Implementação do Protocolo PROFIsafe para o Desenvolvimento de Sistemas Seguros

William Vidal, Rodrigo Dobler, Sérgio Cechin, Taisy Weber e João Netto
Departamento de Informática Aplicada
Universidade Federal do Rio Grande do Sul
Porto Alegre, Brasil
{wrcvidal, rjdobler, cechin, taisy, netto}@inf.ufrgs.br

Resumo — Protocolos de comunicação seguros são essenciais para o desenvolvimento de sistemas seguros a serem utilizados em aplicações críticas na automação industrial, onde falhas não detectadas podem causar danos irreparáveis a vida ou ao meio-ambiente. Esses protocolos seguros são desenvolvidos e certificados de acordo com a norma de Segurança Funcional IEC61508. Essa norma especifica os mecanismos para detecção de erros que devem ser implementados para detectar os erros de comunicação que podem ocorrer durante a transmissão de dados, assegurando assim a troca correta de informações entre os dispositivos. Este artigo apresenta a implementação do protocolo seguro de comunicação PROFIsafe, o qual deve ser utilizado para o desenvolvimento de funções seguras que precisam ser certificadas.

Palavras-chave—comunicação segura; detecção de erros; sistemas seguros; PROFIsafe; IEC61508;

I. INTRODUÇÃO

Os sistemas de automação industrial são baseados em barramentos de comunicação [1], os quais permitem a interligação de sistemas cada vez mais descentralizados nas plantas industriais [2]. Essa interligação deve ser realizada de forma rápida, confiável e robusta, características necessárias no caso de aplicações em processos com altos níveis de criticidade [2].

Com o crescente uso dos barramentos e o desenvolvimento de complexos sistemas de automação industrial e de controle de processos, tornou-se essencial que fossem concebidos os sistemas seguros (*safety*). Aqueles em que defeitos são raros e que, quando eventualmente ocorrem, não provocam danos às pessoas ou ao meio ambiente. Ou seja, são aqueles em que os riscos de provocar um acidente são considerados aceitáveis pelas normas reguladoras.

Esses sistemas são caracterizados por incorporarem mecanismos de diagnóstico, detecção e correção de falhas, que permitem implementar sistemas com altos níveis de Integridade de Segurança. Essa é uma medida da eficiência do sistema em evitar ou mitigar um acidente grave.

Entretanto, para que o sistema como um todo possa ser considerado seguro, é necessário que os mecanismos de comunicação entre os seus componentes também apresentem essa propriedade. Assim, foram desenvolvidos os protocolos de comunicação seguros, tais como o FF SIS [3], openSafety [4], PROFIsafe [5], o Safety over EtherCAT [6], entre outros.

Esses protocolos seguros são especificados de maneira a atender os requisitos de segurança da norma de Segurança Funcional IEC 61508 [7]. A norma estabelece requisitos para a determinação do nível de integridade de uma função de segurança. Essas funções se destinam a atingir ou manter um estado seguro em um processo no que diz respeito a um evento perigoso específico, por exemplo, vazamento de gás, ameaça de incêndio.

Ao se desenvolver uma função de segurança para aplicações críticas, como para a área de óleo e gás, é necessário que ela seja certificada. Nesse processo, o hardware e o software são avaliados em relação às especificações da norma. A comunicação de dados precisa ser coberta por mecanismos que assegurem a entrega de pacotes e a detecção dos erros de comunicação previstos na norma.

Dessa forma não se pode utilizar protocolos tradicionais de comunicação, como o TCP, para implementar a comunicação em funções de segurança para aplicações críticas. Isso ocorre porque ele não possui mecanismos de detecção de erros suficientemente robustos para tratar todos os tipos de falhas de comunicação especificados na norma.

Nesse âmbito, este trabalho apresenta a implementação do protocolo seguro PROFIsafe. escolhido para o projeto RIO-SIL por interesse da empresa parceira. O objetivo desse projeto visa à produção de módulos de entrada e saída digitais para sistemas instrumentados de segurança, os quais devem ser certificados. Além disso, outra justificativa para implementação do protocolo PROFIsafe deve-se ao fato da certificação ser feita em todo o processo de desenvolvimento e não só no resultado final.

O artigo está organizado da seguinte forma: A seção 2 apresenta o protocolo PROFIsafe. A seção 3 apresenta os trabalhos relacionados. A seção 4 mostra alguns equipamentos PROFIsafe. A seção 5 apresenta a implementação do protocolo PROFIsafe. Na seção 6 são comentados os resultados obtidos. A seção 7 apresenta a conclusão e os trabalhos futuros. A seguir são apresentadas as referências utilizadas.

II. PROFISAFE

É um protocolo de comunicação seguro, no nível de transporte, desenvolvido pela Profibus & Profinet Internacional [8] para ser utilizado com as redes PROFIBUS e PROFINET. O uso em conjunto do protocolo com estas redes, permite que os

equipamentos e sistemas desenvolvidos para elas possam ser utilizados na criação de funções de segurança.

A especificação do PROFIsafe [5] está em conformidade com a norma IEC 61508, atendendo os requisitos para sistemas com até SIL 3 (IEC 61508) e FSCP 3 (*Functional Safety Communication Profile* – 3) da IEC 61784-3 [9]. Os níveis de integridade de segurança vão de SIL 1 a SIL 4, sendo SIL 4 o nível de maior integridade. No setor de óleo e gás os dispositivos precisam ser certificados SIL 3 [7] que pode ser alcançado através do uso do protocolo PROFIsafe em aplicações de segurança, e cuja implementação deve ser certificada pela Agência de Inspeção Técnica alemã TÜV SÜD.

O PROFIsafe reduz a probabilidade de erros nos dados transmitidos entre um *F-Host* (controlador seguro) e um *F-Device* (dispositivos com segurança integrada) para o nível exigido por uma norma. Também é possível a comunicação, de informações seguras e não seguras em um único barramento físico de comunicação. Para isso, é necessário garantir que os dois tipos de processamento ocorram de forma logicamente isolada.

O protocolo deve ser implementado sobre um *Black Channel* [5], o que o torna bastante independente dos canais físicos de transmissão, sejam eles fios de cobre, fibras ópticas, *wireless* ou *backplanes* (grupo de conectores ligados de maneira a formar um barramento). As taxas de transmissão e os mecanismos de detecção de erros do *Black Channel* não têm qualquer interferência sobre o protocolo seguro.Esse mecanismo torna desnecessária a avaliação de segurança dos elementos que o compõem: *backplanes* individuais, caminhos de transmissão e redes PROFIBUS e PROFINET

Para detectar erros de comunicação, o protocolo foi especificado com os seguintes mecanismos [5]: número sequencial de mensagens, controle de temporização, identificador único e CRC (Cyclic Redundancy Check). Esses mecanismos são necessários porque quando mensagens são transferidas em redes complexas, vários erros podem ocorrer. Esses erros podem ser ocasionados por falhas de hardware, interferência eletromagnética ou outros tipos de influências e devem ser tratados e corrigidos de alguma forma para garantir a entrega correta de mensagens.

A implementação do protocolo pode ser feita a partir da sua especificação ou obtida através do PROFIsafe StarterKit, o qual contém a implementação da comunicação. para ambos os casos, o código deve ser adaptado para aplicação destino.

III. Trabalhos Relacionados

Åkerberg *et. al.* [10] abordam algumas questões que surgem quando o protocolo PROFIsafe é utilizado para implementar a comunicação segura em redes de sensores sem fio. Neste trabalho, foi proposto um método para integração dos dispositivos, que utilizavam o protocolo WirelessHART [11], PROFI-NET IO e o PROFIsafe. Nos testes realizados, foi observado que a taxa de erros de bit da rede de sensores sem fio deve ser considerada quando se deseja conformidade com os padrões de segurança (IEC 61508 e IEC 61784-3), pois, em alguns casos, essa taxa de erros pode ser muito alta. Também foi notado que, em alguns casos, o tempo de resposta do protocolo WirelessHART é muito longo para implementar algumas funções de segurança que necessitam de um tempo menor de resposta, exigindo uma análise mais detalhada do tempo de resposta do processo a ser controlado. Como principal resultado, apesar das limitações, foi mostrado que é possível estabelecer uma comunicação segura usando-se uma combinação do WirelessHART, PROFINET IO e o PROFIsafe.

No artigo de Malik [12] é apresentada a validação do protocolo seguro PROFIsafe. O objetivo do trabalho era o de garantir a correta especificação do protocolo. Para isso, foi obtido um modelo formal baseado em máquinas de estados finitos a partir da especificação UML do protocolo, a qual define o seu comportamento. Este modelo foi analisado com técnicas de verificação formal para garantir que não existem *loops* e *deadlocks*. Quando uma implementação anterior do protocolo foi verificada quanto aos requisitos para a comunicação segura, foram identificadas falhas. Então foi realizada uma nova versão da implementação que corrigiu as falhas identificadas. Um conjunto de casos de teste foi derivado, baseados no modelo verificado, para executar testes automáticos de conformidade, com a intenção de verificar se a implementação do protocolo tem o mesmo comportamento do modelo verificado.

IV. Equipamentos PROFIsafe

A segurança na engenharia de automação tem recebido muita atenção devido ao risco de lesões corporais, danos materiais e danos ao meio-ambiente ser inerente aos processos industriais [13].

Assim, muitos fabricantes de componentes seguros como, por exemplo, Siemens [14], WAGO [15], BECKHOFF [16], participaram da criação de padrões abertos sob o framework da Profibus & Profinet International. Isso permitiu o desenvolvimento de um extenso portfólio de produtos seguros [13].

Estes produtos são normalmente utilizados para implementar funções de segurança em processos industriais, no setor de transportes, em equipamentos de guindastes, teleféricos, na indústria automotiva, entre outros [13]. Como exemplo dos equipamentos desenvolvidos com PROFIsafe, pode-se citar: remotas de I/O, sensores ópticos, sistemas de controle de segurança, *gateways* seguros, sensores de segurança, dispositivos com funções de segurança integrada, válvulas e bloqueios de válvulas, entre outros [5].

Todos esse equipamentos possuem em comum a necessidade de trocar informações através de uma rede segura de comunicação. E é nesse cenário que os protocolos de comunicação segura, tais como o PROFIsafe, cuja implementação é motivo desse trabalho, se encaixam.

V. Desenvolvimento

O protocolo visa garantir a segurança da comunicação. Então, em qualquer arquitetura de implementação que seja utilizada, o protocolo estará dividido entre uma parte segura e outra não segura. A parte segura é onde está o código da aplicação segura. Esse código deve ser implementado segundo a norma: entre outras limitações pode-se citar o não uso de ponteiros (o que levou ao uso das chamadas de sinalização e passagem de

dados *byte-a-byte*) e o não uso de *threads* (com exceção se houver um sistema de gerência de *threads* que seja certificado). Também é necessária a existência de Hardware (processador) com alto nível de Integridade de Segurança, que garanta a execução correta e que os dados não sejam corrompidos.

Na parte não segura estão os mecanismos padrões de comunicação. A implementação dessa parte pode ser feita de maneira convencional, conforme definido pela técnica de *Black Channel*. Foi necessário controlar o acesso aos *buffers* internos da parte segura, o que levou a implementação de controles através da chamada de uma função específica, usada apenas para leitura.

O modelo de comunicação do PROFIsafe é do tipo um para um, tendo o mestre como o *F-Host* e o escravo como o *F-Device*. Com isso, o *F-Device* só envia mensagens em resposta às mensagens de solicitação de serviços. O resultado final foi uma arquitetura sem *threads*, onde a aplicação determina o passo de execução de todos os mecanismos implementados na parte segura da arquitetura. É importante salientar que as interrupções de recepção da comunicação se encontram na parte não segura da arquitetura.

A. *Pacote PROFIsafe*

O pacote PROFIsafe (*Safety PDU*) é formada por CRC, *Status/Control Byte* e Dados. Há dois modos de operação:

1) I/O binária (processada em alta velocidade): São transmitidos até 12 octetos de dados. É utilizado um CRC de 24 bits (3 octetos).

2) I/O de dados longo (processada mais lentamente): São transmitidos até 123 octetos de dados. É utilizado um CRC de 32 bits (4 octetos).

Em ambas as PDUs o campo *Status/Control Byte* tem 1 octeto. Neste trabalho, levando em consideração a aplicação, decidiu-se pelo modo I/O binária, em que são usados 16 octetos no total para compor a PDU segura.

B. *Arquitetura da Implementação*

A arquitetura é formada por três camadas: a parte segura, onde está a aplicação; a implementação do protocolo seguro; e a parte não segura, onde está a biblioteca do canal de comunicação.

A implementação do PROFIsafe foi feita na linguagem C e definiu-se por utilizar PDUs com tamanho fixo. Entretanto, o programador da aplicação pode decidir o tamanho do *payload* que será transportado, podendo ter no máximo, 12 octetos.

A troca de informações entre camadas de software do *F-Device* é feita através de chamadas de função entre elas e chamadas de sinalização (que não têm parâmetros). O motivo da escolha dessa arquitetura, vista na Fig.1, foi a segurança (*safety*) da implementação de software, que restringe o uso de ponteiros (Norma IEC 61508).

Para recebimento de pacotes, as sinalizações *askRecvMsg()* e *askRecvData()* são implementadas nas camadas superiores, ou seja, para onde o fluxo de dado aponta. Por exemplo, o Protocolo Seguro "pergunta" *(pooling)* para a biblioteca do canal de comunicação através da *askRecvMsg()* se chegou uma nova mensagem. Caso afirmativo é chamada a função

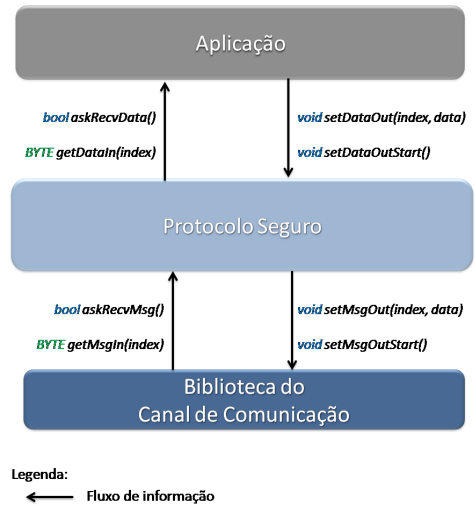

Fig. 1. Arquitetura de implementação em três camadas.

getMsgIn() que busca no buffer de saída do Protocolo de Comunicação o octeto correspondente ao *índex* (parâmetro da função). É importante notar que a camada do Protocolo Seguro realiza o "desempacotamento" da PDU, fazendo com que a *getMsgIn()* transfira até 16 octetos enquanto que a *getDataIn()* transfira apenas o *payload* (que tem 12 octetos).

Para envio de pacotes, as chamadas *setDataOut()* e *setMsgOut()* são implementadas na camada de origem do fluxo de dados. Elas servem para enviar o dado ou pacote, *byte-a-byte*, para o *buffer* de entrada da camada inferior. As sinalizações *setDataOutStart()* e *setMsgOutStart()* informam às camadas inferiores o término, ou seja, que não há mais dados a serem transferidos e que o encapsulamento ou a transmissão podem ser iniciados.

C. *Mecanismo de detecção por CRC*

O uso do CRC por meio de múltiplos níveis, possibilita alto grau de redundância. Primeiramente, ao longo da parametrização inicial do protocolo, é calculado o CRC1 composto de 2 octetos. O CRC que é encapsulado na *Safety PDU* é chamado de CRC2. Ele é formado através de F-Parametros, Dados de saída, *Status/Control Byte* e um Número Consecutivo.

A especificação do protocolo sugere que a implementação do cálculo do CRC seja realizado através do uso de uma tabela. O objetivo dessa técnica é acelerar o cálculo do CRC.

Para trazer mais segurança na técnica de detecção por CRC, esse é recalculado quando o pacote chega ao seu destino e armazenado em uma variável auxiliar que é comparada *byte-a-*

byte, com o campo CRC2 presente no pacote. Isso é possível, pois todos os octetos necessários para recalcular o CRC se encontram na própria *Safety PDU* ou já foram estabelecidos na fase inicial de parametrização do PROFIsafe (caso dos F-Parametros).

VI. RESULTADOS

A tabela I mostra a cobertura de detecção de erros do PROFisafe tendo como referência os protocolos UDP e TCP. Na tabela pode-se perceber a importância de utilizar um protocolo seguro no desenvolvimento de funções de segurança para aplicações críticas. Isso se deve ao fato da maior gama de cobertura de erros que um protocolo seguro oferece em relação aos protocolos de transporte mais tradicionais.

Tabela I. COMPARARIVO DO PROFISAFE COM PROTOCOLOS TRADICIONAIS

Erros	**Protocolo de Comunicação**		
	UDP	***TCP***	***PROFIsafe***
Repetição sem Intenção	✖	✖	✓
Perda	✖	✓	✓
Inserção	✖	✖	✓
Sequência Incorreta	✖	✓	✓
Corrupção	✖	✳	✓
Timeout	✖	✓	✓
Endereçamento	✖	✖	✓
Mascaramento	✖	✖	✓
Falhas Mem.	✖	✖	✓

* Há detecção de corrupção de segmentos no TCP, porém essa é feita através do mecanismo de Checksum, o qual é mais fraco que o CRC realizado pelo PROFIsafe.

Na depuração da implementação foram realizadas a troca de mensagens entre os dispositivos Mestre e Escravo. Foram detectados erros de timeout e corrupção. A corrupção de mensagens foi feita alterando um byte na *Safety PDU*. Essa alteração no pacote foi percebida pelo *F-Device* por meio de CRC.

VII. CONCLUSÕES E TRABALHOS FUTUROS

Neste trabalho foi implementado o protocolo de comunicação seguro PROFIsafe conforme a sua especificação. Essa implementação será utilizada no projeto RIO-SIL para o desenvolvimento de uma Remota de I/O, a ser utilizada na implementação de funções de segurança, em aplicações críticas de automação de processos, na área de óleo e gás. Além disso, por exigência do mercado, é necessário que os equipamentos sejam certificados segundo uma norma de segurança. Assim, a comunicação segura entre equipamentos requer o uso de um protocolo seguro de comunicação.

Os testes realizados mostraram que a troca de mensagens entre os dispositivos mestre e escravo ocorreu corretamente. Quando foi inserido um atraso maior do que o valor máximo tolerado pelo protocolo para o recebimento de mensagens, este foi detectado pelo mecanismo de *timeout*. Ao ser alterado um byte em uma das mensagens trocadas, essa alteração no pacote foi detectada pela verificação do mecanismo de CRC.

Como trabalhos futuros está previsto o teste da implementação através da injeção de falhas com o uso de um injetor de falhas que está em fase de desenvolvimento. O objetivo dos testes é verificar a implementação dos mecanismos de detecção de falhas implementados. Dessa forma, será possível validar corretamente o protocolo implementado e garantir o seu correto funcionamento.

Finalmente, depois de validada a implementação, essa deverá ser integrada ao restante do código da Remota de I/O, onde deverá prover as aplicações de entrada e saída para a implementação de funções de segurança na indústria de petróleo e gás. Durante a realização do trabalho não foram encontrados artigos recentes sobre o PROFIsafe. Isso mostra que se trata de uma área relativamente nova e que academia não tem interesse em implementação de protocolos seguros, denotando que é mais um assunto voltado para industria.

REFERÊNCIAS

[1] Thomesse, J.P. “Fieldbus Technology and Industrial Automation”, Emerging Technologies and Factory Automation, pp.651- 653, September 2005.

[2] Thomesse, J. P. “Fieldbus technology in industrial automation,” Proc. IEEE, vol. 93, no. 6, pp. 1073–1101, June 2005.

[3] FFSYS. Disponível em: < http://www.fieldbus.org/> Acessado em: Setembro 2013.

[4] openSAFETY. Disponível em: < http://www.open-safety.org/> Acessado em: Setembro 2013.

[5] PROFIsafe System Description (2013). Disponível em: < http://www.profibus.com/nc/download/technical-descriptions-books/downloads/profisaf e-technology-and-application-system-description/down load/9594/> Acessado em: Setembro 2013.

[6] EtherCAT FSoE – Safety over EtherCAT Implementation Guide (2010). Disponível em: < http://www.ethercat.org/pdf/english/ETG5101_G_D_V1i1i1_FSoEImplementationGuide.pdf > Acessado em: Setembro 2013.

[7] *International Electrotechnical Commission (2010) “IEC 61508* - Functional Safety Of Eletrical/Eletronic/Programmable Eletronic Safety-Related Systems”.

[8] PI Profibus e Profinet International. Disponível em: < http://www.profibus.com/ home/ >. Acessado em: Setembro 2013.

[9] *International Electrotechnical Commission (2010) “IEC* 61784-3 - Functional Safety Fieldbuses - General rules and profile definitions”.

[10] Åkerberg, J.; Reichenbach, F.; Björkman, M. "Enabling safety-critical wireless communication using WirelessHART and PROFIsafe," IEEE Conference on Emerging Technologies and Factory Automation (ETFA), pp. 1 - 8, September 2010.

[11] Protocolo WirelessHART. Disponível em < www.hartcomm.org/protocol/wihart/wireless_technology.html >. Acessado em: Setembro 2013.

[12] Malik, R. and Mühlfeld, R. "A case study in verification of uml statecharts: the profisafe protocol," Universal Computer Science, vol. 9, no. 2, pp. 138-151, February 2003.

[13] Equipamentos PROFIsafe. Disponível em: < http://www.profibus.com/technology/profisafe/overview/ >. Acessado em: Setembro 2013.

[14] Siemens. Disponível em: < http://www.siemens.com/entry/cc/ en/# >. Acessado em: Setembro 2013.

[15] WAGO. Disponível em: < http://global.wago.com/en/overview /index .jsp >. Acessado em: Setembro 2013.

[16] BECKHOFF. Disponível em: < http://www.beckhoff.com/ >. Acessado em: Setembro 2013.