Estudo e implementação do Protocolo PROFIsafe com base na norma IEC 61508

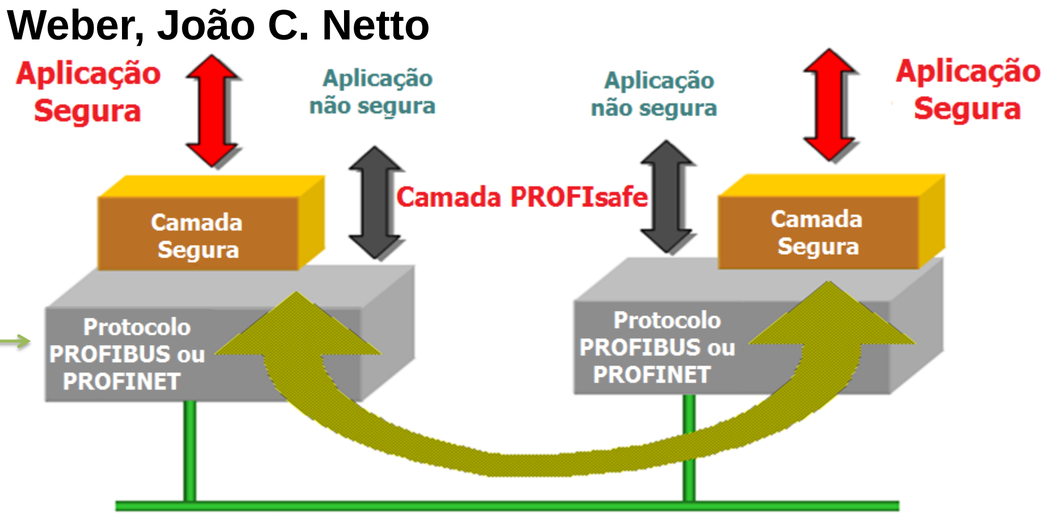
Leandro A. da Silva, William R. C. Vidal, Rodrigo J. Dobler

Orientadores: Sérgio Cechin, Taisy S. Weber, João C. Netto

Universidade Federal do Rio Grande do Sul

INTRODUÇÃO

O trabalho envolve o estudo da norma IEC61508 e a implementação do protocolo seguro de comunicação PROFIsafe .Será analisado o processo de desenvolvimento e certificação de projetos de sistemas tolerantes a falhas, visando a utilização destes em aplicações críticas, buscando diminuir ao máximo os riscos à vida e à saúde das pessoas que utilizarão esses equipamentos.



Funcionamento básico do PROFIsafe
(retirado de "PROFIsafe System Description")

A norma IEC 61508

A norma especifica requisitos para que dispositivos elétricos, eletrônicos ou eletrônicos programáveis relacionados à segurança alcancem um determinado SIL (Safety Integrity Level, indicador da probabilidade de falha das funções de segurança).

Baixa demanda: ***probabilidade média de falhar*** ao realizar função prevista sob demanda

Alta demanda: ***taxa de defeitos perigosos*** por hora

	modo de operação	
SIL	**baixa demanda** PFD	**alta demanda** PFH
4	$\geq 10^{-5}$ a $< 10^{-4}$	$\geq 10^{-9}$ a $< 10^{-8}$
3	$\geq 10^{-4}$ a $< 10^{-3}$	$\geq 10^{-8}$ a $< 10^{-7}$
2	$\geq 10^{-3}$ a $< 10^{-2}$	$\geq 10^{-7}$ a $< 10^{-6}$
1	$\geq 10^{-2}$ a $< 10^{-1}$	$\geq 10^{-6}$ a $< 10^{-5}$

Tabela indicadora do SIL (Nível de Integridade de Segurança)

OBJETIVOS

Estudo do PROFIsafe para a implementação da F-Device de acordo com a sua especificação e documentação do protocolo. Essa implementação será utilizado em uma remota de I/Os com certificação SIL 3.

METODOLOGIA

A metodologia utilizada é a separação em partes da norma e da especificação do PROFIsafe, permitindo seu estudo de forma incremental. Utilizamos a linguagem C para implementação do protocolo, no sistema operacional GNU/Linux e usando para a comunicação UDP sobre Ethernet.

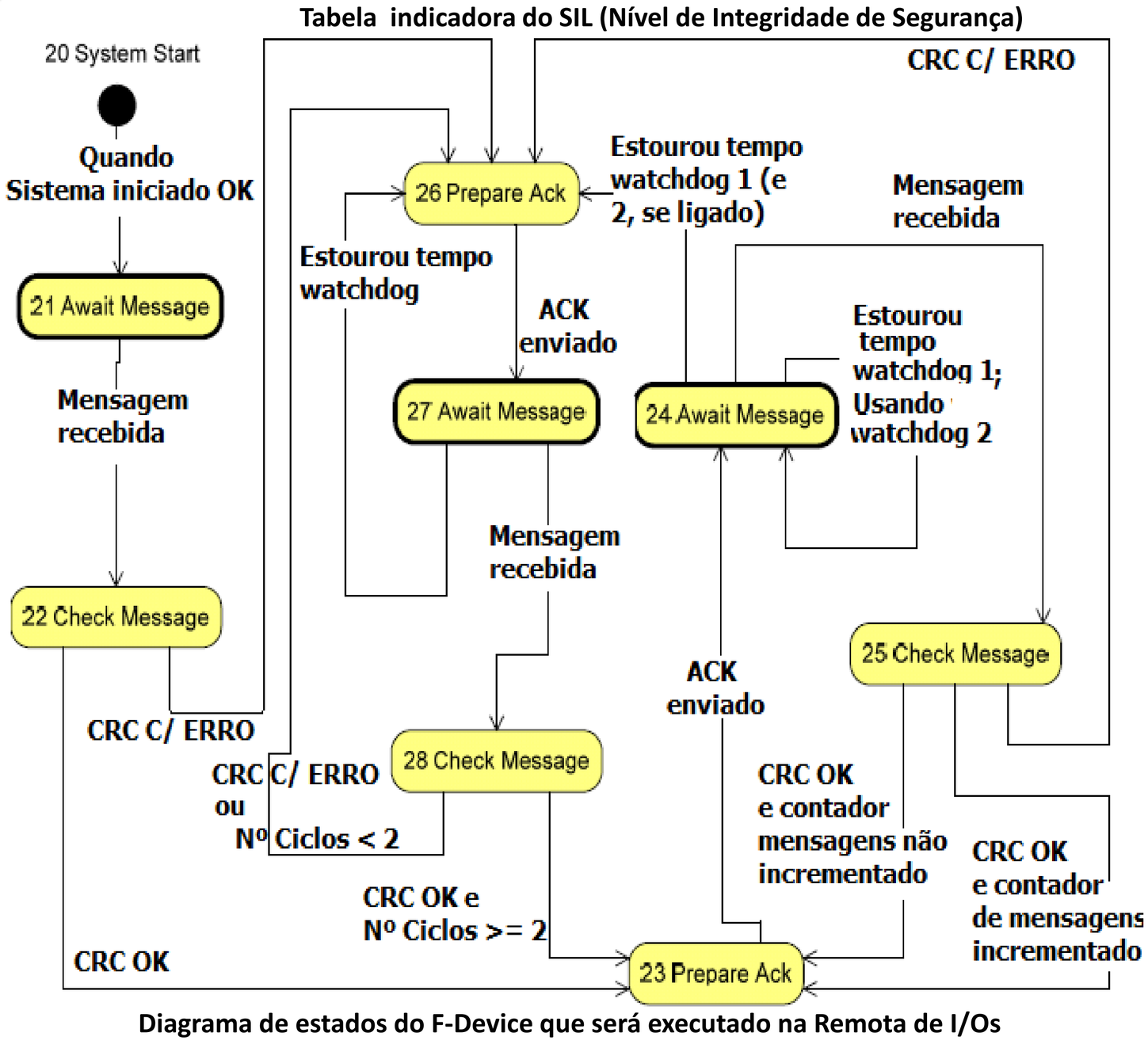


Diagrama de estados do F-Device que será executado na Remota de I/Os
(versão simplificada da encontrada na especificação do PROFIsafe)

RESULTADOS PARCIAIS

- Sólido conhecimento da norma.
- Conhecimento crescente do protocolo.
- Versão preliminar da implementação do protocolo, já contando com os mecanismos de segurança propostos na especificação.

CONCLUSÃO e TRABALHOS FUTUROS

Dificuldades: complexidade e extensão da norma, pouco material de apoio à especificação do protocolo, seguir as rígidas regras de padronização de segurança na programação (como não usar ponteiros, por exemplo) e estruturação dos códigos fontes.

Futuro: realização de testes operacionais, medição de desempenho, implementação de uma API, verificação de eventuais falhas de comunicação, adaptação para um microcontrolador e estrutura de comunicação certificados. Atualmente a implementação está rodando sobre dois computadores usando uma rede Ethernet padrão.

Este trabalho foi parcialmente financiado pela Finep – Rede E3 – Projeto RIO-SIL 01.11.0154.00.