Revista dos Transportes Públicos - ANTP - Ano 28 - 2006 - 2º trimestre

Análise de risco de um sistema de controle de transporte público

João Batista Camargo Jr.
Jorge Rady de Almeida Jr.
Paulo Sérgio Cugnasca
Professores doutores do Departamento de Engenharia de Computação e Sistemas Digitais da Escola Politécnica da Universidade de São Paulo e consultores da Fundação para o Desenvolvimento Tecnológico da Engenharia - FDTE

A metodologia aqui apresentada é parte integrante de um processo mais amplo denominado análise de segurança, constituído pelo gerenciamento da segurança e pela análise de risco propriamente dita.

ANÁLISE DE RISCO

Na análise de risco busca-se avaliar a importância relativa do perigo, bem como pode-se analisar o grau de aceitação ou rejeição desse risco. No sentido de se obter uma melhor compreensão da natureza do risco é extremamente útil considerar a relação entre perigos e acidentes, sendo que estes últimos resultam em danos materiais às pessoas ou ao meio ambiente. Considera-se que o perigo representa uma situação na qual há um acidente potencial associado. O risco referente a um perigo é determinado pela combinação de dois fatores: a freqüência ou probabilidade da ocorrência de um acidente e a severidade da conseqüência envolvida em um eventual acidente. O risco pode ser avaliado tanto qualitativa quanto quantitativamente. As escalas quantitativas podem variar de aplicação para aplicação, apesar do esforço de diversos órgãos internacionais em buscar, através de normas, padronizar essa escala (Storey, 96; Ladkin, 01).

Um determinado risco não é aceitável se existir um determinado perigo com alta probabilidade de ocorrência e que possua conseqüências desastrosas a ele associado. No entanto, poder-se-ia aceitar um risco, em relação a um determinado perigo, com baixíssima probabilidade de ocorrência, apesar de apresentar conseqüências altamente danosas. O nível de aceitabilidade do risco é determinado pelo benefício associado ao risco e pelo esforço requerido para diminuí-lo.

A redução necessária de risco deve ser alcançada para mantê-lo a um nível tolerável em uma determinada situação. O conceito de redução necessária de risco é de fundamental importância na avaliação de sua aceitabilidade (DD ENV 50129, 1999).

A norma IEC 61508-1 define níveis de integridade de segurança (Safety Integrity Level - SIL) para sistemas que operam em regime de baixa demanda e para sistemas que operam em regime de alta demanda ou de modo contínuo (IEC 61508).

Um sistema opera em regime de baixa demanda se a freqüência em que ele é solicitado não for maior que uma vez por ano e não for maior que duas vezes a freqüência em que ele é verificado, ou seja, sofre um processo de manutenção preventiva. Caso contrário, considera-se que o sistema tem um regime de operação de alta demanda ou de modo contínuo.

Para sistemas que operam em baixa demanda, são definidos níveis de integridade de segurança em termos de valores limites da probabilidade média de falha do sistema ao executar a função para a qual ele foi projetado. Para sistemas que operam em regime de alta demanda, os níveis estão em termos de valores limites para a probabilidade de ocorrência de falhas inseguras por hora.

A tabela 1 apresenta os quatro níveis SIL definidos para os dois tipos de modo de operação citados.

Tabela 1
Níveis de integridade de segurança

SIL	Baixa demanda (λ = falha insegura por demanda)	Alta demanda (λ = falha insegura por hora)
4	$10^{-5} \leq \lambda \leq 10^{-4}$	$10^{-9} \leq \lambda \leq 10^{-8}$
3	$10^{-4} \leq \lambda \leq 10^{-3}$	$10^{-8} \leq \lambda \leq 10^{-7}$
2	$10^{-3} \leq \lambda \leq 10^{-2}$	$10^{-7} \leq \lambda \leq 10^{-6}$
1	$10^{-2} \leq \lambda \leq 10^{-1}$	$10^{-6} \leq \lambda \leq 10^{-5}$

Um dos métodos de determinação do risco aceitável é denominado As low as reasonable practible - Alarp (Melchers, 01). A aplicação do princípio Alarp significa tentar reduzir o nível de risco de um sistema a valores tão baixos quanto possível desde que a relação entre o investimento necessário e a melhora do sistema for aceitável. Esta técnica é usada principalmente no Reino Unido.

Em uma aplicação, os níveis de risco são classificados da seguinte forma:

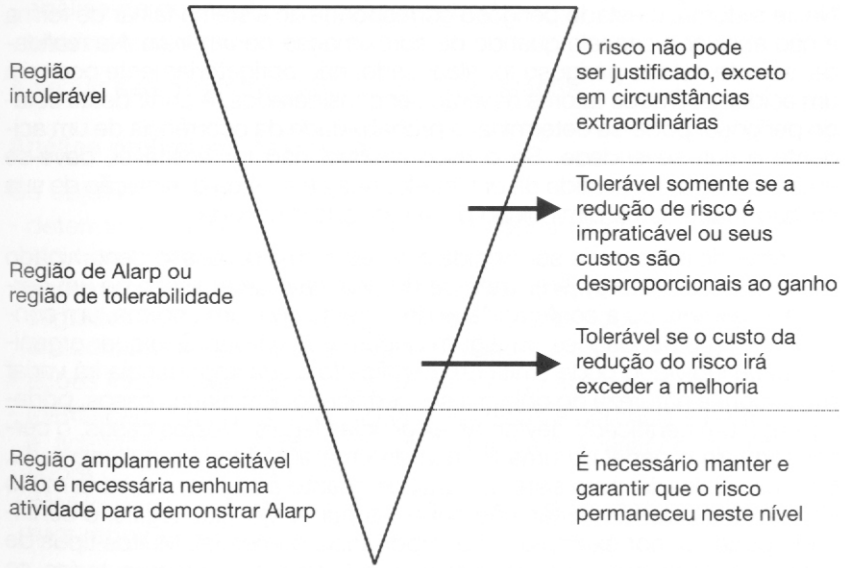
a. o risco é tão grande que não deve ser tolerado; ou
b. risco é ou tornou-se tão pequeno, tornando-se insignificante; ou
c. o risco está entre os dois estados especificados nos itens a e b, tendo sido reduzido ao mais baixo nível praticável, tendo em vista

os benefícios resultantes de sua aceitação e os custos de qualquer redução adicional.

Com respeito ao item c, o princípio Alarp requer que qualquer risco deva ser reduzido, o quanto for razoavelmente praticável, para um nível tão baixo quanto razoavelmente aceitável. As três regiões são mostradas na figura 1.

Acima de um certo nível, um risco é considerado intolerável e não pode ser justificado em qualquer circunstância ordinária. Neste caso, ele está situado na região intolerável. Abaixo desse nível, há a região de tolerabilidade, onde se permite que uma atividade ocorra com seus riscos associados, que são tão baixos quanto o razoavelmente praticável. Ser tolerável significa conviver com riscos, obtendo os benefícios do funcionamento do sistema.

Figura1
Regiões de risco



Ao mesmo tempo, espera-se que este nível de risco seja mantido sob constante acompanhamento, sendo reduzido como e quando isto puder ser feito.

Uma avaliação de custo e benefício é exigida explícita ou implicitamente de forma a se avaliar o custo e a necessidade de melhorias, ou ainda para se avaliar a necessidade de medidas de segurança adicionais.

Após a determinação dos níveis de integridade de segurança, pode-se iniciar o processo de análise de risco (Leveson, 95; Storey, 96) (NASA, 96; DD ENV 50126, 1999), que consta das seguintes etapas:

- definição e descrição do sistema, interfaces e demais informações necessárias para a análise de risco;
- realização do processo de análise de perigo;
- qualificação do risco residual;
- caso o nível de risco residual não seja aceitável, redução da severidade dos acidentes relacionados com o estado perigoso ou redução da probabilidade de sua ocorrência; e
- realimentação e avaliação da experiência operacional.

De forma a exemplificar os conceitos apresentados, considere-se um sistema de controle de uma cancela em uma passagem de nível. Dentro do processo de análise de risco padroniza-se como análise de perigo o ato de determinação da probabilidade do sistema atingir um estado perigoso. Neste sistema, o estado perigoso corresponde ao sistema falhar de forma a não abaixar a cancela quando da aproximação de um trem. Na realidade, se este estado perigoso for alcançado, não obrigatoriamente ocorrerá um acidente. Outros fatores deverão ser considerados. A partir deste estado perigoso, pode-se determinar a probabilidade da ocorrência de um acidente e sua severidade. Se o risco residual não for aceitável, deve-se então trabalhar no sentido de diminuí-lo, seja através da diminuição de sua probabilidade ou da diminuição da severidade envolvida.

A análise de risco pode ser exigida através de um processo denominado de certificação (Storey, 96). Trata-se do processo de emissão de um certificado garantindo a conformidade do sistema com uma norma, um conjunto de recomendações ou algum documento similar. Qualquer organização ou indivíduo pode emitir um certificado e sua importância irá variar muito com a natureza do objeto a ser certificado. Em alguns casos, pode-se exigir um certificado devido às exigências legais. Nestes casos, o certificado tem o papel de uma licença de uma autoridade regulamentada. Esta necessidade, para sistemas críticos quanto à segurança, varia muito conforme o país. Em áreas não cobertas por exigências legais, o certificado pode ter, por exemplo, uma importância comercial. Muitos tipos de indústrias possuem uma autoridade reguladora que governa todos os projetos dentro de um determinado setor. Atualmente não existe no Brasil uma autoridade reguladora na área metro-ferroviária com poderes de certificação. Com o objetivo de obter certificação, o projetista de um produto crítico deve provar, ao órgão certificador, a segurança de seu produto. O projetista deve ser capaz de mostrar que todos os perigos foram identificados e tratados adequadamente e que a integridade do sistema é apropriada para aquela aplicação, ou seja, atende aos níveis de integridade de segurança exigidos. O trabalho envolvido em um processo de certificação é grandioso e requer um planejamento cuidadoso.

ANÁLISE DE PERIGO

O escopo da aplicação de um processo de análise de perigo é basicamente constituído por dois objetivos. O primeiro refere-se ao desenvolvimento de novos sistemas. Neste aspecto, a análise de perigo procura identificar e avaliar perigos potenciais, além de eliminá-los ou controlá-los. O segundo escopo refere-se à análise de perigo de sistemas existentes. Neste caso, o trabalho tem como meta identificar e avaliar perigos, visando quantificar os seus níveis de segurança, formular políticas de segurança, treinar profissionais e aumentar a motivação em se atingir uma operação segura e eficiente. A análise de perigo deve ser um processo contínuo e interativo, estendendo-se por todo o ciclo de vida de um sistema. O processo de análise de perigo pode ser dividido em cinco etapas:

- análise preliminar de perigo;
- análise de perigo do sistema;
- análise de perigo dos subsistemas;
- análise de perigo da operação e suporte;
- análise final de perigo.

A seguir são descritas cada uma destas etapas.

Análise preliminar de perigo

Os objetivos desta etapa são:

- determinar quais perigos podem existir durante a operação do sistema e sua magnitude relativa;
- desenvolver recomendações, especificações e critérios a serem seguidos no projeto do sistema. Neste sentido pode ser estabelecido um conjunto de requisitos gerais de segurança do sistema;
- ações iniciais para o controle de um perigo em particular;
- identificação de responsabilidades técnicas e gerenciais para a ação e aceitação de riscos, como também para avaliação do controle sobre os perigos identificados;
- determinação da magnitude e complexidade dos problemas de segurança.

Análise de perigo do sistema

A análise de perigo do sistema pode ter seu início na revisão preliminar de projeto, devendo se estender ao longo de todo o ciclo de vida de um projeto. O principal objetivo desta atividade é recomendar mudanças, além de controlar e avaliar o atendimento aos requisitos gerais de segurança, tanto em operação normal como em operação degradada do sistema, levando em consideração a presença de falhas. Nesta etapa, os componentes envolvidos são os diversos subsistemas, incluindo a interface homem-máquina. Como no início deste tipo de análise já se tem uma visão preliminar da arquitetura do sistema, deve-se iniciar o estudo da interação entre os diversos subsistemas constituintes e como suas interações podem afetar a segurança do sistema. Em função desse trabalho podem ser determinados os requisitos gerais de segurança relativos aos subsistemas envolvidos.

Análise de perigo dos subsistemas

Esta etapa de análise deve ter início a partir da existência de um projeto relativo aos subsistemas. Ela apresenta os mesmos objetivos da análise anterior, só que focada em cada subsistema, de forma mais detalhada. Outros subsistemas envolvidos, implementados através de outras tecnologias diversas de circuitos eletroeletrônicos, deverão sofrer um processo de análise com técnicas específicas e desenvolvidas para este fim. Tendo em mente os sistemas de controle computacionais, a etapa de análise de perigo dos subsistemas pode ser dividida em: análise de perigo do *hardware* e análise de perigo do *software*.

Análise de perigo do hardware

A análise de perigo do *hardware* pode ser subdividida em análise de perigo do *hardware fail-safe*, análise de perigo do *hardware* redundante, determinação dos meios de detecção e recuperação de falhas implementados por *hardware* e análise dos aspectos construtivos do *hardware*. Um *hardware* é considerado *fail-safe* quando, na presença de qualquer falha, simples ou múltipla, sempre é atingido um estado seguro. A exigência de falhas simples ou múltiplas está intimamente ligada ao grau de tolerância a falhas considerado no conceito *fail-safe* de um determinado projeto. Pode-se dizer que, em sistemas metroviários, o conceito *fail-safe* geralmente considera falhas simples. Já na aplicação aeroviária, o conceito *fail-safe* lida normalmente com falhas duplas.

Um *hardware* é considerado redundante quando diversas réplicas deste módulo de *hardware* são utilizadas no sistema, visando o atendimento a requisitos não funcionais como, por exemplo, segurança e confiabilidade. A diferença básica entre a análise de perigo de um *hardware* redundante e de um *hardware fail-safe* é que, no primeiro, deve haver também uma análise de independência entre os canais redundantes, procurando identificar as falhas de causa comum.

- Análise de perigo do hardware fail-safe

A análise de perigo do *hardware fail-safe* é constituída pelas seguintes atividades:

- descrição funcional e análise do módulo em operação normal: esta atividade tem como função primordial descrever e entender todos os

aspectos funcionais envolvidos na implementação do módulo em questão. No processo de análise são utilizadas técnicas de simulação com o apoio de ferramentas apropriadas, além de discussões sobre a funcionalidade do módulo entre os profissionais da equipe de análise;

- detalhamento dos requisitos gerais de segurança: esta atividade tem a meta de determinar os requisitos de segurança específicos para determinados blocos de *hardware*. O objetivo nesta atividade é fornecer subsídios para as próximas atividades, visando a identificação da presença de estados perigosos;
- análise crítica dos efeitos dos modos de falhas: esta atividade tem como finalidade analisar todos os efeitos locais e no sistema, de cada um dos modos de falhas dos diversos componentes existentes no módulo *fail-safe*. No caso de falhas não detectáveis, devem ser avaliadas as combinações com outras falhas possíveis ou entradas impróprias, no sentido de se avaliar qualquer possibilidade de se atingir um estado perigoso (Beerthuizen, 01). São também realizadas simulações na presença de falhas, tanto operacionais como do próprio *hardware*;
- análise de entradas impróprias: nesta atividade são avaliadas as conseqüências envolvidas quando da ocorrência de entradas impróprias ao módulo, seja através de sinais de entrada errados, não de acordo com a especificação, seja através de variações na alimentação do módulo, considerando os aspectos de diminuição, aumento e oscilação do nível de alimentação.

- *Análise de perigo do hardware redundante*

A análise de perigo do *hardware* redundante é constituída pelas mesmas atividades da análise de perigo do *hardware fail-safe*, acrescentando-se a análise de independência dos canais redundantes. O grande objetivo desta análise de independência é a determinação de focos de falhas de causa comum. Na realidade, este tipo de análise pode ser extremamente rígido, conforme o tipo de aplicação envolvido.

- *Determinação dos meios de detecção e recuperação de falhas implementados por hardware*

Esses meios de detecção influenciam na determinação do fator de cobertura de falhas do sistema e, por conseqüência, interferem na avaliação do grau de segurança avaliado. Esses meios de detecção são determinados a partir da análise do *hardware* redundante e *fail-safe*.

- *Análise dos aspectos construtivos do hardware*

Esta atividade procura identificar possíveis focos de falhas existentes na concepção do *hardware* e que possam levar o sistema a uma condição perigosa.

- *Análise de perigo do software*

Um dos grandes desafios existentes no processo de análise de perigo de um sistema refere-se à análise de perigo do *software*. Esta etapa pode ser subdividida em descrição funcional do *software*, detalhamento dos requisitos gerais de segurança, elaboração da descrição funcional das rotinas a partir do código fonte, identificação dos meios de detecção e recuperação de falhas implementados por *software*, inspeção formal do código fonte e reuniões formais de análise das rotinas do *software*.

- *Descrição funcional do software*

Nesta atividade é elaborada uma descrição funcional do *software* visando identificar a arquitetura utilizada e os atributos funcionais dos módulos envolvidos. Esta atividade tem importância fundamental no sentido de se fornecer uma visão funcional ampla do *software*.

- *Detalhamento dos requisitos gerais de segurança*

Nesta atividade são gerados os requisitos de segurança específicos para o *software*, a partir dos requisitos gerais de segurança, procurando fornecer subsídios para as próximas atividades, visando a identificação da presença de estados perigosos decorrentes de suas ações.

- *Elaboração da descrição funcional das rotinas a partir do código fonte*

Nesta atividade devem ser incluídas descrições textuais, diagramas de fluxo de dados, diagramas estruturados e redes de Petri, em especial na representação de eventos concorrentes e sincronizados.

- *Identificação dos meios de detecção e recuperação de falhas implementados por software*

Esses meios de detecção irão influenciar na determinação do fator de cobertura de falhas do sistema e, por conseqüência, interferir na avaliação do grau de segurança avaliado. Esses meios de detecção são selecionados através de uma classificação das rotinas de *software* do sistema computacional.

- *Inspeção formal do código fonte*

Esta atividade é realizada através da aplicação de uma lista de verificações (*checklist*) desenvolvida especialmente para uma determinada linguagem. Vale ressaltar que este tipo de análise não exige um conhecimento prévio da funcionalidade do sistema em análise, podendo ser realizado por especialistas em *software* sem conhecimento da aplicação prática.

A não observância de qualquer dos itens contidos nesta lista de verificações pode provocar a realização de processamento não correto, ou mesmo não previsto nas especificações do sistema sob análise. A verificação dos pontos apresentados na lista de verificações constitui-se já em um forte indício de que o código verificado tem possibilidade de atender aos requisitos mínimos para utilização em aplicações críticas.

- Reuniões formais de análise das rotinas do software

Nesta atividade, cada uma das rotinas do *software* é avaliada em uma reunião formal de análise. Esta reunião tem a participação de um moderador, um relator, um apresentador da rotina e demais profissionais relacionados com a análise do *software* e do *hardware* do sistema.

Durante essas reuniões, as rotinas são avaliadas e são realizadas simulações, conforme as necessidade envolvidas. As avaliações são realizadas de acordo com critérios preestabelecidos. Em alguns casos são necessários esclarecimentos junto ao operador do sistema sendo avaliado.

Análise de perigo da operação e suporte

Nesta etapa são identificados os perigos e os procedimentos de redução de risco durante a operação e manutenção do sistema. Em especial são analisados os perigos criados através da interface homem-máquina. Nesta etapa são avaliados os procedimentos operacionais visando identificar seqüências operacionais que possam levar o sistema a um estado perigoso e que, portanto, devem ser evitadas ou pelo menos minimizada a sua possibilidade de ocorrência.

Análise final do perigo

A análise final do perigo do sistema constitui-se na determinação do grau de segurança do sistema em análise. Trata-se de uma integração entre a avaliação qualitativa e a avaliação quantitativa.

Na avaliação qualitativa, são apresentados os problemas encontrados no *software*, no *hardware*, nos procedimentos operacionais e no nível de sistema e subsistema. Com relação ao *software* são apresentados os resultados de acordo com a seguinte classificação: problemas potencialmente perigosos, problemas que afetam a disponibilidade do sistema, problemas que afetam a manutenção do sistema, problemas relacionados com aspectos metodológicos além de aspectos estruturais como comentários errados, código não executado. Com relação ao *hardware*, são apresentadas as conclusões da análise destacando as falhas ou entradas impróprias que podem levar o sistema a situações perigosas. São incluídas, nesta análise, as falhas no *software* decorrentes de falhas oriundas do *hardware*. No que diz respeito aos aspectos operacionais são apresentadas as seqüências operacionais, considerando também as falhas no *software* e *hardware*, que podem levar o sistema a alguma condição perigosa. São também avaliados os aspectos de manutenção corretiva relacionada com um alarme de erro fornecido. Com relação aos aspectos de manutenção preventiva é avaliada a cobertura de falha dos testes realizados. Na avaliação quantitativa calcula-se o grau de segurança do sistema representado através do valor do seu *mean time to unsafe failure*, ou seja, tempo médio entre falhas inseguras. Vale ressaltar que o fator de cobertura de falhas, utilizado nesta avaliação, é decorrente da composição dos meios de detecção e recuperação de falhas implementados por *software* e/ou por *hardware*, e já determinados nas suas respectivas análises.

CONCLUSÃO

Vale ressaltar que a metodologia de análise de risco apresentada neste artigo continua sendo amplamente reavaliada através de pesquisas acadêmicas e resultados experimentais obtidos. Essa constante avaliação é fundamental tendo em vista a crescente complexidade dos sistemas de controle envolvidos e o surgimento de novas tecnologias sendo desenvolvidas.

REFERÊNCIAS BIBLIOGRÁFICAS

BEERTHUIZEN, P. G. e KRUIDHOF, W. System and software safety analysis for the ERA control computer. *Reliability Engineering and System Safety Elsevier Science Limited*, n. 71, pp. 285-97, 2001.

CENELEC - European Committee for Electrotechnical Standardization. *Railway applications - The specification and demonstration of reliability, availability, maintainability and safety* (RAMS). ENV 50126. September 1999.

CENELEC - European Committee for Electrotechnical Standardization. *Railway applications: Safety related electronic systems for signalling*. - European Presatandard ENV 50129. May 1998.

IEC - International Electrotechnical Commission. *Functional safety electrical/ electronic/ programmable eletronic safey-related systems*. IEC 61508. 1997.

LADKIN, P. B. *An example of everyday risk assessment*. Faculty of Technology. University of Bielefeld. 12 p. Februaray 2001.

LEVESON, N. G. *Safeware - System safety and computers*. University of Washington, Addison-Wesley Publishing Company, 1995.

MELCHERS, R. E. On the Alarp approach to risk managment. *Reliability Engineering and System Safety, Elsevier Science Limited*, n. 71, pp. 201-8, 2001.

NASA. *Software safety standard*. NSS. 1740.13, 1996.

STOREY, N. *Safety-critical computer systems*. Assison-Wesley Publishing Company, 1996.