o tema Contrato de Manutenção Envolvendo Desempenho e Disponibilidade.

Soluções National Instruments para barramentos industriais

Os Controladores Programáveis para Automação (PACs) da National Instruments e o software LabVIEW podem adicionar uma larga variedade de funcionalidades a controladores lógicos programáveis (CLPs) e sistemas industriais. Monitoramento de condição de máquina, medições analógicas de alta velocidade e aplicações personalizadas de visão são alguns exemplos típicos de aplicações PAC. A comunicação entre sistemas PAC e CLP é extremamente importante e deve ser simples, efetiva e normalmente determinística. Os métodos comuns incluem usar basicamente E/S analógica e digital, bem como o padrão mais difundido, OLE para Controle de Processo (OPC). Para sistemas fieldbus mais complexos, existe um grande número de protocolos industriais utilizados em processos de automação, construção de máquina e outros mercados. Este artigo explica como você pode usar comunicações industriais para conectar suas redes existentes com LabVIEW e PACs.

Tabela de Barramentos Industriais

Esta tabela mostra a lista completa de produtos da National Instruments para comunicações industriais e seus fatores:

Protocolo	PXI	PCI	CompactRIO	PCMCIA	USB	Outros
CANopen	√	√	~	√	~	
DeviceNet	√	√		√		
DNP3	√		√			Single-board RIO, PCs Windows
EtherCAT	√		√			NI 9144
EtherNet/IP	√	√	√			Controladoras Vision
FOUNDATION Fieldbus		√		√	√	
Modbus Serial e TCP	√	√	√			
PROFIBUS	√	√				

Abaixo está um breve resumo de cada protocolo e da oferta de produtos de software e hardware da NI relacionados.

Modbus TCP e Modbus Serial

Modbus TCP e Modbus Serial são dois dos protocolos industriais mais comumente utilizados no Mercado. O LabVIEW introduziu o suporte nativo para Modbus TCP e Modbus Serial em qualquer porta Ethernet ou serial com dois módulos adicionais do LabVIEW: Módulo LabVIEW Real-Time e Módulo LabVIEW Datalogging Supervisory Control (DSC). Qualquer um destes módulos permite criar um servidor Modbus TCP ou Modbus Serial I/O através de um assistente de configuração gráfico.

Com apenas alguns clicks no mouse, você pode criar um Modbus mestre ou escravo e especificar os diferentes registradores para ler e escrever. Visite a página www.ni.com/swf/demos/us/labview/dscmodbus para uma demonstração em vídeo de como criar um servidor Modbus I/O com LabVIEW.

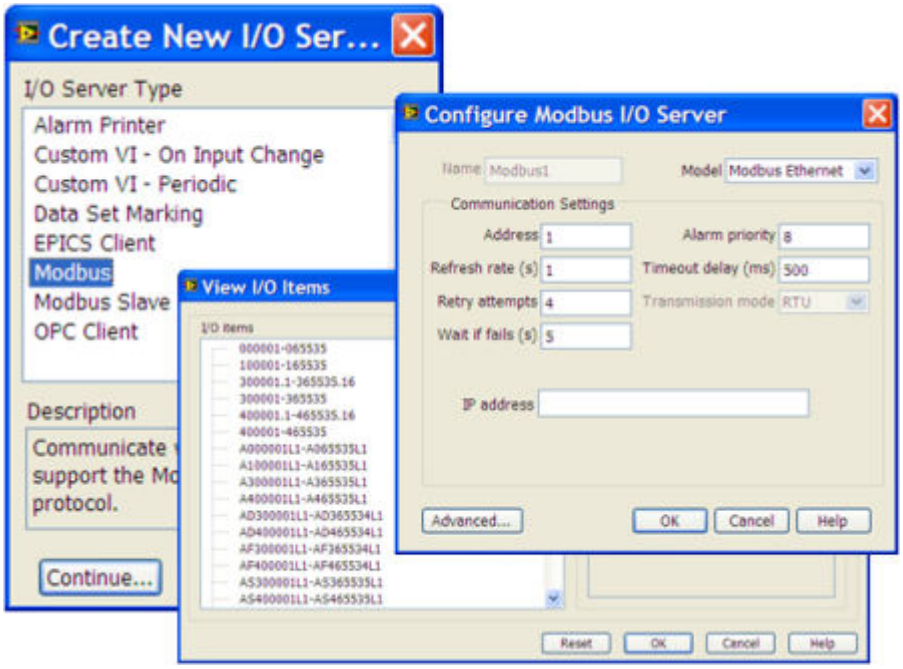


Figura 1. *Crie um servidor Modbus I/O usando o LabVIEW Real-Time e o LabVIEW DSC.*

Se você está utilizando uma versão antiga do LabVIEW ou não possui os módulos LabVIEW Real-Time ou LabVIEW DSC, você pode usar a Biblioteca LabVIEW Modbus gratuita para criar aplicações Modbus mestre ou escravo com quaisquer portas Ethernet ou serial. Esta biblioteca fornece um conjunto de VIs de baixo nível para maior flexibilidade, desempenho e personalização. Baixe a Biblioteca LabVIEW Modbus para começar a programar suas aplicações Modbus em http://sine.ni.com/nips/cds/view/p/lang/en/nid/201711.

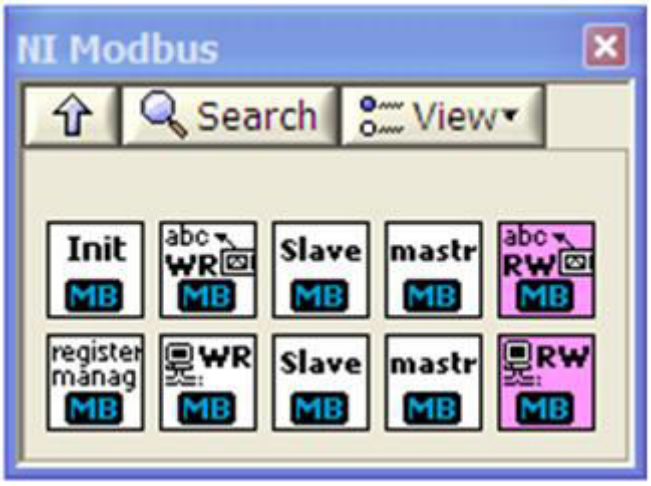


Figura 2. *A Biblioteca LabVIEW Modbus fornece funções de baixo nível para maior flexibilidade e desempenho.*

O Modbus TCP é também uma ferramenta útil para utilizar gateways para uma grande variedade de opções de conectividade.

PROFIBUS

PROFIBUS é um protocolo serial RS485 industrial que foi originalmente desenvolvido na Europa e tem se tornado um dos tipos de fieldbus mais populares do mundo. Com mais de 20.000.000 de nós instalados, o PROFIBUS é o padrão de comunicação para CLPs de Sistemas de Automação, sensores inteligentes, atuadores e E/S. Existem duas variações de PROFIBUS: a mais comum, conhecida como DP (Periféricos Distribuídos), a qual a NI suporta, e a menos usada chamada de PA (Automação de Processo).

Figura 3. *A NI oferece interfaces PROFIBUS DP mestre e escravo para PCI, PXI e CompactRIO.*

As interfaces PROFIBUS para PCI, PXI, e CompactRIO da NI conectam controladores baseados em PC a redes industriais PROFIBUS como poderosos mestres ou escravos. As interfaces PROFIBUS da NI incluem um configurador autônomo e um driver NI LabVIEW para interface homem-máquina (IHM) e aplicações SCADA. Você pode desempenhar testes automáticos em dispositivos PROFIBUS usando estas interfaces. A API de programação trabalha com LabVIEW e Módulo LabVIEW Real-Time e inclui exemplos pré-configurados.

EtherCAT

EtherCAT (Ethernet for Control Automation Technology – Ethernet para Tecnologia de Controle de Automação) é um protocolo industrial de comunicação, de alto desempenho, para Ethernet determinística, popularmente conhecido na Europa. Publicado como parte do IEC 61158, este padrão aberto implementa uma arquitetura mestra escrava cascateada sobre cabeamento padrão Ethernet, tipicamente em uma topologia linear. Como um barramento de controle, ele foca no determinismo, alta velocidade de E/S para aplicações de ponto único, como controle de máquina e movimento.

A National Instruments oferece ambos os dispositivos, o mestre e o escravo, que são compatíveis com o padrão EtherCAT. Para controladoras mestre, você pode usar PACs em tempo real da NI com duas portas Ethernet sobre o NI CompactRIO, PXI, e plataformas de controladores industriais. A NI também fornece o primeiro dispositivo

escravo EtherCAT com FPGA (field-programmable gate array) embarcado, o Chassi NI 9144 de 8 slots para módulos de E/S da Série C.

Figura 4. *A controladora CompactRIO conecta com o chassi escravo EtherCAT NI 9144.*

Para programar a controladora NI mestre, o LabVIEW Real-Time acessa os canais físicos dos escravos com um simples clique, arrastando a variável de E/S. Você pode também usar o Módulo LabVIEW FPGA para programar a lógica sobre um FPGA do chassi NI 9144, permitindo-lhe reduzir o tempo de resposta tomando decisões no nó. E mais, estes dispositivos distribuídos inteligentes podem descarregar o processamento da controladora com análises integradas, temporização personalizada e manipulação de sinal antes de enviar os resultados de volta ao mestre.

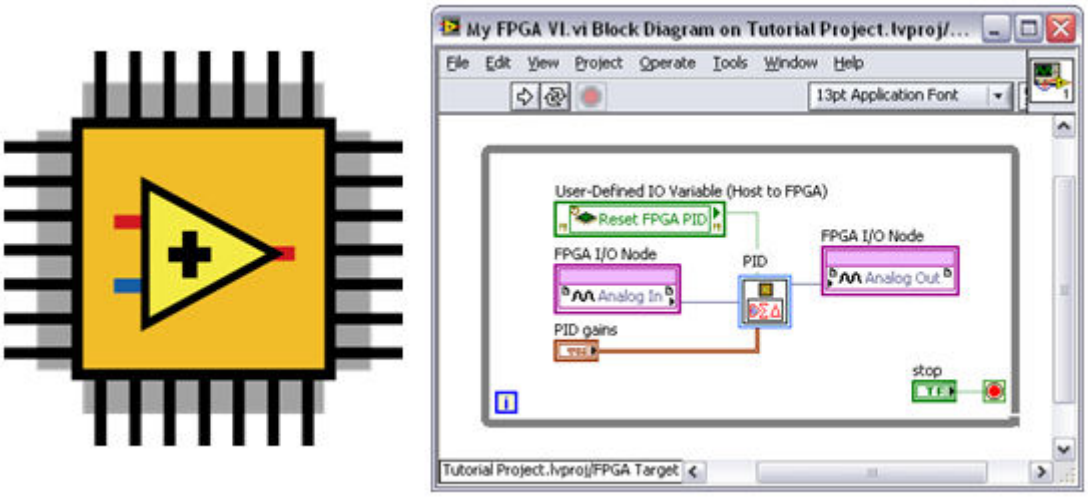


Figura 5. *O LabVIEW fornece uma fácil ferramenta de programação gráfica para a controladora NI EtherCAT e o chip FPGA do NI 9144.*

EtherNet/IP

EtherNet/IP é também um protocolo Ethernet em tempo real, gerenciado pela Open DeviceNet Vendors Association (ODVA) e comumente encontrado em CLPs Rockwell Automation (Allen-Bradley). Ele se comunica sobre o padrão Ethernet usando TCP/IP e UDP/IP usando uma arquitetura de rede mestre (scanner) e escravo (adaptador).

A NI oferece o driver EtherNet/IP para comunicação industrial gratuita para baixar no NI Labs. O driver é suportado no LabVIEW rodando em Windows (como PCs desktop),

bem como em sistemas NI LabVIEW Real-Time (como controladoras PXI, CompactRIO e de visão). Instalando o software sobre a controladora de sua escolha o LabVIEW lhe fornece funções tanto para mensagens explícitas como adaptadores de comunicação. O LabVIEW pode usar mensagem explícita para ler e escrever para tags em um CLP suportado pela RSLogix 5000 e RSLogix 500. O adaptador de comunicação permite ao LabVIEW funcionar como um escravo (adaptador), fornecendo dados implícitos de E/S para um CLP remoto.

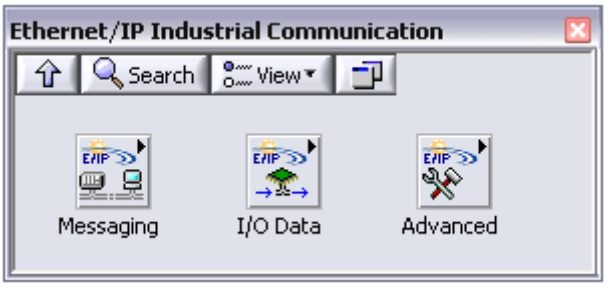


Figura 6. *O Driver EtherNet/IP de Comunicação Industrial fornece mensagem explícita e adaptador de comunicação do LabVIEW.*

DeviceNet

DeviceNet é outro protocolo industrial que a ODVA gerencia e é comumente encontrado em CLPs Rockwell Automation (Allen-Bradley). Diferente do Ethernet/IP, que é baseado na camada física Ethernet, o DeviceNet é baseado na camada física CAN e aumenta a interconectividade especificando vários parâmetros, como o comprimento de cabo requerido, conectores e baud rates.

A NI oferece duas plataformas de interface DeviceNet para aplicações de controle e testes. DeviceNet para Controle fornece interfaces mestre (scanner) PCI e PXI projetadas para gerenciar facilmente e controlar uma rede cheia de escravos DeviceNet. Incluso com estas interfaces esta o software NI-Industrial Communications for DeviceNet, que oferece uma API de alto nível que suporta arrastar e soltar variáveis de E/S interligando blocos de funções de mensagem explícita. Interfaces DeviceNet para Teste PCI, PXI, e PCMCIA tem suporte a mestre (scanner) e escravo (adaptador), melhor usado para testar produtos DeviceNet. O software incluso consiste de um configurador, analizador, e o driver NI-DNET, o qual fornece funções de baixo nível para criar aplicações DeviceNet personalizadas.

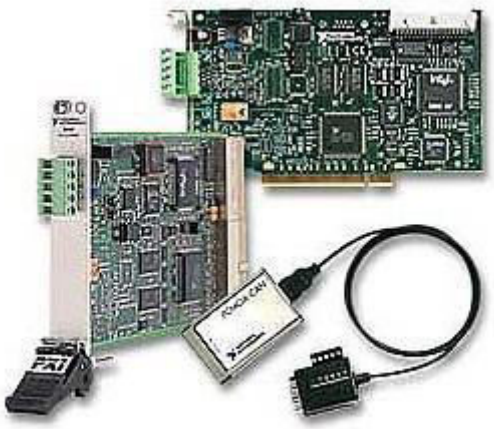


Figura 7. *As interfaces NI plug-in DeviceNet são projetadas para aplicações de controle e teste.*

CANopen

CANopen é um protocolo de alto nível também baseado na camada física CAN e foi desenvolvido como uma rede integrada padronizada com capacidades de configuração altamente flexíveis. Originalmente projetado para aplicações de controle de movimento, o protocolo CANopen é comum em muitos segmentos industriais incluindo equipamento médico, veículos fora da estrada, transporte público e automação predial.

Para a funcionalidade mestre do CANopen, a National Instruments oferece a Biblioteca CANopen LabVIEW, a qual fornece funções LabVIEW de alto nível, fácil de usar, para criar aplicações mestre CANopen. Ela fornece funcionalidades que cobre todo o espectro de aplicações mestre CANopen, incluindo transmitir e receber service data objects (SDOs) e process data objects (PDOs), gerenciamento da rede, baud rate, nós de segurança, e objetos de sincronização. Como as funções CANopen trabalham sobre o driver NI-CAN, todos os dispositivos de alta velocidade NI Series 2 CAN podem operar como interface CANopen mestre totalmente funcional. Isto inclui as plataformas PCI, PXI e PCMCIA. Para outros fatores, tente exemplos de programas CANopen para CompactRIO e USB, como alternativa da biblioteca LabVIEW CANopen.

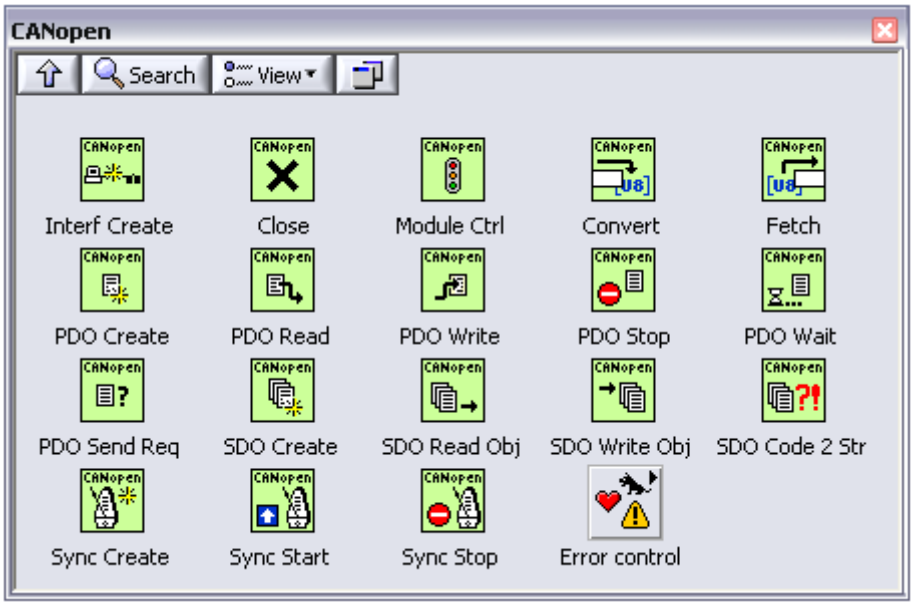


Figura 8. *A Biblioteca LabVIEW CANopen consiste de uma larga variedade de funções para aplicações mestre.*

DNP3

DNP3 (Distributed Network Protocol) foi desenvolvido pela GE Harris para criar uma especificação de protocolo para fabricantes de componentes SCADA (Supervisory Control and Data Acquisition) para padronizar redes de energia. Desde 1993, este protocolo aberto e público tem sido gerenciado pela DNP3 Users Group. O DNP3 é comumente usado nas distribuições elétricas de água Norte Americana para comunicação entre estações SCADA mestres e estações remotas como Unidades de Terminal Remoto (RTUs).

A NI oferece o driver NI-Industrial Communications for DNP3 para programar targets NI LabVIEW como dispositivos de estações remotas DNP3 com funcionalidades avançadas, como monitoramento de qualidade de energia, medições de fase, e outras análises relacionadas a redes inteligentes. Estas funções podem ser programadas em computadores Windows para desenvolvimento e depois implementadas em controladoras de tempo real da NI como CompactRIO, Single-board RIO, PXI, e PXIe para aplicações em campo. O driver DNP3 suporta comunicação Ethernet, transferência de arquivo e tempo de sincronização entre mestre e estações remotas. Também podem ser usados múltiplos canais de comunicação por estação remota e múltiplas sessões (dispositivos lógicos) por canal.

Figura 9. *O driver NI-IndCom for DNP3 consiste de uma larga variedade de funções para aplicações de estações remotas.*

FOUNDATION Fieldbus

FOUNDATION Fieldbus é um protocolo de comunicação totalmente digital e serial de duas vias, comumente usado em processos de automação. Ele usa sistema de controle distribuído com dispositivos inteligentes, onde o sistema de controle pode ser baixado para os dispositivos em vez de um sistema de controle central. O FOUNDATION Fieldbus tem duas versões, H1 e HSE (High Speed Ethernet – Ethernet de Alta Velocidade) e as interfaces da NI suportam a versão mais popular, H1.

As Séries NI USB-8486, PCI-FBUS e PCMCIA-FBUS são interfaces FOUNDATION Fieldbus que conectam dispositivos Foundation Fieldbus a desktops, PCs industriais e notebooks. Com a PCI-FBUS, um computador desktop industrial pode atuar como o host em um sistema FOUNDATION Fieldbus. Para aplicações usando o USB-8486 e o PCMCIA-FBUS inclui log de dados portátil, configuração de campo e manutenção de dispositivos e de rede.

Figura 10. *A NI oferece interfaces Fieldbus USB, PCI, e PCMCIA com uma variedade de opções de programação.*

O NI-FBUS Communications Manager (CM) é incluso com as interfaces Fieldbus e inclui funções Fieldbus que podem ser programadas em LabVIEW, NI Lookout, Microsoft Visual C / C + + e Visual Basic. NI também oferece o NI-FBUS Fieldbus

Configurator para configuração e programação dos blocos de função, bem como o NI-FBUS Monitor para a análise e depuração de pacotes de dados Fieldbus.

Saneamento de alarmes nas unidades da RLAM, a partir de técnicas de gerenciamento

Larissa S. Severo
larissa.severo@br.yokogawa.com
Yokogawa Service Ltda.

Francisco Neves Brasileiro Neto
francisco.brasileiro@br.yokogawa.com
Yokogawa Service Ltda.

Leandro Ariel Caputo
leandro.caputo@petrobras.com.br
Petrobras - RLAM

Sistemas de Alarmes

Sistemas de Alarmes são projetados para fornecer as indicações necessárias para o operador intervir no processo e corrigir uma condição anormal na planta, retornando o processo ao seu estado normal, ou para prevenir que o processo convirja para uma condição anormal e insegura. Alarmes devem alertar o operador a uma mudança, informá-lo da natureza da mudança e orientá-lo a fim de tomar uma ação de correção.

Entretanto, um sistema de alarmes configurado inadequadamente pode gerar uma quantidade excessiva de alarmes. A era dos sistemas digitais, introduziu práticas de custo zero para adição de alarmes: na dúvida, configure um alarme; alarmes são configurados em *startup* e não são mais modificados. Quando esses são gerados desnecessariamente, acabam por interferir na habilidade do operador, usuário final do sistema, de atingir/corresponder aos objetivos de desempenho da planta.

A principal questão com sistemas de alarmes é que há muita informação para o operador assimilar e agir prontamente. De acordo com a EEMUA (*Engineering Equipament and Materials Users Association*), o operador deve ter, pelo menos, 10 minutos para poder avaliar corretamente cada alarme em uma planta operando em condições estáveis, sem perda do seu desempenho em outras atividades de sua responsabilidade; em condições de instabilidade, o número de alarmes recebidos pelo operador não deve ser superior a 1 por minuto, para garantir que todos os alarmes sejam observados; o número de alarmes contínuos não deve ser superior a 10, para que a lista de alarmes não fique poluída e o operador possa determinar quais alarmes realmente estão pendentes; o percentual de tempo com a planta operando em condições de instabilidade deve ser inferior a 1%. Por sistema instável entende-se o período onde cada operador recebe mais de 30 alarmes em uma hora; a distribuição de prioridades dos alarmes ativos deve ser: 80% de alarmes de baixa, 15% de alarmes de média, 5% de alarmes com alta prioridade. Entretanto, os valores típicos reportados para diferentes tipos de indústrias mostram um cenário distante do ideal, como observado na Tabela 1.

Tabela 1: Volume de alarmes recomendado pela EEMUA e o típico encontrado em diferentes setores industriais (Fonte: Pinto e Farina, 2007).

	EEMUA	Óleo & Gás	Petroquímica	Energia
Média de alarmes por dia	144	1200	1500	2000
Média de alarmes constantes	9	50	100	65
Pico de alarmes por 10 minutos	10	220	180	350
Média de alarmes por 10 minutos	1	6	9	8
Distribuição de prioridade (%) Baixa/Média/Alta	80/15/5	25/40/35	25/40/35	25/40/35

O maior problema em sistemas de alarmes são os alarmes falsos, disparados na ausência de situações anormais ou quando nenhuma ação do operador é necessária. Uma freqüente causa desses alarmes é a manutenção. A ocorrência desses alarmes desnecessários pode fazer com que os operadores reconheçam alarmes sem dar a devida atenção e sem fazer o juízo necessário sobre os mesmos. Outro problema comum são os alarmes continuamente ativados ou porque nenhuma ação do operador é exigida ou porque não são liberados após a ação. Esses alarmes mascaram outras mensagens e acabam levando o sistema ao descrédito e, consequentemente, alarmes importantes passam despercebidos.

Outro problema mais perigoso e complexo de se solucionar é a enxurrada de alarmes usualmente associada a um evento. Essa enxurrada sobrecarrega o operador tornando difícil determinar a causa do evento. A falta de clareza nas mensagens de alarmes reais também é um fator prejudicial; quando a causa ou a resposta ao alarme não está clara, a ação desejada é retardada ou não tomada, tornando o alarme ineficaz.

De acordo com pesquisas no setor industrial, a ineficiência nas estratégias de gerenciamento de alarmes tem um impacto negativo nas operações, no desempenho, na lucratividade e na segurança da planta. Por exemplo, segundo O'Brien & Woll (2004), as perdas por desvios em alarmes pode representar um custo típico de 2 - 6 mil dólares por alarme ou pode causar uma perda de carga de batelada. Em plantas de processos complexo, um alarme de emergência pode escalonar para um incidente e resultar em uma parada. Paradas não programadas chegam a custar de 2% a 5% da produtividade anual. Ainda, segundo estudos da ARC Advisoy Group, associam-se ao custo de sistemas de alarmes mal configurados: à redução de qualidade, à perda de tempo de produção, o prejuízo aos ativos de producção e o riscos a vida humana.

Gerenciamento de Alarmes

Para solucionar esses problemas surgiu o Gerenciamento de Alarmes que corresponde ao processo e as práticas para determinação, documentação, projeto, monitoramento e manutenção das mensagens de alarmes que advém de um processo automatizado e sistemas de segurança, conforme o comitê de pesquisa 18 da ISA. Este recentemente aprovou a norma S18.2 (*Management of Alarm Systems in the Process Industries*, 2009), que tem o propósito de estabelecer a terminologia e as práticas de sistemas de alarmes, incluindo: definições, instalação, operação, manutenção e modificações para um gerenciamento eficiente ao longo do tempo. Essa norma está baseada na publicação N°191 da EEMUA (2004), que tem sido a referência mais utilizada para auxiliar no projeto adequado de novos sistemas de alarmes e na otimização dos existentes, devido aos parâmetros definidos a partir da experiência de diversas industrias de grande porte. Esse guia é focado em quatro áreas do sistema de alarmes: segurança, operação, engenharia e monitoramento do desempenho.

As boas práticas de gerenciamento de alarmes devem distinguir claramente alarmes de alertas. Alertas tem a funcionalidade de advertir, mas não exigem necessariamente uma ação imediata. Alarmes não devem ser usados como advertência e devem sempre exigir uma ação do operador (O'Brien & Woll, 2004). Abaixo, outras características de alarmes:

- Alarmes são para pessoas: se o operador não consegue tomar uma ação a respeito do alarme, então, não deveria existir tal alarme; deve ser relevante, claro e de fácil interpretação; deve permitir um tempo para resposta; não deve ser excessivo (sem enxurrada de alarmes).
- Alarmes não são para condições "normais". Exemplos: não distrair o operador com um alarme que informe que o processo automatizado avançou etapa por etapa (mudanças de estados e evolução de processo devem ser indicadas em telas gráficas e não através de acionamento de alarmes); não se deve acionar alarmes para informar que o equipamento está em modo OFF, a menos que ele esteja em OFF quando deveria estar em ON.
- Alarmes devem informar a verdade, por exemplo, equipamento fora de serviço não deve gerar alarmes.

A elaboração e adoção de uma Filosofia de Alarmes é o primeiro passo para a implementação sistemática do Gerenciamento de Alarmes. O objetivo é estabelecer: *i)* a finalidade do sistema de alarme; *ii)* como os alarmes devem ser escolhidos; *iii)* como os alarmes devem ser priorizados; *iv)* manutenção e testes; *v)* gestão da mudança; *vi)* monitoração e avaliação (métricas) e *vii)* tratamentos de alarmes específicos (ex.: segurança). Reconhecidas as boas práticas de gerenciamento de alarmes, o segundo passo é estabelecer uma metodologia que forneça uma estruturação para executar essas melhores práticas e facilitar o melhoramento contínuo; metodologia seis-sigma, por exemplo. Posteriormente, há a necessidade de ferramentas que mensurem, rastreiem e arquivem o desempenho, fornecendo indicadores de qualidade e disponibilizando análises prontamente.

Gerenciamento de Alarmes na Refinaria Landulpho Alves - RLAM

O trabalho de gerenciamento de alarmes na RLAM surgiu após uma solicitação da coordenação de Confiabilidade à Automação, para que fosse feito um levantamento do perfil de alarmes da refinaria. Nesse levantamento, foi constatado que o volume de alarmes encontrava-se muito acima da faixa "Não Aceitável", recomendada pelo Centro de Pesquisas da Petrobrás (CENPES) e baseada na publicação N° 191 da EEMUA. Também foi constado que os alarmes por IOP (*input open*) representavam 40% a 60% do total, sendo que os dez instrumentos mais acionados (Top 10 ou *bad actors*) representavam 25% a 40%.

Inicialmente, o objetivo era tratar somente esses alarmes por IOP. Para tal, a estratégia adotada pela RLAM estabeleceu uma equipe de trabalho multidisciplinar:

i) um facilitador no Setor de Otimização e Automação: encarregado de manter uma estatística dos alarmes, a fim de direcionar os trabalhos, priorizando as malhas e instrumentos críticos (Top 10 IOP geral da refinaria). Para essa atividade, foi utilizado, como ferramenta de apoio, o EXAPLOG®, para acompanhamento contínuo dos alarmes acionados e intervenções dos operadores;

ii) um engenheiro de automação (consultor externo): responsável pela análise crítica das malhas priorizadas, especificando as causas básicas: range do instrumento, sintonia do controlador, problema físico com a instrumentação, processo (p. ex., tanque quase transbordando, com nível acima do máximo do medidor), etc., e encaminhando as medidas corretivas. Para problemas de instrumentação, era solicitado, pela operação, o serviço juntamente ao Setor de Manutenção;

iii) um facilitador no Setor de Manutenção e Elétrica: coordenava os trabalhos de uma equipe de quatro instrumentistas dedicados ao saneamento dos alarmes.

Avaliação do sistema de alarmes

Os parâmetros de referência para o desempenho do sistema de alarmes recomendados pela EEMUA (Tabela 2) foram utilizados para a análise da distribuição estatística por prioridade nas unidades da RLAM. Utilizou-se o número de operadores para calcular a quantidade de alarmes por minutos aceitáveis.

Tabela 2: Métricas de desempenho durante operação em regime permanente (Fonte: publicação N°191 EEMUA, 2004).

Taxa de Alarmes/operador	Nível de Aceitação
Maior que 1 por minuto	Não Aceitável
1 a cada 2 minutos	Demanda Excessiva
1 a cada 5 minutos	Gerenciável
1 a cada 10 minutos	Aceitável

A distribuição dos alarmes no tempo é a primeira análise que deve ser realizada em um sistema de alarmes. Esse estudo é o primeiro indicativo da saúde do sistema e serve como ponto de partida para as análises que virão em seguida. Em um sistema de alarmes com bom desempenho, essa distribuição não deve apresentar variações bruscas no tempo. Os resultados para as unidades da refinaria RLAM, para um período de nove meses, encontram-se nas Figuras 1 e 2.

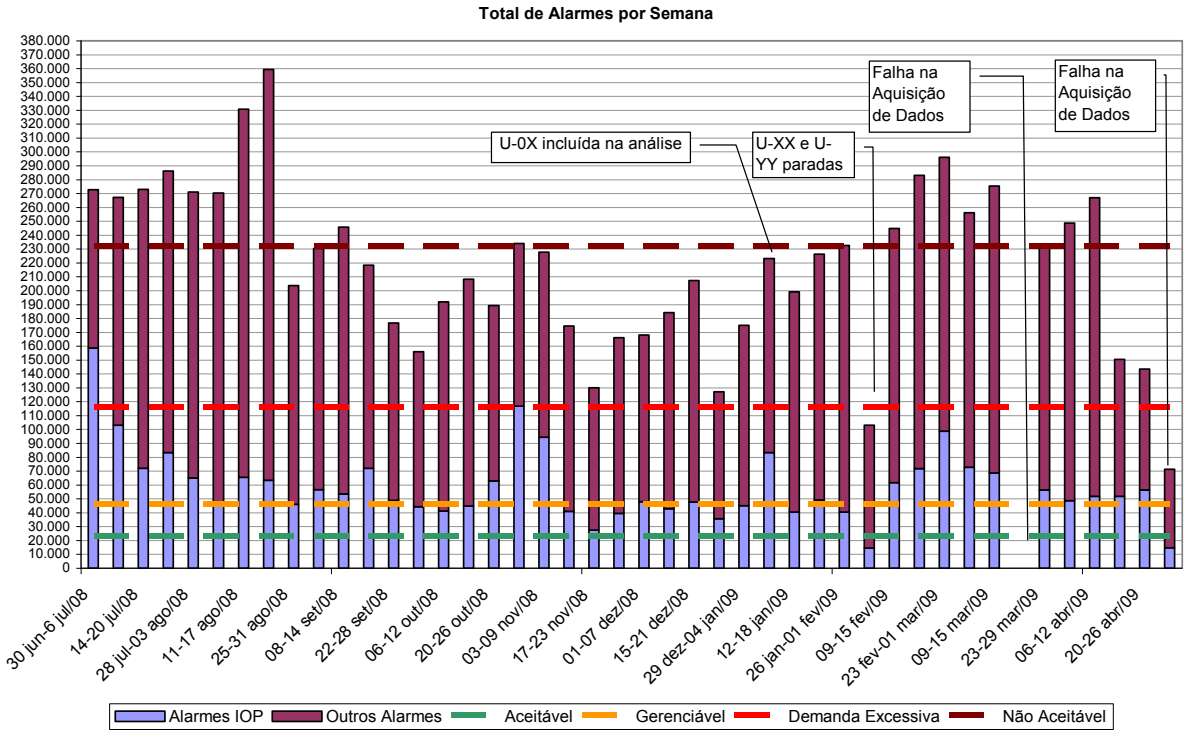


Figura 1: Distribuição dos alarmes no período de nove meses.

A partir da distribuição dos alarmes no tempo, é possível determinar períodos específicos onde ocorreu grande quantidade de alarmes. Na Figura 1, observa-se o período de 11-31 de agosto um volume superior à média dos outros períodos. Essa quantidade excessiva de alarmes é denominada enxurrada e ocorre quando a planta passa a apresentar comportamento instável. A análise dos dados de enxurrada de alarmes pode fornecer os primeiros indícios de alarmes configurados incorretamente; de que maneira os alarmes estão intervindo nas condições normais de operação.

Comparando o volume real com o volume recomendado pela EEMUA, o sistema de alarmes, no período avaliado, está gerando quantidades muito superiores as aceitáveis. Após o início do saneamento, percebe-se uma redução da demanda, porém, ainda insuficiente em relação os padrões utilizados.

A Figura 2 apresenta o volume de alarmes por IOP para o mesmo período, destacando os alarmes mais freqüentes. Essa tendência aponta os instrumentos que mais alarmaram em um determinado período. Na maioria dos casos, os alarmes no topo da lista são alarmes ruidosos. Eles podem representar em torno de 50% dos alarmes e devem ter prioridade para a redução de alarmes em uma planta.

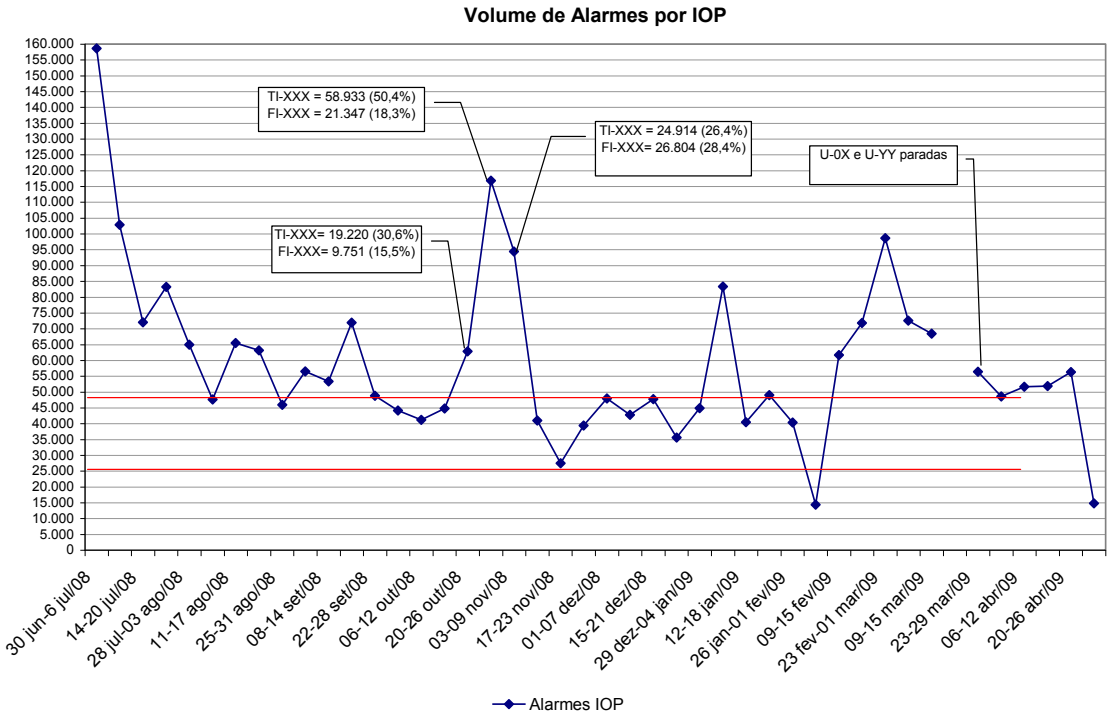


Figura 2: Volume de alarmes IOP para o mesmo período.

A partir da Figura 2, verifica-se que, após seis semanas, foi obtida uma redução de cerca de 65% no total de alarmes por IOP. Entretanto, existem períodos com picos de acionamento, especificamente de dois instrumentos que, entre 27/out e 09/nov, representaram mais de 50%, em média, dos alarmes acionados. A redução desses alarmes resulta numa melhora significativa do sistema de alarmes.

A monitoração do perfil de alarmes passou a ser mantida como rotina semanal na RLAM, abrangendo toda refinaria. Adicionalmente, iniciou-se um trabalho de saneamento dos alarmes de processo das unidades que apresentavam mais alarmes na refinaria: Planta de

Parafinas e Lubrificantes, Unidade de Craqueamento Catalítico, Unidade de n-Parafinas, Casa de Força e Destilações.

A mesma equipe de trabalho foi mantida com a inclusão de um facilitador da Operação, por unidade tratada. Foram selecionados os operadores mais experientes, deslocando-os para o turno administrativo com dedicação exclusiva ao saneamento de alarmes.

A duração do trabalho, por unidade, era cerca de duas a três semanas. Todos os instrumentos e malhas de controle deveriam ser avaliados pelo engenheiro de automação com o apoio do operador. Inicialmente, foram verificados aqueles instrumentos priorizados pelo levantamento estatístico, realizado pelo facilitador da otimização. Observou-se, por exemplo, que, em certas unidades, havia mais de 500 instrumentos alarmando no período de três meses, porém 33 deles eram responsáveis sozinhos por 85% do volume total de alarmes da unidade. Ainda, verificaram-se muitos alarmes associados a instrumentos que ou não estavam mais instalados no campo ou cujos equipamentos estavam desativados. Esses alarmes, evidentemente, foram excluídos.

Outra verificação importante que contribuiu para a redução dos alarmes: muitos alarmes de processo estavam muito próximos aos limites operacionais normais das unidades. Os pontos nominais de operação foram alterados ao longo do tempo em função de demandas da otimização ou desgastes dos equipamentos ou devido a projetos de ampliação (revamps), sem que os alarmes fossem devidamente re-parametrizados. As faixas de alarmes foram reavaliadas e configuradas de acordo com a definição estabelecida em conjunto pelos facilitadores da automação e da operação.

Uma convenção adotada, ao longo do desenvolvimento do saneamento, foi de, a princípio, excluir os alarmes de indicação muito alto (HH) e muito baixo (LL) para instrumentos que não estavam associados ao intertravamento das unidades. A Figura 3 apresenta o resultado do saneamento de alarmes de processo de uma unidade da RLAM; observa-se a redução significativa dos acionamentos.

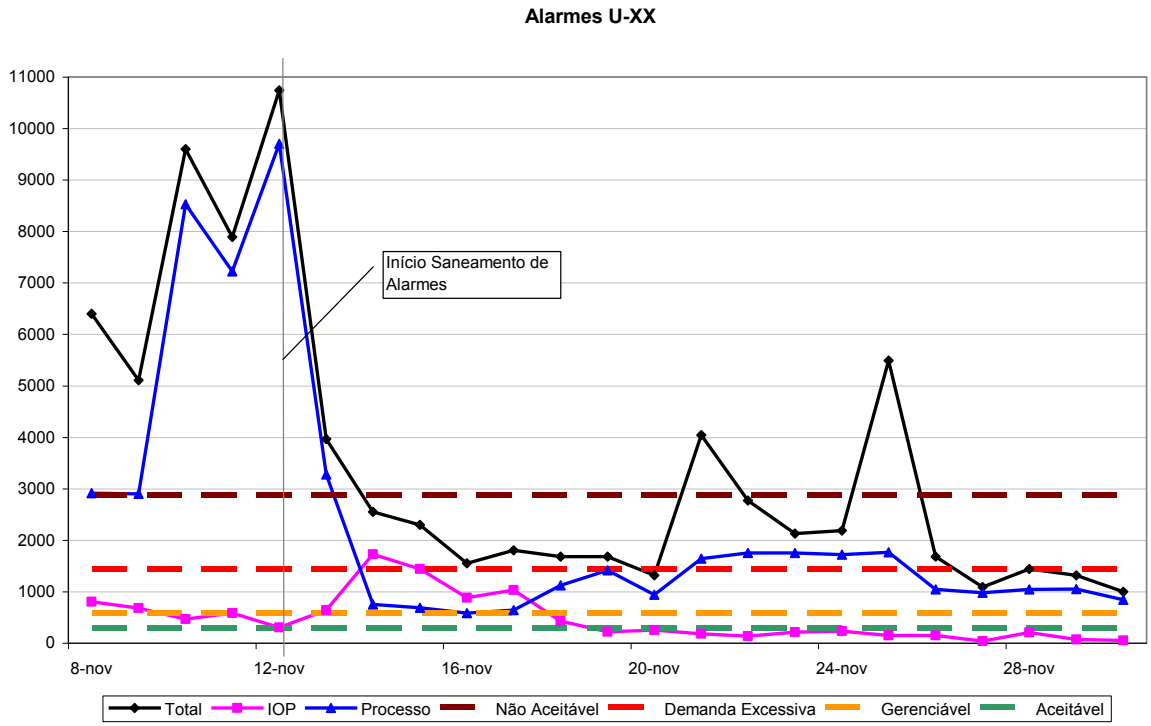


Figura 3: Distribuição dos alarmes diários de uma unidade (Total = IOP + Processo + Outros).

A Figura 4 apresenta a proporção de alarmes de processo modificados ou excluídos por unidades, resultados alcançados ao longo do trabalho de saneamento.

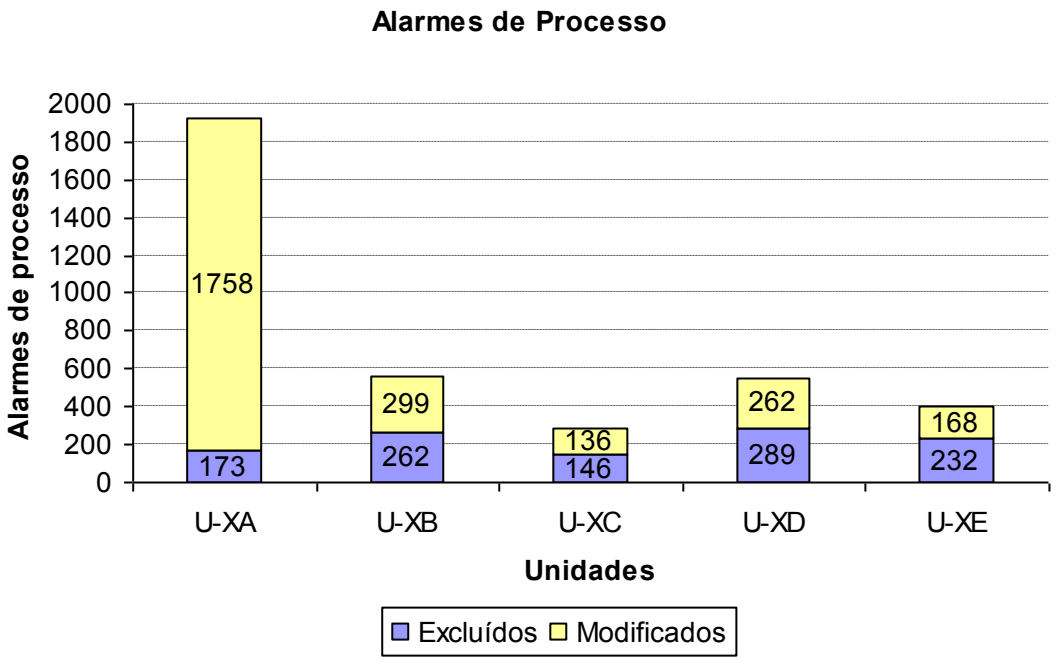


Figura 4: Saneamento dos alarmes de processo (muito alto, alto, muito baixo, baixo).

<u>Considerações Finais</u>

O saneamento de alarmes não objetiva simplesmente a redução dos alarmes. Essa conseqüência é resultado da má configuração inicial ou falta de atualização do sistema. O saneamento possibilitou a parametrização mais apropriada e consistente dos alarmes, assegurando que esses estejam projetados adequadamente; possibilitou também a eliminação de alarmes duplicados, a definição de uma mensagem clara e relevante, conforme a necessidade da operação.

A atividade de saneamento de alarmes na RLAM iniciou com o propósito de apenas reduzir a quantidade de alarmes da faixa "Não Aceitável" para um patamar inferior, atacando os *bad actors*. Após o relativo sucesso dessa etapa, a RLAM pretende expandir a metodologia para outras unidades, mantendo a equipe multidisplinar de trabalho para reavaliação dos alarmes existentes. Pretende-se obter, ao final da implementação do gerenciamento de alarmes, um manual do sistema de alarmes, como documentação para o processo de melhoria contínua.

Referências

[1] Alarm Systems – A Guide to design, management and procurement, EEMUA (Engineering Equipment and Material Users Association), Publication N° 191, 2004.

[2] O'Brien, L.; Woll, D. Alarm Management Strategies. ARC Strategies, 2004.

[3] Pinto, L. D.; Farina, L. A. Sistema de gerenciamento de alarmes em uma indústria petroquímica, ISA Show, 2007.

[4] Management of Alarm Systems for the Process Industries, ISA-SP18.2.

Sobre os Autores

Larissa S. Severo, Consultora Técnica – YOKOGAWA
Francisco Neves Brasileiro Neto, Engenheiro de Sistemas – YOKOGAWA
Leandro Ariel Caputo, Engenheiro de Processamento Pl. – Petrobras/RLAM

05 de Agosto de 2010 - Por Ian Verhappen, editor e contribuidor do site ControlDesign.com

Tecnologia Poe – O link perdido

Tem havido muita discussão sobre a Ethernet e o IP (Internet Protocol) como os próximos estágios na evolução da comunicação industrial. Um dos impedimentos ao uso da Ethernet no nível de campo tem sido a necessidade de puxar dois pares de cabos para os dispositivos - um para alimentação e outro para comunicação. Assim como no escritório, onde a tecnologia Power over Ethernet (PoE) conecta seu telefone IP com um único cabo, é possível fazer o mesmo no campo, pelo menos em teoria.

Digo "em teoria" porque, como em qualquer outra tecnologia, a Ethernet tem seus limites, tanto físicos quanto lógicos ou, mais precisamente, limitações de nível superior baseadas no protocolo. Os protocolos não são estritamente Ethernet, os quais que compõem as camadas inferiores do modelo OSI; mas, sem o protocolo para interpretar a mensagem transmitida pelas camadas Ethernet, tudo seria ruído.

A mais óbvia limitação na camada física é que a Ethernet é geralmente limitada a um comprimento máximo de 100 m nas suas derivações. Em muitos casos, isso não será um problema, mas para conectar um dispositivo a uma distância superior a esta, será necessária a instalação de hardware adicional para limpar e melhorar o sinal, levando-o de volta a níveis aceitáveis antes de retransmiti-lo por mais 100 m. Além disso, o número máximo de repetidores é limitado a quatro, a menos que você utilize fibra óptica. Porém, a fibra ótica não é compatível com a tecnologia Poe. Neste sentido, você precisará de um suprimento confiável de energia em cada um dos repetidores, caso contrário teremos o enigma do moto contínuo - energia para nada. Felizmente, com a tendência de salas de interface distribuídas, essa diferença média continua a diminuir.

A tecnologia PoE de classe industrial está ganhando força, com produtos disponíveis de diversos fabricantes. E, como eles são compatíveis com a norma 802.3af, eles são intercambiáveis e capazes de se conectar uns com os outros ou com componentes do ambiente corporativo, assim como outros produtos Ethernet.

A gama de equipamentos de rede PoE também inclui splitters – separam eletricidade do sinal de dados para os dispositivos incapazes de detectar Poe ou para derivar um ponto de alimentação - e injetores, que adicionam energia na rede em algum lugar que não seja o dispositivo final. O aumento do interesse em redes wireless e a necessidade por pontos de acessos wireless distribuídos parece ser a aplicação lógica que irá impulsionar a adoção da tecnologia PoE industrial.

Um segundo desafio para a tecnologia PoE para aplicações de automação é que o padrão 802.3af especifica uma tensão de 48 Vdc, enquanto que este negócio padroniza a tensão em 24 Vdc. Pelo menos um fornecedor de equipamentos industriais Ethernet tem um splitter PoE com saída em 24 Vdc.

Outra limitação de camada física, que ocorre em cerca de 20% das instalações, é a transmissão via Ethernet em uma área classificada. Há sempre a opção de gabinete à prova de explosão, mas também é possível ir com uma solução de segurança intrínseca da MTL e da Controlled Systems, fornecendo até 500 mA de energia ao longo de um cabo intrinsecamente seguro RJ45. Esta solução não é um padrão aberto, embora haja alguma discussão dentro do British Standards Institute (BSI) sobre a tentativa de desenvolver algo através da IEC (International Electrotechnical Commission) nesta área.

O hardware e o sinal físico associado são apenas uma parte da equação de comunicação; a outra parte é o protocolo ou linguagem utilizada. Infelizmente, é improvável uma única norma. Assim como com os protocolos fieldbus, é provável que tenhamos protocolos

divididos por indústria, tornando-os mais resistentes para os dispositivos de campo e para os fabricantes de sistemas de controle, visando justificar os gastos necessários para o desenvolvimento da tecnologia.

Nós estamos chegando lá. Esperemos que os dispositivos de campo Ethernet entrarão em breve no mercado em quantidade, e não apenas a fazer o mesmo sinal em maior largura de banda, mas como um facilitador para novas e inovadoras formas de fazer as coisas ou fazer medições. Minha nova aplicação favorita é um espectrômetro distribuído, semelhante a um termopoço com um LED para iluminação, arranjo de diodos para capturar os dados Ethernet e enviá-lo de volta a um sistema central de processamento. Nenhum sistema de amostra ou partes móveis.

A tecnologia PoE removeu o cabo único para um problema de dispositivo, mas limitações menores ainda precisam ser resolvidas. Esta tecnologia não é ainda uma bala de prata ou um elixir mágico, embora, espero que em breve, irá se aproximar disso. Mas isso é outra história para outro momento...

Brazil Automation 2010

Vem aí mais um Brazil Automation! Atualmente em sua 14ª edição, este é o maior evento de instrumentação, Sistema e Automação da América Latina e um dos mais importantes do mundo. Além de apresentar tendências tecnológicas e os mais expressivos lançamentos do mercado mundial, proporciona capacitação técnica e uma ampla integração entre usuários, fabricantes, distribuidores, pesquisadores, estudantes, prestadores de serviços e demais profissionais do setor, constituindo um ótimo ambiente para networking profissional, troca de informações e oportunidades de negócios.

O evento será realizado no mês de Novembro, entre os dias 09 e 11, nos pavilhões Branco 7 e 8 do Expo Center Norte, no endereço abaixo:

Rua José Bernardo Pinto, 333 – Vila Guilherme
São Paulo – SP – Brasil
Fone: +55 11 6224.5900
www.centernorte.com.br

CALENDÁRIO DE EVENTOS

Evento	Local	Dt. Inicio
NOVEMBRO		
Treinamento: Nova Regulamentação para Atmosferas Explosivas	São Paulo /SP	16-11-2010
Novas Metodologias de Contrato de Manutenção envolvendo Desempenho, Disponibilidade, dentre outras	Pólo Capuava - Mauá/SP	24-11-2010
DEZEMBRO		
Evento de Confraternização Anual - Sócios	São Paulo /SP	01-12-2010

FAÇA PARTE DE UM SELETO GRUPO DE PROFISSIONAIS

Conheça as vantagens:

- **NORMAS GRATUITAS** - Associados ISA tem acesso ao banco de normas técnicas, e na sua maioria são gratuitas para sócios. Para as normas pagas, associados recebem um desconto expressivo!
- **SEMINÁRIOS WEB** - Acesso livre e ilimitado a uma biblioteca de mais de 40 seminários on-line que cobrem os tópicos mais atuais do setor.
- **BIBLIOTECA TÉCNICA** - Acesso ilimitado a downloads a partir da biblioteca ISA, que possui mais de 2.500 documentos técnicos publicados em conferências/simpósios próprios.
- **REVISTA INTECH** - Assinatura gratuita da InTech Magazine (Inglês) e da InTech America da Sul (português), as duas publicações mais qualificadas para profissionais de automação.
- **DIVISÕES TÉCNICAS** - Una-se a uma rede de profissionais de automação que compartilham os mesmos interesses técnicos que você. Os membros estudantes ganham duas inscrições gratuitas em divisões técnicas.

Expanda sua rede de contatos:

- **ISAJOBS.ORG** - Inscrição on-line gratuita de seu currículo profissional.
- **SEÇÃO LOCAL** - Oportunidade de relacionamento com profissionais de automação em sua área local: para reuniões, treinamentos, eventos, e mais.

Desenvolvimento Profissional

- **OPORTUNIDADES DE LIDERANÇA** - Desenvolva suas habilidades de liderança participando de forma on-line e gratuita, do Leadership Development Certificate Program (Programa de Certificação e Desenvolvimento de Lideranças);
- **DESCONTOS** - Aproveite as vantagens exclusivas para membros associados, como ótimos descontos em produtos da ISA, treinamentos e inscrições em eventos;
- **CERTIFICAÇÃO E LICENCIATURA** - Orgulhe-se da sua profissão! A ISA oferece programas de certificação profissional como: Certificação de Profissional de Automação (CAP); Certificação de Técnico de Sistemas de Controle (CCST), e Certificação de Mecânico de Manutenção Industrial (CIMM), além do programa de licenciatura para Engenheiro de Sistemas de Controle (CSE);
- **PROGRAMA DE ORIENTADORES** - Estude on-line orientado pelos profissionais mais experientes do setor.

Taxas: **U$ 50 (profissional) e U$ 10 (Estudante)**