UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL
INSTITUTO DE INFORMÁTICA
CURSO DE CIÊNCIA DA COMPUTAÇÃO

DIEGO COSTANTIN BANDEIRA

Aplicação da Norma IEC 61508 em Sistemas Críticos

Trabalho de Graduação

Prof. Dra. Taisy Weber
Orientadora

Porto Alegre, dezembro de 2011

AGRADECIMENTOS

Agradeço primeiramente aos meus pais, Elito e Marlene, por sempre incentivar e apoiar os meus estudos.

Agradeço à minha orientadora, Prof. Dra. Taisy Weber, pela disponibilidade e paciência, bem como o incentivo à realização deste trabalho.

Agradeço à UFRGS e em especial ao Instituto de Informática pelo ensino de alta qualidade do qual pude usufruir.

Agradeço aos meus amigos e amigas, sejam de longa data ou conhecidos recentemente, pois estiveram sempre presentes compartilhando a alegria dos bons momentos e dando apoio nas horas difíceis.

SUMÁRIO

LISTA DE ABREVIATURAS E SIGLAS

E/E/EP	Elétrico(s) / Eletrônico(s) / Eletrônico(s) Programável(eis)
HR	Highly Recommended
IEC	International Electrotechnical Comission
NR	Not Recommended
SIL	Safety Integrity Levels

LISTA DE FIGURAS

LISTA DE TABELAS

RESUMO

A crescente demanda na utilização de componentes eletrônicos em questões de segurança faz com que aumente também a necessidade de se obter garantias sobre quão seguros são os componentes envolvidos. Uma das formas de assegurar a qualidade dos dispositivos utilizados é a verificação de que estes apresentam riscos baixos à segurança, através da obtenção de certificações de segurança.

O presente trabalho apresenta um estudo geral da norma internacional IEC 61508, a qual é amplamente empregada na tentativa de obter a comprovação de qualidade dos componentes utilizados em sistemas críticos. São esclarecidos também alguns conceitos inerentes à segurança, visando auxiliar na compreensão de pontos importantes da norma. A parte 61508-3 da norma, a qual apresenta aspectos relacionados diretamente à parte de software, recebe maior enfoque. Nela estão presentes os requisitos de software para dispositivos e sistemas relativos à segurança. Este estudo tem como objetivo principal proporcionar um entendimento sobre a norma e conceitos fundamentais relacionados, além de apresentar críticas sobre a IEC 61508, e também servir como apoio básico na aplicação da norma IEC 61508-3.

Palavras-chave: IEC 61508, norma, requisitos, risco, segurança, software.

Implementation of IEC 61508 in Critical Systems

ABSTRACT

The growing demand in the use of electronics in safety systems increases also the need to obtain assurances about how safe are the involved components. One way to ensure the quality of the used devices is to verify that they present low safety risks, by obtaining safety certifications.

This work presents a general study about international standard IEC 61508, which is widely used in the attempt to obtain quality evidences around components that are used in critical systems. Also, this work intends to clarify some concepts inherent to safety, to assist in understanding some important aspects related to the standard. The part 61508-3 of the standard, which has it main point based on software aspects, receives greater focus. It contains the software requirements for devices and systems related to safety. This study's main objective is to provide some understanding about IEC 61508 fundamental related concepts, besides presenting criticism of the IEC 61508, and also helps as basic support in implementing the standard IEC 61508-3.

Keywords: IEC 61508, standard, requirements, risk, security, software.

1 INTRODUÇÃO

Durante a década de 80, houve uma ascensão no uso de sistemas computadorizados nas tarefas relacionadas a funções de segurança. Este fato fez com que várias empresas, de diversos setores, elaborassem normas de segurança de software. No segundo semestre de 1985, foi criada pela IEC (International Electrotechnical Commission) a norma IEC 61508. Esta norma consiste em padrões internacionais genéricos de segurança funcional voltada a dispositivos elétricos, eletrônicos ou eletrônicos programáveis. Ao longo deste trabalho, será dado enfoque para a IEC 61508-3 da versão 1.0, que corresponde à parcela da norma dedicada a requisitos de software.

O aumento na utilização de componentes eletrônicos em questões de segurança, e por consequência a necessidade de se obter garantias sobre quão seguros são estes componentes, foi o que ocasionou a criação da norma. Quando levamos em consideração a parte relativa ao software, a complexidade torna inviável o teste de todas as falhas em todos os cenários possíveis. No entanto, a aplicação de diferentes avaliações e testes englobados pela norma, seguindo métricas especificadas, possibilita a obtenção de taxas muito baixas de riscos de falhas. Não é possível a eliminação completa do risco de que uma falha aconteça, porém estas são consideradas então taxas de risco aceitáveis, uma vez que são de rara ocorrência.

A norma tem a sua aplicação difundida entre várias áreas, dentre as quais podemos destacar a de dispositivos embarcados com funções críticas de segurança. Exemplos de algumas aplicações destes sistemas:

- em automóveis, nos controles de tração e freios ABS;
- sistemas de parada emergencial em equipamentos e maquinários;
- em aeronaves, nos sistemas de controle de vôo e orientadores de mísseis;
- urnas eletrônicas;
- em hospitais, nos aparelhos de suporte a vida;

Sistemas que envolvem estes dispositivos devem ter um nível de segurança comprovadamente alto, tendo em vista que a sua aplicação tende a envolver situações em que uma falha poderia ocasionar incidentes de grande impacto.

Ao longo deste trabalho alguns conceitos são mencionados e a compreensão destes é importante para possibilitar a avaliação da segurança dos sistemas E / E / EP. A concepção de segurança se origina da palavra safety, que segundo Siqueira (2006) representa “a segurança de funcionamento em situações críticas”. Outro relevante conceito é a definição de dano, originado da palavra harm. Dano tem, então, como

significado o dano à saúde ou lesões físicas causadas a um indivíduo por avarias à propriedade ou meio ambiente, seja direta ou indiretamente (LADKIN, 2008).

Para avaliar a segurança de um determinado sistema crítico, é realizada uma análise com base na documentação fornecida, a qual deve conter a especificação dos resultados que foram obtidos. Considera-se um sistema seguro quando este atinge na totalidade os requisitos necessários, ou seja, cumprindo as exigências métricas do nível de integridade de segurança (safety integrity level - SIL) que é exigido para um determinado tipo de aplicação.

No primeiro semestre de 2010 foi lançada a versão 2.0 da IEC 61508, a qual foi adquirida pela instituição de ensino recentemente. Desta forma, este trabalho tem por base ainda a versão 1.0, com alguns comentários sobre alterações pontuais apresentados na conclusão.

A demanda crescente na área de segurança impulsiona a busca por certificações, que visam assegurar a qualidade dos sistemas de segurança. Ao contrário do hardware, que tem seus métodos de avaliação mais concretamente definidos, o software não dispõe de métodos de avaliação de segurança que sejam considerados como consenso universal. Assim, o enfoque deste trabalho é direcionado à parte 3 da norma, a qual é responsável pela especificação de requisitos para software de segurança.

2 DEFINIÇÕES GERAIS SOBRE SEGURANÇA

A norma é relativamente extensa, abrangendo o ciclo de vida completo de segurança. Inerente à norma, temos alguns conceitos de grande relevância, sendo alguns destes os seguintes:

- avaliação com base em riscos;

- segurança e segurança funcional;

- níveis de integridade de segurança;

Ao longo deste capítulo serão feitos esclarecimentos a respeito dos conceitos supracitados, a fim de proporcionar uma compreensão mais adequada de como funciona a norma IEC 61508.

2.1 Avaliação com base em riscos

A finalidade da análise de riscos é assegurar que uma determinada função de segurança cumpra eficientemente o seu papel. Em outras palavras, significa obter garantias de que não haja a exposição de nenhum indivíduo a riscos que possam ser considerados inaceitáveis, associados à ocorrência de um evento perigoso.

O fator que liga a ocorrência de uma avaria no sistema a uma fatalidade que aconteça em razão desta falha é o que chamamos de perigo (ou hazard). Pode ser definido mais concretamente como uma determinada situação, seja ela potencial ou real, que ocasione:

- prejuízos ao meio ambiente;

- doenças, lesões ou morte;

- prejuízos ou perda de equipamentos, sistemas ou patrimônios.

De uma forma geral, a avaliação do perigo tem como principal foco apontar quais os fatores que podem levar um componente de determinada aplicação a falhar. Os componentes podem ter suas falhas originadas das mais diversas formas, as quais incluem:

- estresse ambiental;

- defeitos no processo de fabricação;

- equívocos no projeto;

- erros de programação;

- falhas randômicas no hardware;

- manutenção malfeita.

A análise das fontes de problemas nos componentes é o que fornece informação para possibilitar a ligação das falhas nos componentes com eventuais acidentes. (DUNN, 2003).

As principais causas de falhas por fase variam conforme o setor e complexidade da aplicação. Estudos apontam que grande parte das falhas são incorporadas nos sistemas relacionados à segurança antes mesmo que estes sejam colocados em funcionamento, ou seja, ainda nas fases iniciais. A figura 2.1 ilustra essa questão:

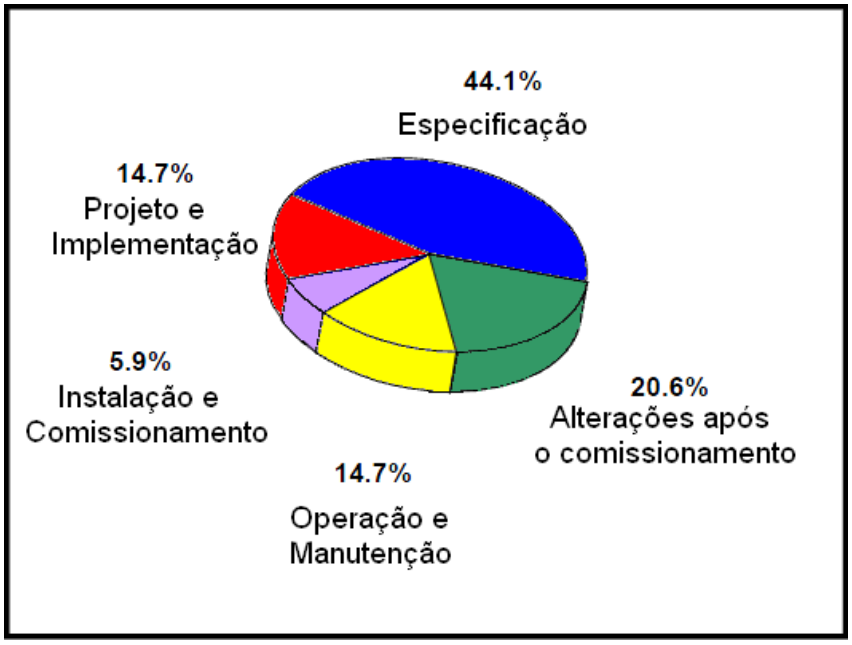

Figura 2.1 Causas primárias, por fase, de falhas no sistema de controle (BELL, 2005).

Na maior parte dos casos, é determinado um risco admissível para um dado tipo de acidente, através de um consenso geral. Isso ocorre em casos em que estes eventos prejudiciais não ocorrem freqüentemente. Duas preocupações são essencialmente levadas em consideração nestes casos: a probabilidade de ocorrer e sua virtual gravidade.

Muitas normas de segurança fazem uso das técnicas de avaliação com base em risco para definir o que pode ser considerado como risco aceitável. No caso específico da norma IEC 61508, é empregado o nível de integridade de segurança (SIL), que será detalhado mais adiante neste capítulo.

2.2 Definindo segurança e segurança funcional

Sistemas podem executar uma determinada função, ou ainda um conjunto de funções que visam assegurar a manutenção dos riscos dentro de um limite tolerável. Estas funções são denominadas funções de segurança, e o termo segurança está ligado diretamente à descrição desses sistemas.

A definição de sistema seguro, na visão da norma IEC 61508, representa basicamente um sistema que não apresenta riscos considerados inaceitáveis. Como citado anteriormente, esses riscos envolvem danos ou prejuízos para a saúde dos

indivíduos. Podem ser originados de forma direta ou ainda indireta de prejuízos à propriedade ou meio ambiente.

O grupo de determinadas funções de segurança de um sistema é o que se pode chamar de segurança funcional. A segurança funcional representa uma parcela da segurança na sua integralidade, e depende de um mecanismo ou sistema que opere apropriadamente de acordo com as entradas fornecidas. Para Bell (2005), não é possível definir segurança ou segurança funcional sem levar em conta o sistema como um todo e a interação deste com o ambiente.

As falhas na segurança estão diretamente ligadas aos usuários e criadores dos sistemas (DUNN, 2003). Na prática, podem ser mencionados como os três motivos fundamentais:

- falta de compreensão completa sobre o que torna um sistema seguro;

- desconsiderar pontos únicos de falha, o que na prática acaba por fazer com que o conceito de segurança não seja mais garantidamente seguro;

- não dar atenção ao contexto maior em que o conceito implantado venha a ser embarcado.

Na busca por atingir a segurança funcional de um sistema, é necessário que sejam observados e cumpridos alguns requisitos fundamentais, que são:

- de integridade de segurança;

- da função de segurança.

Aos requisitos de integridade, originados da análise de riscos, está relacionada à probabilidade de uma dada função de segurança operar de maneira correta. Em outras palavras, o nível de certeza de execução satisfatória de uma função de segurança. A probabilidade de ocorrência de uma falha considerada perigosa diminui à medida que aumenta o nível de integridade de segurança. Quanto aos requisitos da função, destacam-se as operações e quais as finalidades da função de segurança. Estes requisitos derivam-se essencialmente da avaliação de perigo.

É importante ressaltar que a segurança funcional é somente uma dentre várias medidas disponíveis para enfrentar as situações que envolvem perigo. Riscos podem ser eliminados ou reduzidos através da elaboração de um projeto consistente, detalhado e bem estruturado.

Habitualmente, a exigência e rigorosidade da engenharia de um sistema voltado à segurança crescem proporcionalmente em relação ao nível de integridade de segurança. Um sistema que tenha dentre as suas atribuições a execução de funções de segurança é considerado sistema ligado à segurança, independentemente da tecnologia em que esteja implantado. Este sistema pode estar ou não embutido em um equipamento de controle, ou mesmo como parte de outro sistema de controle.

2.3 Nível de Integridade de Segurança (SIL)

As funções de segurança estão relacionadas a uma quantidade considerável de fatores. Níveis que representem a especificação de uma meta de diminuição de riscos, ou um nível relativo à atenuação de riscos proporcionados por uma dada função de segurança, são conceitos que definem os níveis de integridade de segurança (SIL). No

contexto da norma IEC 61508, o SIL é definido com uma métrica para avaliação de desempenho de segurança para a obtenção da certificação. Essa medida varia conforme o nível de segurança almejado pela aplicação.

Dentre as exigências, o nível de integridade de segurança correlacionado a uma determinada função de segurança deve ser suficiente para assegurar que os sistemas alterem eventos conseqüentes de falhas, de forma a atingir um patamar de risco aceitável. Além disso, a repetição sistemática de falhas deve ser pequena a fim de manter a quantidade de ocorrência de eventos perigosos inferior a um nível não aceitável.

No contexto da norma IEC 61508, são definidos quatro níveis possíveis de integridade de segurança. O SIL 4 é o nível mais alto de integridade e, conseqüentemente, acarreta em um número maior de exigências, enquanto o nível menos exigente é o SIL 1.

Dentre os aspectos analisados nos cálculos de probabilidade de falhas encontra-se o modo de operação, que pode ser:

- de baixa demanda, onde a probabilidade representa a taxa média de falhas ao realizar uma função prevista sob demanda;

- de alta demanda, onde a probabilidade expressa a taxa de defeitos perigosos por hora.

A tabela 2.1 mostra algumas medidas probabilísticas de taxas de defeitos:

Tabela 2.1: Medidas de taxa de falhas em relação ao SIL e modo de operação.

SIL	*Modo de Operação*	
	Baixa Demanda (funções sob demanda)	*Alta Demanda (contínuo)*
1	$\geq 10^{-2}$ a $<10^{-1}$	$\geq 10^{-6}$ a $<10^{-5}$
2	$\geq 10^{-3}$ a $<10^{-2}$	$\geq 10^{-7}$ a $<10^{-6}$
3	$\geq 10^{-4}$ a $<10^{-3}$	$\geq 10^{-8}$ a $<10^{-7}$
4	$\geq 10^{-5}$ a $<10^{-4}$	$\geq 10^{-9}$ a $<10^{-8}$

Os requisitos são analisados mediante o emprego de métricas pré-determinadas, e variam conforme o SIL almejado. A IEC 61508 traz um detalhamento dos requisitos essências para a obtenção de um nível de integridade de segurança estipulado. Para um nível SIL mais alto, os requisitos tornam-se mais rigorosos visando atingir a probabilidade mínima requerida de falhas perigosas.

A norma define três classificações mais relevantes na aplicação das métricas, que são:

- não recomendado (NR);

- recomendado (R);

- altamente recomendado (HR).

É importante ressaltar que, ao não empregar uma métrica considerada HR, é necessário fazer uso de uma justificativa. No entanto, não são fornecidos modelos ou exemplos do que é aceito como justificativa válida.

2.4 Exemplos de sistemas relativos à segurança

Um determinado sistema que apresente a capacidade de cumprir os requisitos determinados de cada função de segurança e de executar estes requisitos conforme o nível de integridade de segurança requerido é considerado um sistema relacionado à segurança (BELL, 2005).

Alguns exemplos comuns de sistemas ligados à segurança são:

- mecanismos de controle de dosagem de exposição e bloqueio para equipamentos utilizados em radioterapia;

- mostradores de carga de segurança para guindastes e similares;

- sistemas de controle de vôo nas aeronaves;

- mecanismos para sinalização em ferrovias;

- sistemas de posicionamento dinâmico;

- controle de parada emergencial em indústrias de processos químicos danosos;

- ferramentas de auxílio à decisões, com base em informações onde ações equivocadas acarretam em redução da segurança;

- parada emergencial e bloqueio preventivo em maquinários pesados.

- sinais luminosos de alerta e de antitravamento dos freios em automóveis.

2.5 Componentes básicos de sistemas relacionados à segurança

Segundo Dunn (2003), teoricamente qualquer sistema de computador envolvido em alguma de função relacionada à segurança engloba cinco elementos básicos, independente do tipo de função de segurança que o sistema executa. Estes elementos são:

2.5.1 Aplicação

A entidade material sobre a qual o sistema exerce operações de controle e monitoramento é o que chamamos de aplicação (ou processo). Dentre os exemplos de aplicação estão o braço mecânico de um robô, o freio de um veículo, uma aeronave durante o vôo, a refrigeração em reatores nucleares.

2.5.2 Operador

O indivíduo que realiza o acompanhamento e ativação de um sistema de computador em tempo real é denominado operador. Exemplos clássicos de operadores incluem operadores de usinas nucleares, técnicos da área da saúde, pilotos de avião.

2.5.3 Sensor

Sensor é a designação dada a um elemento que efetua a conversão de uma medida ou característica física da aplicação para um sinal elétrico utilizado como entrada em

um computador. Aparelhos que medem a tensão, transdutores de pressão e acelerômetros são exemplos típicos de sensores.

2.5.4 Computador

O componente que utiliza atuadores e sensores para exercer funções de controle e monitoramento em tempo real da aplicação, constituído de software e hardware é denominado computador. Como exemplos das inúmeras formas de computadores podem ser citados os controladores lógicos programáveis, computadores de bordo em aeronaves e sistema-em-um-chip.

2.5.5 Atuador

Atuador é o componente que transmuta o sinal elétrico correspondente à saída do computador em uma ação física que efetua o controle de alguma função da aplicação. Válvulas, dispositivos de freio e motores são tipos comuns de atuadores.

3 A NORMA INTERNACIONAL IEC 61508

3.1 Subdivisões da norma

A IEC 61508 traz um conjunto de regras e especificações de segurança funcional para sistemas dos tipos E / E / EP. Sua composição é dividida em 7 segmentos, que são mostrados na tabela 3.1:

Tabela 3.1: Seções da norma IEC 61508 e seus respectivos conteúdos.

Norma Internacional IEC 61508	
Seção	*Conteúdo*
IEC 61508-1	Requisitos globais
IEC 61508-2	Requisitos para sistemas E / E / EP ligados à segurança
IEC 61508-3	Requisitos para a parte de software
IEC 61508-4	Abreviaturas e definições de conceitos
IEC 61508-5	Exemplos de processos de avaliação de níveis de integridade de segurança
IEC 61508-6	Diretrizes para a aplicação das partes IEC 61508-2 e IEC 61508-3
IEC 61508-7	Visão global de técnicas e métricas utilizadas

3.2 Objetivos da norma IEC 61508

A IEC 61508 foi criada no intuito de atender às necessidades relacionadas à segurança, inerentes ao aumento na demanda de tecnologia e produtividade por parte de diversos setores industriais. Tem como objetivos principais:

- fornecer uma abordagem que tem por base a analisa dos riscos, visando definir e estruturar as exigências de desempenho dos sistemas relativos à segurança;

- dar enfoque para a segurança, incentivando o crescimento das tecnologias a ela relacionadas;

- estabelecimento de modelos universais, com finalidade de aplicação direta pelo setor industrial, bem como incentivo a elaboração de normas mais específicas para diversos segmentos e produtos;

- prover uma abordagem sistemática que seja flexível para adaptações futuras, fazendo uso de técnicas bem fundamentadas;

- elevar os ganhos em questões de economia e segurança, através do aperfeiçoamento das tecnologias empregadas;

- aumentar a confiabilidade de operadores e usuários para com as tecnologias e sistemas computadorizados;

- facilitar a criação de métodos para a avaliação de adequação aos requisitos;

- definir requisitos tendo por base conceitos genéricos, tendo em vista proporcionar uma rede eficiente de fornecimento aos provedores de componentes e subsistemas em diversas áreas.

3.3 Particularidades e caracterização

A norma apresenta uma série de características, dentre as quais estão:

- definição de métricas e técnicas a serem empregadas para alcançar os níveis necessários de integridade de segurança;

- exemplificação de como efetuar a abordagem com base em riscos, visando estabelecer os requisitos necessários de integridade de segurança para diversos dispositivos E / E / EP;

- cobertura total das práticas de segurança pertencentes ao ciclo de vida. As etapas envolvem desde a concepção inicial, passando pela análise de riscos e perigos, elaboração das prescrições de segurança, fase de especificação, arquitetura e implementação, operação e eventuais manutenções, alterações no sistema, até a sua inativação;

- abrangência de requisitos visando prevenir a ocorrência de falhas, assim como requisitos voltados à manutenção da segurança mesmo em casos de ocorrência de falhas;

- abordagem dos mecanismos de falha, como hardwares com comportamento sistemático ou randômico. Abrange também características do sistema, englobando os subsistemas que desempenham alguma função de segurança, sejam eles compostos por software e/ou hardware;

- utilização de um padrão de ciclo de vida na totalidade, na forma de um conjunto de definições técnicas, com o objetivo de que as necessidades para garantia da segurança funcional sejam satisfeitas pelos dispositivos E / E / EP.

3.4 Considerações sobre a IEC 61508

Em geral, a IEC 61508 recebe críticas em relação a vários aspectos. A assimilação da norma muitas vezes não ocorre facilmente, em grande parte devido à sua vasta extensão. Muitas vezes isto acarreta numa interpretação dúbia, reduzindo sua confiabilidade. Além disso, alguns pontos são considerados excessivamente formais, o que eventualmente acaba dificultando uma compreensão precisa para pessoas que não tenham um nível avançado de conhecimento na área.

Caso sejam apresentadas justificativas, a norma permite a utilização de métodos que não constem como recomendados. Todavia, não há uma determinação ou consenso sobre o que seria uma justificativa considerada aceitável num eventual processo de avaliação.

Em relação à programação, a norma apresenta algumas considerações que acabam por limitar as escolhas do desenvolvedor. Dentre elas, a recomendação para utilização de linguagens que sejam consideradas fortemente tipadas, além de não aconselhar o paradigma de orientação a objetos.

Algumas críticas são direcionadas ao fato de que, apesar de apresentar orientações pertinentes e importantes, a norma por vezes parece não correlacionar as métricas e especificações definidas com conceitos intrínsecos de segurança (MCDERMID, 2001).

Outro ponto muitas vezes criticado diz respeito quanto ao emprego dos níveis de integridade de segurança. A complexidade que envolve os sistemas muitas vezes dificulta ou praticamente impossibilita uma estimativa precisa de SIL. Alia-se a isso o fato de que a interpretação do SIL apresenta divergências entre normas, além dos cálculos estimativos serem feitos baseados em considerações sobre confiabilidade.

No escopo da norma IEC 61508, há uma relação direta da taxa de ocorrência de falhas consideradas como perigosas com a definição de SIL. Muitas vezes, os processos e conceitos relacionados não são considerados da maneira mais adequada. Esta imprecisão de interpretação pode acarretar em asserções incorretas sobre qual o nível de integridade de segurança de um dado sistema.

Por último, a utilização da norma encontra-se basicamente concentrada no âmbito de grandes empresas, uma vez que é considerada de difícil adequação para projetos de pequenas proporções. Isto acaba por encarecer o processo fazendo com que empresas menores não invistam tanto nesta área da segurança funcional.

4 SEGURANÇA DE SOFTWARE

A norma IEC 61508 apresenta a definição de ciclos de vida, entre eles os ciclos de vida de segurança funcional e ciclo de vida de segurança de software. Ao longo deste capítulo serão apresentadas algumas características referentes a estes ciclos.

4.1 Ciclo de vida da segurança funcional

Em relação ao ciclo de vida de segurança funcional, a norma IEC 61508 apresenta um ciclo formado por 16 fases, que são ilustradas na figura 4.1:

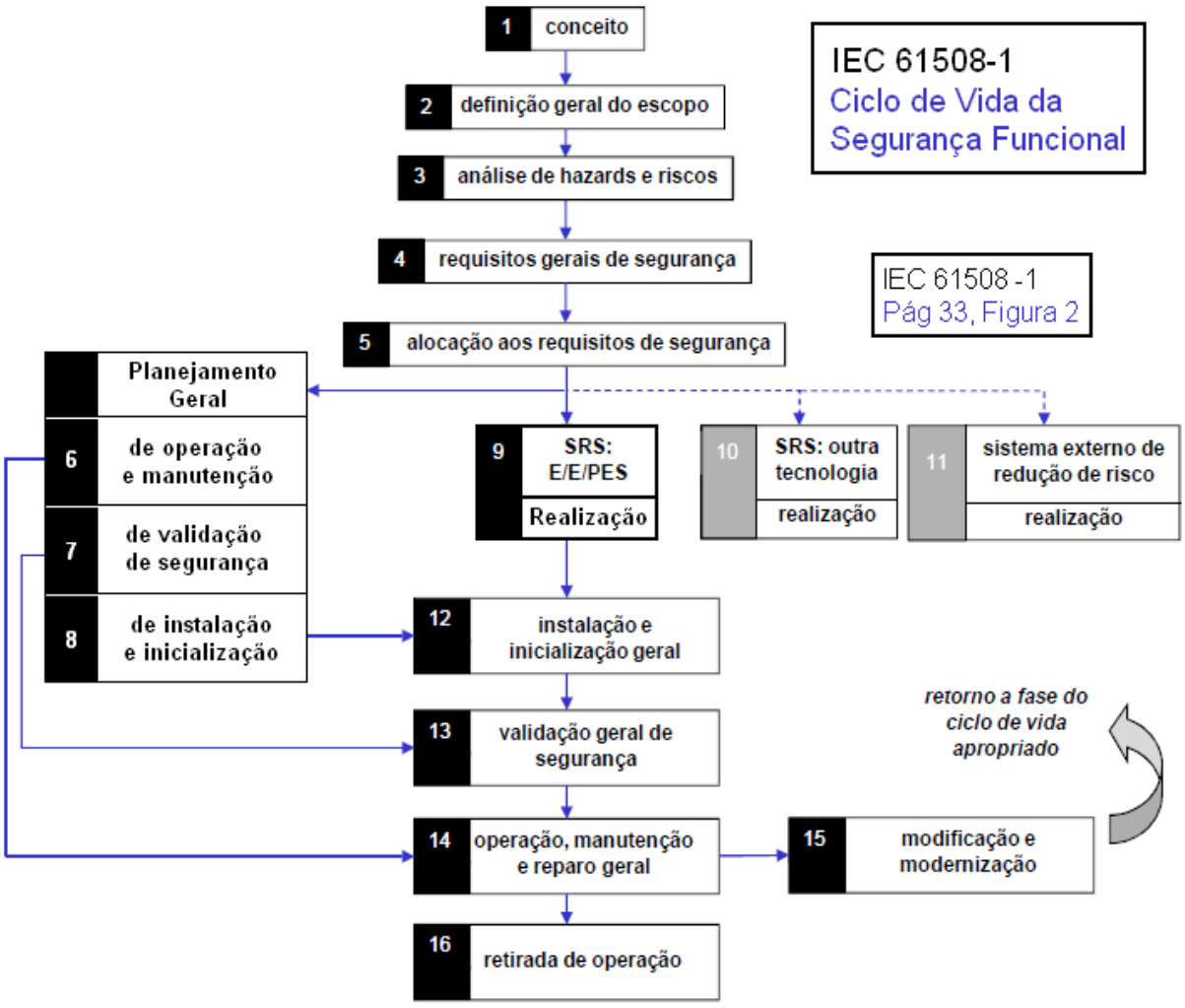

Figura 4.1: Ciclo de vida da segurança funcional (WEBER).

Uma breve descrição sobre cada etapa do ciclo de vida é apresentada nas seções 4.1.1 a 4.1.16.

4.1.1 Conceito

A fase inicial visa obter um entendimento geral do sistema e do ambiente relacionado. Deve ser satisfatório a ponto de possibilitar a execução correta das próximas fases do ciclo de vida.

4.1.2 Definição geral do escopo

A fase de definição de escopo tem por finalidade estabelecer a limitação do sistema de controle, bem como do sistema que estará sendo controlado. Auxilia na especificação do escopo das análises de risco e de perigo.

4.1.3 Análise de hazards e riscos

A etapa de análise de perigos (hazards) e riscos visa definir quais os riscos e eventos perigosos que possam ocorrer em determinado sistema. Isto se aplica em todas as situações passíveis de previsão e para os diversos modos de operação.

4.1.4 Requisitos gerais de segurança

Nesta parte do ciclo de vida devem ser especificados e desenvolvidos os requisitos gerais de segurança. Inclui os requisitos ligados à integridade de segurança e funções de segurança.

4.1.5 Alocação aos requisitos de segurança

Fase em que são feitas as alocações necessárias das funções de segurança, definidas nos requisitos gerais de segurança, para atingir o nível desejado de segurança funcional. As funções são alocadas aos sistemas de controle, sistemas externos de redução de risco e sistemas com outras tecnologias que estejam relacionadas à segurança.

4.1.6 Planejamento de operação e manutenção

Fase voltada ao planejamento dos processos de operação e manutenção de um sistema, visando assegurar a conservação das condições gerais de segurança ao longo d destes processos.

4.1.7 Planejamento de validação de segurança

Esta etapa tem como finalidade a elaboração de uma estratégia que auxilie na aprovação da segurança do sistema como um todo.

4.1.8 Planejamento de instalação e inicialização

Esta fase tem como objetivo formular um plano para que tanto a instalação quanto a inicialização do sistema ocorram de forma controlada, para assegurar que sejam atingidas as metas de segurança funcional.

4.1.9 Realização

A fase de realização tem por finalidade a elaboração do sistema responsável por efetuar o controle, de acordo com os requisitos levantados tanto com relação à integridade de segurança, quanto para as funções de segurança.

4.1.10 Sistemas de segurança – outras tecnologias

Etapa referente à aplicação de outras tecnologias aos sistemas, com o intuito de ajudar no cumprimento dos requisitos de segurança estabelecidos.

4.1.11 Sistema externo de redução de risco

Fase que tem como meta a inclusão de sistemas externos que atuem na redução de riscos (não pertence ao escopo da IEC 61508).

4.1.12 Instalação e inicialização geral

Fase onde é realizada a instalação e inicialização do sistema, seguindo os processos definidos anteriormente.

4.1.13 Validação geral de segurança

Nesta fase é executada a verificação do sistema de controle, para assegurar que esta satisfaça as especificações globais de segurança (nível de integridade de segurança e funções de segurança). Considera a alocação, anteriormente estabelecida, para os requisitos de segurança.

4.1.14 Operação, manutenção e reparo geral

Fase que tem por objetivo assegurar que a segurança funcional do sistema se mantenha durante os processos de operação, manutenção e reparos eventuais do sistema.

4.1.15 Modificação e modernização

Esta etapa tem como responsabilidade assegurar a manutenção da segurança funcional, seja antes ou depois de modificações feitas no sistema.

4.1.16 Retirada de operação

Etapa que tem como foco assegurar que as atribuições de segurança funcional sejam satisfatórias ao longo do processo de retirada de operação do sistema, bem como ao término deste processo.

4.2 Ciclo de vida de segurança do software

O ciclo de vida de segurança de software é um modelo que tem por finalidade organizar e distribuir o processo de desenvolvimento de software em etapas e práticas bem determinadas. As fases do ciclo de vida de segurança do software dividem-se de acordo com a figura 4.2:

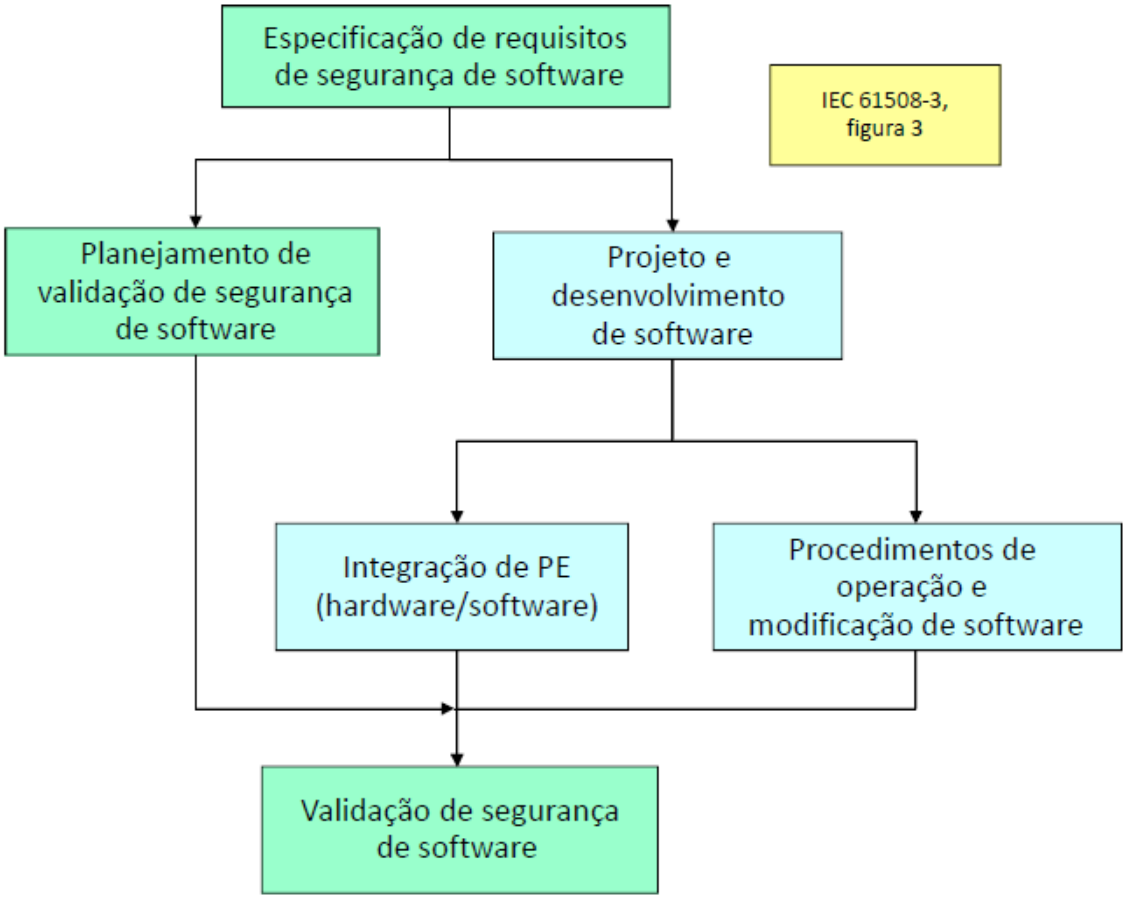

Figura 4.2: Ciclo de vida da segurança de software (WEBER).

Este ciclo de vida representa a figura 3 da IEC 61508-3. As fases serão descritas resumidamente nos itens 4.2.1 até 4.2.6 deste trabalho.

4.2.1 Especificação dos requisitos de segurança de software

A especificação de requisitos de segurança do software deve abranger a definição de quais as funções de segurança serão executadas, assim como o modo de operação e quais os níveis de integridade de cada uma das funções de segurança.

4.2.2 Plano de validação de segurança de software

O plano de validação de segurança do software deve apresentar a estruturação do gerenciamento de segurança, as atividades relativas à segurança e também os marcos de aprovação presentes no ciclo de vida. Deve ser elaborado no início do ciclo de vida, sofrendo revisões caso sejam feitas mudanças no sistema inicial.

4.2.3 Projeto e desenvolvimento de software

A fase de projeto e desenvolvimento de software contém várias etapas, que serão abordadas sucintamente na seção 4.3.

4.2.4 Integração (hardware/software)

A etapa de integração visa comprovar que a interação entre hardware e software durante o desempenho de determinada função ocorre de forma correta. No caso de softwares com SIL superior a zero, é necessária a elaboração de um plano de teste de integração entre software e hardware no começo do ciclo de desenvolvimento.

4.2.5 Procedimentos de operação e manutenção de software

Esta fase tem como objetivo definir procedimentos para assegurar a conservação da segurança funcional ao longo dos processos de operação e manutenção do software. Devem-se estabelecer condutas a serem seguidas quando da ocorrência de falhas de software, bem como procedimentos para diagnosticar os defeitos. Igualmente, é necessário a definir processos para revalidação e quais os requisitos do relatório de manutenção.

4.2.6 Validação de segurança de software

Consiste em verificar se cada fase do ciclo satisfaz seus requisitos específicos de segurança, identificado nas fases anteriores. Ou seja, é a validação do software contra sua especificação de requisitos de segurança.

A análise de segurança e os testes adequados devem ser executados e documentados, com as evidências de que o software cumpre os requisitos apresentadas em um documento de justificativa de segurança.

4.3 Fases de projeto e desenvolvimento de software

A IEC 61508-3 prevê as fases de projeto e desenvolvimento representadas na figura 4.3:

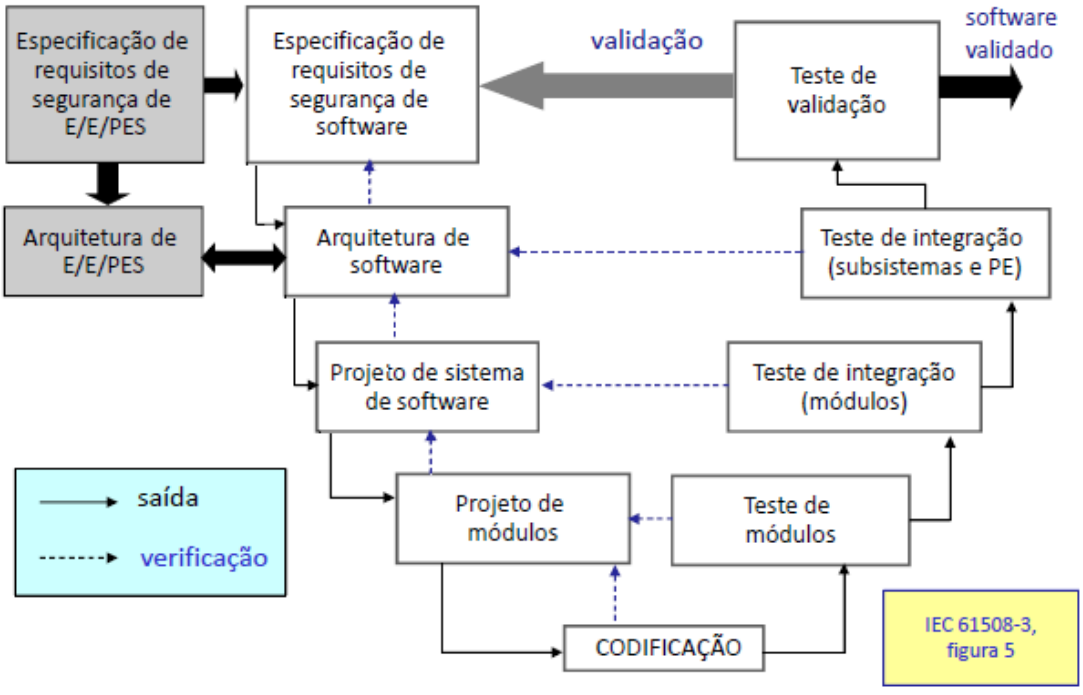

Figura 4.3: Fases do projeto e desenvolvimento de software (WEBER).

4.3.1 Arquitetura

A fase de arquitetura tem por objetivo elaborar a arquitetura de software visando cumprir os requisitos de segurança definidos, de acordo com o nível de integridade de segurança solicitado. Também leva em consideração requisitos que tenham sido inseridos no software através da arquitetura do hardware e as interações software/hardware que possam ocorrer.

4.3.2 Suporte a ferramentas e linguagens de programação

O objetivo desta etapa é apurar um grupo de ferramentas que irão assessorar os processos de avaliação, validação, verificação e modificação do software. Estas ferramentas, dentre as quais estão os compiladores e linguagens de programação, devem ser apropriadas para o nível de integridade de segurança desejado.

4.3.3 Projeto de sistema

A meta desta etapa é elaborar o projeto de um software que seja passível de verificação, análise e que mantenha a segurança durante processos de modificação. Além disso, deve satisfazer os requisitos de segurança de software especificados para o nível de integridade de segurança exigido.

4.3.4 Projeto de módulos

Esta fase tem como finalidade a análise e divisão do software em módulos, refinando o projeto de arquitetura inicial de acordo com os subsistemas identificados. Da mesma forma, deve ser especificado o projeto de cada módulo individualmente, bem como os testes a serem efetuados em um determinado módulo do software.

4.3.5 Codificação

Ao longo da etapa de codificação, devem ser utilizadas normas que contenham boas práticas de codificação, especificando regras que restringem o uso de estruturas da linguagem, quando empregadas em módulos com requisitos de segurança. Ainda, devem ser usadas ferramentas que detenham um certificado de validação com reconhecimento internacional.

A linguagem de programação deve ser compatível com os métodos de desenvolvimento e possuir mecanismos que auxiliem na identificação de incorreções no programa.

4.3.6 Teste de módulos

Esta etapa é responsável pelo teste de cada módulo do software, visando verificar se cada um destes executa as funções para as quais foram projetados e que satisfazem as definições exigidas de integridade e funções de segurança.

4.3.7 Teste de integração

Esta fase tem como finalidade verificar o cumprimento dos requisitos de segurança estabelecidos para o software. A validação é feita através de procedimentos que comprovem a interação correta e adequada entre os módulos, subsistemas e seus componentes. As atividades de teste de integração devem ser elaboradas concorrentemente ao longo das etapas de projeto e desenvolvimento.

4.4 Documentação e sua importância

Nos processos de avaliação, é importante que sejam evidenciadas as precauções adotadas por todos os membros envolvidos, bem como a segurança operacional e capacidade do sistema relacionado à segurança. Desta forma, é essencial que a documentação receba atenção especial, visando assegurar a verificação dos aspectos de segurança evidenciados e enfatizar a prudência adotada no desenvolvimento.

No contexto da norma IEC 61508, o objetivo geral relacionado à documentação é prevenir falhas e auxiliar na avaliação dos níveis de segurança do sistema, através da documentação de todas as fases relativas ao processo de desenvolvimento. De uma maneira mais formal, a documentação tem por objetivo definir as informações necessárias que devem ser documentadas de forma que:

- seja possível a realização de todas as etapas de todo o processo, E / E / EP e do ciclo de vida de segurança de software;

- seja possível efetivamente realizar os processos de verificação e avaliação da segurança funcional, bem como a gestão de segurança funcional como um todo.

A norma geralmente não demanda a apresentação de documentos físicos, salvo quando indicado claramente nas subseções pertinentes. A documentação pode ser exibida de várias maneiras, desde papel impresso, filmes ou outra forma qualquer de apresentação em displays.

Devido à grande quantidade de artefatos envolvidos, a utilização de guias e ferramentas digitais de auxílio são medidas importantes para tentar amenizar o custo de gerenciamento da documentação.

5 IMPLEMENTAÇÃO: SOFTWARE VALIDATION ASSISTANT

Este capítulo aborda descrições técnicas e o funcionamento do software desenvolvido – Software Validation Assistant (SVA). O objetivo do SVA é servir como ferramenta de apoio na busca pela certificação de dispositivos relacionados à segurança, e tem como base a norma IEC61508-3, que é referente à parte de software. É importante ressaltar que, no entanto, a utilização desta ferramenta se restringe a auxiliar o processo. A opção por elaborar uma ferramenta de apoio para a parte de software se deve ao fato de que é uma área que apresenta técnicas e medidas que nem sempre representam um consenso geral, o que aumenta a complexidade na interpretação. Além disso, as ferramentas disponíveis no mercado são na grande maioria ferramentas proprietárias e caras. O SVA, que não tem fins comerciais, tem o intuito de servir como alternativa a estas ferramentas. A garantia de certificação não está assegurada mesmo quando do seguimento de todos os passos corretamente, uma vez que não existem meios determinísticos para se avaliar determinada documentação.

5.1 Embasamento técnico

A base de referências técnicas para o software encontra-se na IEC 61508-3. Esta seção da norma contém em anexo as tabelas A.1 até A.10 (Anexo A), representando as fases do ciclo de vida de segurança de software, além das tabelas B.1 até B.9 (Anexo B) que podem ser referenciadas por técnicas presentes nas tabelas do anexo A. Estas técnicas carregam níveis de recomendação de sua utilização, que variam de acordo com o SIL almejado. A classificação das técnicas e medidas é a seguinte:

- NR (Not Recommended): não é recomendada a utilização desta técnica;

- -----: a utilização da técnica é indiferente, não possui recomendações a favor ou contra;

- R (Recommended): recomenda-se a aplicação desta técnica;

- HR (Higly Recommended): o uso desta técnica ou medida é fortemente recomendado.

O uso de uma técnica NR, bem com a ausência de utilização de uma técnica HR, implica na necessidade de uma justificativa. São apresentadas, também, técnicas que são consideradas alternativas entre si, identificadas com o número referente à técnica sucedido por uma letra. Assim, o uso de apenas uma das técnicas alternativas é o suficiente, pois são consideradas similares. As descrições de cada técnica estão presentes na IEC 61508-7, sendo referenciadas nas tabelas da IEC61508-3 pela coluna Ref.

5.2 Funcionalidades e características

O software SVA apresenta uma tela inicial (figura 5.1), na qual aparece o logo do sistema e os menus, que ao serem clicados expandem revelando os subitens do menu selecionado. A seguir serão ilustradas algumas telas do sistema, além de explicações gerais sobre as funcionalidades.

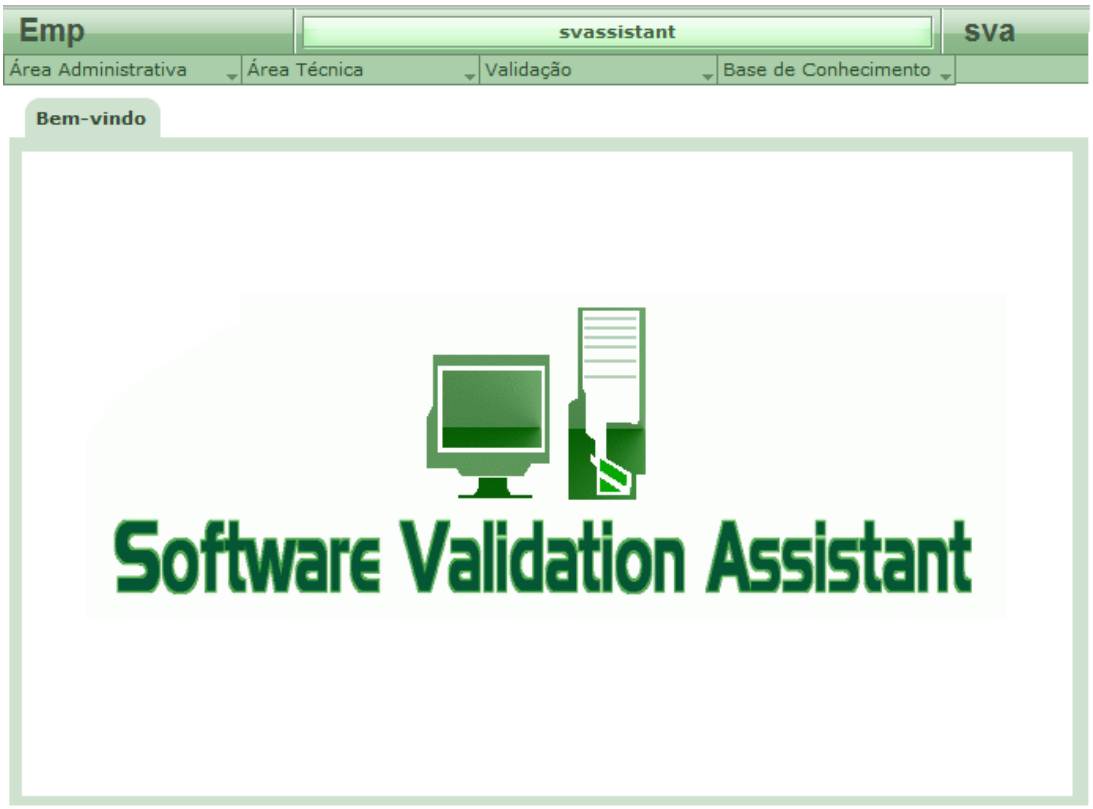

Figura 5.1: Tela inicial do sistema.

Um dos itens do menu Área Administrativa é o cadastro de eventos. Esta tela permite a inclusão de eventos com suas respectivas datas e horas de ocorrência. Tem por objetivo auxiliar os usuários a manterem-se atualizados sobre os eventos importantes. A figura 5.2 ilustra resultados de pesquisa de eventos:

Figura 5.2: Resultados de pesquisa de eventos.

De maneira geral, as telas de pesquisa oferecem a possibilidade de edição de um registro existente. Para tanto, basta clicar na linha que contém as informações do registro desejado.

O menu Base de Conhecimento apresenta as seguintes funcionalidades:

- Tópicos: permite cadastro, edição e consulta de tópicos importantes diretamente na tela, na forma de texto;

- Documentos Gerais: funcionalidade que possibilita a gravação e consulta de arquivos que contenham conteúdo técnico relevante;

- Links Úteis: utilizada para cadastrar e manter links (url) que sejam considerados interessantes. A figura 5.3 ilustra um resultado de pesquisa na tela de pesquisa de links:

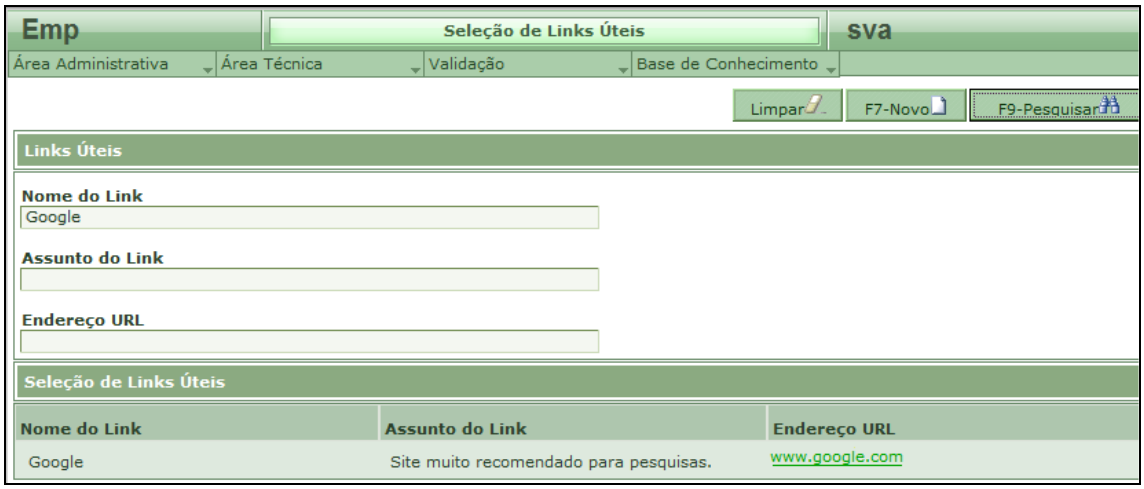

Figura 5.3: Resultados de pesquisa de links.

Dentre as outras funcionalidades do menu Área Administrativa estão as referentes ao gerenciamento de usuários e de projetos. A figura 5.4 mostra os resultados de uma busca de usuários:

Figura 5.4: Resultados de pesquisa de usuários.

A tela de cadastro de projetos permite ao usuário do sistema cadastrar um projeto onde é informado o nome do projeto, a empresa para a qual o projeto está sendo

desenvolvido, o SIL pretendido, além do gerente e responsável técnico. Os dois últimos são preenchidos através de uma popup de busca de usuários já cadastrados, que é mostrada quando do clique no botão "..." do campo desejado.

Figura 5.5: Tela de cadastro de projetos.

Ao clicar no menu Validação, são apresentados 4 submenus (SIL 1, SIL 2, SIL 3 e SIL 4). Ao selecionar o SIL desejado, o sistema carrega uma tela com os ciclos de vida e as técnicas a ele relacionadas, bem como o índice de referência da técnica e o nível de recomendação para o SIL selecionado. As informações sobre as fases do ciclo de vida de segurança de software, bem como suas respectivas técnicas, encontram-se ao longo das tabelas A.1 até A.10 do Anexo A da IEC 61508-3. O código do ciclo de vida representa a qual tabela de técnicas da norma ele está associado. No caso de uma técnica, representa o próprio código da técnica dentro da tabela da fase do ciclo de vida a qual pertence. Para efetuar a verificação, o usuário seleciona as técnicas que estão sendo utilizadas através da checkbox associada a cada técnica. Ao acionar o botão Validar, o sistema verifica se alguma técnica HR não foi marcada, e/ou se alguma técnica NR foi selecionada. Caso aconteça, o sistema avisa que em ambos os casos há a necessidade de apresentar uma justificativa.

Figura 5.6: Exemplo de tela de validação para SIL 1.

Além das funcionalidades já citadas, no menu Área Técnica estão presentes as funcionalidades que permitem o gerenciamento dos ciclos de vida, bem como das técnicas/medidas presentes nas tabelas dos anexos A e B da IEC 61508-3, além das respectivas referências. Tem por objetivo proporcionar flexibilidade à aplicação, para torná-la adaptável a eventuais mudanças.

5.3 Particularidades do desenvolvimento

Para a implementação do software SVA a linguagem de programação utilizada foi o Java, que tem como paradigma a orientação a objetos. Diferentemente das linguagens convencionais, que são compiladas para código nativo, a linguagem Java é compilada para um bytecode, o qual é então executado por uma máquina virtual.

O sistema roda em um servidor Apache Tomcat, que é um servidor web Java, ou mais especificamente um container de servlets. Permite acesso remoto, tendo suas páginas web desenvolvidas com a tecnologia JSP (Java Server Pages), que é uma tecnologia utilizada no desenvolvimento de aplicações web, semelhante às tecnologias ASP ou PHP. Permite ao desenvolvedor produzir aplicações que acessem o banco de dados, manipulem arquivos no formato texto, capturem informações a partir de formulários e captem informações sobre o visitante e sobre o servidor.

Quanto ao banco de dados, é utilizada uma instância de banco de dados relacional Apache Derby para efetuar o armazenamento e manipulação dos dados.

As classes do sistema (figura 5.1) dividem-se entre 11 classes e 3 enumerações, totalizando 14 classes:

- *EventoAgenda*: classe que representa eventos da agenda, com os atributos *data*, *hora*, *nomeEvento* e *infoEvento* (descrição);

- *DocumentoConhecimento*: responsável por abstrair objetos que contém o arquivo, o nome informado pelo usuário (*nomeDoc*), descrição do arquivo e o nome do arquivo no sistema (*docName*);

- *LinkConteudo*: representa os objetos formados pelo nome, assunto e endereço url;

- *Topico:* abstrai objetos que contém *nomeTopico*, *assuntoTopico* e *conteudoTopico*, todos no formato String;

- *DocumentoProjeto*: semelhante à classe *DocumentoConhecimento*, com a adição de um atributo que faz referência a um projeto;

- *Usuario*, que representa a abstração dos dados de usuários, com os atributos *email*, *nome*, *perfil* e *username*;

- *Projeto*: representa os objetos que contém *nomeProjeto*, *nomeEmpresa*, *silPretendido*, *gerenteProjeto* e *responsavelTecnico* (sendo os 2 últimos instâncias da classe *Usuario*);

- *CicloVida*: define os atributos dos objetos que representam as fases do ciclo de vida, dentre eles *código*, *nome descricao* e uma lista de técnicas que são referenciadas;

- *TecnicaMedidaA*: representa as técnicas e medidas através dos atributos *codigo*, *nome*, *cicloVida* (referência a qual fase do ciclo de vida a técnica pertence), *sil1*, *sil2*, *sil3*, *sil4*, além de uma lista de técnicas das tabelas do anexo B as quais referencia;

- *TecnicaMedidaB*: representa objetos parecidos com os da classe *TecnicaMedidaA*, diferindo destes pois tem ligação com um objeto do tipo *TecnicaMedidaA* ao invés de um objeto do tipo *CicloVida*;

- *Referencia*: objetos que possuem os atributos *codigo*, *nome*, *descricao* e *objetivo*, além de listas de técnicas (das tabelas dos anexos A ou B da IEC 61503-3) pelas quais são referenciadas;

- As enumerações *PerfilUsuario*, *Sil* e *NivelRecomendacao*, cujos valores representam um conjunto finito de identificadores previamente definidos.

A figura 5.1 ilustra o diagrama de classes do sistema implementado, apresentando as classes do sistema, bem como seus atributos e a relação entre elas:

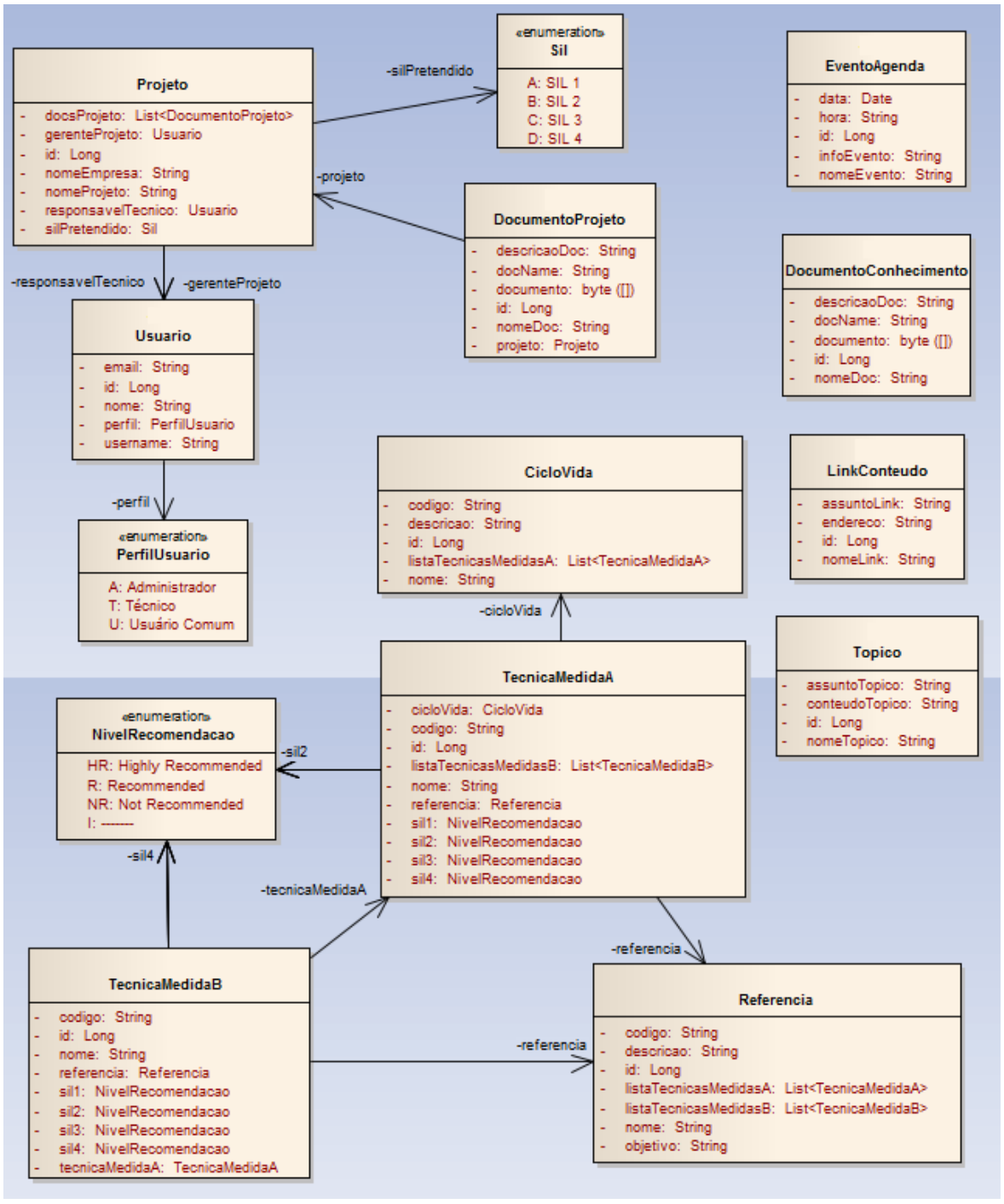

Figura 5.7: Diagrama de classes do sistema.

O diagrama de classes é uma representação da estrutura e relações das classes que servem de modelo para objetos. Define as classes que o sistema necessita possuir e serve como base para a construção de outros elementos da documentação.

A figura 5.8 ilustra os tipos de usuário do sistema e as funcionalidades (ou Use Cases - UC) que cada perfil tem acesso:

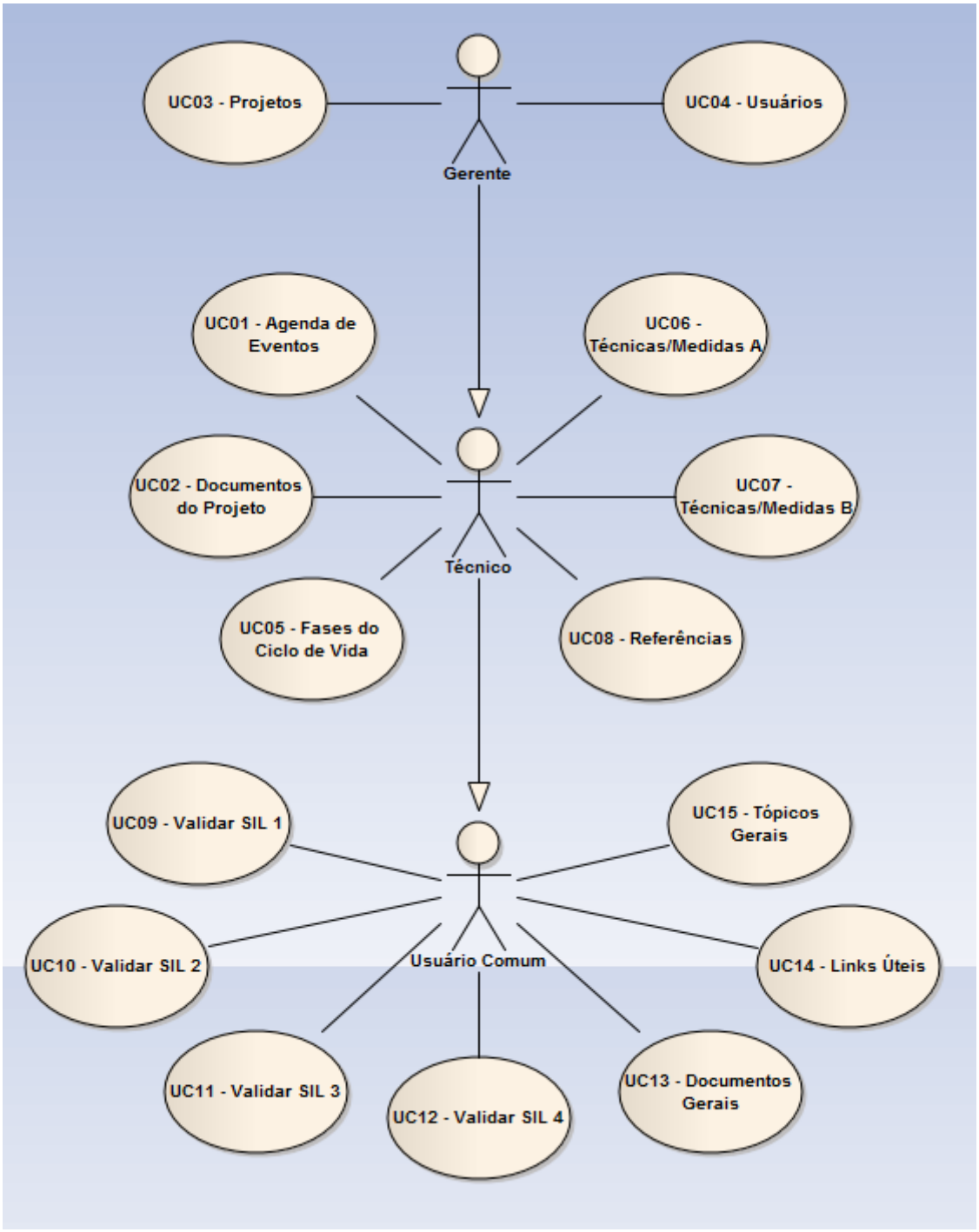

Figura 5.8: Permissão dos usuários do sistema em relação aos casos de uso.

Os perfis de usuário são: gerente (ou administrador), técnico e usuário comum. A hierarquia entre os perfis ocorre da seguinte forma (como apresentado na figura 5.8):

- um usuário comum possui acesso apenas às funcionalidades UC09 a UC15;

- usuário com perfil técnico tem acesso às funcionalidades de um usuário comum, acrescentando-se as funcionalidades de perfil técnico. São representadas pelos UC01, UC02 e UC05 a UC08;

- um usuário administrador (ou gerente) tem acesso pleno ao sistema.

5.4 Trabalhos futuros

A norma internacional IEC 61508 é bastante abrangente. Uma opção para dar continuidade ao trabalho seria desenvolver uma extensão ao SVA, onde o foco seria um tutorial interativo, exemplificando e ilustrando as etapas funcionais para a aplicação das normas de software e hardware. Outra forma de estender a aplicação seria através da implantação de um mecanismo de envio de email automático aos envolvidos em um projeto. Este envio seria acionado quando da alteração de datas, documentação, participantes ou qualquer informação relevante para o projeto.

CONCLUSÃO

Ao longo deste trabalho, várias características da norma internacional IEC 61508 foram abordadas, visando fornecer uma visão geral sobre o seu funcionamento e importância. A IEC 61508 estabelece os requisitos necessários para assegurar que os sistemas sejam projetados, implementados e operados para suprir as exigências do nível de integridade de segurança (SIL) requerido. A norma define também um processo a ser seguido por todas as partes envolvidas, com o objetivo de uniformizar a terminologia e os parâmetros do sistema.

Embora elogiada por sua adaptabilidade a vários setores e por fornecer uma série de técnicas e medidas interessantes, a norma recebe também várias críticas. A IEC 61508 peca ao deixar muitos pontos vagos em relação à documentação, sem apresentar exemplos consistentes de protótipos de documentos ou justificavas para a adoção de técnicas alternativas. Da mesma forma, muitas vezes é necessário recorrer a outras normas para complementar o conhecimento requerido para o processo de certificação.

No Brasil, a crescente demanda por componentes certificados para questões de segurança faz com que este ramo de software para segurança seja igualmente impulsionado. O software SVA elaborado ao longo deste trabalho tem o intuito de esclarecer vários aspectos relacionados à norma. Igualmente, tem por objetivo servir como uma alternativa de ferramenta de apoio à aplicação das padronizações em sistemas relacionadas à segurança, uma vez que as ferramentas existentes não são, na sua maioria, gratuitas.

O SVA foi planejado e implementado em Java, linguagem de programação que tem como paradigma a orientação a objetos. Tem por caracterísitca a compilação do código fonte para um bytecode, o qual é executado por uma máquina virtual, permitindo a portabilidade entre sistemas. O SVA abrange todas as fases do ciclo de vida de segurança de software, permitindo desde a inclusão de novas fases, como também a alteração das fases existentes. Isto se mostra muito útil no intuito de tornar o sistema adaptável a eventuais mudanças na norma, mesmo que estas não ocorram com grande frequência. O mesmo comportamento é apresentado para as técnicas relacionadas às fases do ciclo de vida, o que proporciona flexibilidade à aplicação. Além de auxiliar na verificação da utilização das técnicas pertinentes, o SVA permite a manutenção de registros de usuários, projetos e eventos. Oferece apoio também para a criação de uma espécie de base de conhecimento, através de funcionalidades de cadastro e busca de links, tópicos e documentos. Isto possibilita a criação de um banco de informações que sejam relevantes ao contexto e que estejam disponíveis para consulta e acesso rápido pelos usuários do sistema.

REFERÊNCIAS

SMITH D.J.; SIMPSON, K.G.L.; **Functional Safety: a straightforward guide to applying IEC 61508 and related standards**, Elsevier, Butterworth-Heinemann, U.K. 2ªedição, 2004.

BELL, R. **Introduction to IEC 61508** ACS Workshop on Tools and Standards, Conference in Research and Practice in Information Technology, Vol. Nº 55, 2005.

BROWN, S. **Overview of IEC 61508 Design of electrical/electronic/programmable electronic safety-related systems** IEEE Computing and Control, Engineering Journal, fevereiro 2000.

BLACK, W.S. **IEC 61508 – what it doesn't tell you** IEEE Computing and Control, Engineering Journal, fevereiro 2000.

DUNN, W. R. (2003). **Designing safety-critical computer systems**. IEEE Computer, 36(11):40 – 46. ISSN 0018-9162, novembro 2003.

FALLER, R. **Project Experience with IEC 61508 and Its Consequences** U. Voges (Ed.): SAFECOMP 2001, LNCS 2187, v. 2187 p. 200–214, 2001.

INTERNATIONAL ELECTROTECHNICAL COMISSION. **IEC 61508**: functional safety of eletrical/eletronic/programmable eletronic safety-related systems. Geneva, 2000-05.

LADKIN, P. B.; **An Overview of IEC 61508 on E/E/PE Functional Safety,** Bielefeld**,** 2008, disponível em: <http://www.causalis.com/IEC61508FunctionalSafety.pdf>, acesso em: out. 2011.

MCDERMID, J.A. **Software Safety: Where's the Evidence?** Proc. 6th Australian Workshop on Industrial Experience, v.3, 2001.

SIQUEIRA T. F.; MENEGOTTO, C.C.; WEBER, T. S.; NETTO, J.C.; WAGNER, F.R. **Desenvolvimento de Sistemas Embarcados para Aplicações Críticas** IV Escola Regional de Redes de Computadores, Passo Fundo, setembro 2006.

WEBER, T.S. **Norma IEC 61508 – Parte 3: Software**, slides de curso ministrado.

Páginas na internet (acessadas entre setembro e novembro de 2011):

Wikipedia: The Free Encyclopedia – IEC 61508

http://en.wikipedia.org/wiki/IEC_61508

Functional Safety and IEC 61508

http://www.iec.ch/functionalsafety/

ISO, International Organization for Standardization
http://www.iso.org/

The 61508 Association
http://www.61508.org/

Inside Functional Safety - IEC 61508:2010 Terms and definitions
http://www.insidefunctionalsafety.com/knowledge/glossary.html?letter=All&glossid=8