PROFIsafe – o perfil de segurança PROFIBUS

César Cassiolato
Gerente de Produtos - Smar Equipamentos Industriais Ltda e Vice-Presidente da Associação PROFIBUS Brasil.

INTRODUÇÃO

A demanda por mais e mais recursos na automação e controle de processos com o advento da tecnologia digital e com o "boom" do Fieldbus, favorecem o desenvolvimento da tecnologia dedicada ao diagnóstico e tratamento de falhas seguras, principalmente voltada à proteção de pessoas, equipamentos/máquinas e ambiente, ou seja, é a busca pelo sistema seguro.
Um sistema seguro requer, em outras palavras, que os dados e informações possam ser validados em relação aos seus valores e ao domínio do tempo, o que deve se aplicável no sistema como um todo.Isto implica em garantir que um dado recebido, foi enviado corretamente e que quem o enviou, também é o correto transmissor, e além disso, é a informação que se esperava neste instante; a informação que foi recebida esta seqüencialmente correta, etc.
Atualmente, o exemplo mais típico de padrão de segurança internacional e que envolve a maior parte dos desenvolvedores e implementadores de sistemas com segurança é o chamado IEC 61508. Este padrão mostra as atividades envolvidas em todo ciclo de vida de sistemas eletrônicos programáveis em relação à segurança.Portanto, trata tanto de requisitos de hardware quanto de software.
O perigo de acidentes em processos industriais é vasto e a probabilidade de acontecer um acidente depende das probabilidades de falhas do sistema.A implicação de falhas depende do tipo e requisitos de segurança da aplicação.

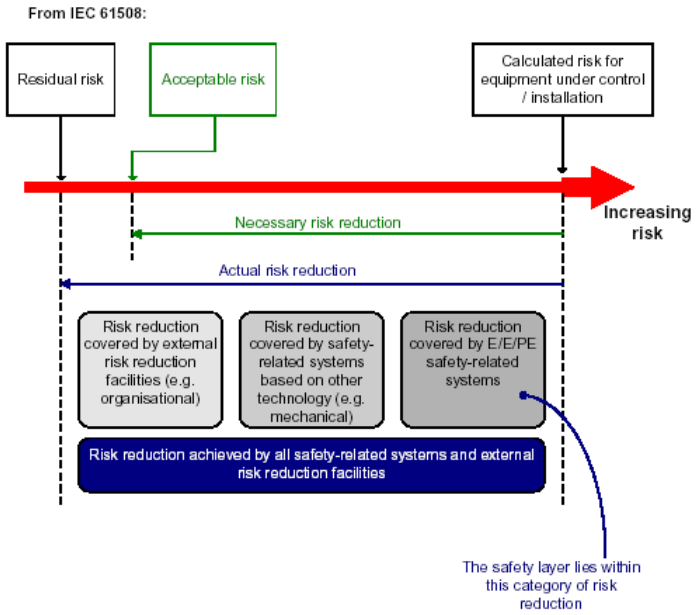

Figura 1- Considerações de risco de acordo com a IEC 61508.

O perfil de aplicação PROFIBUS, "PROFIsafe" - Perfil para Tecnologia Segura - descreve mecanismos de comunicação segura entre periféricos sujeitos à falha-segura (Fail-Safe) e controladores seguros.É baseado nos requisitos dos padrões e diretivas para aplicações com segurança orientada, como a IEC 61508 e EN954-1, bem como na experiência dos fabricantes de equipamentos com Fail-Safe e na comunidade de fabricantes de PLCs.

Veremos a seguir, de forma resumida, seus principais conceitos.

PROFIsafe

Este perfil suporta aplicações seguras em uma extensa área de aplicações em campo que ao invés de utilizar barramentos especiais para as funções de segurança, permite a implementação da automação segura através de uma solução aberta e no padrão PROFIBUS, garantindo os custos efetivos de cablagem, consistência do sistema em relação à parametrização e funções remotas de diagnósticos. Garante a segurança em sistemas de controle descentralizados através da comunicação Fail-Safe e dos mecanismos de segurança dos dispositivos e equipamentos.

Veja a seguir alguns exemplos de áreas de aplicação deste perfil de segurança;

- Indústria de Manufatura
- Proteção rápida de pessoas, máquinas e ambiente
- Funções de paradas de emergência
- Barreiras de luz
- Controle de entrada

- Scanners
- Drivers com segurança integrada
- Controle de processos em geral
- Áreas química e petroquímica
- Transporte público
- etc.

A tecnologia aberta PROFIBUS atende a uma série de requisitos das aplicações em termos de segurança de acordo com o PROFIsafe:

- independência entre comunicação relevantemente segura e a comunicação segura.
- aplicável a níveis SIL3(IEC61508), AK6 (DIN V 19250) e categoria de controle 4(KAT4) (EN 954-1).
- A redundância é usada somente para aumentar a confiabilidade.
- Qualquer master ou link DP pode ser usado;
- Na implementação, masters DP, ASICs, links e couplers não devem sofrer modificações, desde que as funções de segurança são implementadas acima da camada OSI layer 7(isto é, nenhuma mudança ou acomodações no protocolo DP).
- A implementação das funções de transmissão segura devem ser restritas à comunicação e o equipamento e não devem restringir o número de equipamentos.
- É sempre uma relação de comunicação 1:1 entre os dispositivos F
- Os tempos de transmissões devem ser monitorados.

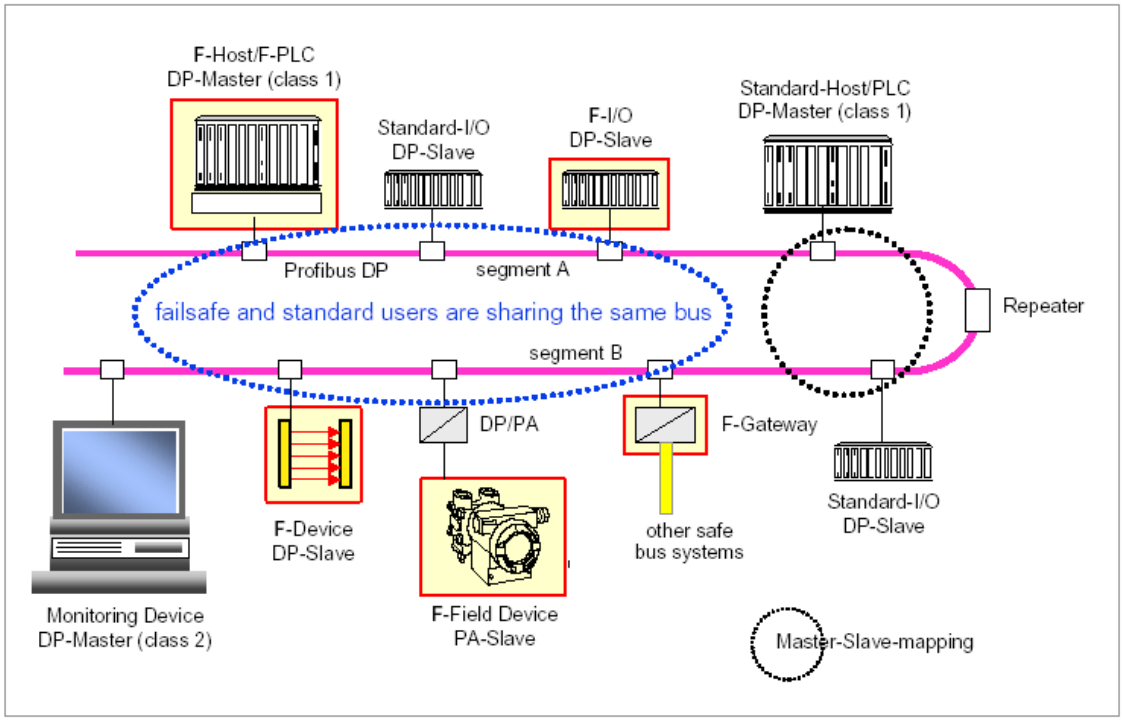

Figura 2 – Sistema típico onde se tem a comunicação padrão e segura compartilhando o mesmo barramento e protocolo.

Na prática, aplicações segura e padrão estarão compartilhando os sistemas de comunicação Profibus DP simultaneamente. As funções de transmissões seguras incluem todas as medidas que podem estar deterministicamente descobertas pelas possíveis falhas perigosas que podem ser infiltradas no sistema de transmissão padrão, com a intenção de minimizar seus efeitos. Isto incluem as funções de mau funcionamento randômico, por exemplo,efeitos de EMI, falhas sistemáticas de hardware ou software, etc.
Por exemplo, é possível que durante uma comunicação que se perca parte do frame, ou que parte do mesmo apareça repetida ou ainda que apareça em ordem errada ou mesmo em atraso.
No PROFIsafe algumas medidas preventivas são tomadas, com o intuito de cercar as possíveis causas de falhas e quando as mesmas ocorrerem, que aconteçam com segurança:

- Numeração consecutiva de todas as mensagens seguras: aqui pretende-se minimizar a perda de comunicação, inserção de bytes no frame e seqüência incorreta.
- Sistema de watchdog timer para as mensagens e seus reconhecimentos: controlando os atrasos.
- Uma senha(password) entre emissor e receptor: evitando linking entre as mensagens padrão e segura.
- Proteção adicional do telegrama com a inclusão de 2 a 4 bytes de CRC: evitando a corrupção dos dados de usuário e linking entre as mensagens padrão e segura.

Estas medidas devem ser analisadas e tomadas em uma unidade de dado Fail-Safe.Veja a seguir o modelo de mensagem F.

A SOLUÇÃO PROFIsafe

O PROFIsafe é uma solução em software com canal único que é implementada como uma camada adicional acima do layer 7 nos dispositivos. Um layer seguro define métodos de aumentar a probabilidade de se detectar erros que possam ocorrer entre dois equipamentos/dispositivos se comunicando em fieldbus.
A grande vantagem é que pode ser implementada sem mudanças, provendo proteção aos usuários de seus investimentos.
Se utiliza dos mecanismos da comunicação cíclica nos meio físicos 485 ou H1(31.25kbits/s). A comunicação acíclica é utilizada para níveis irrelevantes de segurança de dados.Garante tempos muito curtos de respostas, ideal em manufaturas e operação intrínseca segura, de acordo com as exigências da área de controle de processos.A figura 3 mostra a arquitetura do PROFIsafe.

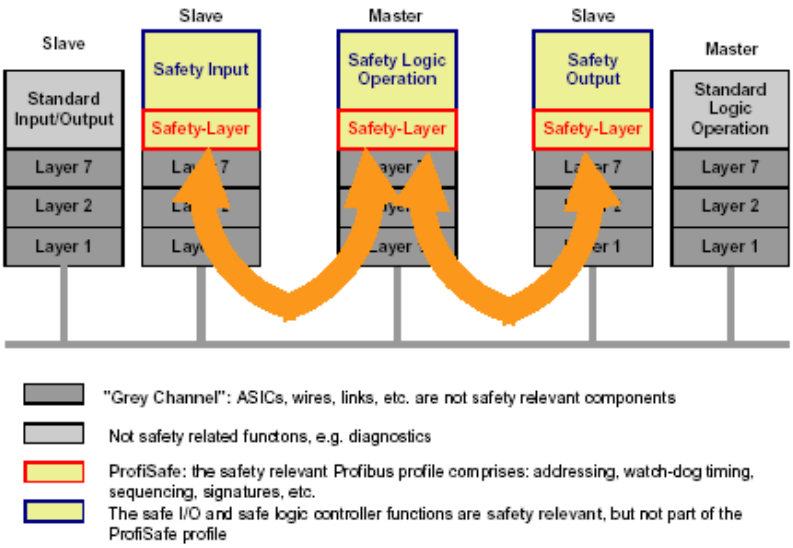

Figura 3 – A arquitetura do PROFIsafe

A figura 4 mostra o modelo da estrutura de mensagem na transmissão. O perfil seguro (F-Profile) é embutido no protocolo de transmissão DP(layer 7) e na codificação(layer 2).

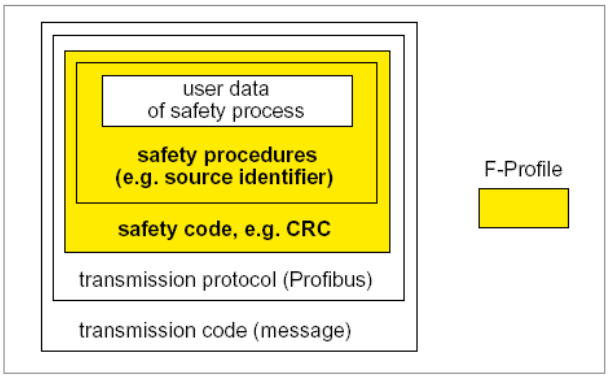

Figura 4 – modelo para dados seguros

O PROFIsafe utiliza o mecanismo de detecção de erros para manter os níveis desejáveis de segurança. É responsabilidade deste perfil detectar erros de comunicação como frames duplicados, perda de frames, seqüências incorretas de frames, frames corrompidos, atrasos nos frames e endereçamento errados de frames. O perfil PROFIsafe utiliza a redundância da informação para validar a comunicação entre dois dispositivos. A informação de segurança relevante é transmitida em conjunto com os dados de processos, isto é, estes dados são embutidos no frame básico do Profibus DP.Um frame deste tipo pode tratar no máximo 244 bytes de dados de processo.O PROFIsafe reserva 128 bytes deste total para os dados de segurança.Além destes, 4 ou 6 bytes são tratados à parte como bytes de status e controle dependendo da quantidade de dados seguros transmitidos.Sempre dois bytes de controles são enviados em cada frame, um de status e

outro com a seqüência dos frames.Os quatro bytes restantes são reservados para o checksum que é gerado para proteger a informação de segurança redundante. Uma pequena quantidade de dados de segurança relevante transmitida implica em um CRC de 16 bits e em 4 bytes de controle.Para transmissões com mais de 12 bytes de dados seguros(até 122), um CRC de 32 bits é usado e 6 bytes de controle são necessários.
A figura 5 mostra o modelo de frame DP que contém em sua informação os já conhecidos bytes deste frame, mais os dados de Fail-safe (no máximo 128 bytes em 244 bytes, devido a limitação de 64 words na troca de dados de uma só vez, entre o Host e o mestre DP), assim como os recursos de segurança de paridade e FCS(Frame Checking Sequence).

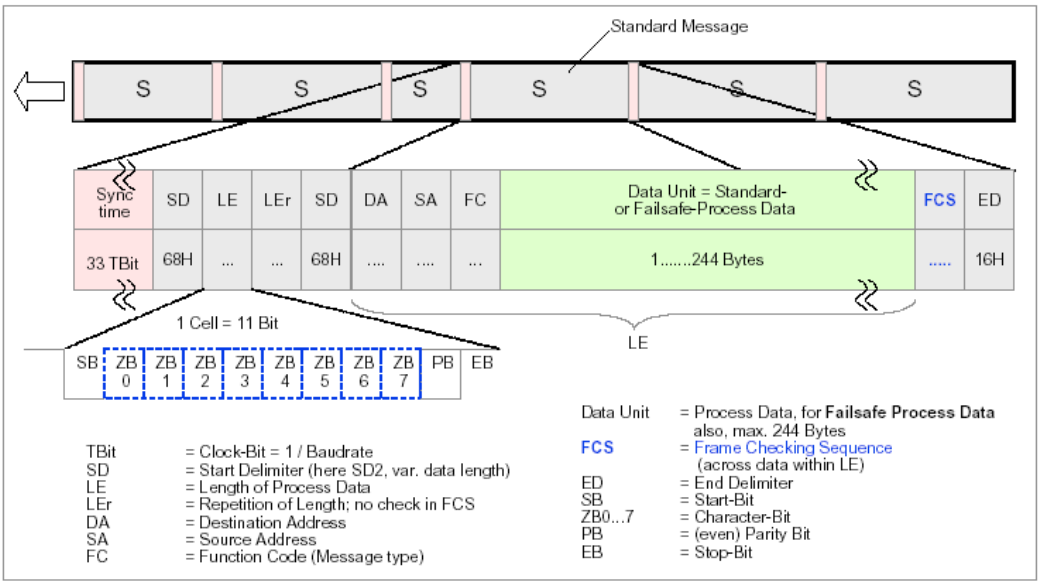

Figura 5 – modelo do frame do DP

A figura 6 mostra o modelo de mensagem F(mensagem segura), onde podem ver vistos os bytes de controle de integridade e minimização de erros descritos anteriormente como medidas preventivas.

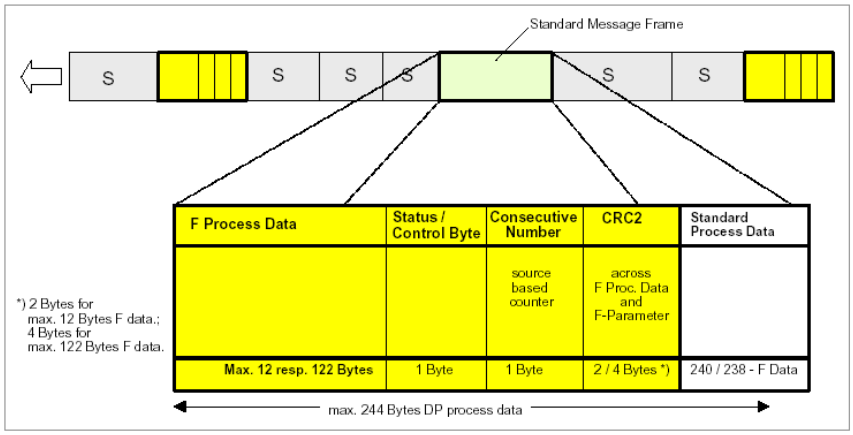

Figura 6 – modelo da mensagem F

A figura 7 nos mostra detalhes do tratamento da falha segura, comunicação, timerouts, CRCs, numeração das mensagens, etc.

Bit7	Bit6	Bit5	Bit4	Bit3	Bit2	Bit1	Bit0
tbd	res	res	Failsafe values (FV) activated	Communication failure: WD-timeout	Communication failure: CRC or consecutive number	Failure exists in F slave or F module	F slave has new i-parameter values assigned

Figura 7 – modelo do status/control byte

Através da monitoração e controle de informações entre mestres e escravos seguros, tais como: sincronização, ciclo de protocolo F, watch dog timers, ordem das mensagens, repetições do frame, monitor SIL(contador de mensagens corrompidas em um período de tempo) pode-se garantir a segurança aos níveis de integridade:

SIL	CRC	Length of process data	Time period (h)
3	16 Bit	< 16 Bytes	10
2	16 Bit	< 16 Bytes	1
3	32 Bit	< 128 Bytes	0.1
2	32 Bit	< 128 Bytes	0.01

Figura 8 – SIL monitor

ARQUIVOS GSD & PROFIsafe

Equipamentos suportando as características PROFIsafe têm a inclusão em seu arquivo GSD da seguinte palavra chave:

F_Device_supp = 1 ; 1 = F-device

CONCLUSÃO

O PROFIsafe é uma solução em software com canal único que é implementada segundo os padrões mais rigorosos em termos de segurança e sua grande vantagem é que pode ser implementada sem mudanças, provendo proteção aos usuários de seus investimentos.Não existem restrições ao número de dispositivos no barramento e taxas de comunicação.
A não necessidade de convivência de protocolos proprietários voltados à segurança, a abertura do protocolo, proporcionando interoperabilidade/intercambiabilidade entre os vários fornecedores, a fácil integração em PLCs e os sistemas já existentes são exemplos dos benefícios de tal funcionalidade.
Além disso, equipamentos e dispositivos com tal característica disponibiliza uma série de vantagens: os dados de qualquer dispositivo pode ser visto de qualquer ponto da rede,

incluindo os níveis gerenciais e de escritório. Pode-se monitorar a performance da planta mesmo no chão de fábrica e fazer o planejamento em manutenções em busca da otimização de paradas.Isto tudo em modo real-time e com a grande vantagem, num mesmo protocolo de comunicação.É a inteligência distribuída combinada com a tecnologia de software.
A lista de produtos com tal funcionalidade ainda não é extensa, mas cada vez mais encoraja os fabricantes a lançarem seus produtos com tal tecnologia.
Mesmo em outros protocolos de comunicação é inevitável a demanda por tais requisitos.

BIBLIOGRAFIA

- PROFIBUS-DP/PA - ProfiSafe, Profile for Failsafe Technology.
- IEC 61508 – Functional safety of electrical/electronic/programmable electronic safety-related systems.