APLICAÇÃO DE MÉTODOS SISTÊMICOS NA ANÁLISE DE CULTURA DE SEGURANÇA DO CENTRO DE RADIOFARMÁCIA DO IPEN

Francisco Luiz de Lemos – CEN- IPEN
Professor John Carroll – MIT- USA
fllemos@ipen.br – Ramal: 9440

RESUMO

Esta proposta tem por objetivo a análise de fatores sistêmicos que influenciam a segurança operacional do CR, incluindo todo o ciclo de produção. Segurança neste texto inclui os significados dos termos em inglês, “security” e “safety”. Esse significado ficará mais claro durante esclarecimentos sobre a análise sistêmica.

A análise será baseada na metodologia STAMP (Systems-Theoretic Accident Model and Processes), desenvolvida pela professora Nancy Leveson do MIT, (Leveson, 2012).

O objetivo desta proposta seria muito ambicioso para ser cumprido em dois anos. Porém, a análise sistêmica possibilita estudar o sistema (ou organização) em níveis de complexidade, numa abordagem top-down. Nesta abordagem começamos a análise pelo nível mais alto, ou nível do sistema, até os níveis mais baixos, ou de componentes.

Assim, sistemas extremamente complexos podem ser modelados, e analisados, em termos de hierarquia funcional onde os elementos são representações de funções essenciais ao funcionamento do sistema. Dessa forma, o sistema pode ser analisado a partir de diferentes perspectivas de complexidade.

Em STAMP, para ser seguro as interações entre os componentes de um sistema devem ser restritas de forma correta para que não gerem resultados inesperados. Portanto, a aplicação de STAMP tem o objetivo de verificar se as interações entre esses elementos podem gerar conflitos inesperados e, consequentemente, resultados indesejáveis, como por exemplo, vulnerabilidades que facilitem a ação de “insiders”, ou acidentes relacionados a segurança. As situações de vulnerabilidade junto com piores casos de condições externas geram as perdas, ou acidentes.

Fatores humanos são de extrema importância na manutenção da segurança de um sistema. Em STAMP os controladores (humanos ou automáticos) emitem as ações de controle (ou decisões) de acordo com o conhecimento que tem a respeito do estado do sistema.

Esse conhecimento sobre o estado do sistema é representado como “modelo mental” para os humanos, ou modelo do processo no caso de controladores automáticos. Se o modelo mental não está atualizado corretamente, ou seja, não estiver consistente com o estado real do sistema, então existe alta probabilidade de que as decisões (ou ações de controle, de acordo com STAMP terminologia) levem o sistema para estados perigosos.

A cultura tem um papel crucial na composição dos modelos mentais das pessoas. Portanto, o estudo da cultura de segurança é de extrema importância para um programa de melhoramento da segurança de uma instalação.

A aplicação de STAMP será mais bem detalhada a seguir.

REVISÃO DA LITERATURA

Para uma melhor compreensão sobre a proposta de trabalho, apresentamos uma breve descrição de termos e conceitos relativos à análise sistêmica, e STAMP.
Para maiores esclarecimentos recomendamos pesquisar as referencias no final deste documento, ou contatar o autor.

Sistema

De acordo com a teoria de sistemas, um sistema é um conjunto de elementos ordenados hierarquicamente em níveis de controle que trabalham para um objetivo comum.
Ainda de acordo com a teoria de sistemas, o comportamento dos níveis mais altos da hierarquia é o resultado (emerge) das interações entre os componentes dos níveis imediatamente abaixo.

Uma das consequências dessa definição é que segurança (safety e security), propriedade emergente, é consequência das interações entre os componentes do sistema.
Pela definição de "propriedade emergente" podemos ver que, em ultima análise, as interações entre os componentes são as responsáveis pela manifestação da propriedade "segurança" do sistema.

Assim, podemos concluir que os acidentes são o resultado de controle inadequado sobre as interações entre os componentes do sistema, e não apenas por falhas de componentes ou erro humano.

O STAMP avalia os modos como essas interações são controladas. Para isso, a primeira etapa da análise de um sistema consiste na representação do sistema em termos de um diagrama de controle hierárquico.
A Figura 1 mostra um exemplo de diagrama de controle hierárquico bem simplificado.

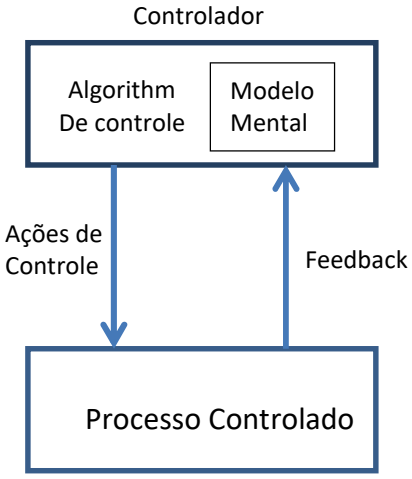

Figure 1: *Todos os controladores contém um modelo do processo controlado (Leveson, 2012)*

A figura 1 mostra os elementos de um loop de controle: controlador, processo controlado, ação de controle e feedback. Esses são os elementos de um loop que são analisados pelas ferramentas baseadas em STAMP. Os principais métodos, que usaremos no nosso projeto, são STPA _ Systems Threretic Process Ananlysis, e CAST _ Causal Analysis based on Systems Theory.

Definições

Algumas definições são necessárias para melhor compreensão desta proposta.
As definições são apresentadas de acordo com a terminologia usada em STAMP, Systems Theoretic Accident Model and Processes. [Leveson, 2012].

1- Perda inaceitável: são eventos ou situações, definidas pelos stakeholders, consideradas inaceitáveis. Em análise sistêmica "perda inaceitável" é também definida como "acidente".

Exemplos de perdas inaceitáveis (ou "acidentes") podem ser:
- Perda de reputação perante o público
- Perda de reputação junto a CNEN
- Perda de reputação perante a classe médica
- Prejuízos financeiros
- Morte ou incapacitação de indivíduos do público ou empregados
- Danos a equipamentos, etc.

2- Estados de vulnerabilidade: São os estados do sistema que antecedem à perda inaceitável (acidente), como definido no item anterior. Estes estados são necessários, mas não suficientes para que a perda do sistema ocorra.

Exemplo:
- Se consideremos o acidente, ou perda, como: Dano ao equipamento.

Para que haja dano ao equipamento, seria necessário, por exemplo, seu uso fora dos limites especificados em projeto. Um dos fatores que poderiam ter contribuído para isso poderia ser a existência de equipe sem o conhecimento técnico necessário.

Neste caso, o fato de não ter o treinamento adequado seria a vulnerabilidade.

Note que o simples fato de não ter treinamento adequado, por si mesmo não provoca a perda, ou acidente. Somente quando existe a situação, "operação do equipamento", é que as condições para a perda se manifestam. Seria preciso dois fatores:

a) Falta de treinamento
b) Operação do equipamento

Em STAMP, essa segunda condição, "b", é chamada de "condições exteriores".

Assume-se que os projetistas do sistema tenham controle apenas sobre o item "a", ou seja, sobre as condições de hazard, ou vulnerabilidade.

Assim, no exemplo acima, o sistema teria controle, ou seja, poderia atuar sobre a condição de ter ou não ter treinamento.
Porém, não teria controle sobre a demanda para operação do equipamento. Por exemplo, pode ser que o equipamento só opere em caso de demanda de clientes. Neste caso não se pode saber quando haverá a demanda.
Este é apenas um exemplo bem simples para mostrar as diferenças de conceitos em STAMP, e pode não refletir a realidade dos fatos.

3- Circunstancias exteriores: São as condições exteriores ao sistema em análise
Para maiores explicações sugerimos consultar a literatura.

4- Segurança: A palavra segurança abrange situações bem mais amplas que simples análise de acidentes. Neste documento segurança inclui conceitos do termo em inglês “safety” e “security”. A análise de segurança usando STPA procura na verdade mostrar as vulnerabilidades do sistema, e não apenas mostrar que é seguro.

Essa definição tem várias implicações que estão fora do escopo deste documento.

O termo “security” engloba temas como cybersecurity, roubo de material radiativo, roubo de informação, além de segurança física.
Os estados de vulnerabilidade do sistema são praticamente os mesmos tanto para assuntos ligados a safety como security. A diferença maior seria nas condições externas onde, no caso de segurança não existe necessariamente a intenção de agentes maliciosos. No caso de security sempre existe a intenção maliciosa.

Interações entre componentes do sistema

As interações entre os componentes do sistema podem tomar várias formas. É muito importante saber identificar e analisar as interações quanto a consequências inesperadas levando o sistema a estados de vulnerabilidade.

Podemos encontrar muitos exemplos de interações, com resultados inesperados, em casos históricos como do cientista Sr. Khan, do Paquistão nos anos 1980´s que se aproveitou de situações aparentemente inocentes para facilitar o roubo de informações confidenciais.

Outro exemplo interessante seria o caso onde se usam termos em inglês para indicação de abrir ou fechar portas, para usuários de língua portuguesa. Há relatos de casos em que torneiras e portas dos banheiros foram quebradas, e até mesmo pessoas sendo feridas por tentarem abrir uma porta de modo não adequado, devido casos de falsos cognatos, onde se confunde “push” com “puxe”, por exemplo.

Esse exemplo evidencia um caso interessante de interação entre o usuário e os arquitetos do prédio. Podemos notar que não há falhas nos componentes do sistema, pois todos fizeram exatamente o que deveriam fazer de acordo com seus modelos mentais de como o sistema deveria funcionar. Ou seja, o usuário tem no seu modelo mental que “push = puxe” significa abrir.
Já os arquitetos podem ter imaginado um prédio com dizeres em inglês para mostrar certa sofisticação. Faltou na verdade um estudo mais detalhado dos usuários, ou seja, houve problemas no projeto.

Do mesmo modo, se examinarmos o caso do cientista Khan, veremos uma série de fatos, aparentemente inocentes, que de forma direta ou indireta, o ajudaram a concretizar seus planos. Por exemplo, uma das unidades onde trabalhou tinha restrição de movimentação de pessoas. Ele não poderia deixar o local sem escolta, porém, não havia banheiro disponível dentro dessa área. Por isso, ele conseguia permissão para sair da área e, assim, teria acesso a outras áreas ainda mais restritas sem a necessária permissão, o que facilitava seus planos.

STAMP/ STPA _ Systems Threretic Process Analysis

STAMP, Systems Theoretic Accident Model and Processes é baseadp em “systems thinking” e teoria de sistemas [1].
Em STAMP um sistema é modelado como uma estrutura de controle hierarquico, que é um loop de controle por feedback.
Os controladores atualizam seu modelo do processo (ou modelo mental para humanos) atraves do feedback que eles recebem do processo controlado, e input de outras fontes.

Com essa atualização sobre o estado do sistema os controladores emitem as ações de controle para modificar o processo controlado de acordo com um algoritimo.

Em STAMP segurança é considerada como propriedade emergente das interações entre os componentes do sistema, [1].

Acidentes sao definidos como perdas inaceitáveis para o sistema. Podem ser perdas de vidas, equipamento, credibilidade ou monetária. Acidentes deve ser uma combinação de estado de hazard do sistema e um conjunto das piores condições exteriores [1].

O estado de hazard (ou vulnerabilidade) ocorre devido a controle inadequado das interações entre os componentes do sistema.

STPA/ Systems Theoretic Process Analysis, é baseado em STAMP e é usado para análise de segurança e security [4]. Para iniciar a análise por STPA é necessario definir os limites do sistema, e então definir os acidentes, ou perdas inaceitaveis.

Após identificação dos acidentes, podemos definir quais os estados de hazard necessitam ser considerados como condição para que as perdas ocorram.

Note que acidentes são definidos de acordo com os stakeholders. Por exemplo, para a CNEN (órgão regulador) um acidente poderia ser definido como “ danos ao público e meio ambiente”, enquanto para a empresa de utilidade, acidente seria a “perda de reputação”.

Quanto aos limites de um sistema, podemos, por exemplo, determinar que uma NPP tenha seus limites coincidindo com os limites fisicos. O público seria entao considerado como estando fora dos limites do sistema ou NPP.

Se o acidente for definido como “pessoas do público afetadas por radiação”, então temos:

(a) Condição de hazard: a liberação de material radiotivo da NPP
(b) Piores condições externas: Público estando perto o suficiente para ser afetado pelo meterial radioativo.

Entao temos:

Accidente = Condicção de Hazard + Piores condições externas

Deve ser notado que o termos “condições externas” refere a condições fora dos limites sistema. São condições sobre as quais os projetistas do sistema não tem controle. Em outras palavras, o comportamento do público não pode ser controlado para ajustar ao comportamento do sistema.

Estrutura Hierárquica de Controle

A estrutura hierárquica de controle é um modelo de controle funcional de como o sistema reforça as restrições de segurança nas interações. Esta estrutura é organizada hierarquicamente.
Os controladores dos níveis superiores emitem as ações de controle que afetam os controladores dos processos nos niveis inferiores.

Feedback é fornecido pelos componentes dos niveis inferiores e é usado pelos controladores de niveis superiores para decidir quais ações de controle devem ser emitidas.

Figure 2 mostra uma estrutura genérica de controle. Note que os controladores podem ser componentes individuais, por exemplo um operador, ou representações de um departamento inteiro com uma estrutura interna de ocntrole. [3].

Cada controlador – humano ou computador – contém um modelo do processo controlado, chamdo de modelo do processo ou modelo mental. O modelo do processo representa o conhecimento que o controlador tem a respeito do estado do sistema. Este conhecimento deve estar em concordancia com o estado real do sistema de modo a que o controlador possa fazer decisões seguras.

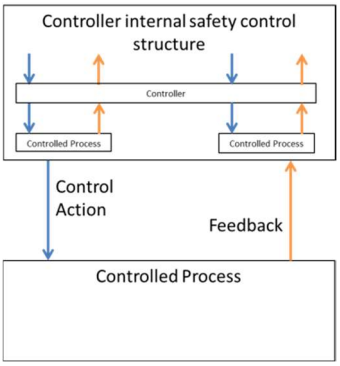

Figura 2. *Uma estrutura genérica de controle, adaptada de [3]*

Havendo inconsistências entre o estado real do sistema e o modelo de processo, ou se as restrições não são propriamente aplicadas, pode levar o sistema a estados de hazard [3].

As variáveis do processo capturam a informação necessaria para cada controlador decidir qual a ação de controle a ser editada. Diferentes variáveis de processos podem ser associadas a cada ação de controle.

STPA pode ser aplicado em 2 passos:

Passo 1: identificação de ações de controle potencialmente perigosas

Essas ações de controle, CA, podem potencialemente ser inseguras se estiverem incoscistentes com o estado do sistema. Se o conhecimento sobre o estado do sistema não for propriamente atualizado, então a CA pode ser insegura.

As condições em que as ações de controle são emitidas é que determinam se essas serão ou não inseguras.
As ações potencialmente inseguras podem ser classificadas em quatro categorias:

(a) A ação requerida não é emitida ou é emitida e não é seguida.
(b) A ação requerida é emitida e leva o sistema a estado de hazard
(c) A ação requerida é emitida muiot cedo ou muito tarde, ou em ordem errada
(d) A ação requerida é abortada muito rapido ou aplicada por muito tempo
(e) Ação de controle é emitida mas não é seguida.[3, 5].

Para assegurar que as ações de controle estejam em concordância com o estado do sistema é necessario aplicar as restrições de segurança corretamente

Passo 2: Identificando fatores causais

Uma vez as restrições de segurança estejam definidas, podemos identificar os fatores causais que podem levar a violações das restrições de segurança. Figura 3 mostra os componentes de um loop de controle. Esta representação ajuda a identificar os fatores causais para que a ação de controle seja potencialmente insegura [5].

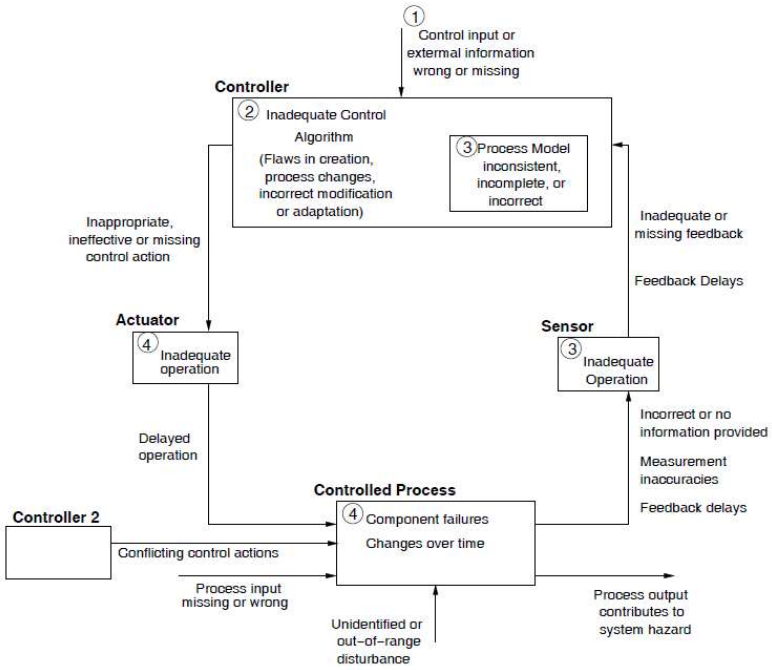

Figure 3: *Alguns fatores que podem influenciar as açoes de controle (adaptado de Leveson, 2012)*

Para exemplificar como STPA poderá ser util, apresentamos dois casos bem simplificados:

1- Descoberta de corrosão do vaso do reator da usina de Devis-Besse, nos Estados Unidos. A usina era muito bem avaliada, tanto pelo US NRC como pelo IMPO. Acontece que essa avaliação gerou uma necessidade de que o pessoal da usina desejasse manter o status de otima produtividade.

Então, mesmo após alertas, e sinais, de possibilidade de existencia de focos de corrosão no vaso de pressão, a usina fez várias diligencisa junto ao NRC para adiar uma inspeção mais rigorosa. O NRC concordou com adiamentos, até a parada da usina para manutenção, quando a corrosão foi descoberta.

Vários outros fatores contribuiram para que a corrosão não fosse descoberta com mais antecedencia. Pode-se inclusive identificar fatores de projeto da arquitetura dos equipamentos.

Recomendamos que o leitor leia os relatórios sobre o acidente de Devis-Besse para maiores esclarecimentos.

2- Considere agora um caso diferente, agora hipotético. Suponha que um empregado que abre um email, pensando que se trata de uma requisição urgene de seu chefe, que por acaso é muito autoritário. Então foi descoberto que o email era “phishing”.

Os dois casos resultariam numa parada da usina, causando perdas monetárias e de reputação. Porém, vemos que são casos de naturezas bem diferentes. Podemos então planejar com mais certeza uma análise de quais fatores na cultura da instituição poderiam contribuir para facilitar a ocorrencia desses eventos
.
Note que esta abordagem não faz menção a erros humanos ou falhas. Isso porque o principal objetivo desse tipo de análise é compreender melhor como os acidentes acontecem mesmo quando os operadores estão fazendo o seu trabalho de dia-a-dia, e as ações tomadas imediatamente antes de um acidente pareceram normais para eles.

PROPOSTA DE TRABALHO

Objetivos geral e especificos

No contexto de análise sistêmica o termo segurança tem uma conotação bem mais ampla que nos métodos tradicionais. Assim como danos a equipamentos, meio ambiente e mortes são tratados como acidentes, outros eventos menos obvios tais como perda de reputação, perda financeira, ou roubo de informação e sabotagem também são tratados como acidentes.

Esses conceitos decorrem do fato de que, na visão sistêmica, todo o sistema é interligado e não podemos considerar partes do sistema isoladamente. Um exemplo simples, se a empresa tem baixa reputação, pode influenciar a moral dos trabalhadores, que por sua vez podem não seguir regras simples de segurança, facilitando a ação de insiders.

A análise sistêmica pode contribuir para o aperfeiçoamento de vários aspectos da segurança de uma organização, lembrando que o termo segurança aqui se refere aos significados em inglês: “safety” e “security”.

Essa análise inclui:

- Análise das vulnerabilidades do sistema que poderiam facilitar a ocorrencia de incidentes de “security”, tais como: insiders, sabotagem, roubos de material radioativo, roubo de informação.

- Relações entre safety e security: Apesar de ter muitos pontos em comum, “security” e “safety” podem ser contraditórias e seria necessário uma análise profunda das implicações de restrições devido a objetivos conflitantes desses dois aspectos da operação organizaçional.

- Análise de normas e regulamentação em geral - Muitas vezes o excesso de normas de seguranca pode comprometer o bom funcionamento da produção e, até mesmo, comprometer a segurança. Isso porque muitas vezes as normas podem ser contraditorias.

A cultura de segurança seria um dos pilares da segurança do sistema. A cultura permeia todo o sistema de várias formas, como nas lideranças, treianmentos, etc.

De acordo com a IAEA (2008), os principios de cultura de segurança são:

- Motivação
- Liderança
- Comprometimento e responsabilidade
- Profissionalismo e competência
- Aprendizado e melhoramentos

Note que estes são tambem os mesmos principios para cultura organizacional. Todos estes aspectos da vida organizacional são de algum modo mensuráveis, mas devido a sua natureza genérica, estas medidas podem não refletir o nivel real de segurançaa (security e safety) da organização.

O método proposto visa contribuir para um melhor entendimento de como todos esses fatôres se relacionam com a segurança da organização em seus mais variados aspectos, gerando situações de vulnerabiliadades.

Como resultado desse projeto esperamos poder fazer sugestões de melhorias no gerenciamento tais como reestrturação de funções, realocação de recursos, melhores relações de cooperação, reformulação de objetivos e valores, e modos de avaliação de modelos mentais.
Teremos a valiosa colaboração do Professor John Carroll, da Sloan School of Management, MIT.

Método de trabalho

O trabalho será dividido em duas partes:
Na primeira parte do trabalho a organização técnica (ou sistema socio-técnico) será representada como por uma estrutura de controle hierárquico.
Nós chamaremos esse sistema de S1. Nesse sistema todos os componentes, humanos e máquinas, são considerados.

A operação do sistema é analisado de acordo com os passos 1 e 2 do STPA. O STPA passo 1 é sobre a identificação das ações de controle que potencialmente poderiam levar o sistema a estados de perigo, ou vulnerabilidade. O STPA passo 2 é sobre análise das possiveis causas, ou contribuições, para que as ações de controle potencialmente perigosas possam ocorrer. O STPA passo 2 dará subsidios para sugestões para melhorias no sistema.

Algumas vezes não é suficiente identificar as possíveis causas para as ações potencialmente perigosas ao sistema, especialmente quando se tratam de ações de controle dadas por seres humanos. Precisamos de uma análise mais profunda para encontrar os fatores sistêmicos, que podem ter bases psicológicas, politicas e culturais. Para uma análise mais detalhada, desenvolvemos a segunda parte do trabalho.

Na segunda parte somente as relações humanas serão consideradas. Chamamos esse sistema de S2.
O sistema S2 é importante porque as ações potencialmente perigosas podem ser baseadas em processos de tomada de decisões que são essencialmente governados por relações humanas. Essas relações, ou interações, afetam o modelo mental do controlador humano, como na figura 1. O modelo mental (modelo do processo no caso de controladores automáticos) é a representação do conhecimento que o controlador tem sobre o estado do sistema.

Se este modelo mental estiver inconsistente com o estado real do sistema, então decisões potencialmente perigosas ao sistema podem ser tomadas. No caso de Three Miles Island, por exemplo, os operadores foram treinados para impedir que o pressurizador fosse sobre-alimentado (devido a treinamento em pequenos submarinos) e portanto, nao protegeram contra um limite minimo de agua para o nucleo; o treinamento foi posteriormente modificado para melhor refletir a realidade de uma usina maior.

Nesta fase utilizaremos o processo de auto avaliação da IAEA, Self-assessment of Nuclear Security Culture in Facilities and Activities that use Nuclear and/or Radioactive Material, NST026.

Após identificar as caractieriticas da cultura de segurança que vamos identificar um conjunto de indicadores de cultura para cada caracteristica.

Como as caracteristicas, assim como os indicadores, são definidos em termos genéricos, usamos então os recursos da análise de STPA para identificar quais caracteristicas, e portanto,indicadores, precisamos avaliar.

Após as possíveis causas das ações de controle serem identificadas no STPA Passo 2, essas devem ser analisadas por equipe de técnicos com bom conhecimento do sistema.
Então, as caracteriticas de cultura de segurança relacionadas com essas causas são então identificadas.

Esse procedimento torna o trabalho de identificação de quais indicadores escolher para cada caractaritica bem mais facil e objetivo.
Note também que, com o uso de método sistêmico, o sistema em análise não fica limitado à instituição em estudo.

O diagrama de controle hierárquico pode facilmente ser estendido para outras instituições, como os órgãos reguladores, IAEA, congresso (onde as leis são feitas), opinião publica, etc..

Aplicação Prática

O estudo será conduzido como segue:

PARTE 1

Análise do sistema S1:
A organização será modelada como uma estrutura de controle como na figura 1. Para essa fase precisaremos de obter informações tais como:

1- Documentação sobre a filosofia de projeto, autitorias, relatórios para órgãos reguladores, IAEA, etc..
2- Entrevistas com pessoal sobre o funcionamento do sistema, avaliação de conhecimento sobre ameaças, como lidam com ameaças, etc..
3- Reunião de grupos com peritos em áreas especificas para desenvolver a análise de STPA
4- Discussão com especialistas externos para enriquecimento do trabalho, por exemplo, Professores do MIT e possivelmente um especialista em security da universidade de Havard.

PARTE 2

Para tornar a análise ainda mais especifica esta parte 2 irá considerar somente as relações humanas. Procuraremos responder as questões:

1) quais são as interações entre os componentes desse sistema levariam o sistema a um estado de vulnerabilidade;
e 2) quais os estados possiveis de vulnerabilidade.

O sistema será modelado em termos de controle hierarquico, como na Figura 3. Os elementos da estrutura de controle S2 precisam ser identificados através de processo similar ao usado para S1. Porém, os elementos de S2 são menos obvios devido a sua natureza de relações humanas.

A identificação desses elementos será importante contribuição dessa pesquisa para a compreensão de mecanismos sistemicos que levam o sistema a estados de vulnerabilidade.

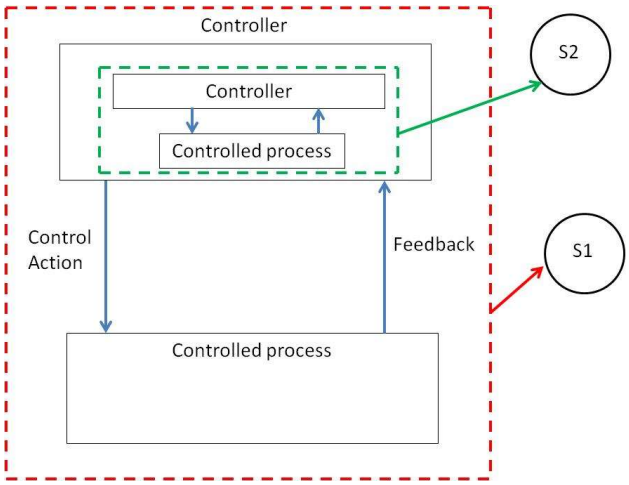

Figure 3: Representação dos sistemas S1 e S2

O objetivo desse trabalho será então identificar quais fatores sistemicos formam os modelos mentais dos controladores em relação a um probema especifico encontrado na análise de S1.

Algumas questões a serem abordadas serão:

Liderança: qual a eficácia das lideranças para esse problema em particular?
São as regras, guias e leis claras o suficiente para resolver os problemas encontrados?
Como os empregados são educados e treinados em relação ao problema em particular?
Eles tem capacidade de ler e entender as regras, manuais, etc??
Os manuais são claros e faceis de usar?
Os empregados entendem bem como são os regulamentos informais e formais?
Como a cultura popular (e individuais) influencia a cultura organizacional?
Como as muitas subculturas (engenheiros, tecnicos, departamentos, etc..) afstam soluções para o problema em particular?

Podemos encontrar aspectos culturais, politicos e estategicos no sistema social que afeta o processo de decisões. Podemos assim indentificar as necessidades da organização em relação a aspectos especificos da estrutura de controle me geral, e cultura de segurnça em particular, que precisam ser melhoradas. Esta demonstração irá ajudar no futuro desenvolvimento de um sistema integrado de avaliação de segurança e mios para melhoramentos.

Equipe de trabalho

Francisco Luiz de Lemos, CEN/IPEN
Professor John Carroll, Sloan School of Management, MIT

Orçamento

R$50.000,00
Usado para pagar viagem :
Professor Carroll ao Brasil para análise do trabalho: uma ou duas vezes. 1 semana cada vez
Francisco Luiz de Lemos: Uma ou duas viagens aos EUA para avaliação dos trabalhos, Uma semana cada vez.

Existe a possibilidade de trazer o professor Carroll por meio da IAEA, projeto ManPower. Esse processo é centralizado pela CNEN Sede, que coloca prioridade de acordo com interesses que podem não coincidir com o deste projeto.

Assim, não é garantido que será obtido. Como a visita do Porfessor Carroll é vital pra o sucesso do projeto, pedimos a verba acima.

Cronograma de Atividades

Atividade / Mês - Ano	**2017**												**2018**											
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**1**	**2**	**3**	**5**	**4**	**6**	**7**	**8**	**9**	**10**	**11**	**12**
Identificação do sistema (organização) S1 – identificação dos acidentes e estados de “hazard” – construir a estrutura hierárquica de controle																								
Aplicação de STPA passos 1 e 2 – identificação das condições para as ações de controle potencialmente perigosas																								
Classificação das causas e identificação de ações de controle potencialmente perigosas a serem analisadas																								
Identificação do sistema S2 (social) bem como identificação dos acidentes (perdas inaceitáveis) e estados de “hazard” para S2- preparação para avaliação da cultura de segurança																								
Applicação de STPA Passos 1e 2. Identificação das condições para que as ações de controle sejam perigosas Analise de dados																								
Analise de causas Analise de dados																								
Apresentação de relatório final com sugestões de modificações em relação a cultura de segurança: mudanças de normas, estrutura de gerenciamento, etc..																								

Referências

Ancona, D. G., T. A. Kochan, M. Scully, J. Van Maanen, and D. E. Westney. 2004. *Managing for the Future: Organizational Behavior and Processes, 3rd Ed*. Boston: South-Western College Publishing.

Ashby, W. R. Design for a Brain: The Origin of Adaptive Behavior, 2nd ed. New York: John Wiley, 1960.

International Atomic Energy Agency (IAEA). Nuclear Security Culture (Nuclear Security Series 7). Vienna: IAEA, 2008.

Leveson, N. 2012. *Engineering a Safer World: Applying Systems Thinking to Safety*. Cambridge, MA: MIT Press.

National Diet of Japan Fukushima Nuclear Accident Independent Investigation Commission. The official report of The Fukushima Nuclear Accident Independent Investigation Commission - Executive summary. Tokyo: Japanese Government, 2012.

Young, W. & Leveson, N. Inside Risks: An Integrated Approach to Safety and Security Based on Systems Theory. Proceedings of the ACM, 2014, 57(2), 31-5.