

**LIGA DE ENSINO DO RIO GRANDE DO NORTE
FACULDADE NATALENSE PARA O DESENVOLVIMENTO DO RN
ESPECIALIZAÇÃO EM REDES DE COMPUTADORES**

ADMINISTRAÇÃO E GERÊNCIA DE REDES INDUSTRIAIS

Monografia apresentada ao curso de
Especialização em Redes de Computadores da
Faculdade Natalense para o Desenvolvimento
do Rio Grande do Norte como requisito para
obtenção do título de Especialista em Redes de
Computadores.

Aécio da Silva Gonzaga

Orientador:

Alcirio Pereira da Rocha Neto, M. Sc.

NATAL/RN

2008

ADMINISTRAÇÃO E GERÊNCIA DE REDES INDUSTRIAIS

Orientador:

Aluizio Ferreira da M.

2008

Catálogo na Publicação – Biblioteca da FARN
Setor de Processos Técnicos

Gonzaga, Aécio da Silva

Administração e gerência de redes industriais / Aécio da Silva
Gonzaga. – Natal: FARN, 2008.
42 f.

Orientador: Aluizio Ferreira da Rocha Neto (M.Sc.)

Monografia (Especialização em Redes de Computadores) – Faculdade
Natalense para o Desenvolvimento do Rio Grande do Norte.

1. Redes de Computadores – Monografia. 2. Redes Industriais –
Monografia. 3. Gerência de Redes – Monografia. I. Título.

RN/FARN/BC

CDU 004.7



004.7
G65a
2008
ex 01

**LIGA DE ENSINO DO RIO GRANDE DO NORTE
FACULDADE NATALENSE PARA O DESENVOLVIMENTO DO RN
ESPECIALIZAÇÃO EM REDES DE COMPUTADORES**

ADMINISTRAÇÃO E GERÊNCIA DE REDES INDUSTRIAIS

Aécio da Silva Gonzaga

Monografia apresentada e aprovada em 13 de Junho de 2008, pela banca examinadora composta pelos seguintes membros:

Aluízio Ferreira da Rocha Neto, M. Sc.
Orientador

Gleydson Azevedo Ferreira Lima, M. Sc.

Membro examinador

Natal/RN
2008

DEDICATÓRIA

A DEUS por me conceder a oportunidade de poder compartilhar conhecimento e experiências.

A minha mulher e filhas pelo incentivo e apoio.

Ao Prof. Aluizio Rocha, pela dedicação e proeza.

A FARN – Faculdade Natalense para o Desenvolvimento do Rio Grande do Norte e a todos os colegas e professores pela dedicação e empenho demonstrados ao longo do curso.

Se dois homens vão andando por uma estrada, cada um carregando um fardo, do se encontrarem, eles trocam os fardos, cada homem vai embora com um fardo, se dois homens vão andando por uma estrada cada um carregando um fardo, e se se encontrarem, eles trocam os fardos, cada homem vai embora com um fardo.

A minha família, que sempre compreendeu os momentos de ausência no transcorrer do curso e, mais recentemente, durante a produção desta monografia.

Diana Clara

AGRADECIMENTOS

A DEUS por me conceder a oportunidade de poder compartilhar conhecimento e experiência.

A minha mulher e filhos pelo incentivo e apoio.

Ao Prof. Aluizio Rocha, pela dedicação e presteza.

A FARN – Faculdade Natalense para o Desenvolvimento do Rio Grande do Norte e a todos os colegas e professores pela dedicação e entusiasmo demonstrados ao longo do curso.

“Se dois homens vêm andando por uma estrada, cada um carregando um pão, e, ao se encontrarem, eles trocam os pães, cada homem vai embora com um. Porém, se dois homens vêm andando por uma estrada cada um carregando uma idéia, e, ao se encontrarem, eles trocam as idéias, cada homem vai embora com duas.

Sempre que possível troque idéias, elas esclarecem, acrescentam, ajudam, evoluem... ainda que você não precise, servirão para o outro.”

Ditado Chinês.

SUMÁRIO

1	INTRODUÇÃO	13
1.1	OBJETIVOS	14
1.1.1	OBJETIVO GERAL	14
1.1.2	OBJETIVOS ESPECÍFICOS	14
1.2	ORGANIZAÇÃO DO TRABALHO.....	15
2	REFERENCIAL TEÓRICO	16
2.1	REDES DE COMPUTADORES	16
2.2	REDES INDUSTRIAIS	17
2.3	ADMINISTRAÇÃO DE REDES.....	22
2.4	GERÊNCIA DE REDES – ARQUITETURA OSI.....	25
2.5	OS PADRÕES ISA	27
2.6	OS PADRÕES DE MERCADO – GERÊNCIA SNMP	30
2.7	OS PADRÕES DE MERCADO - OPC	33
2.8	PLANOS DE CONTINGÊNCIA	34
2.9	ACORDOS DE NÍVEL DE SERVIÇOS	36
3	O MODELO PROPOSTO	38
4	CONSIDERAÇÕES FINAIS.....	40
	REFERÊNCIAS BIBLIOGRÁFICAS	42

LISTA DE FIGURAS

Figura 1 – Arquitetura de Rede Industrial integrada	16
Figura 2 - Estrutura de uma rede industrial típica	18
Figura 3 - Exemplo de aplicações de um sistema de supervisão e controle	20
Figura 4 - O modelo ITIL	23
Figura 5 - Arquitetura de gerenciamento OSI	25
Figura 6- Gerência Integrada de Redes e Serviços	27
Figura 7 - ISA SP-99 Standard Series	28
Figura 8- SNMP – Camadas TCP.....	30
Figura 9- entidades funcionais do SNMP	32
Figura 10 - Integração OPC-SNMP.....	38

CMIS	<i>Common Management Information Services</i>
CMIS	<i>Common Management Information Services</i>
EFQM	<i>European Foundation for Quality Management</i>
GIRS	<i>Gerência Integrada de Redes e Serviços</i>
HART	<i>Highway Addressable Remote Transducer</i>
ICT	<i>Information and Communication Technology</i>
ISA	<i>International Standard for Automation</i>
ISO	<i>International Organization for Standardization</i>
ITIL	<i>Information Technology Infrastructure Library</i>
ITU	<i>International Telecommunications Union</i>
MB	<i>Management Information Base</i>
OLE	<i>Object Linking and Embedding</i>
OPC	<i>OLE for Process Control</i>
OSI	<i>Open Systems Interconnection</i>
OSMIS	<i>OSI Management Information Service</i>
PC	<i>Personal Computer</i>
PLC	<i>Programmable Logic Controller</i>
RMON	<i>Remote Network Monitoring</i>
RPM	<i>Real-time Performance Management</i>
RTU	<i>Remote Terminal Unit</i>
SCADA	<i>Supervisory Control and Data Acquisition</i>
SDCD	<i>Sistema Digital de Controle Distribuído</i>
SLA	<i>Service Level Agreement</i>
SLM	<i>Service Level Management</i>
SMI	<i>Structure of Management Information</i>

LISTA DE ABREVIATURAS

ABNT	<i>Associação Brasileira de Normas</i>
ANSI	<i>American National Standards Institute</i>
BSM	<i>Business Service Manangement</i>
CAN	<i>Control Area Network</i>
CCTA	<i>Central Communications and Telecom Agency</i>
CLP	<i>Controlador Lógico Programável</i>
CMIP	<i>Common Management Information Protocol</i>
CMIS	<i>Commom Management Information Services</i>
EFQM	<i>European Foundation for Quality Management</i>
GIRS	<i>Gerência Integrada de Redes e Serviços</i>
HART	<i>Highway Addressable Remote Transducer</i>
ICT	<i>Information and Communication Technology</i>
ISA	<i>International Standard for Automation</i>
ISO	<i>International Organization for Standardization</i>
ITIL	<i>Information Technology Infrastructure Library</i>
ITU	<i>International Telecommunications Union</i>
MIB	<i>Management Information Base</i>
OLE	<i>Object Linking and Embedding</i>
OPC	<i>OLE for Process Control</i>
OSI	<i>Open Systems Interconnection</i>
OSIMIS	<i>OSI Management Information Service</i>
PC	<i>Personal Computer</i>
PLC	<i>Programmable Logic Controller</i>
RMON	<i>Remote Network Monitoring</i>
RPM	<i>Real-time Performance Management</i>
RTU	<i>Remote Terminal Unit</i>
SCADA	<i>Supervisory Control and Data Aquisition</i>
SDCD	<i>Sistema Digital de Controle Distribuído</i>
SLA	<i>Service Level Agreement</i>
SLM	<i>Service Level Management</i>
SMI	<i>Structure of Management Information</i>

TA	<i>Tecnologia da Automação</i>
TCOM	<i>Telecomunicações</i>
TCP/IP	<i>Transmission Control Protocol / Internet Protocol</i>
TIC	<i>Tecnologia da Informação e Telecomunicações</i>
TI	<i>Tecnologia da Informação</i>
TMN	<i>Telecommunications Management Network</i>

Neste trabalho propõe-se a administração e gestão das redes industriais, considerando as normas e padrões internacionais publicados pela ISA, os produtos do mercado, e o modelo ISO-OSI, agregando à gestão de redes industriais as boas práticas de Gestão de Falhas, Desempenho, Configuração, Segurança e Contabilização, já consolidadas na gestão de redes "convencionais" pelas áreas de Informática e Telecomunicações.

Palavras-chave: Redes de computadores, Redes industriais, Administração, Gestão de Redes.

RESUMO

Para garantir alta disponibilidade e desempenho em redes industriais, com alto grau de confiabilidade e segurança é necessário um conjunto de práticas e procedimentos de administração e gerência de redes similar ao gerenciamento de redes convencionais para o transporte de dados corporativos, fazendo crer que os mesmos conceitos, técnicas e ferramentas das normas ISO possam ser adotadas nas redes de automação. Entretanto sabemos que o gerenciamento destas redes apresenta particularidades específicas, tornando-o mais complexo que o de redes convencionais, pois, as redes industriais ainda não estão completamente padronizadas e empregam muitos sistemas legados e proprietários. Nestas redes, falhas causam além da perda de dados, a perda de produção, o impacto ambiental, acidentes fatais, danos a equipamentos, violação da lei, etc. Além disso, as áreas de TI e Telecomunicações não conhecem detalhadamente os sistemas de controle e automação.

Nesse trabalho propõe-se a administração e gerência das redes industriais, considerando as normas e padrões internacionais publicadas pela ISA, os produtos de mercado, e o modelo ISO-OSI, agregando à gestão de redes industriais as boas práticas de Gerência de Falhas, Desempenho, Configuração, Segurança e Contabilização, já consolidados na gerência de redes "convencionais" pelas áreas de Informática e Telecomunicações.

Palavras-chave: Redes de computadores, Redes Industriais, Administração, Gerência de Redes.

Keywords: Computers Networks, Industrial Networks, Network Administration, Network Management

1 INTRODUÇÃO

ABSTRACT

To guarantee high availability and performance in industrial networks, with high degree of trustworthiness and security is necessary a set of practicals and procedures for networks administration and management similar to the conventional networks management for the corporative data transport, making to believe that the same concepts, techniques and tools of ISO norms can be adopted in the automation networks. However, we know that the management of these nets presents specific particularities, becoming it more complex than conventional nets, therefore, the industrial nets still are not completely standardized and use many legacies and proprietors systems. In these networks, faults cause beyond the loss of data, the production loss, ambient impacts, fatal accidents, equipment damages, breaking of the law, etc. Moreover, the areas of IT and Telecommunications do not know deeply the automation control systems.

In this work it is considered administration and management of the industrial networks, considering the norms and international standards published by the ISA, the products of market, and model ISO-OSI, adding to the management of industrial nets the best practicals for Faults Management, Performance, Configuration, Security and Accounting, already consolidated for the "conventional" networks for the Computer science and Telecommunications.

Key-words: Computers Networks, Industriais Networks, Network Administration, Network Management

1 INTRODUÇÃO

É consenso entre os gerentes e administradores de redes de computadores, que falhas são inevitáveis e, portanto, devemos administrá-las de forma eficaz, visando garantir a manutenção dos níveis de serviço dentro de padrões adequados aos requisitos dos clientes e perseguir um baixo tempo para solução de problemas, através da elaboração de planos de contingências e procedimentos operacionais que garantam a facilidade de modificação e adequação do ambiente operacional, aderentes às políticas de uso previamente estabelecidas, dando ao ambiente operacional CONFIABILIDADE, DISPONIBILIDADE e FLEXIBILIDADE respectivamente.

Dependendo do porte das redes ou da organização que as utilize pode-se resumir em quatro as formas de gerenciá-las:

- Gerenciamento Reativo – Help Desk /Reclamação;
- Gerenciamento por Monitoração – Request SNMP;
- Gerenciamento Proativo – SNMP TRAPS, Agentes RMON, Análise de relatórios;
- Gerenciamento Planejado – Gerenciamento integrado, utilizando-se ferramentas específicas através de políticas estabelecidas e contratos de prestação de serviços – SLA – *Service Level Agreement* – Acordos de nível de serviços.

Nos últimos anos as empresas passaram a cobrar de seus departamentos de Informática e Telecomunicações, ações que garantam o atendimento das exigências de qualidade e custos dos seus produtos ou serviços, com lucratividade e competitividade comparadas às de seus concorrentes externos.

Com a efetiva gerência de redes, é possível para os executivos visualizarem o desempenho da atividade de TI, através de relatórios que lhe dizem como está a disponibilidade dos serviços, quais suas principais falhas e com base nessas informações, terem subsídios reais para orientar suas decisões na condução dos negócios. A gerência de redes também garante aos profissionais de TI e TELECOMUNICAÇÕES, os argumentos necessários à justificativa de investimentos, melhorias e modernização.

Ao estabelecermos uma gerência de redes baseada em Acordos de Níveis de Serviço e fundamentada em POLÍTICAS bem definidas estaremos assegurando confiabilidade, disponibilidade, flexibilidade e qualidade às nossas redes.

A administração e gerenciamento de redes industriais preconizam um conjunto de atividades que visam à garantia da disponibilidade e do desempenho das redes utilizadas no ambiente industrial, como alto grau de confiabilidade e sigilo. Aqui o consenso já é outro: O

gerenciamento das redes de automação apresenta muitas dificuldades específicas, tornando-a muito mais complexa, pois, as redes industriais ainda não estão completamente padronizadas e integradas ao mundo da Tecnologia da Informação, por estarem em uso mais acentuado nos últimos 10 anos e, principalmente, devido aos sistemas de automação e controle serem diferentes em muitos aspectos dos sistemas de informação em geral, onde possíveis falhas, nos sistemas TA, envolvem não apenas quebra de sigilo e perda de dados, mas também perda de produção, impacto ambiental, acidentes, danos a equipamentos, violação da lei, etc.

Em redes industriais são empregados muitos sistemas legados ou proprietários, e as necessidades de gerenciamento variam de acordo com a área, porém sempre necessárias. Além disso, os especialistas em Tecnologias da Informação da empresa não conhecem detalhadamente os sistemas de controle e automação.

1.1 OBJETIVOS

1.1.1 Objetivo Geral

O trabalho propõe a administração e gerência das redes industriais, considerando as normas e padrões internacionais publicadas pela ISA, os produtos de mercado, e o modelo ISO-OSI, agregando à gestão de redes industriais as boas práticas de Gerência de Falhas, Desempenho, Configuração, Segurança e Contabilização, já consolidados na gerência de redes "convencionais" pelas áreas de TI e TCOM (Telecomunicações).

1.1.2 Objetivos Específicos

O objetivo específico deste trabalho é aperfeiçoar os processos de comunicação entre as equipes de TA e TIC, familiarizando os profissionais de automação industrial com as áreas de administração e gerência de redes bem como oferecer um referencial teórico de redes de automação e controle aos profissionais das áreas de tecnologia da informação e telecomunicações, viabilizando uma forma consistente de trabalho conjunto com uma terminologia padronizada.

1.2 ORGANIZAÇÃO DO TRABALHO

Esta monografia está assim organizada:

O capítulo 1 além da introdução trata dos objetivos gerais e específicos.

O capítulo 2 traça o referencial teórico necessário à compreensão do tema Administração e Gerência de redes abordando as redes de computadores corporativas, as redes dedicadas à operação, supervisão e controle de processos industriais, os modelos adotados para administração e gerências de redes, as plataformas de gerência, além das normas nacionais e internacionais inerentes ao tema, bem como, os padrões de mercado atualmente adotados, finalizando com uma abordagem informativa sobre Planos de Contingências e Acordos de Nível de Serviço.

O modelo proposto é abordado no capítulo 4 e as conclusões e recomendações no capítulo 5. Os documentos consultados estão relacionados no capítulo 6.

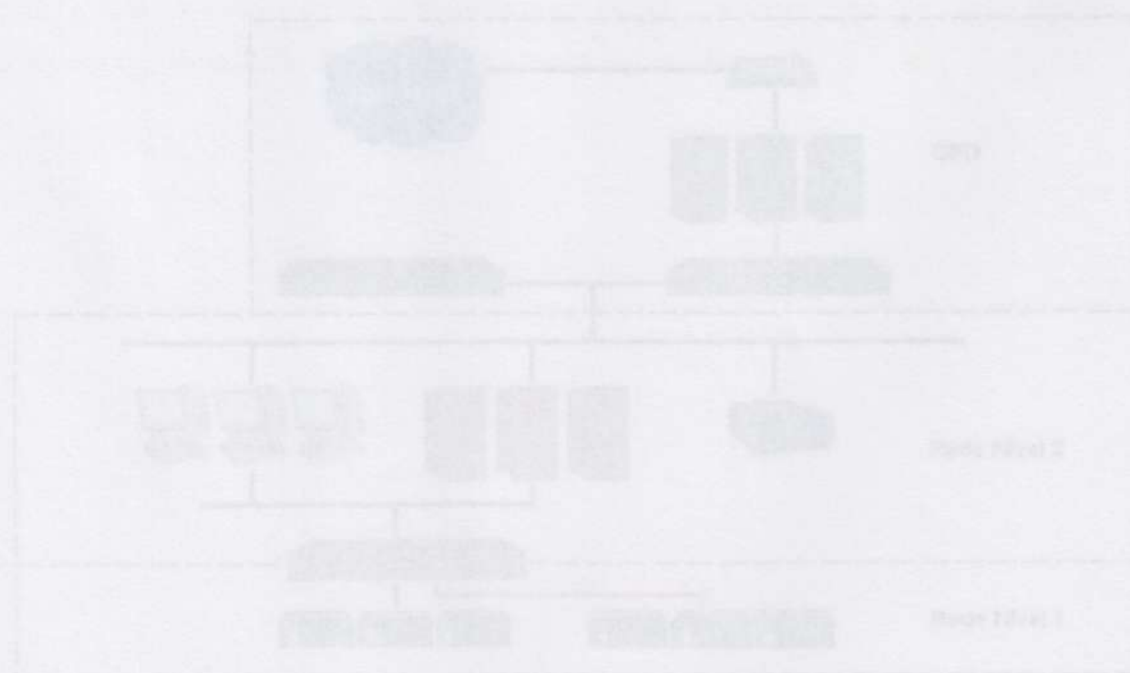


Figura 1 - Arquitetura de Rede Industrial Integrada

2 REFERENCIAL TEÓRICO

O objetivo deste capítulo é familiarizar os profissionais de automação industrial com as áreas de administração e gerência de redes bem como oferecer um referencial teórico de redes de automação e controle aos profissionais das áreas de tecnologia da informação e telecomunicações.

2.1 REDES DE COMPUTADORES

As redes de computadores foram concebidas, inicialmente, apenas para compartilhar impressoras, terminais e unidades de armazenamento de dados. Com a evolução da informática, o compartilhamento dos dispositivos tornou-se secundário em comparação às outras vantagens oferecidas por uma rede de computadores e hoje fazem parte do nosso cotidiano como uma ferramenta que oferece recursos e serviços que permitem uma maior interação entre os usuários e um conseqüente aumento de produtividade, com uma grande heterogeneidade de padrões, sistemas operacionais, equipamentos, etc.

As redes de computadores atuais já contemplam a integração dos sistemas de automação da manufatura com os sistemas de informação corporativos (FIGURA 1), permitindo que os dados em tempo-real gerem informações estratégicas para a condução dos negócios.

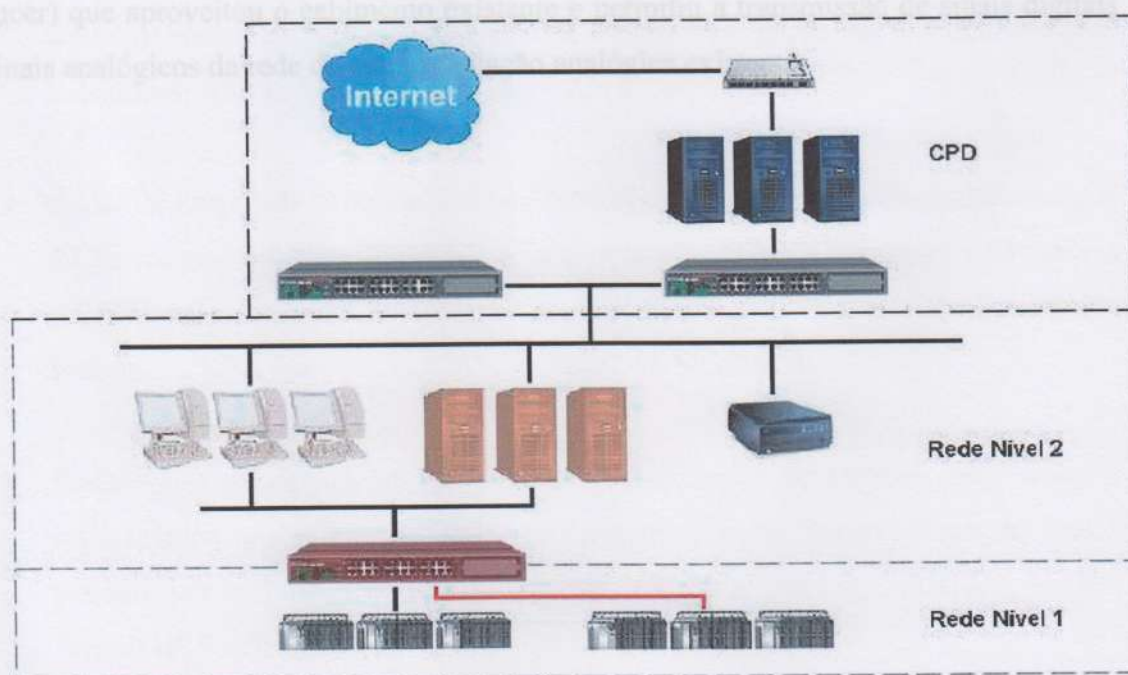


Figura 1 – Arquitetura de Rede Industrial integrada

É fácil compreender a necessidade de um gerenciamento eficiente das redes de computadores para mantê-las funcionando corretamente de forma a atender as necessidades dos usuários e às expectativas dos negócios.

2.2 REDES INDUSTRIAIS

É largamente citado pela literatura especializada, que o processo de automação industrial iniciou-se na década de 1920 quando Henry Ford idealizou e desenvolveu a sua linha de montagem de automóveis e permitiu a indústria de forma geral adotar, ao longo do tempo, a automação de processos produtivos, utilizando forças pneumáticas, hidráulicas e eletromagnéticas, para a execução de tarefas repetitivas, que exijam a aplicação de muita força e em condições insalubres com ganhos de produtividade, lucratividade e qualidade. A partir dos anos de 1960, o desenvolvimento da microeletrônica permitiu a construção dos CLP's (Controladores Lógicos Programáveis), que substituíram os painéis de controle com válvulas e atuadores nos sistemas hidráulicos pneumáticos e os relés nos sistemas elétricos, até então largamente utilizados.

Na área de instrumentação a evolução ocorreu com a necessidade de se fazer os instrumentos comunicarem-se em rede com os CLPs, através de transmissão digital. O primeiro protocolo digital para redes industriais foi o HART (Highway Addressable Remote Transducer) que aproveitou o cabimento existente e permitiu a transmissão de sinais digitais sobre sinais analógicos da rede de instrumentação analógica existente.

- *Redes de Dispositivos ou Devicebus* - Interligam dispositivos mais genéricos como CLPs, outras estações remotas de aquisição de dados e controle, conversores AC/DC, relés de medição inteligentes, etc. Exemplos: Profibus-DP, DeviceNet, Interbus-S, SDS, LonWorks, CAN, ControlNet, ModbusPlus.
- *Redes de instrumentação ou fieldbus* - São redes concebidas para integrar instrumentos analógicos no ambiente industrial, como transmissores de vazão, pressão, temperatura, válvulas de controle, etc. Exemplos: IECSP50-H1, HART, WorldFIP, Profibus-PA.

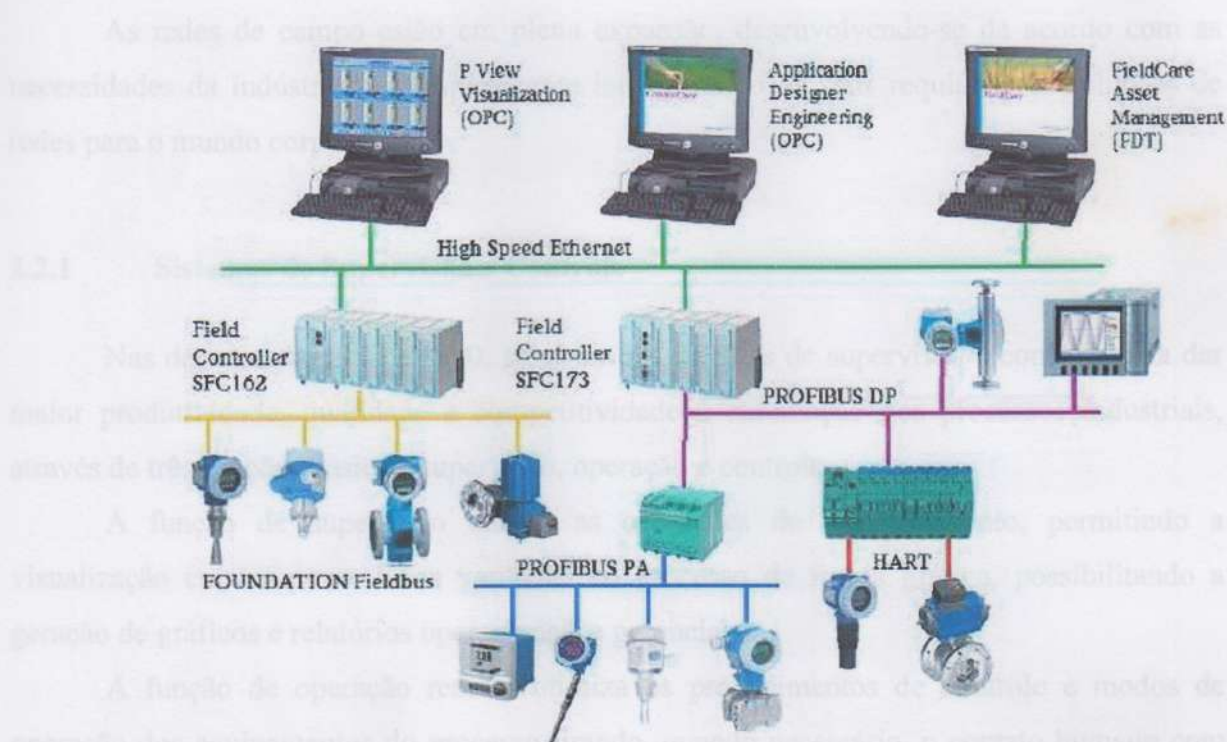


Figura 2 - Estrutura de uma rede industrial típica

As redes industriais (FIGURA 2), ou redes de campo, são responsáveis pela comunicação em todo o processo de automação industrial, também denominadas fieldbus ou barramento de campo, dividem-se em três tipos diferentes:

- **Redes de sensores ou Sensorbus** - Redes para interligação de sensores e atuadores discretos como, contactores, desviadores, e chaves em geral. São exemplos de rede Sensorbus: ASI da Siemens, Seriplex, CAN e LonWorks.
- **Redes de Dispositivos ou Devicebus** - Interligam dispositivos mais genéricos como CLPs, outras estações remotas de aquisição de dados e controle, conversores AC/DC, relés de medição inteligentes, etc. Exemplos: Profibus-DP, DeviceNet, Interbus-S, SDS, LonWorks, CAN, ControlNet, ModbusPlus.
- **Redes de instrumentação ou fieldbus** - São redes concebidas para integrar instrumentos analógicos no ambiente industrial, como transmissores de vazão, pressão, temperatura, válvulas de controle, etc. Exemplos: IECSP50-H1, HART, WorldFIP, Profibus-PA.

As redes de campo estão em plena expansão, desenvolvendo-se de acordo com as necessidades da indústria ou simplesmente incorporando os seus requisitos às soluções de redes para o mundo corporativo.

2.2.1 Sistemas de Supervisão e Controle

Nas décadas de 1980 e 1990, surgiram os sistemas de supervisão e controle para dar maior produtividade, qualidade e competitividade à automação dos processos industriais, através de três funções básicas: supervisão, operação e controle.

A função de supervisão realiza as operações de monitoramento, permitindo a visualização em tempo real das variáveis do processo de forma gráfica, possibilitando a geração de gráficos e relatórios operacionais e gerenciais.

A função de operação remota otimiza os procedimentos de controle e modos de operação dos equipamentos do processo tirando, quando necessário, o contato humano com áreas insalubres e inseguras.

A função de controle possibilita a ação de controle sem a dependência de níveis intermediários do processo, através do sistema supervisor, onde o controle é realizado dinamicamente, de acordo com o comportamento global do processo.

Com a evolução da tecnologia, os microcomputadores passaram a ter um papel importante nos sistemas de supervisão abertos, propiciando o tratamento e processamento dos dados do processo e garantindo a integridade das informações. Neste aspecto, o uso dos computadores permitiu a diminuição de grande parte os custos, complexidades e riscos nas tarefas dos processos de produção.

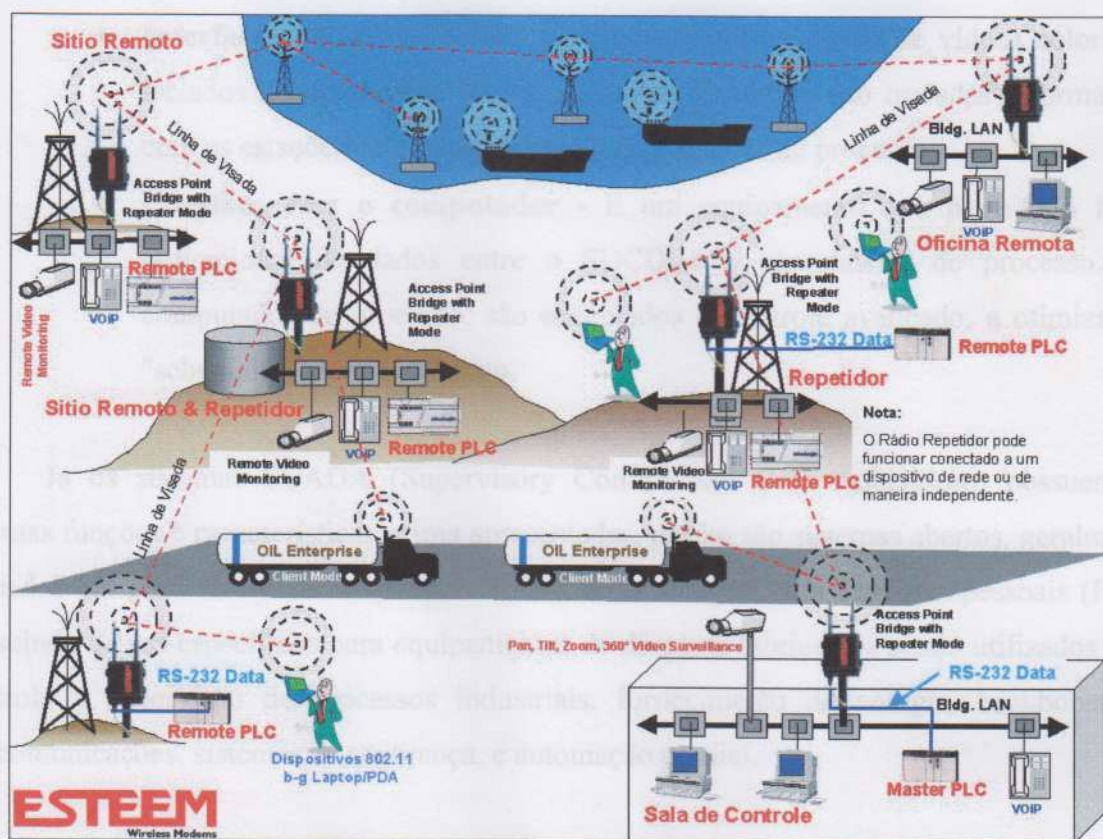


Figura 3 - Exemplo de aplicações de um sistema de supervisão e controle

Desenvolvidos para o gerenciamento das instalações industriais em tempo real os sistemas para supervisão e controle, denominados SDCC (Sistema Digital de Controle Distribuído) foram concebidas e comercializadas pelos grandes fabricantes e fornecedores de equipamentos para automação, como solução fechada e proprietária, com o objetivo de controlar e operar toda uma unidade fabril, sendo bastante utilizadas na indústria petroquímica e de geração de energia elétrica. A arquitetura SDCC, caracteriza-se por um elevado nível de redundância de servidores, de rede de comunicação de dados e de dispositivos de entrada e saída.

O sistema é dotado de três tipos de componentes interligados por uma rede de comunicação de dados:

- **Interface com o processo** - É formada por estações de controle onde são implementados os algoritmos de controle de regulatório, seqüenciamento de operações e monitoração das variáveis. Ela recebe e envia dados para os sensores e atuadores do processo.

- **Interface com a operação** - É composta por terminais de vídeos coloridos, teclados e impressoras. Através de telas dinâmicas são trocadas informações com as estações de controle e com o computador de processo.
- **Interface com o computador** - É um equipamento que permite o fluxo bidirecional de dados entre o SDCD e o computador de processo. No computador de processo, são executados o controle avançado, a otimização, "scheduling" e planejamento.

Já os sistemas SCADA (Supervisory Control and Data Acquisition), possuem as mesmas funções e características acima apresentadas, porém são sistemas abertos, geralmente baseados em hardware e sistemas operacionais utilizados em computadores pessoais (PCs), possuindo drives específicos para equipamentos de diversos fabricantes sendo utilizados para controle e supervisão de processos industriais, fornecimento de energia, backbones de telecomunicações, sistemas de segurança, e automação predial.

Um sistema SCADA composto por sensores e atuadores, estações remotas e estações de controle central, todos se comunicando através de uma rede de comunicação com as seguintes funções:

- **Sensores e Atuadores** - São os dispositivos conectados aos equipamentos controlados e monitorados pelo sistema. Os sensores convertem parâmetros físicos, tais como velocidade, níveis de líquido e temperatura, para sinais analógicos e digitais que são enviados para as estações remotas. Já os atuadores são utilizados para agir sobre o sistema, ligando, desligando ou movimentando determinados equipamentos.
- **Estações remotas** - Os processos de controle local e a aquisição de dados são executados nas estações remotas através dos PLC's (Programmable Logic Controllers) e RTU's (Remote Terminal Units), realizando a leitura dos valores apresentados pelos dispositivos de campo.
- **Estações de controle central** - Realizam a aquisição e o armazenamento dos dados gerados pelos diversos sensores (presença, luminosidade, temperatura, pressão, vazão, etc.) e atuadores, coletados pelas estações remotas.

2.3 ADMINISTRAÇÃO DE REDES

A atividade de administração de redes contempla principalmente as tarefas diárias para manter em funcionamento um ambiente com dois ou mais computadores conectados entre si:

- Instalação e manutenção de hardware;
- Instalação e manutenção de software;
- Gerenciamento de contas de usuários;
- Administração de dados e Backup;
- Monitoramento do sistema;
- Controle de versão e licenças de softwares;
- Segurança da Informação.

Dependendo do sistema operacional utilizado, da complexidade da estrutura e do porte de uma rede, as atividades de administração acima citadas têm maior ou menor importância. Especificamente no contexto da segurança, há diversos requisitos e atividades que permeiam e completam as demais atividades da administração de redes:

- Confidencialidade – Garantir que a informação não estará acessível a usuários ou processos não autorizados;
- Integridade de dados – Garantir a fidelidade dos dados, evitando a alteração ou descartes não autorizados;
- Disponibilidade – Garantir que os recursos computacionais estarão em operação durante os períodos acordados, segundo a necessidade dos usuários;
- Consistência - Garantir que os sistemas se comportam da maneira esperada perante os usuários autorizados.
- Auditoria - Verificação dos requisitos através da leitura dos diversos registros gravados pelo sistema, além da verificação das configurações individuais de cada computador da rede.

2.3.1 Modelo ITIL Para Administração de Redes

A cada dia é mais importante poder mensurar os serviços prestados pela área de Tecnologia da Informação. Para auxiliar na condução e na solução destes e outros problemas relacionados à Tecnologia da Informação, as grandes empresas, principalmente os conglomerados multinacionais estão utilizando o conjunto de melhores práticas ITIL (Information Technology Infrastructure Library) (FIGURA 4).

Segundo [1] a ITIL foi formada no final da década de 1980 pela CCTA (Central Communications and Telecom Agency), atual OGC10 (Office of Government Commerce), como um esforço para disciplinar e permitir a comparação entre as propostas dos diversos proponentes a prestadores de serviços de TI para o governo britânico, haja vista a grande adoção da metodologia de gerenciamento denominada outsourcing e da subcontratação de serviços de TI pelos seus diferentes órgãos, agências e instituições, objetivando garantir um mínimo de padronização de atendimento em termos de processos, terminologia, desempenho, qualidade e custo.

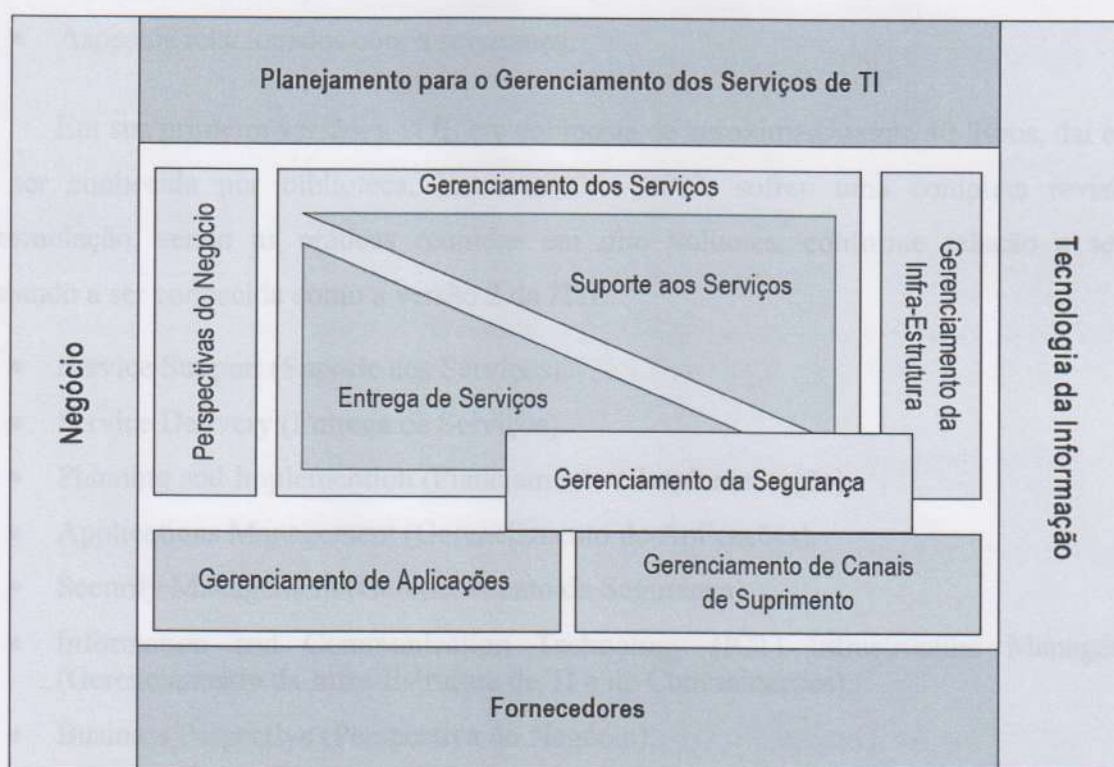


Figura 4 - O modelo ITIL

Durante a década de 1990, as práticas reunidas na ITIL passaram a ser adotadas pelas organizações europeias privadas, uma vez que a ITIL foi concebida como um padrão aberto, sobretudo pelo grande enfoque em qualidade, garantido pela definição de processos e a proposição de melhores práticas para o Gerenciamento dos Serviços de TI, viabilizando a aderência à prática ISO 9.000 e ao modelo de referência da European Foundation for Quality Management (EFQM). Com o avançar dos anos, a ITIL passou a ser também utilizada pelos países da América do Norte, tornando-se o “padrão de fato” da atualidade no segmento de TI. Hoje, a ITIL é conhecida e utilizada por organizações públicas e privadas de países de todo o

mundo. Dentre os fatores motivadores da atual corrida pela adoção das práticas reunidas na ITIL, pode-se citar o incremento dos seguintes aspectos:

- Custos de entrega e manutenção dos serviços de TI.
- Requerimentos da organização em relação à qualidade e ao custo/benefício dos serviços de TI.
- Demanda em obter a medição do retorno dos investimentos em TI.
- Complexidade da infra-estrutura de TI.
- Ritmo de mudanças nos serviços de TI.
- Necessidade de disponibilidade dos serviços de TI.
- Aspectos relacionados com a segurança.

Em sua primeira versão, a ITIL era composta de aproximadamente 40 livros, daí o fato de ser conhecida por biblioteca. Entre 2000 e 2002, sofreu uma completa revisão e reformulação, sendo as práticas reunidas em oito volumes, conforme relação a seguir, passando a ser conhecida como a versão 2 da ITIL.

- Service Support (Suporte aos Serviços).
- Service Delivery (Entrega de Serviços).
- Planning and Implementation (Planejamento e Implementação).
- Applications Management (Gerenciamento de Aplicações).
- Security Management (Gerenciamento da Segurança).
- Information and Communication Technology (ICT) Infrastructure Management (Gerenciamento da Infra-Estrutura de TI e de Comunicações).
- Business Perspective (Perspectiva do Negócio).
- Software Asset Management (Gerenciamento dos Ativos de Software).

Vê-se então, que independentemente do modelo adotado, a administração de redes deve buscar a garantia do desempenho e dos indicadores acordados através do cumprimento das **POLÍTICAS DE USO DOS RECURSOS DE INFORMÁTICA** definidas pela corporação, (normas e obrigações dos usuários, política de senhas, política de backup, etc.) dos **ACORDOS DE NÍVEIS DE SERVIÇO**, dos **PROCEDIMENTOS OPERACIONAIS** específicos de cada atividade e principalmente por um sólido **PLANO DE CONTINGÊNCIAS**.

Entendemos, pois, que todas estas atividades até aqui colocadas também se aplicam às redes industriais e são perfeitamente aplicáveis.

2.4 GERÊNCIA DE REDES – ARQUITETURA OSI

Assim como a administração de redes é amplamente reconhecida como atividade de TI e cuida do bom desempenho dos ativos de informática, dos softwares e de como os utilizamos, a gerência de redes está fortemente relacionada ao mundo das Telecomunicações, cuidando para que os equipamentos que compõem a infra-estrutura de redes se comportem conforme as necessidades dos usuários.

A arquitetura de gerenciamento OSI (Open Systems Interconnection), é descrita através de um conjunto de normas, resultado do trabalho conjunto da ISO (International Organization for Standardization) e do ITU SG 7 (International Telecommunications Union Study Group 7). O grupo designado pela ISO para o estudo de gerenciamento no modelo OSI publicou em 1989 o OSI Management Framework, ISO/IEC 7498-4 [2], que estabelece cinco áreas funcionais para o gerenciamento no modelo OSI (FIGURA 5):

- Gerência de configuração - Baseada em procedimentos que permitem documentar a rede, fornecendo informações de instalação, controle e identificação dos recursos da rede;
- Gerência de desempenho - Especifica procedimentos necessários à avaliação do comportamento dos objetos gerenciados;
- Gerência de falhas - Define procedimentos que permitem a detecção, isolamento e correção de falhas que exigem intervenção imediata;
- Gerência de contabilidade - Conjunto de facilidades que possibilita a identificação de custos de implantação e utilização dos objetos gerenciados;
- Gerência de segurança - Define procedimentos necessários à proteção dos objetos gerenciados, permitindo o controle de licença de software, permissão para acesso a aplicações, auditoria, criação e manutenção de usuários etc.

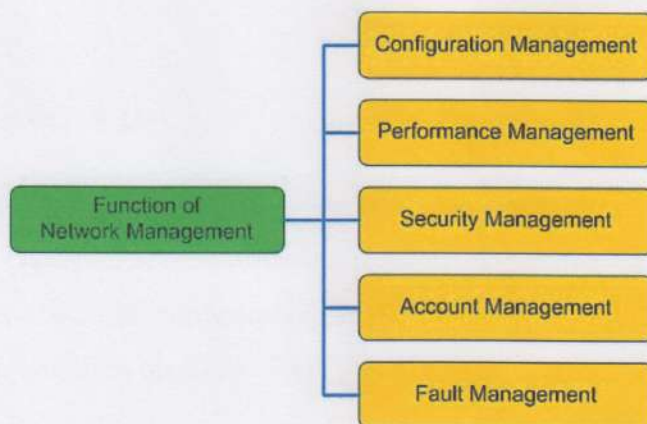


Figura 5 - Arquitetura de gerenciamento OSI

Complementam a arquitetura OSI, os modelos de Informação (SMI - Structure of Management Information) e os modelos de comunicação o (CMIP - Common Management Information Protocol) e CMIS (Common Management Information Services).

Com o avanço da Internet o protocolo padrão de gerência de redes passou a ser o SNMP, definido na tecnologia TCP/IP. O modelo ISO-OSI definiu então, a plataforma OSIMIS (OSI Management Information Service) apresenta um modelo de conversão, para prover mecanismos capazes de permitir a co-existência destas duas plataformas em um ambiente de gerenciamento de redes.

O modelo de gerencia de redes ideal é aquele composto por um conjunto de procedimentos e padrões operacionais desenvolvidos conforme preconiza a norma ISO-9000:2000, suportado por uma plataforma de softwares de gerência integrada que engloba além das definições ISO-OSI com SNMP, os conceitos TMN (Telecommunications Management Network), definidos no ITU-T(International Telecommunications Union-Telecommunications Standardization Section), que fornecem uma estrutura para gerenciar sistemas heterogêneos, que incluem: Sistemas de transmissão digital, multiplexadores, centrais telefônicas e demais sistemas de suporte às telecomunicações geralmente sem suporte SNMP.

Figura 4- Interface Integrada de Rede Service

O gerenciamento de redes industriais ainda não conta com produtos de mercado que integrem todas as funcionalidades necessárias a gestão de redes, principalmente com a integração de sistemas de controle.

2.3 OS PADRÕES ISA

Os padrões ISA, disponíveis neste capítulo, abrangem as principais áreas funcionais da administração e gestão de redes, com foco em segurança de redes, na norma ISA SP-99 Standard Series - Security for Industrial Automation & Control Systems series, composta por 4 seções e dois relatórios técnicos (FIGURA 7):

- ISA-99.00.01- Concepts, Terminology, and Models

2.4.1 Gerência de Redes – Gerência Integrada de Redes e Serviços

A GIRS - (Gerência Integrada de Redes e Serviços) (FIGURA 6) representa um conjunto de atividades e sistemas necessários ao suporte e gerenciamento da rede de telecomunicações e seus serviços, incluindo-se as atividades de projeto, planejamento, aprovisionamento, instalação, manutenção, operação, administração e logística.

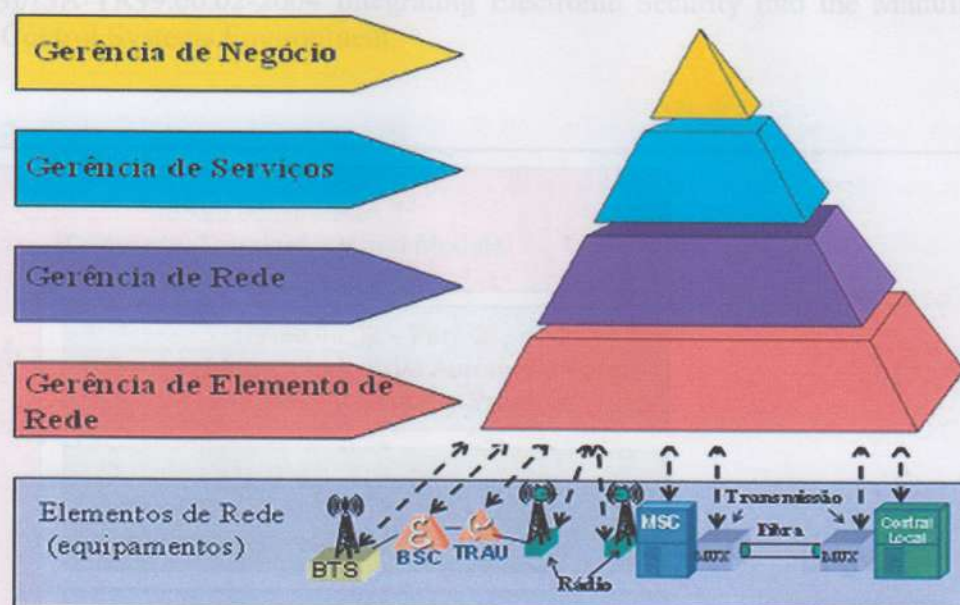


Figura 6- Gerência Integrada de Redes e Serviços

O gerenciamento de redes industriais ainda não conta com produtos de mercado que agreguem todas as funcionalidades necessárias a gerência dessas redes, principalmente com a abrangência até aqui descrita.

2.5 OS PADRÕES ISA

Os padrões ISA, disponíveis neste contexto, agregam as principais áreas funcionais da administração e gerência de redes, com foco em segurança de redes, na norma ISA SP-99 Standard Series - Security for Industrial Automation & Control Systems series, composta por 4 seções e dois relatórios técnicos (FIGURA 7):

- ISA-99.00.01-Concepts, Terminology, and Models.

- ISA-99.00.02—Establishing an Industrial Automation & Control System Security Program.
- ISA-99.00.03—Operating an Industrial Automation & Control System Security Program.
- ISA-99.00.04—Specific Security Requirements for Industrial Automation & Control Systems.
- ANSI/ISA-TR99.00.01-2004 – Technologies for Protecting Manufacturing and Control Systems.
- ANSI/ISA-TR99.00.02-2004 Integrating Electronic Security into the Manufacturing and Control Systems Environment.

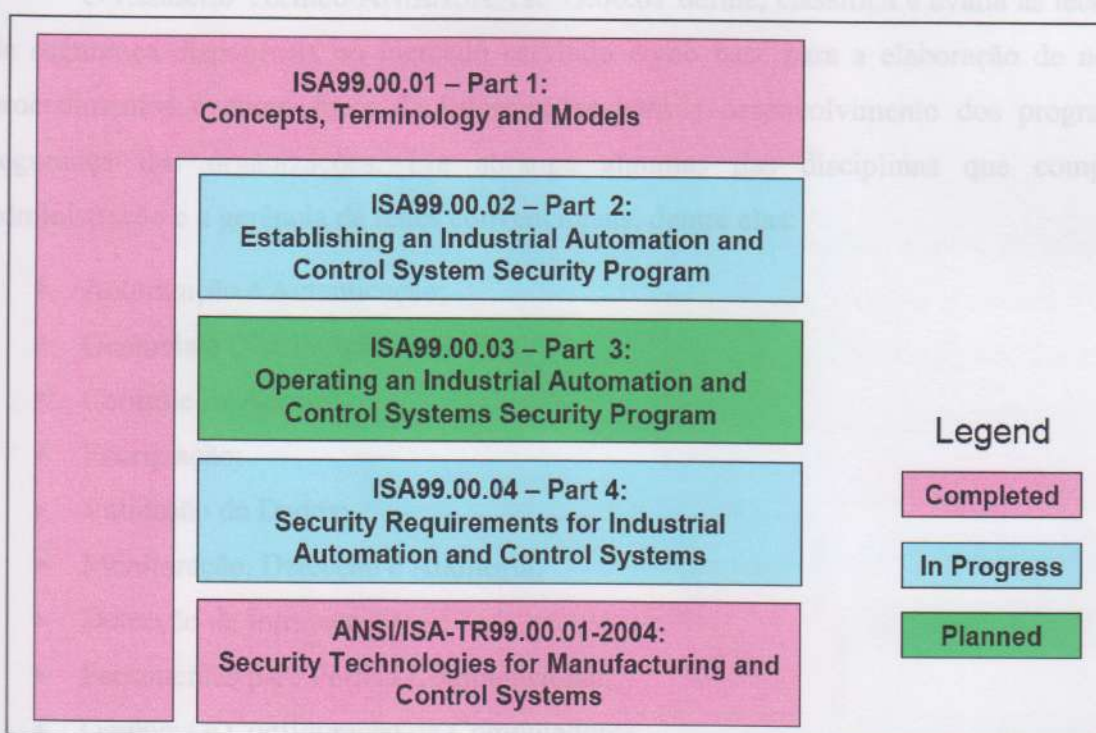


Figura 7 - ISA SP-99 Standard Series

A ISA-99.00.01 categoriza e define as principais tecnologias e ferramentas atualmente disponíveis que servirão como base para a elaboração dos relatórios técnicos que serão disponibilizados como referência para definição de programas de segurança a serem implantados nas áreas de automação e controle. O documento referencia as definições e termos comuns, traça uma visão geral do objetivo da norma, e descreve detalhadamente as várias classes de tecnologias de segurança disponíveis.

A parte 2 da ISA-99 é um guia de como provê a segurança adequada para os sistemas de manufatura e controle, considerando: operação, manutenção, suprimento, e

projeto/engenharia, com foco no planejamento, desenvolvimento, auditoria e análise de riscos, implementando procedimentos para a integração da segurança nos sistemas de automação.

A parte 3 descreverá como o programa de segurança funcionará após a definição e implementação incluindo as métricas para avaliação de performance, auditorias e implementação de políticas e gerenciamento.

A ISA-99.00.04 enfatiza principalmente as características que diferenciam os sistemas de automação e controle, sob a ótica da segurança, dos sistemas convencionais de TI, com o objetivo de caracterizar as especificidades do ambiente de automação e controle, e definir políticas, procedimentos e métricas apropriadas.

O Relatório Técnico ANSI/ISA TR 99.00.01 define, classifica e avalia as tecnologias de segurança disponíveis no mercado servindo como base para a elaboração de normas e procedimentos e como fonte de informações para o desenvolvimento dos programas de segurança das organizações. Ele abrange algumas das disciplinas que compõem a administração e a gerência de redes convencionais, dentre elas:

- Autorização e Autenticação;
- Gerência e Distribuição de Senhas;
- Controle de Acesso;
- Encriptação;
- Validação de Dados;
- Monitoração, Detecção e Auditoria;
- Detecção de Intrusos;
- Ferramentas para Perícia Computacional;
- Gerência e Configuração de Computadores;
- Gerência Automática de Software;
- Software e Sistemas Operacionais para Servidores e Estações de Trabalho;
- Internet, Intranet e Web;
- Controle da Segurança Física.

Já o relatório ISA TR 99.00.02 apresenta sugestões para o desenvolvimento, implementação e operação de programas de segurança, enfatizando o comprometimento organizacional e profissional para a implantação e execução considerando as especificidades dos sistemas de Automação. O relatório detalha como elaborar entre outros:

- Missão e o Escopo;
- Detalhamento do Programa;

- Desenvolvimento dos elementos do programa;
- Plano de Gerência de Mudanças;
- Definição do nível de risco aceitável;
- Identificação do sistema e dos ativos existentes;
- Definição de procedimentos de avaliação e de análise de risco;
- Obtenção, identificação, seleção e implementação de medidas corretivas;
- Definição e realização de planos de testes de componentes e de medidas corretivas;
- Definição e realização de testes de desempenho de integração e pré-operação;
- Definição do plano de testes de validação e de desempenho do sistema;
- Finalização operacional das medidas de segurança.

2.6 OS PADRÕES DE MERCADO – GERÊNCIA SNMP

O SNMP é um protocolo da camada de aplicação que facilita a troca de informações de gerência entre elementos da rede. Parte do Transmission Control Protocol / Internet Protocol, habilita os administradores da rede a gerenciar seu desempenho, identificar e resolver problemas e planejar o seu crescimento.

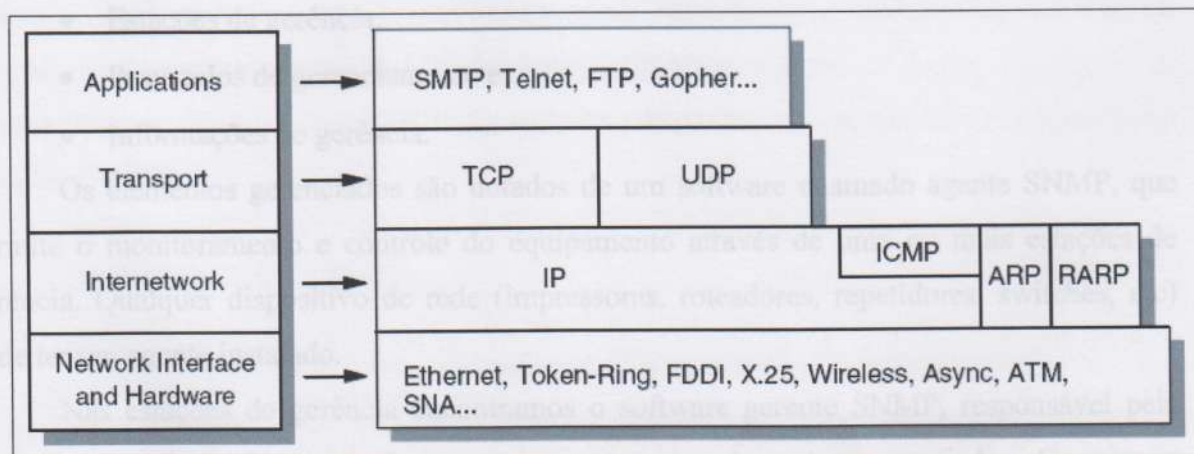


Figura 8- SNMP – Camadas TCP

As variáveis do SNMP permitem a visão do estado da rede através do monitoramento das variáveis de funcionamento dos protocolos das camadas físicas e de redes, de transporte e aplicação, além de viabilizar a determinação de indicadores de performance, disponibilidade e confiabilidade.

2.6.1 Gerenciamento de Redes Utilizando SNMP

De uma maneira geral, o gerenciamento de redes é realizado em três etapas:

- Coleta de dados;
- Diagnóstico;
- Ação ou controle.

A coleta de dados é um processo, automático que consiste de monitoração sobre os recursos gerenciados, o diagnóstico consiste do tratamento e análise realizados a partir dos dados coletados e uma ação ou controle é tomada em resposta à ocorrência de um evento anormal ou a um estado previamente configurado nos elementos gerenciados.

Um sistema de gerência consiste de um conjunto de ferramentas integradas para o monitoramento e controle dos elementos da rede através de uma interface gráfica que provê informações sobre o status da rede podendo oferecer ainda um conjunto de comandos que visam executar praticamente todas as atividades de gerenciamento sobre o sistema em questão. Todo o processo é suportado pelo SNMP.

São compostos por quatro componentes básicos:

- Elementos gerenciados;
- Estações de gerência;
- Protocolos de gerenciamento e;
- Informações de gerência.

Os elementos gerenciados são dotados de um software chamado agente SNMP, que permite o monitoramento e controle do equipamento através de uma ou mais estações de gerência. Qualquer dispositivo de rede (impressoras, roteadores, repetidores, switches, etc) pode ter um agente instalado.

Nas estações de gerência encontramos o software gerente SNMP, responsável pela comunicação direta desta estação com os agentes nos elementos gerenciados. Gerentes e agentes podem trocar tipos específicos de informações, conhecidas como informações de gerência.

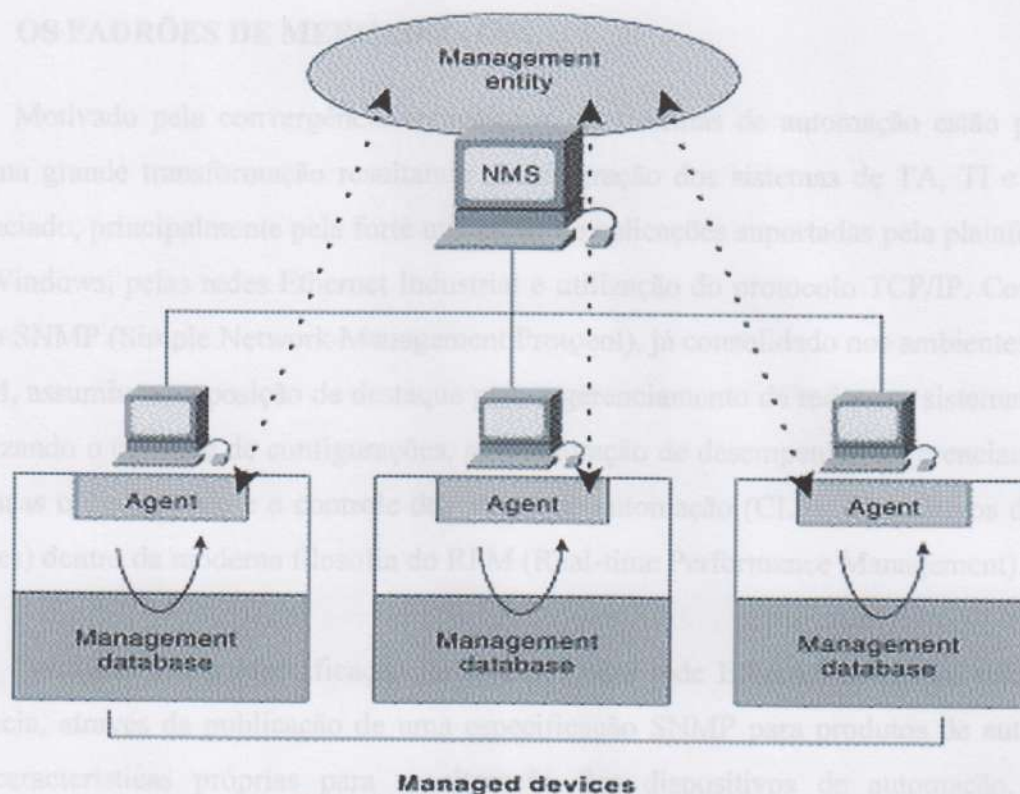


Figura 9- entidades funcionais do SNMP

O gerenciamento da rede através do SNMP permite o completo acompanhamento do estado, em tempo real, da rede, podendo ser utilizado para gerenciar diferentes tipos de sistemas. Este gerenciamento é conhecido como modelo de gerenciamento SNMP, ou simplesmente, gerenciamento SNMP. Portanto, o SNMP é o nome do protocolo no qual as informações são trocadas entre a MIB e a aplicação de gerência como também é o nome deste modelo de gerência.

Os comandos são limitados e baseados no mecanismo de busca/alteração. No mecanismo de busca/alteração estão disponíveis as operações de alteração de um valor de um objeto, de obtenção dos valores de um objeto e suas variações. A utilização de um número limitado de operações, baseadas em um mecanismo de busca/alteração, torna o protocolo de fácil implementação, simples, estável e flexível. Como consequência reduz o tráfego de mensagens de gerenciamento através da rede.

Como o funcionamento do SNMP é baseado em dois dispositivos o agente e o gerente, cada elemento gerenciado é visto como um conjunto de variáveis que representam informações referentes ao seu estado atual, estas informações ficam disponíveis ao gerente através de consulta e podem ser alteradas por ele. Cada máquina gerenciada pelo SNMP deve possuir um agente e uma base de informações MIB (Management Information Base).

2.7 OS PADRÕES DE MERCADO - OPC

Motivado pela convergência tecnológica, os sistemas de automação estão passando por uma grande transformação resultando na integração dos sistemas de TA, TI e TCOM, evidenciado, principalmente pela forte utilização de aplicações suportadas pela plataforma PC com Windows, pelas redes Ethernet Industrial e utilização do protocolo TCP/IP. Com isso o padrão SNMP (Simple Network Management Protocol), já consolidado nos ambientes de TI e TCOM, assumiu uma posição de destaque para o gerenciamento de redes em sistemas de TA, viabilizando o controle de configurações, a monitoração de desempenho, o gerenciamento de mudanças o diagnóstico e o controle dos ativos de automação (CLPs, dispositivos de rede e estações) dentro da moderna filosofia do RPM (Real-time Performance Management).

Conforme [5] a especificação da IAONA para rede Ethernet industrial reforça esta tendência, através da publicação de uma especificação SNMP para produtos de automação, com características próprias para monitoração dos dispositivos de automação. Alguns exemplos de OIDs (Object Identifier) adicionais encontrados nas MIBs (Management Information Base) 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.

2.7.1 Gerenciamento de Redes Industriais Utilizando OPC e SNMP

Visando contornar a falta de integração das ferramentas de gerenciamento de redes convencionais com os sistemas de automação, a tendência observada no mercado de TA é a utilização de soluções baseadas em SNMP e OPC (OLE for Process Control) integradas aos sistemas de automação, para o gerenciamento dos sistemas de automação (Scada, SDCD, Híbridos, PIMS, MES, etc.), que já reúnem características desejáveis para a monitoração de redes, por possuírem um cliente OPC.

Dessa forma é possível, que os operadores dos sistemas para monitoração do processo, 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.

2.8 PLANOS DE CONTINGÊNCIA

Um Plano de Contingência visa estabelecer os procedimentos básicos para a garantia da capacidade de recuperação dos serviços dentro das necessidades da organização como um todo. A implantação de um Plano de Contingência é resultado de um projeto típico com início, meio e fim definidos. A capacidade de uma organização responder a desastres é função da existência de um Plano de Contingência e da permanente atualização do mesmo.

A implantação de um plano depende de investimentos, do desenvolvimento de novos processos de trabalho e da documentação do desenvolvimento do Plano e dos procedimentos de contingência previstos. A documentação deve:

- Apresentar os critérios utilizados na construção do plano;
- Assinalar as mudanças necessárias nos processos de trabalho para que o plano possa ser executável e,
- Apresentar os procedimentos de contingência.

O conjunto dos procedimentos de contingência comporá o Plano de Contingência propriamente dito.

O projeto de desenvolvimento de um Plano pode ser dividido em três grandes fases:

- Fase 1: Ante Projeto ou Definição da Estratégia de Contingência;
 - Definição do Escopo
 - Análise de Impacto de Desastres
 - Seleção dos Serviços / Sistemas Críticos
 - Definição dos Pressupostos
 - Análise dos Riscos de Paralisação dos serviços/sistemas Críticos
 - Gestão dos Riscos dos Pressupostos
 - Seleção das Estratégias de Contingência
- Fase 2: Detalhamento e Implantação do Plano;
 - Detalhamento das Estratégias
 - Implantação dos Planos
- Fase 3: Testes e Manutenção do Plano;
 - Testes dos Planos
 - Manutenção dos Planos
 - Mudanças Internas
 - Mudanças externas

A ABNT – Associação Brasileira de Normas Técnicas homologou como norma brasileira em 2001, a NBR ISO/IEC 17799 – Código de Prática para a Gestão da Segurança da Informação, que é a base regular para a construção de planos de contingências, pois seu conteúdo cobre todos os assuntos inerentes à área de segurança da informação.

Os objetivos desta norma são:

- Estabelecer referencial para as organizações desenvolverem, implementarem e avaliarem a gestão da segurança da informação;
- Promover a confiança nas transações comerciais entre as organizações;
- Manter a segurança dos recursos de processamento da informação por prestadores de serviços, controlando o seu acesso;
- Proteger adequadamente os ativos da informação, inventariando-os e alocando uma equipe responsável para cada um;
- Reduzir os riscos de erros humanos, roubo, fraude ou uso indevido das instalações;
- Assegurar que os usuários estejam cientes das ameaças, treinando-os nos procedimentos de segurança e no uso correto das instalações de processamento da informação;
- Prevenir acesso não autorizado às informações e instalações da empresa;
- Minimizar o risco de falhas nos sistemas. Proteger a integridade do software e da informação;
- Estabelecer procedimentos de rotina para execução de cópias de segurança e para a disponibilização dos recursos de reserva;
- Garantir a proteção da infra-estrutura de suporte, principalmente do gerenciamento da rede;
- Prevenir a perda, modificação ou mau uso de informações trocadas entre organizações; e
- Proteger a confidencialidade, autenticidade ou integridade das informações, garantindo que a segurança seja parte integrante dos sistemas de informação.

A norma especifica 127 controles que podem compor o escopo do Sistema de Gerência de Segurança, tratando além de como estabelecer uma Política de Segurança, a construção de Planos de Contingências, Planos de Continuidade de Negócios, Organização da Segurança Física e Ambiental, Controle de Acesso, Legislação, etc.

Para implantação destes controles, a norma exige que seja realizada uma Análise de Risco, que deve ser documentada, determinando as necessidades, viabilidades e melhor relação custo/benefício implantação de um sistema de segurança da informação.

2.9 ACORDOS DE NÍVEL DE SERVIÇOS

Um acordo de nível de serviço é um contrato utilizado para a gestão das expectativas do cliente, fundamentado nas políticas e procedimentos de prestação dos serviços oferecidos. Tem como meta é definir uma estrutura para a gestão da qualidade e quantidade dos serviços entregues e, por conseguinte, atender à demanda dos clientes a partir de um entendimento claro do conjunto de compromissos. É um instrumento, de comunicação e de prevenção de conflitos, deve ser sempre atualizado para revisão do acordo, adequação dos serviços e negociação de ajustes no acordo e é base para garantir que ambas as partes usarão os mesmos critérios para avaliar a qualidade do serviço.

Observamos que área de TA assim como algumas outras áreas das empresas em geral não têm um entendimento claro de qual é a responsabilidade de cada uma das partes, quando o assunto é a prestação de serviços de TI, gerando expectativas diferentes para cada parte e insatisfação para ambas. Nas áreas de telecomunicações, manutenção de hardware e prestação de serviços de Internet, observa-se um movimento forte em direção à contratação por níveis de serviço. Principalmente porque isso envolve a área de infra-estrutura, que é o meio pelo qual o serviço de TI é prestado.

Para prover, bens ou serviços com eficiência é necessária a gestão dos níveis de serviço e dos custos contratados. Implicando na necessidade do entendimento claro do conjunto de compromissos entre um fornecedor e um cliente. Na área de Tecnologia da Informação e Comunicações (TIC), essa abordagem é conhecida como Gestão de Serviços ou Gestão de Serviços de TIC ou Gestão de Nível de Serviços (Service Level Management – SLM). Seu principal instrumento é o Acordo de Nível de Serviço (Service Level Agreement – SLA).

Quando o acordo de nível de serviço está implantado, a tarefa mais difícil passa a ser garantir que os níveis de serviço requeridos e especificados no acordo sejam atendidos. Para isto, é preciso definir indicadores e métricas que permitam acompanhar os níveis de serviço

bem como mecanismos e relatórios para seu monitoramento. O ideal é que o monitoramento seja feito de forma automatizada. Os métodos para capturar métricas de serviço devem contemplar o monitoramento de todos os componentes usados pelo serviço (sistema operacional, rede, banco de dados) e agregá-los para derivar as medidas de disponibilidade e desempenho geral.

Os relatórios de nível de serviço são um veículo de comunicação importante entre a área de TI, a comunidade usuária e as linhas de negócio. O público alvo e os detalhes das informações contidas nos relatórios a serem providos pela área de TI devem determinar a sua frequência de geração: diariamente, semanalmente, mensalmente e/ou trimestralmente. Relatórios efetivos permitem endereçar pró-ativamente dificuldades do serviço e reduzir o efeito negativo da reputação do departamento de TI como resultado de serviços indisponíveis ou da degradação de um serviço. Também podem reduzir a quantidade de chamadas ao help desk, quando usuários buscam conhecimento acerca de serviços de TI comprometidos.

Como já citado, a metodologia ITIL (Information Technology Infrastructure Library) [Brittain & Mingay, 2002] para o gerenciamento de serviços em TI, inclui a gerência de nível de serviço. Além disso, a identificação do impacto dos níveis de serviço nos negócios também tem sido foco de diversas iniciativas, tal como BSM (Business Service Management), que identifica, por exemplo, o impacto de uma falha na operação do ambiente de banco de dados sobre o negócio.

Figura 18 - Integração OPC-SNMP

Propõe-se então que as áreas de TA e TIC contribuam um grupo multidisciplinar, composto por especialistas das áreas de instrumentação, controle e automação com o objetivo de conjuntamente com os especialistas em administração e gerência de redes, estabelecerem políticas sólidas para projeto, operação e manutenção das redes industriais, contemplando também um conjunto de métricas e indicadores de acompanhamento de desempenho e mitigação de falhas, a serem utilizadas como base para a construção de um conjunto de procedimentos e padrões operacionais, na execução dos serviços com forte carga de atividades de TI e TCOM, como por exemplo:

- Administração de contas de usuários;
- Administração de backups e restores;
- Controle de licenças de software;

3 O MODELO PROPOSTO

O modelo aqui proposto considera principalmente o aproveitamento da atual experiência em administração e gerência de redes de computadores das áreas de TI e TCOM através de suas políticas e procedimentos operacionais, complementada com a tendência de mercado de automação industrial, na utilização do OPC com o SNMP, embasado na norma ISA SP-99, respeitando as particularidades das redes de automação e controle.

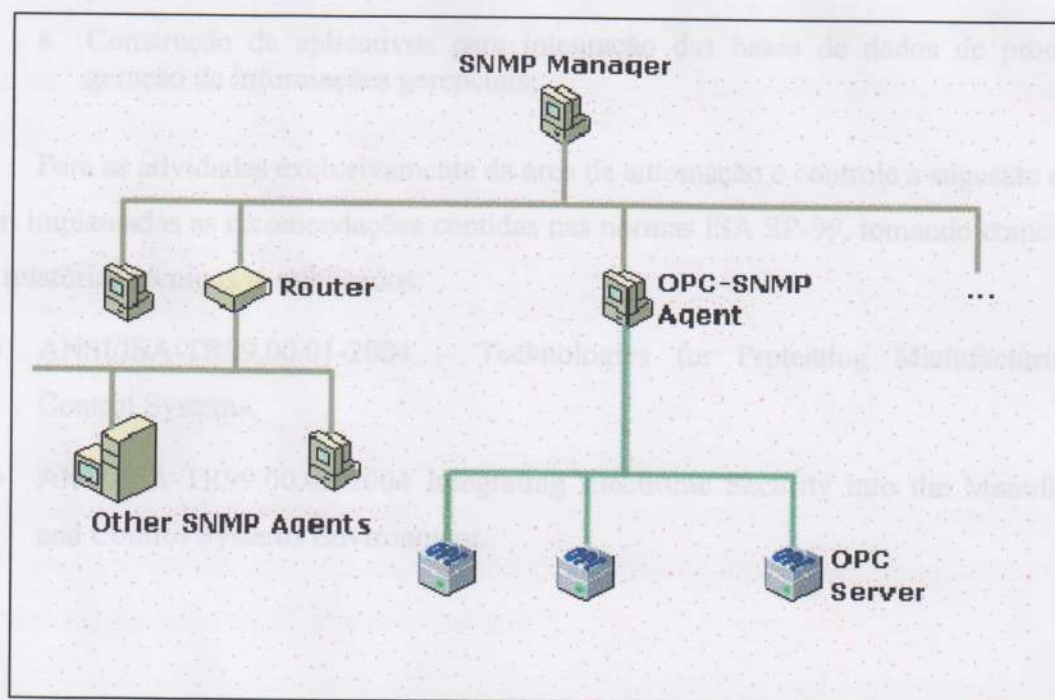


Figura 10 - Integração OPC-SNMP

Propõe-se então que as áreas de TA e TIC constituam um grupo multidisciplinar, composto por especialistas das áreas de instrumentação, controle e automação com o objetivo de conjuntamente com os especialistas em administração e gerência de redes, estabelecerem políticas sólidas para projeto, operação e manutenção das redes industriais, contemplando também um conjunto de métricas e indicadores de acompanhamento de desempenho e mitigação de falhas, a serem utilizadas como base para a construção de um conjunto de procedimentos e padrões operacionais, na execução dos serviços com forte carga de atividades de TI e TCOM, como por exemplo:

- Administração de contas de usuários;
- Administração de backups e restores;
- Controle de licenças de software;

- Controle e Inventário de ativos de informática e de redes locais;
- Especificação, instalação e configuração de Servidores, Estações, Impressoras, Switches, Firewalls e Roteadores;
- Gerência de desempenho e de falhas, com monitoração de alarmes e geração de relatórios periódicos;
- Controle e documentação da topologia de redes físicas e de endereçamento IP;
- Monitoração de segurança – Alteração de configurações, alerta para ataques e política antivírus, etc.;
- Construção de aplicativos para integração das bases de dados de processos e geração de informações gerenciais;

Para as atividades exclusivamente da área de automação e controle a sugestão é de que sejam implantadas as recomendações contidas nas normas ISA SP-99, tomando como base os dois relatórios técnicos já publicados:

- ANSI/ISA-TR99.00.01-2004 – Technologies for Protecting Manufacturing and Control Systems.
- ANSI/ISA-TR99.00.02-2004 Integrating Electronic Security into the Manufacturing and Control Systems Environment.

Considera-se, pois, que através do conjunto atual de normas e procedimentos de gerência de redes baseadas no modelo ISO-OSI juntamente com as definições TMN-GRS, suportadas por uma plataforma computacional (hardware e software de gerenciamento) fundamentada em políticas e procedimentos, e considerando também as recomendações e conceitos apresentados pela norma ISA 99-99, é possível agregar às redes industriais os ganhos proporcionados pelo gerenciamento de redes.

Os benefícios para empresa compreendem a redução de custos dos serviços de TIC para TA, a criação de um padrão de comunicação com as demais áreas da organização e a ampliação da visão dos profissionais de ambas as áreas, além de permitir:

- Tornar os processos de gerenciamento dos serviços de TIC para TA mensuráveis;
- Fornecer uma forma consistente de trabalho conjunta com uma terminologia padronizada;

4 CONSIDERAÇÕES FINAIS

A integração entre os sistemas de Tecnologia da Automação (TA) e da Informação (TIC) dá aos processos produtivos e aos sistemas de gestão empresarial maior eficiência na tomada de decisão baseada na real capacidade produtiva. Esta integração viabiliza, por exemplo, que as informações do chão de fábrica alimentem em tempo real os sistemas ERP de uma empresa. (A indústria automobilística já se utiliza destas facilidades.)

Além disso, a convergência tecnológica observada para os sistemas de TA, levou às redes de automação os padrões abertos, viabilizando, para estas redes, a utilização das mesmas tecnologias das redes “convencionais”:

- Protocolo TCP/IP;
- Servidores e estações Intel e RISC;
- Sistemas operacionais UNIX e WINDOWS;
- Switches Ethernet com SNMP;
- WEB Services, etc.

Sabemos que a rede Ethernet, juntamente com o protocolo TCP/IP, é um padrão “de facto” para os sistemas de TIC, sendo considerada pelos especialistas como a rede que será utilizada, em todos os níveis dos sistemas de TA.

Considere-se, pois, que através do conjunto atual de normas e procedimentos de gerência de redes baseadas no modelo ISO-OSI juntamente com as definições TMN-GIRS, suportadas por uma plataforma computacional (hardware e software de gerenciamento) fortemente embasada em políticas e procedimentos, e considerando também as recomendações e conceitos apresentados pela norma ISA SP-99, é possível agregar às redes industriais os ganhos proporcionados pelo gerenciamento de redes.

Os benefícios para empresa compreendem a redução de custos dos serviços de TIC para TA, a criação de um padrão de comunicação com as demais áreas da organização e a ampliação da visão dos profissionais de ambas as áreas, além de permitir:

- Tornar os processos de gerenciamento dos serviços de TIC para TA mensuráveis;
- Fornecer uma forma consistente de trabalho conjunto com uma terminologia padronizada;

- Aperfeiçoar os processos de comunicação;
 - Saber quanto custa manter a infra-estrutura de TIC para TA;
- [1] Magalhães, L. E. e Figueira, W. B. (2007) – “Gerenciamento de Serviços de TI na Prática – Uma abordagem com base na ITIL”, Novatec, São Paulo, SP.
- [2] ISO/IEC 7498-4:1989 - Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 4: Multilayered framework, Geneva.
- [3] WWW.TELECO.COM – março de 2003.
- [4] Cooman, E. C. - “An Overview of ISA99 Part 1” – Apresentado na ISA EXPO 2005, Reliant Center, Houston, TX, U.S.A.
- [5] Fonseca, M. D. ET AL – “Monitoração do Desempenho de Redes de Automação Usando SNMP” – Apresentado no Seminário de Automação de Processos, 2005, Curitiba, PR.
- [6] Miranda dos Anjos, I. e Motta Pires, P. S. - “Uma Visão Geral Sobre Propostas de Políticas de Administração de Segurança em Ambientes de Automação Industrial” – Apresentado no 6º Congresso de Automação, Sistemas e Instrumentação, 2006, São Paulo, SP.
- [7] Córdaro, S. - “Melhores Práticas para o Gerenciamento de Redes de Automação” – Apresentado no 6º Congresso de Automação, Sistemas e Instrumentação, 2006, São Paulo, SP.
- [8] WWW.ISA-99.COM – abril de 2003.
- [9] Müller, M. - “Managing Internetworks with SNMP” (1996) – M&T Books, New York, NY, U.S.A.
- [10] WWW.SNMP-OPC-GATEWAY.COM – abril de 2003.
- [11] WWW.REDESDecomPUTADORES.COM.BR - maio de 2003.
- [12] Macoda, Paloma de Oliveira – “Plano de contingências do setor de Tecnologia da Informação para empresa de telecomunicações” – Monografia – ULBRA – Canoas – RS.
- [13] Goncal, Silvia Bogica, ET AL – “Um Modelo para Acordo de Nível de Serviço na ITIL” – UFES – Vitória – ES.
- [14] HTTP://WWW.PROFIRUS.ORG.BR – maio de 2003.

REFERÊNCIAS BIBLIOGRÁFICAS

- [1] Magalhães, I. L. e Pinheiro, W. B. (2007) – “Gerenciamento de Serviços de TI na Prática - Uma abordagem com base na ITIL”, Novatec, São Paulo, SP.
- [2] ISO/IEC 7498-4:1989 - Information processing systems -- Open Systems Interconnection -- Basic Reference Model -- Part 4: Management framework, Geneva.
- [3] WWW.TELECO.COM – março de 2008.
- [4] Cosman, E. C. - “An Overview of ISA99 Part 1” - Apresentado na ISA EXPO 2007, Reliant Center, Houston, TX, U.S.A.
- [5] Fonseca, M. O. ET All – “Monitoração do Desempenho de Redes de Automação Usando SNMP” – Apresentado no Seminário de Automação de Processos, 2005, Curitiba, PR.
- [6] Miranda dos Anjos, I. e Motta Pires, P. S. – “Uma Visão Geral Sobre Propostas de Políticas de Administração de Segurança em Ambientes de Automação Industrial” – Apresentado no 6º Congresso de Automação, Sistemas e Instrumentação, 2006, São Paulo, SP.
- [7] Cordeiro, S. – “Melhores Práticas para o Gerenciamento de Redes de Automação - Apresentado no 6º Congresso de Automação, Sistemas e Instrumentação, 2006, São Paulo, SP.
- [8] WWW.ISA-99.COM – abril de 2008.
- [9] Miller, M. – “Managing Internetworks with SNMP” (1996) – M&T Books, New York, NY, U.S.A.
- [10] WWW.SNMP-OPC-GATEWAY.COM – abril de 2008.
- [11] WWW.REDESDECOMPUTADORES.COM.BR – maio de 2008.
- [12] Macedo, Paloma de Oliveira – “Plano de contingências do setor de Tecnologia da informação para empresa de telecomunicações” – Monografia – ULBRA – Canoas – RS.
- [13] Gomes, Silvia Bogéa . ET All – “Um Modelo para Acordo de Nível de Serviço em TI”, UFES – Vitória – ES.
- [14] HTTP:// WWW.PROFIBUS.ORG.BR – maio de 2008.