|  |
| --- |
| **Universidade Federal de Pernambuco**  **CIn – Centro de Informática** |
| **Pré-Projeto de Mestrado** |
| Área: **Engenharia de Software** |
| Título: **Gerador de Modelos SCR a Partir de Modelos SCADE** |
| Aluno: **Francisco Ioneiton da Silva** |

**Justificativa**

O desenvolvimento de sistemas críticos engloba uma série questões no que diz respeito a sua implantação.Para que tais sistemas possam ser postos em funcionamento,estes sistemas devem satisfazer determinados padrões, que regem normas para seu desenvolvimento. Para sistemas aviônicos, a norma DO-178C é o padrão que regulamenta o desenvolvimento de software para aeronaves. Este padrão é adotado pela FAA (*Federal Aviation Administration*) dos EUA, pela ANAC no Brasil e EASA na Europa [1,4].

Estar de acordo com tais normas e padrões implica na aptidão do sistema a receber certificação de segurança (*safety*) [2]. Certificados de segurança garantem a sociedade como um todo que a implantação de um dado sistema não representa um risco de dano inaceitável[2]. Para as entidades certificadoras, é necessário que todos os artefatos do projeto satisfaçam os altos padrões de qualidade como, por exemplo, o DO-178C.Porem, como discutido em [3], os requisitos de um sistema normalmente sãodescritos informalmente, usando linguagem natural. Por meio do SCR (Software Cost Reduction), pode-se obter a descrição formal de requisitos em uma linguagem amigável, mas isso não é suficiente para obtenção de certificado de segurança, código certificado é um outro ponto chave para certificação do sistema, é possível se obter código certificado de acordo com DO-178C utilizando SCADE (ambiente de desenvolvimento baseado em modelos) [3].A norma DO-178C exige que sejam adotadas estratégias para rastreabilidade entre estes artefatos de forma que garanta que, ao final do processo de desenvolvimento estes artefatos satisfação as exigências dos órgãos certificadores [3, 6].

Empresas que desenvolvem sistemas críticos, como a Embraer, que trabalham mais diretamente com sistemas de controle, lidam com maiorfreqüência com modelos de simulação (Simulink/SCADE, entre outros), do que com requisitos no desenvolvimento de seus sistemas. O uso de modelos de simulaçãogera resultados (curva de resposta) que muitas vezes vão de encontro à descrição dos requisitos. Fato que acarreta a necessidade de atualizar o documento de requisitos, a cada vez que uma simulação e rodada,para que ambos os artefatos estejam em conformidade um com o outro. Atualmente, o processo de atualização do documento de requisitos apôs o resultado das simulações com os modelos, é feito por seres humanos, o que pode gerar inconsistências na rastreabilidade destes artefatos.

Deste modo, a criação de um tradutor de modelos SCADE para requisitos SCR, seria uma ferramenta de grande valia para essas empresas. Visto que, a automação desse processo,garante que os requisitos ajustados de acordo com os modelos de simulação Simulink/SCADE satisfazem as normas de certificação internacionais como a DO-178C que exige uma correta a rastreabilidade dos artefatos do projeto. Facilitando a gerencia dos requisitos do sistema em desenvolvimento, bem como assegurar a equivalência entre modelos de desenvolvimento e o documento de requisitos.

**Revisão da Literatura**

Sistemas de controle utilizados na aviação apresentam-se como um conjunto de softwares e outros sistemas que são responsáveis por diversas funções importantes em aeronaves modernas. Alguns destes sistemas operam em solo, como sistemas para controle de trafego aéreo, bem como podem ser embarcados nas aeronaves, sendo então denominados aviônicos [1].

Sistemas aviônicos são classificados com sistemas críticos, visto que o mau funcionamento deste pode acarretar em risco para os que o operam ou o utilizam de outras formas. Sistemas desta natureza requerem regulamentação por órgãos competentes para que possam entrar em atividade [1, 3]. Estas entidades emitem certificados de segurança (*safety*) garantindo a sociedade que o sistema funcionará como planejado. A certificação de sistemas aviônicos, devido a acordos internacionais se dá de acordo com o padrão adotado pela FAA, atualmente o padrão DO-178C é o padrão utilizado por este órgão.

O padrão DO-178 (e seu equivalente na Europa o ED-12) fornece várias orientações sobre os diversos processos do ciclo de vida de softwares críticos, com forte ênfase na verificação. Sua versão mais bem sucedida a DO-178B foi introduzida em 1992, durante os vinte anos de vigência deste padrão não foram registradas nenhuma fatalidade devido à falhas na implementação de requisitos de software [6]. O DO-178B passou por um processo de revisão e sofreu mudanças para esclarecer algumas inconsistências, e introduzir novas metodologias e tecnologias [4]. O padrão DO-178C, dentre outras melhorias, inclui um suplemento para métodos formais conhecido como DO-3334 [4, 6].

As normas estabelecidas no DO-178C, para certificação de software aviônico requerem atividades de verificação (fig. 1) que demonstrem que o software em execução satisfaz estes requisitos, este fluxo de atividades reforça a necessidade, de haver rastreabilidade entre os artefatos do projeto, para que o software desenvolvido esteja de acordo com as exigências dos órgãos competentes [6].

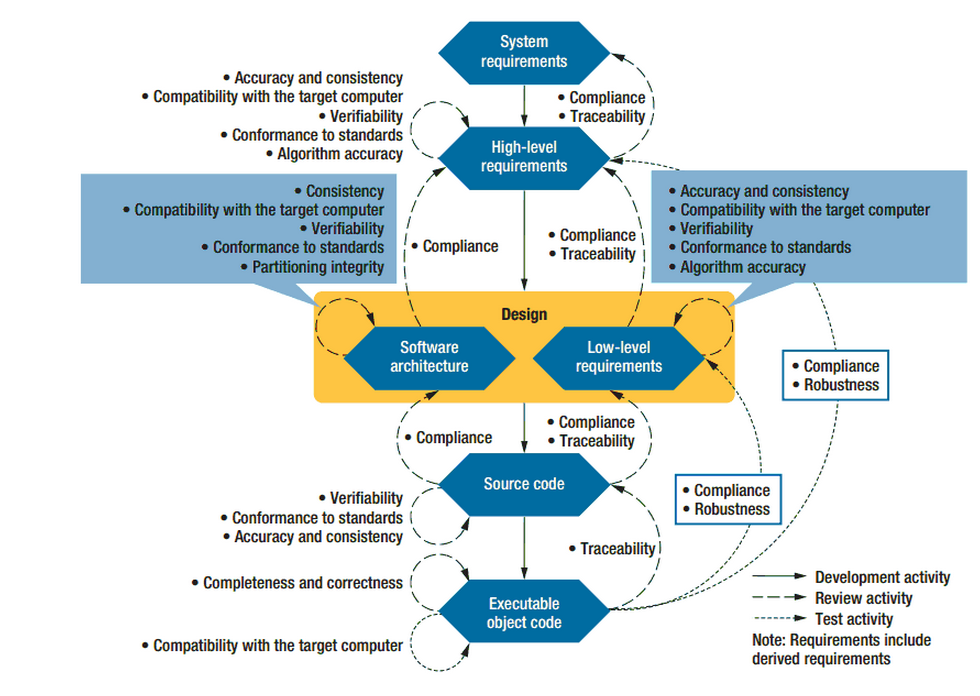


Figura 1: Atividades de verificação do padrão DO-178C [6]

O documento de requisitos é o artefato mais importante em um processo de desenvolvimento de sistemas. Porém os requisitos geralmente são expressos de maneira informal, por meio de linguagem natural [3], que pode gerar ambigüidade e incompletudes. Uma alternativa para formalização de requisitos é utilizar SCR (Software Cost Reduction), um método formal para descrever comportamento de sistemas complexos usando tabelas, e expressões lógicas simples [3]. SCR foi desenvolvido pelo laboratório de pesquisas navais dos Estados Unidos, para documentar as especificações do programa de vôo da aeronave U.S. Navy’s A-7 [3, 7].

Por meio da composição de tabelas SCR, se define o comportamento do sistema, cada tabela por sua vez define os valores de uma determinada variável, por meio de avaliação de expressões booleanas (predicados), a tabela 1 traz um exemplo de uma tabela SCR. As variáveis em SCR podem ser de quatro tipos; as variáveis controladas e monitoradas que referem-se às entradas e saídas advindas do ambiente, e as variáveis auxiliares Termo e Classe de Modo [3, 7]. Algumas ferramentas podem ser utilizadas para apoiar ouso de SCR, o SCR Toolset que sua permissão de uso é cedida apenas a agencias do governo dos EUA, e T-Vec que enfatiza o desenvolvimento de especificações e geração automática de casos de teste.

A respeito da certificação de código fonte para sistemas críticos, tem-se a suíte SCADE (Safety Critical Application Development Environment), a linguagem de programação do SCADE utiliza notação de blocos que se conectam, é baseada no paradigma síncrono e na linguagem Lustre [3, 5]. O ambiente de desenvolvimento possui um gerador automático de código, que produz código na linguagem C, certificado segundo o padrão Do-178C [3, 5].

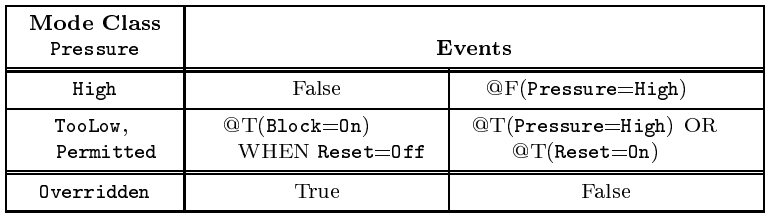


Tabela 1: Exemplo de uma tabela SCR [7]

Podemos ver no trabalho desenvolvido em [3] a criação de uma ferramenta que torna possível se obter numa única solução, requisitos formais e código certificado. Por meio de regras de tradução, os requisitos SCR, são mapeados para modelos SCADE, além da criação das regras de tradução o trabalho de [3] inclui a criação de um tradutor automático utilizando o framework de transformação de software Stratego/XT.

Porém, uma questão a ser considerada durante o ciclo de desenvolvimento de um sistema de software para aeronaves é a gestão dos requisitos do sistema. O documento de requisitos ao longo do ciclo de desenvolvimento, sofre refinamentos, devido aos resultados das simulações com os modelos, a curva de resposta pode não corresponder em uma proporção de um para um com os requisitos do sistema. Atualmente esta atualização no documento é feita manualmente, fato que pode causar incompletudes, ambigüidades e inconsistências neste artefato

**Objetivo**

Portanto, esta proposta de projeto de mestrado visa à construção de um tradutor de modelos SCADE para requisitos em SCR, e por meio desse aperfeiçoar o processo de rastreabilidade e gestão de requisitos do sistema, garantindo a consistência entre os artefatos gerados no processo de desenvolvimento. Além disto, busca-se neste projeto a integração com o tradutor gerado em [3], tanto para realizar uma verificação nas saídas obtidas pela solução proposta, como também possibilitar a criação de uma estratégia de desenvolvimento Round Trip.

**Metodologia**

O desenvolvimento do tradutor de diagramas SCADE para requisitos SCR se dará da seguinte forma:

1. Criação de regras de tradução que permita a integração entre as duas linguagens;
2. Utilizar o framework Stratego/XT para geração de um tradutor automático;
3. Integrar a ferramenta apresentada em [3] com o tradutor desenvolvido a fim de se obter tradução em duas vias (roundtrip);
4. Utilizar a ferramenta T-Vec para gerar casos de teste
5. Realizar a verificação, dos requisitos SRC gerados após a tradução, utilizando os estudos de casos que validaram o tradutor de [3], e observar se as saídas gerada pelo tradutor criado nesta proposta corresponde com as produzidas pelo tradutor de [3] (Fig. 2);

|  |
| --- |
| SCR.PNG  Ca  Cb  SCADE.PNG **SCR** **SCADE**  Ca = Cb |

**Cronograma**

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **2014** | **Fev** | **Mar** | **Abr** | **Mai** | **Jun** | **Jul** | **Ago** | **Set** | **Out** | **Nov** | **Dez** |
| Cursando carga horária |  |  |  |  |  |  |  |  |  |  |  |
| Pesquisa Bibliográfica |  |  |  |  |  |  |  |  |  |  |  |
| Desenvolvimento de sistema de testes |  |  |  |  |  |  |  |  |  |  |  |
| Aplicação de testes temporais |  |  |  |  |  |  |  |  |  |  |  |
| Escrita da dissertação |  |  |  |  |  |  |  |  |  |  |  |
| **2015** | **Fev** | **Mar** | **Abr** | **Mai** | **Jun** | **Jul** | **Ago** | **Set** | **Out** | **Nov** | **Dez** |
| Cursando carga horária |  |  |  |  |  |  |  |  |  |  |  |
| Pesquisa Bibliográfica |  |  |  |  |  |  |  |  |  |  |  |
| Desenvolvimento de sistema de testes |  |  |  |  |  |  |  |  |  |  |  |
| Aplicação de testes temporais |  |  |  |  |  |  |  |  |  |  |  |
| Escrita da dissertação |  |  |  |  |  |  |  |  |  |  |  |

De inicio será realizada um levantamento bibliográfico, este levantamento terá a finalidade de formar uma base de conhecimento acerta do assunto. Após esta etapa iniciará a construção do sistema proposto partindo da definição das regras de tradução, em seguida se inicia a criação do tradutor automático, que vai gerar os requisitos em SCR.

Logo em seguida, se iniciará a fase de testes a fim de observar o comportamento da ferramenta e realizar a verificação dos requisitos obtidos. A ultima etapa do desenvolvimento, contempla a integração da ferramenta que será desenvolvida neste projeto com a ferramenta apresentada em [3].

**ReferênciasBibliográficas**

[1] I. R.de Oliveira; Considerações Sobre Reuso de Software Aviônico. In: VII SITRAER - Simpósio Brasileiro de Pesquisa em Transporte Aéreo, 2008, Rio de Janeiro. Avanços do TransporteAéreoBrasileiro, 2008.

[2] J. Rushby; New challenges in certiﬁcation for aircraft software. In Proceedings of

the ninth ACM international conference on Embedded software, EMSOFT ’11, pages

211–218, New York, NY, USA.ACM.

[3] M. Andrade, A. Mota, M. Cornélio;Generating SCADE Models From SCR

Specications

[4] S. Nordhoff, 2012, Através dewww.sqs.com\_de-group\_\_download\_DO-178C\_ED-12C.pdf

[5] http://www.esterel-technologies.com/products/scade-suite/

[6] Y. Moy, E. Ledinot, H. Delseny, V. Viels, B. Monate. (2013, Set) Testing or Formal Verification: DO-178C Alternatives and Industrial Experience. IEEE Software. 30(3), 50-57. Available: http://ieeexplore.ieee.org/xpl/abstractAuthors.jsp?tp=&arnumber=6471965&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs\_all.jsp%3Farnumber%3D6471965

[7] http://www.nrl.navy.mil/itd/chacs/5546/SCR