

Conceito de segurança em níveis para a conectividade industrial

Eng^o Márcio Vaz
Gerente de vendas de automação da Phoenix Contact

A conectividade e os seus riscos

Em 2003 houve uma queda de energia repentina na região nordeste dos Estados Unidos, que provavelmente foi causada por um acesso não autorizado ao sistema de controle, através de um canal de comunicação utilizado pela concessionária para manutenção remota. Problemas como esse tem sido cada vez mais comum no dias atuais, pois o acesso remoto tem sido um dos melhores caminhos para a diminuição de custos de operação.

Situações inesperadas como essa e muitas outras podem ocorrer causando diversos danos, tais como:

- Perda de produção/qualidade;
- Dano às pessoas ou à propriedade;
- Reclamações por dano e por perdas financeiras;
- Perda de propriedade intelectual;
- Perda de imagem frente ao mercado.

Muitas variáveis, (figura 1), compõem as causas que comprometem o funcionamento de um sistema, sendo três deles os de maior destaque: o erro humano, os hackers e o vírus. Não há uma receita de segurança que seja infalível a todos eles, mas diversos cuidados podem ser adotados para que situações como a que ocorreu em 2003 possam ser evitadas.



Figura 1: Segurança em níveis para Ethernet Industrial

A conectividade no ambiente industrial

Muitas empresas atualmente procuram otimizar as suas redes tanto no escritório quanto em seu parque fabril

com a finalidade de melhorar a comunicação em todos os níveis buscando assim o aumento da produtividade enquanto obviamente protegem seu negócio, mas está mais que comprovado que a infra-estrutura técnica precisa ser maior e mais complexa, demandando um gerenciamento diferenciado para a rede de automação que é o coração da produtividade e da competitividade da empresa, por isso é essencial assegurar que aspectos de segurança nunca sejam negligenciados.

A palavra segurança em português serve para traduzir do inglês as palavras: safety e security, mas elas são distintas dentro do conceito de automação, sendo que a primeira está relacionada com a segurança humana e a segunda com a segurança de acesso ou de informação. Um grande empreendedor industrial do segmento de soluções de conectividade, resumiu essa analogia pelas seguintes palavras: “*algo Safety é proteger as pessoas das máquinas e algo Security é proteger os dados das pessoas*”.

Atualmente a automação baseada em soluções em tecnologia da informação, assim como são as redes no escritório, já é uma realidade na interligação de controladores e outros dispositivos, mas a tendência é de que os conhecidos barramentos de campo, (Interbus, Profibus, Modbus, As-i, Devicenet, etc...), serão gradualmente integrados a outros sistemas de automação com procedimentos de comunicação baseados na Ethernet, tais como: Profinet, modbus TCP, Ethernet IP, etc... , ou seja o padrão RJ45 para conectores já alcança os módulos de entrada e saída no chão de fábrica, dessa forma termos como: MAC ADDRESS e ENDEREÇO IP passam a compor o vocabulário dos profissionais de automação, mas isso também indica que os mesmos problemas que as redes de escritório têm enfrentado são os mesmos que a planta fabril terá ou passou a enfrentar, dessa forma o conceito para a segurança de um sistema de automação deve contemplar os seguintes requisitos:

- Implementação da segurança através da infra-estrutura;
- Não afetar os sistemas existentes;
- Benefícios na implementação sem a necessidade de profundo conhecimento em TI;
- Detecção de violações de segurança e o envio de mensagens de aviso;
- Possibilidades de adaptação as demandas dos sistemas de automação.



Classificação de níveis de segurança na conectividade da automação

Tendo em mente que as dificuldades em defender as redes do escritório e de automação contra erros humanos, sejam eles propositais ou não são as mesmas, o planejamento com redes de automação baseados em ethernet deve avaliar que é na rede em que está a maior vulnerabilidade do sistema. Para uma analogia usa-se o sistema vascular humano, onde o vírus e as bactérias podem ser transportados por todas as partes do corpo humano causando problemas ao organismo e podendo até mesmo levar ao colapso total, então o melhor é evitar o contato do sistema circulatório com qualquer coisa alheio ao corpo humano evitando assim a contaminação, mas muitas vezes medicamentos e exames invasivos precisam ser realizados.

Com a analogia do parágrafo anterior fica claro que é através da rede de comunicação que erros podem ser propagados e levar todo o sistema conectado ao colapso. Pelo dinamismo do processo produtivo às vezes são necessárias intervenções e acessos à rede para correções ou implementação de melhorias, mas esses acessos devem ser seguros o suficiente para não comprometerem a funcionalidade do sistema por “contaminação”.

Para a implementação de um sistema de segurança na rede de chão de fábrica três pontos principais devem ser atendidos: o primeiro é o de se adaptar a estrutura atual de rede, o segundo é o de ter a possibilidade de aceitar as tecnologias de redes futuras e o terceiro é de ser de fácil utilização respeitando os padrões industriais.

Muitas vezes o fato de implementar uma segurança por apenas limitar o acesso externo pode não ser a decisão mais efetiva para a defesa da rede de automação, mas uma defesa gradual em pontos estratégicos e frágeis pode ser a melhor opção para uma defesa mais completa contra acessos não autorizados e esse tipo de artifício não é nada novo, pois essa tática foi usada por séculos na defesa de castelos e fortalezas, somente esse tipo de defesa, por níveis, pode proteger contra fraquezas internas e sabotagens. Ao

manter a tática de segurança descentralizada no ambiente de comunicação industrial, onde também é respeitado o modelo ISO/OSI, (figura 2), conclui-se que é necessário um tipo de proteção diferentes nomeadas por níveis para cada uma das três primeiras camadas (layers), conforme é descrito a seguir.

Nível um: Segurança mecânica

Limitar o acesso. Uma solução simples é utilizar uma trava junto com o conector de rede, que após ser introduzido na porta RJ45 não é possível retirá-lo a menos que se possua uma ferramenta especial que somente pessoas autorizadas podem possuir, e para as portas que não são utilizadas usa-se uma tampa que também é removida através do uso da mesma ferramenta (figura 3). Essa simples medida de proteção protege a rede de

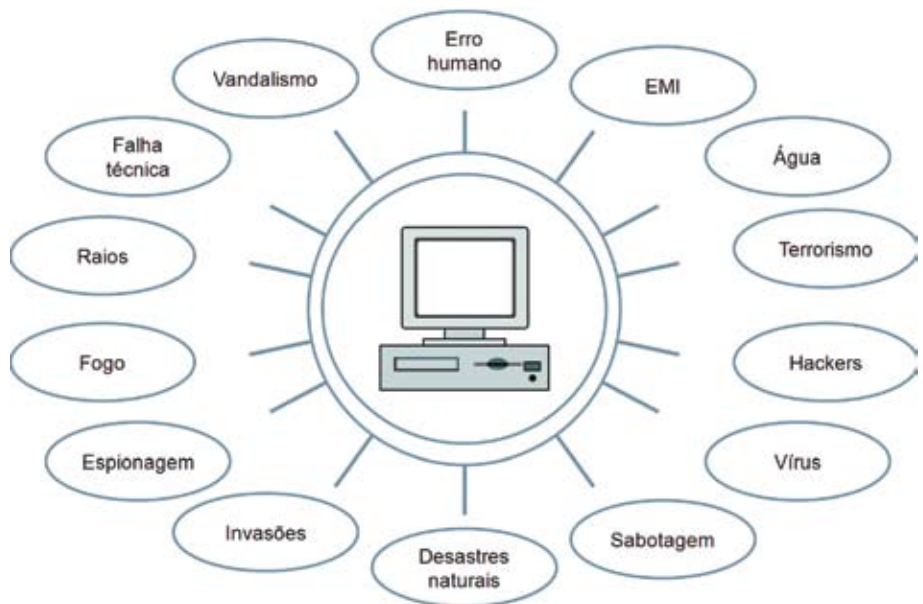


Figura 2: Situações de risco para o funcionamento pleno de um sistema de comunicação e dados

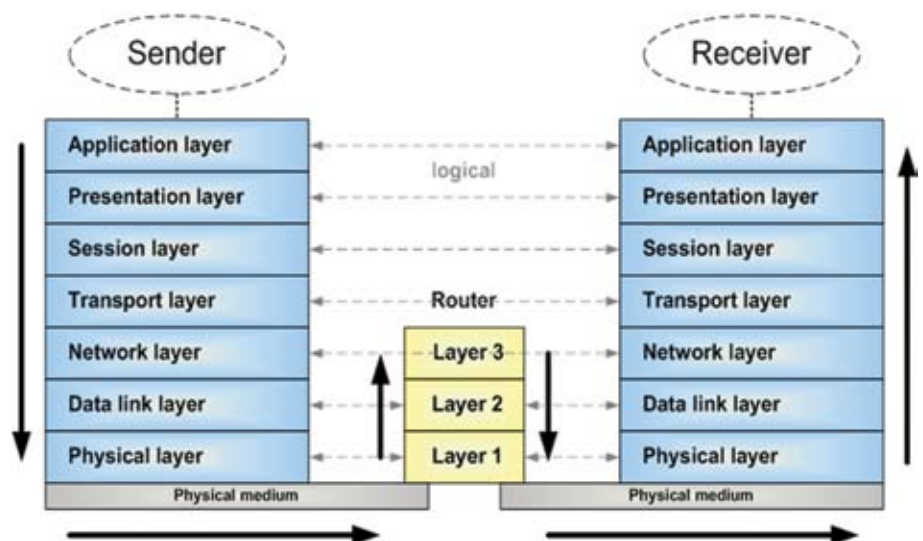


Figura 3: Princípio básico de comunicação – modelo ISO/OSI

potenciais de fraquezas, como: conexões não autorizadas, desconexão do cabo de rede de importantes linhas de comunicação que podem comprometer todo o processo.

Nível dois: uso de switches gerenciáveis

Os switches gerenciáveis possibilitam um grande espectro de opções de segurança contra pontos fracos, mas em contrapartida há o aumento do custo inicial durante a fase de instalação, por isso a frase "O quanto vale a informação segura e no tempo certo?", deve ser o ponto principal para o início de um projeto no chão de fábrica bem estruturado. Segue alguns pontos positivos referentes ao uso do switch industrial no ambiente fabril:

- Senha de segurança para prevenir que pessoas não autorizadas possam reconfigurar a infra-estrutura da corrente;
- Limitador de broadcast previne ataques por infiltração (figura 4);
- Controle de acesso, onde as configurações somente serão alteradas, conforme endereço de IP previamente autorizado pelo administrador;
- Segurança por porta. Esse modelo de segurança permite ao administrador da rede, determinar qual é o endereço MAC (Media Access Control) que pode ter acesso a rede através de uma específica porta RJ45 (figura 5);
- Detecção de violação usando o protocolo SNMP (Simple Network Management Protocol) ou uma condição de sinalização para o administrador responsável para reação imediata.

VLAN (Virtual Local Area Networks), torna possível separar fisicamente as redes conectadas. As linhas de comunicação somente permitem o acesso a rede virtual a qual o componente foi parametrizado pelo administrador (figura 6).

Nível três: roteadores e firewalls

O uso de firewalls e roteadores possibilita a proteção de um sistema de automação de forma descentralizada por combinar amplos mecanismos de segurança e funcionalidades diversas para o ambiente fabril (figura 7).

Um sistema central de firewall protege a rede da empresa inteira



Figura 4: Bloqueios e travas mecânicas para a segurança de acesso físico.



Figura 5: Configuração simples de Broadcast com alta eficiência na segurança



Figura 6: Configuração simples de acesso por endereço MAC, incluindo descrições para informar o sistema o ponto exato de tentativa de violação

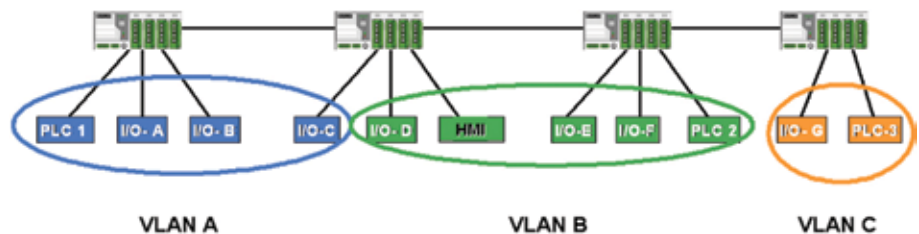


Figura 7: Configuração simples de uma rede virtual onde alguns equipamentos utilizam o mesmo switch gerenciável, mas a troca de informações somente ocorrerá entre as portas pertencentes à mesma rede virtual



Figura 8: Roteador e firewall atende os requisitos para o ambiente industrial (alimentação em 24Vdc, fixação em trilho DIN e contatos adicionais para sinalização mecânica)

ou a conexão entre duas redes que não podem sofrer interferências de outras redes. Células de produção autônomas podem somente ser protegidas usando um conceito de descentralização, por subdividir o sistema produtivo em células de segurança independentes, onde cada uma terá o seu conceito, dessa forma operadores podem alcançar o grau de flexibilidade e confiança necessário para a célula, dessa forma uma célula segura é o equivalente a uma célula produtiva com uma funcionalidade específica, e hoje está disponível três funções escalonadas com a utilização do componente da figura 7:

- Roteamento industrial;
- Segurança de rede;
- Acesso remoto ou tele serviços.

Roteamento Industrial

Direcionamento para melhorar a disponibilidade e a segurança, por evitar o acesso do escritório (internet) para os periféricos conectados a máquinas na fábrica e duplicação de endereço IP, utilizando a opção NAT 1:1, (Network Address Translation), sem interferir na funcionalidade da rede (figura 8). Seguem alguns dos principais benefícios:

Segurança da rede industrial

Firewall para controlar e filtrar os direitos de acesso, também serve para proteger a rede de pessoas não autorizadas através do firewall (figura 9)

Acesso remoto ou tele serviço

Transferência de dados encriptografados para proteger dados sensíveis (receitas e bateladas) e habilitar o acesso remoto seguro (para manutenção remota, no caso de acordo de serviços). (figura 10)

Conclusão

Não há uma receita padrão para alcançar um alto nível de segurança em uma rede de automação, ou uma confiabilidade total em informações corporativas, pois a segurança da comunicação é um processo dinâmico, não é simplesmente uma condição alcançada devendo ser apenas mantida, mas é algo que deve acompanhar os desenvolvimentos tecnológicos com os devidos cuidados orientados para a segurança na troca de informações. Quando é analisado o investimento inicial em um sistema de segurança de automação pode-se idealizar que o investimento é desnecessário, mas vale refletir na seguinte pergunta: "O quanto custa não obter essa ou aquela informação para a tomada de decisão dentro de uma planta fabril? Ou quanto custa uma planta parada por um erro não intencional? Ou melhor, o quanto custa o seu segredo industrial?". Perguntas como essa devem estimular os planejadores e administradores financeiros a avaliar a necessidade de proteger o investimento fabril.



Figura 9: Modelo de segurança entre por isolar a planta fabril do escritório



Figura 10: Controle de acesso externo

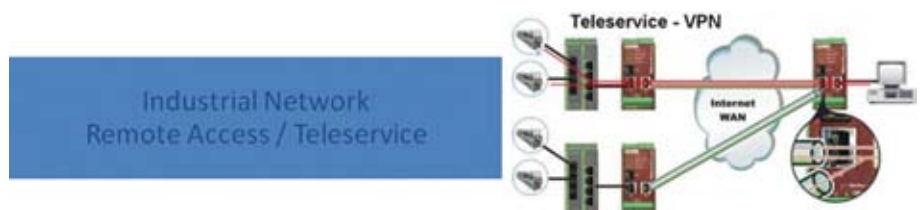


Figura 11: Acesso remoto