

MONITORAÇÃO DE DESEMPENHO DE REDES DE AUTOMAÇÃO USANDO SNMP¹

Marcos de Oliveira Fonseca²
Constantino Seixas Filho³
Alexandre Valente Duarte Ferreira⁴
René Silva Daré⁵

Resumo

Os sistemas de automação estão passando por uma grande transformação decorrente da inevitável integração entre os sistemas de TA e de TI e a convergência tecnológica. Dentro deste contexto, as redes de controle e de comunicação são a espinha dorsal das organizações, com destaque para as redes Ethernet. O correto funcionamento das redes de automação dentro dos quesitos de desempenho e confiabilidade garantem o perfeito atendimento das redes às exigências dos sistemas de automação e de negócios. O padrão SNMP, já consolidado em TI, passa a assumir uma posição de destaque para gerenciamento de redes em sistemas de TA, assim como garantia de desempenho e disponibilidade. Este trabalho apresenta as tendências do gerenciamento de redes, um importante ativo de automação, destacando a utilização prática em sistemas industriais.

Palavras-chave: Desempenho; SNMP; Redes; Automação.

¹ IX Seminário de Automação de Processos, Associação Brasileira de Metalurgia e Materiais, 05-07 de outubro de 2005 – Curitiba – PR, Brasil.

² ¹ Engenheiro Eletricista, M.Sc., Diretor da Divisão de Tecnologia da Automação da ATAN Sistemas, Belo Horizonte – MG, Brasil.

³ Engenheiro Eletrônico, M.Sc., Diretor de P&D da ATAN Sistemas, Belo Horizonte – MG, Brasil.

⁴ Engenheiro Eletricista, Gerente de Produto da ATAN Sistemas, Belo Horizonte – MG, Brasil.

⁵ Engenheiro de Controle, Engenheiro de Sistemas da ATAN Sistemas, Belo Horizonte – MG, Brasil

1 INTRODUÇÃO

O desenvolvimento tecnológico tem desempenhado um importante papel dentro das organizações, principalmente como motor para o crescimento dos negócios e de seus resultados. O mercado globalizado obriga as empresas a colocarem em prática as tecnologias de ponta com o objetivo de aumentar a agilidade e eficiência dos processos produtivos e dos sistemas de gestão. Neste contexto, dois fatores têm alterado a realidade dos sistemas de automação.

O primeiro é a inevitável integração entre os sistemas de Tecnologia da Automação (TA) e da Informação (TI). Esta integração permite que os processos produtivos tenham a agilidade exigida pela gestão no atendimento às demandas do mercado, e propiciam aos sistemas de gestão maior eficiência na tomada de decisões com base na real capacidade produtiva. O segundo é a convergência tecnológica observada para os sistemas de TA e TI. A constante busca por padrões abertos, tecnologias de ponta e custos reduzidos, tem feito com que o desenvolvimento tecnológico de sistemas de TA e TI busquem por soluções comuns.

As redes de controle dos modernos sistemas de TA e as redes de comunicação dos sistemas de TI desempenham um papel fundamental para a troca de informações entre o processo produtivo e a alta direção das empresas. A rede Ethernet é um padrão “de facto” para os sistemas de TI e é considerada pelos especialistas como a rede que será utilizada em todos os níveis dos sistemas de TA. O grupo ARC estima um crescimento anual de 51% no uso da rede Ethernet Industrial até 2009. Apesar de possuir características não determinísticas, a rede Ethernet TCP/IP tem sido utilizada com sucesso em sistemas de TA onde o tempo de resposta não é muito crítico (comunicação entre CLPs, sistemas de aquisição de dados e até remotas de controle). As soluções de mercado (segmentação de rede, priorização de serviços, equipamentos de rede e cabos para aplicação industrial, etc.) juntamente com a alta velocidade (100 Mbits/s, 1 e 10 Gbits/s) e com o baixo custo, tornam a Ethernet TCP/IP um forte padrão para todos os níveis de TA (sensores, instrumentos, etc.) mesmo para aplicações críticas. Outro termômetro importante, é a criação de organizações e entidades patrocinadas pelos principais fabricantes de sistemas de TA, com o objetivo de se estabelecer o padrão Ethernet TCP/IP para utilização plena na indústria. As principais entidades que estão neste processo são a IAONA (www.iaona.org), ODVA (www.odva.org), Modbus IDA (www.modbus.org), Fieldbus Foundation (www.fieldbus.org) e Profibus International (www.profibus.com).

Todas estas entidades já adotaram o padrão Ethernet TCP/IP para o chão de fábrica, sendo que as diferentes abordagens de cada entidade está na camada de aplicação (OSI/ISO). Ou seja, independentemente da abordagem vencedora, a mesma será baseada no meio físico Ethernet IEEE 802.3, na camada de rede IP e transporte TCP/UDP. A IAONA tem assumido um papel importante recentemente, devido ao fato de ser uma associação independente e desta estar conseguindo estabelecer alianças importantes com as demais entidades e organizações, de forma a definir soluções comuns. Um exemplo disso é um documento⁽¹⁾ disponibilizado pela IAONA, o qual apresenta diretrizes e recomendações para a instalação da rede Ethernet no ambiente industrial.

Com a consolidação da Ethernet TCP/IP no ambiente industrial, um conjunto de padrões complementares passam a fazer parte do mundo de TA. Um bom exemplo disso é o uso do *Simple Network Management Protocol* (SNMP). Este protocolo faz parte da suíte de protocolos TCP/IP (HTTP, FTP, SMTP, etc.) e já está disponível na grande maioria dos computadores e em todos os dispositivos de rede gerenciáveis. O SNMP é um protocolo simples destinado à monitoração e gerenciamento de redes que utilizam o padrão TCP/IP. A IAONA orienta em seu documento, que sejam utilizados servidores OPC para SNMP em soluções para gerenciamento de redes Ethernet em ambiente industrial. Equipamentos de automação, tais como CLPs, já disponibilizam o SNMP em suas interfaces de comunicação.

Independentemente das soluções de redes de TA e de TI, a crescente integração entre estes sistemas, juntamente com a crescente demanda por troca de dados e informações entre os mesmos, tornam as redes um ponto nevrálgico do *core business* das empresas. Problemas de desempenho e disponibilidade das redes comprometem todos os sistemas e conseqüentemente o resultado das organizações. Além disso, os sistemas de TA passam a ser vulneráveis para os aspectos de segurança contra acessos indevidos e ataques de hackers. A ANSI/ISA está elaborando uma nova norma, a ISA SP99, sobre segurança dos sistemas de automação, em função dos crescentes problemas observados pelas organizações. Portanto, torna-se imprescindível que as redes de automação e os sistemas como um todo sejam devidamente monitorados contra problemas de desempenho e segurança..

Este trabalho faz uma introdução ao SNMP e apresenta como o mesmo pode ser utilizado para a monitoração de desempenho, gerenciamento de mudanças (*Change Management*), diagnóstico e solução de problemas dos ativos de automação (CLPs, dispositivos de rede e estações) dentro da moderna filosofia do RPM (*Real-time Performance Management*).

2 SNMP NA AUTOMAÇÃO

O SNMP é um protocolo não orientado a conexões da suíte IEEE TCP/IP 802, definido por um conjunto de especificações (RFCs). O SNMP trabalha sobre a camada de transporte UDP, sendo uma implementação leve. Atualmente está na versão 3, a qual já suporta criptografia e controle de acesso, sendo que a grande maioria dos dispositivos suporta a versão 2c. Qualquer dispositivo inteligente para rede Ethernet pode ser um SNMP Agent. Atualmente, a maioria dos modernos dispositivos de rede para uso industrial ou não, assim como as estações de trabalho e até mesmo CLPs ou remotas são gerenciáveis. Isto é, estes dispositivos e equipamentos podem fornecer dados e informações através do protocolo SNMP para uma estação chamada de SNMP Manager (*Network Management Station* ou NMS). O Agente SNMP funciona como um servidor de dados de gerenciamento da rede para o Manager, o qual pode ler os dados dos agentes e enviar comandos, Figura 1.

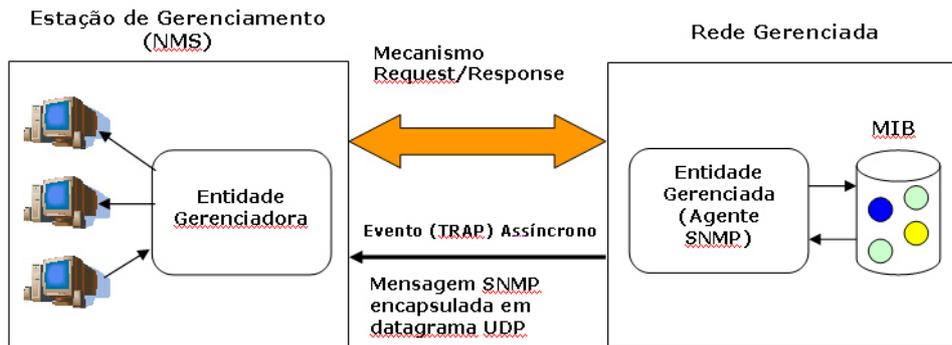


Figura 1. Agent e Manager SNMP.

As informações que os dispositivos gerenciáveis podem trocar entre si usando SNMP são definidas pelos MIBs (*Management Information Base*). Os MIBs são definições de dados para gerenciamento de redes TCP/IP especificadas por RFCs complementares. Atualmente a especificação está na versão 2, chamada de MIBII e já está em uso há muito tempo pelas equipes de TI. O MIB consiste de um conjunto de objetos de dados, os quais são chamados de OID (*Object ID*). Os OIDs são definidos em grupos, de acordo com suas características de aplicação, tipos de dados e permissões de leitura e escrita. Basicamente, os OIDs definidos como padrões são destinados ao gerenciamento de redes. Entretanto, OIDs complementares podem ser definidos pelos fabricantes de equipamentos para ampliar os MIBs padrões em função das necessidades da aplicação.

Os OIDs padrões fornecem dados sobre o estado, configuração e monitoração dos links de rede. As equipes de TI já utilizam estes dados para gerenciamento das redes no nível corporativo. As principais informações utilizadas atualmente são:

- Taxa de utilização dos links/portas
- Contadores de erros, colisões, pacotes, broadcast, unicast, etc.
- Endereçamento e estado das portas (link ativo/inativo)
- Tabelas de roteamento
- Configurações do dispositivo (portas do Spanning Tree, por exemplo)
- Utilização de recursos (processamento, memória, etc.)
- Outros

Os dados podem ser lidos pelo Manager ou ser enviados pelos Agentes como eventos (comunicação por exceção), denominados Traps SNMP. Somente os OIDs definidos como Trap no MIB podem ser enviados pelo Agent por exceção. Desta forma, é possível fazer uma monitoração de forma eficiente da rede como um todo. Tipicamente, os modernos dispositivos de rede disponibilizam diversos dados para cada porta. Um único switch com 24 portas pode disponibilizar mais de 4000 OIDs.

Recentemente, com o crescimento do uso da rede Ethernet nos sistemas de automação, os fabricantes de equipamentos para uso industrial (principalmente CLPs), começaram a disponibilizar módulos de comunicação com SNMP. Esta é uma tendência real para a monitoração de redes de automação, em todos os níveis. A especificação da IAONA para rede Ethernet industrial reforça esta tendência, através da publicação de uma especificação de MIB SNMP⁽²⁾ para aplicações industriais. Os fabricantes estão disponibilizando MIBs para os seus produtos, os quais acrescentam OIDs específicos para monitoração dos dispositivos de

automação. Alguns exemplos de OIDs adicionais encontrados nos MIBs de equipamentos de automação e da IAONA são:

- Dados e estados da aplicação (nome, parada, funcionando, etc.)
- Dados dos protocolos de controle usados (Ethernet/IP, ModbusTCP, etc.)
- Nome do dispositivo, número de série, nome do fornecedor, revisão do hardware, versão do firmware, etc.
- Outros

Apesar dos usuários de TI já fazerem uso de ferramentas de gerenciamento de rede no nível corporativo, alguns aspectos dificultam a sua utilização plena na automação. Os principais aspectos que dificultam o uso das ferramentas de gerenciamento de redes de TI na automação são:

- Não são projetadas para uso com sistemas industriais, principalmente quanto ao desempenho e aplicabilidade (requisitos inerentes aos sistemas de TA).
- Não permitem uma integração com os sistemas de automação (via OPC, por exemplo) para monitoramento em tempo-real das redes de automação.
- As equipes de TI não são responsáveis pela manutenção das redes de controle na maioria das empresas. Além disso, o universo dos sistemas de TA não faz parte da cultura de TI.

A falta de integração das ferramentas de gerenciamento de redes com os sistemas de automação, juntamente com os problemas de desempenho para aplicação em tempo real, obrigam aos usuários de TA a utilizarem soluções voltadas para as suas necessidades. A tendência observada no mercado de TA é a utilização de soluções baseadas em SNMP e OPC, juntamente com os sistemas de automação.

3 GERENCIAMENTO DE REDES INDUSTRIAIS E MONITORAÇÃO DE DESEMPENHO

A integração dos dados de gerenciamento de redes com os sistemas de automação ainda não é uma prática corrente. Entretanto, já são encontrados no mercado servidores OPC para SNMP. Através destes servidores, é possível a integração dos dados de gerenciamento de rede nos sistemas de automação (SCADA, SDCD, Híbridos, PIMS, MES, etc.) usando a comunicação OPC, a qual é um padrão “de facto”.

Um ponto importante a se observar no uso do SNMP em aplicações de TA, é que os sistemas de supervisão (SCADA, SDCD e Híbridos) reúnem características desejáveis para a monitoração de redes, tais como:

- a) Esses sistemas possuem um cliente OPC e a tendência atual é que sejam isoladas fisicamente as redes de nível 0 (campo) e 1 (controle) das redes de nível 2 (comunicação) e 3 (corporativa), através do uso de servidores de dados de processo (RTDS). Dessa forma, esses sistemas podem integrar a monitoração de redes em todos os níveis.
- b) A existência de operadores dedicados à utilização desses sistemas para monitoração do processo, permitem que os mesmos possam agir de forma pró-ativa no caso de problemas de desempenho de redes no momento de sua ocorrência (tempo-real), dentro da filosofia do RPM.

- c) No âmbito do RPM, além das informações de rede, estes sistemas podem reunir dados de desempenho dos elementos de automação (CLPs, instrumentos, etc.) e das estações de operação. Permitindo a geração de alarmes e diagnósticos para correção de problemas objetivando o aumento da disponibilidade dos sistemas. Essas informações já são disponibilizadas pelos elementos de automação ou podem ser acessadas através de servidores OPC disponíveis no mercado (como acesso aos contadores de performance das estações Windows, por exemplo).
- d) Esses sistemas integram também outras redes de automação (Profibus, Fieldbus, ControlNet, Modbus, etc.), as quais também já disponibilizam dados de desempenho via OPC, permitindo que todas as redes sejam monitoradas.
- e) Estes sistemas normalmente são integrados aos níveis superiores (PIMS, MES, ERP, etc), de forma que as informações de gerenciamento de redes possam ser compartilhadas, principalmente para gerenciamento de ativos e de mudanças.

Em função das características acima, os sistemas de supervisão passam a ser ambientes desejáveis para a monitoração de redes de automação.

A monitoração de redes de automação, principalmente a rede Ethernet, permite que problemas críticos sejam devidamente controlados antes que os mesmos causem impactos indesejáveis no controle do processo. Problemas crônicos que devem ser devidamente monitorados são:

- Defeitos na infra-estrutura física da rede, tais como quebra de cabos, problemas de conexão e atenuação de sinais, falha em equipamentos de rede, etc.
- Comprometimento da banda de comunicação devido a excesso de tráfego oriundo de defeito nos equipamentos, aumento da demanda de uso, presença de vírus ou invasões no sistema, configurações inadequadas, etc.
- Degradação de desempenho devido a gargalos de comunicação dos dispositivos de rede (hubs, switches, routers, firewalls, gateways), assim como CLPs, estações de operação, etc.

Os fatores que promovem a ocorrência dos problemas acima devem ser devidamente monitorados e ações preventivas e corretivas devem ser tomadas de forma pró-ativa para evitar que o desempenho e a disponibilidade dos sistemas de automação sejam comprometidos, chegando a impactar nos resultados da empresa. Atualmente, observa-se em muitas empresas que esses problemas não são devidamente entendidos e monitorados, fazendo com que os ativos de automação (controladores, redes, estações, etc.) estejam sujeitos a problemas de lentidão e erros indesejáveis, os quais levam a uma redução da eficiência, paradas e até mesmo sinistros. Essas são questões que devem ser solucionadas dentro da realidade da Excelência Operacional.

O gerenciamento de mudanças também deve ser considerado de forma pró-ativa. Os sistemas de TA não param de crescer e novas funcionalidades são continuamente adicionadas às configurações existentes. Dessa forma, manter um registro do comportamento das redes ao longo da vida útil dos sistemas e analisar a tendência de como os mesmos evoluem, é fundamental para evitarmos que os problemas venham a ocorrer. A integração da monitoração das redes aos sistemas PIMS, permitem um acompanhamento de longo prazo, sendo uma solução adequada para sistemas de TA.

As empresas também devem se preparar para adequar os seus sistemas à realidade dos riscos de segurança de redes para os sistemas de TA, decorrentes da vulnerabilidade a invasões aos quais os mesmos estão sujeitos. Um dos aspectos relevantes cobertos pela norma ISA SP99 é a monitoração dos ativos de automação visando a identificação de comportamentos suspeitos e disparando ações de contenção, as quais devem ser condizentes com os sistemas de TA.

O SNMP permite que comandos sejam enviados para os dispositivos de rede, principalmente com a finalidade de alterar configurações. Este recurso pode ser explorado para reconfiguração de sistemas no caso de falhas ou mesmo de comportamento anormal. Entretanto, nos sistemas de TA, o envio de comandos deve ser feito de forma cautelosa para não comprometer a estabilidade da comunicação.

4 CASO PRÁTICO

Para verificarmos como o SNMP pode ser utilizado em sistemas de TA, iremos apresentar os resultados práticos da utilização de um servidor OPC para SNMP, o qual pode ser integrado a sistemas SCADA e sistemas PIMS.

A idéia de se usar o protocolo SNMP para transportar informações de outros dispositivos que não sejam equipamentos de rede não é nova. A Telemig, hoje Telemar, e a UFMG desenvolveram na década de 90 o SIS - Sistema Integrado de Supervisão que envia a uma central de operações alarmes de toda natureza, descrevendo as atividades de estações distribuídas de telecomunicações, usando o protocolo SNMP.⁽³⁾ Na central de controle vários canhões projetam uma visão unificada dos alarmes de toda a organização.

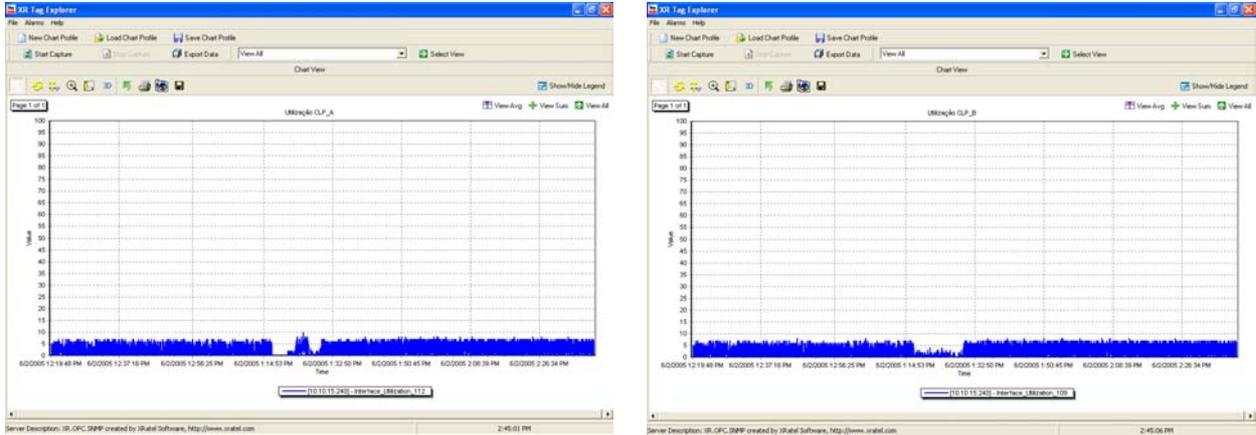
Em sistemas de automação, a detecção de problemas na comunicação é uma tarefa difícil que exige uma abordagem diferente, de modo a analisar informações que geralmente são desprezadas.

Neste caso pratico, temos dois controladores programáveis conectados via Ethernet através de um switch gerenciável. Os controladores mantêm uma comunicação constante entre si para troca de informações do processo (intertravamentos, variáveis analógicas, etc) e uma comunicação adicional com os sistemas de supervisão. Utilizamos os seguintes equipamentos neste caso pratico:

- Controlador CompactLogix L39E
- Servidor de Comunicação – RSLinx OPC Server / XR SNMP Tools
- Rede Ethernet 10 Mbits/s com Switch 3COM Superstack III

O servidor de comunicação e gerenciamento coleta variáveis de ambos os controladores para disponibilizá-los no sistema SCADA e monitora o desempenho da rede através do software XR SNMP Tools. A ferramenta é um servidor OPC que coleta em tempo real as informações do agente SNMP implementado no switch e disponibiliza estas informações para qualquer cliente OPC (SDADA, PIMS, MES). Uma correta monitoração de redes de automação deve observar os níveis de utilização e as taxas de erro para cada ponto da rede que tenha impacto direto no funcionamento do processo, seja ele uma estação de supervisão, um sistema de aquisição de dados ou um controlador programável.

No estudo, monitoramos a rede Ethernet dos controladores durante cerca de duas horas, registrando as utilização e a taxa de erros da rede em intervalos regulares de 1 segundo. Os controladores foram conectados nas portas 9 e 12 do switch, onde foram monitorados os contadores de erros e de utilização via SNMP, apresentados nas figuras a seguir.



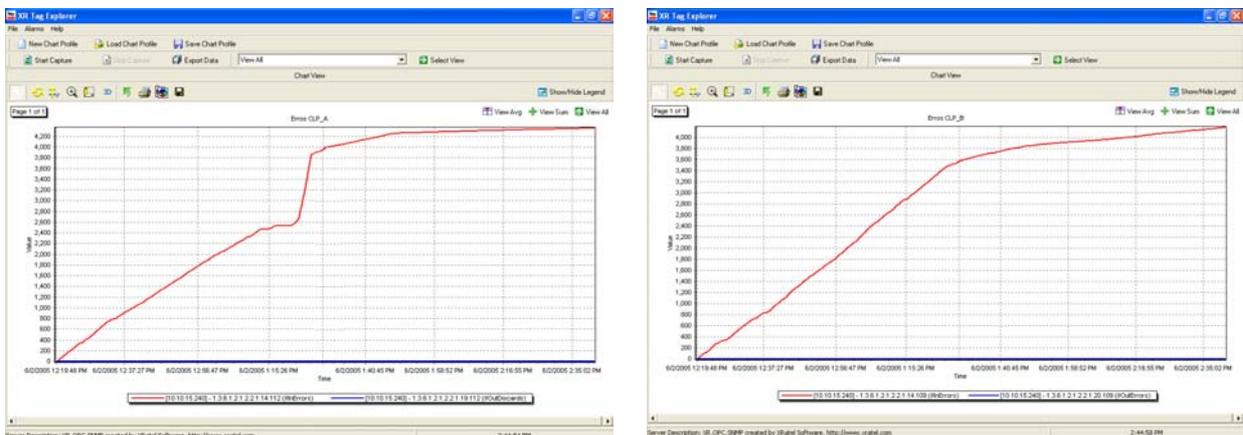
CLP A

CLP B

Figura 2. Taxa de utilização no link do CLP usando produto XRateI.

Os gráficos de utilização nos mostram que a rede não esteve congestionada durante a operação do sistema, pois a utilização estava abaixo de 10%⁽⁴⁾ em uma primeira análise, indicando um comportamento normal para TA. Este tipo de conclusão é bastante comum quando são utilizados sistemas de monitoração para redes de TI em redes industriais. As redes industriais trafegam pacotes pequenos mas com uma frequência muito elevada, uma vez que isto é essencial para garantir o sincronismo das variáveis nos diversos controladores.

Entretanto, o grande volume de pacotes com erro descartados pelo switch demonstra que a rede funcionou no limite o tempo inteiro, implicando na necessidade de retransmissão de pacotes e conseqüentemente degradando o desempenho da comunicação.



CLP A

CLP B

Figura 3. Erros acumulados nas portas monitoradas usando produto XRateI.

A gravidade do problema de comunicação pôde ser evidenciada cerca de uma hora após o início da operação. Houve problemas de comunicação com os controladores levando à interrupção da comunicação do sistema durante cerca de dez minutos (esta interrupção pode ser vista nos gráficos de utilização e de erros). A comunicação só foi restabelecida após a reinicialização do sistema de supervisão.

5 CONCLUSÕES

O gerenciamento de redes de TA é uma exigência atual para que os sistemas de automação possam continuar atendendo às necessidades de controle de processos e de tomada de decisão. Esses são requisitos essenciais para que as empresas tenham bons resultados dentro do mercado globalizado objetivando a Excelência Operacional.

Os ativos de automação (CLPs, redes, estações, etc.) devem ter seu desempenho continuamente monitorado dentro da filosofia do RPM, de forma que as equipes de manutenção possam ser pró-ativas na solução de problemas e na sustentabilidade do desempenho dos sistemas de TA e, conseqüentemente, do negócio das empresas.

O uso do SNMP com o padrão OPC permite que as redes Ethernet possam ser gerenciadas pelos sistemas de TA, especialmente os sistemas de supervisão, os quais podem reunir dados de outras redes e ativos de automação, possibilitando um ambiente propício para gestão destes ativos.

A utilização de historiadores de longo prazo, principalmente sistemas PIMS, facilita o acompanhamento e análise do comportamento das redes, possibilitando o gerenciamento de mudanças.

As entidades internacionais que estão buscando padronizações para o uso da Ethernet em ambientes industriais, assim como os fabricantes de sistemas de TA, já estão disponibilizando especificações e produtos que orientam o uso do SNMP e OPC com sistemas de supervisão. As especificações disponíveis estimulam a disponibilização de informações (dados e eventos) específicas para aplicação industrial em sistemas de TA, adicionalmente às já existentes para sistemas de TI.

REFERÊNCIAS BIBLIOGRÁFICAS

- 1 “**Industrial Ethernet Planning and Installation Guide – Version 4.0**” IAONA (www.iaona.org), 2003.
- 2 “**IAONA SNMP MIB – Draft/RFC 1.0**” IAONA (www.iaona.org), 2003.
- 3 SILVA, R. G. R. “**Contribuições para a Integração de sistemas de supervisão de redes de computadores e de telecomunicações à plataforma SIS**”, Dissertação de mestrado, DCC, UFMG, 28 de março de 1996.
- 4 FONSECA, M. O. “**Desempenho de Sistemas de Automação – Métricas e Práticas**”, VIII Seminário de Automação da ABM, 2004.

BIBLIOGRAFIA

- 1 MCCLOGHRIE, K; Rose, M. T. “**RFC 1213 - Management Information Base for Network Management of TCP/IP-based internets:MIB-II**”, IEEE, 1991.
- 2 “**XRatel SNMP OPC Server Manual**”, XRatel Software (www.xratel.com), 2005.
- 3 Dooley Kevin “**Designing large-scale LANs**”, O’Reilly & Associates, 2002

AUTOMATION NETWORKS PERFORMANCE MONITORING THROUGH SNMP

Marcos de Oliveira Fonseca¹
Constantino Seixas Filho²
Alexandre Valente Duarte Ferreira³
René Silva Daré⁴

Abstract

Automation systems are suffering a big transformation due to IT and AT integration and technology convergence. In this context control and communication networks, with emphasis to Ethernet networks, represents the backbone of industrial corporations. The correct behavior of automation networks concerning both performance and reliability assures the fulfillment of industrial and business applications requirements. The SNMP standard, already consolidated in IT, assumes an important role in network management and in performance and availability assurance. This paper presents the trends in network management, considered as an important automation asset, and focuses the practical application of SNMP in industrial systems.

Key-words: Performance; SNMP; Networks; Automation.

¹ IX Process Automation Seminar, Associação Brasileira de Metalurgia e Materiais, October 05-07th, 2005 – Curitiba – PR, Brazil.

² Electrical Engineer, M.Sc, Automation Technology Division's Director, ATAN Sistemas, Belo Horizonte – MG, Brazil.

³ Electrical Engineer, M.Sc, R&D Director, ATAN Sistemas, Belo Horizonte – MG, Brazil.

⁴ Electrical Engineer, Product Manager, ATAN Sistemas, Belo Horizonte – MG, Brazil.

⁵ Electrical Engineer, System Engineer, ATAN Sistemas, Belo Horizonte – MG, Brazil.