Revista Tecnologia e Sociedade
ISSN: 1984-3526

https://periodicos.utfpr.edu.br/rts

Avaliação sistêmica de tolerância a falhas em sistemas de proteção de reatores nucleares

Alexander Lucas Busse
alexlucasb@gmail.com
Amazônia Azul Tecnologias de Defesa S.A

João Manoel Losada Moreira
Joao.moreira@ufabc.edu.br
Universidade Federal do ABC

Tatiana Yuri Boncristiano Ozeki
tatiana.ozeki@gmail.com
Atech S.A

Luis Geraldo Gomes da Silva
acidente.energia@gmail.com
Universidade Federal do ABC

RESUMO

O conceito de tolerância a falhas tornou-se importante nas últimas décadas na indústria nuclear devido à utilização de sistemas de Instrumentação e Controle (I&C) digitais. Uma falha é uma anomalia indesejada em um item ou sistema que pode levar a um estado inseguro e eventualmente gerar incidentes ou acidentes de consequências indesejáveis do ponto de vista socioambiental. Atualmente as soluções digitais são muito atraentes, não obstante, requererem avaliações de software quanto a tolerância a falhas. Nosso artigo pretende realizar uma investigação teórica de confiabilidade e taxa de falha, com base em um Diagrama de Blocos de Confiabilidade, em um sistema de proteção digital para reatores nucleares. Adicionalmente, discute sobre a necessidade de cultura de segurança nos segmentos de operação do reator, monitoramento e fiscalização para garantir que eventos acidentais indesejados sejam evitados.

PALAVRAS-CHAVE: Tolerância a Falhas. Diagrama de bloco de confiabilidade. Segurança Nuclear. Sistemas de proteção digital.

INTRODUÇÃO

O entendimento de que acidentes e incidentes são resultados de múltiplos fatores em interação não prevista é um motivador fundamental para o aprimoramento contínuo da segurança industrial em geral e no setor energético em particular. Ter claro este entendimento auxilia em coibir a prática de atribuição de culpa às vítimas de acidentes e na responsabilização dos envolvidos e confronta a ideia do "puro acaso" ou "vontade de Deus" RAOUF (1998).

Vários autores enfatizam o uso de uma visão sistêmica e considerações de cultura de segurança em projetos e construção de reatores (MAIORINO et al., 1989; MOREIRA et al., 2013) e também em eventos que desencadeiam acidentes como ato inseguro, condição insegura, ambiente de insegurança ou equivalentes WAHLSTROM, 2018; CORREA e CARDOSO JUNIOR, 2007; SILVA, 2017). ; MAIORINO et al., 1989). Estes conceitos são aplicados também para sistemas digitais que podem falhar devido incorreções no software desde a especificação, codificação até implementação no hardware (CORREA e CARDOSO JUNIOR, 2007; LU et al., 2015; YANG et al., 2018; WAHLSTROM, 2018; WAHLSTROM, 2011; SILVA, 2017; ZOU et al., 2017). Exemplos de desastres a serem evitados são acidentes nucleares como o de *Three Mile Island* em 1979, rompimentos das barragens de Mariana-MG em 2015 e de Brumadinho-MG em 2019 e outros. A origem do acidente de *Fukushima* foi diferente, pois deveu-se a sucessão de 2 eventos naturais, terremoto e *tsunami* e a seguir a condição de *blackout* (falta de energia) por longo tempo. Esses eventos catastróficos são custosos com fortes impactos socioambientais e afetam a sustentabilidade de comunidades e meio ambiente (MOREIRA et al., 2015; CARAJILESCOV e MOREIRA, 2008).

Consolidou-se nas últimas décadas a percepção do risco, dos impactos socioambientais e da necessidade de uma visão sistêmica da segurança dos empreendimentos envolvendo projeto, construção, operação e fiscalização das plantas industriais. Esta percepção é em grande medida resultado da difusão de eventos nos meios de comunicação. Esta constatação reforça a necessidade de aprimoramento constante de tecnologias e filosofias de projeto que agreguem condições melhores de controle do processo ainda que haja falhas não previstas, sabotagem ou catástrofes naturais (CORREA e CARDOSO JUNIOR, 2007; LU et al., 2015; YANG et al., 2018; WAHLSTROM, 2018; SILVA, 2017; ZOU et al., 2017). Adicionalmente, as respectivas indústrias devem estudar esses eventos indesejados, buscar encontrar um conjunto de lições aprendidas e definir cronogramas de implementação de melhorias nas plantas existentes (WAHLSTROM, 2018; SILVA, 2017).

Neste contexto, este artigo avalia as usinas nucleares e seus sistemas monitoração e fiscalização quanto a robustez para evitar acidentes e suas consequências. A abordagem é sistêmica e importante para a sustentabilidade, pois acidentes nucleares podem produzir impactos importantes na sociedade e no meio ambiente. Em sua primeira parte verificam-se quais características de projeto o sistema de proteção de um reator nuclear (RPS – *Reactor Protection Systems*) deve atender para, na ocorrência de qualquer falha, evoluir para um estado seguro. Note que o RPS está inserido no contexto dos sistemas de instrumentação e controle (I&C) de uma planta nuclear. Os I&C são considerados como o sistema nervoso de uma Planta de Potência Nuclear (NPP - *Nuclear Power Plant*). Esses sistemas realizam a proteção, o controle, a supervisão e o monitoramento de

todos os parâmetros necessários de uma NPP (LU et al., 2015; YANG et al., 2018; WAHLSTROM, 2018; SOUZA e MOREIRA, 2006; IAEA, 2008).

Na segunda parte discute-se a garantia da segurança na ocorrência de acidentes segundo uma visão sistêmica e de sustentabilidade. Busca-se garantir a segurança não só durante a operação de um empreendimento, mas em todo o seu ciclo de vida que inclui o projeto, construção, operação, monitoramento e fiscalização (MOREIRA et al., 2015).

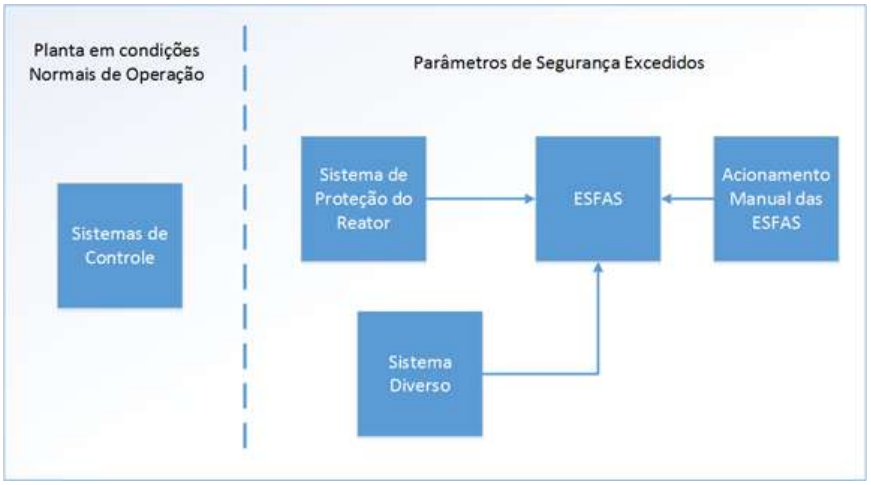
O artigo começa apresentando as características do sistema de controle e de proteção de reatores nucleares e discorre sobre a questão de diversidade, redundância e outras características de projeto que levam a segurança. A seguir apresenta a metodologia, resultados, discussões e considerações finais.

CARACTERÍSTICAS DE UM SISTEMA DE CONTROLE E PROTEÇÃO DE REATORES NUCLEARES

A Agência Internacional de Energia Atômica (IAEA) define um sistema importante para a segurança como “um equipamento fornecido para garantir o desligamento seguro do reator e/ou remoção de calor residual do núcleo, ou para limitar as consequências de ocorrências operacionais postuladas e acidentes de projeto básico” (IAEA, 2016). Portanto, são sistemas diretamente envolvidos em ações para evitar a ocorrência de acidentes indesejados que afetam as pessoas e o meio ambiente. Esses sistemas são denominados “críticos” para a segurança e desempenham funções de alta “criticidade” para a segurança das plantas.

O controle e a proteção de uma planta nuclear, em geral, são divididos em três grupos de sistemas principais: 1- Sistemas de Controle; 2- Sistemas de Proteção e ESFAS (*Engineering Safety Function Actuation System*); e 3 - Sistemas Diversos. A Figura 1 apresenta de forma geral a relação entre esses sistemas descritos ao longo deste artigo.

Figura 1 – Esquema do sistema de controle e proteção de uma planta nuclear.

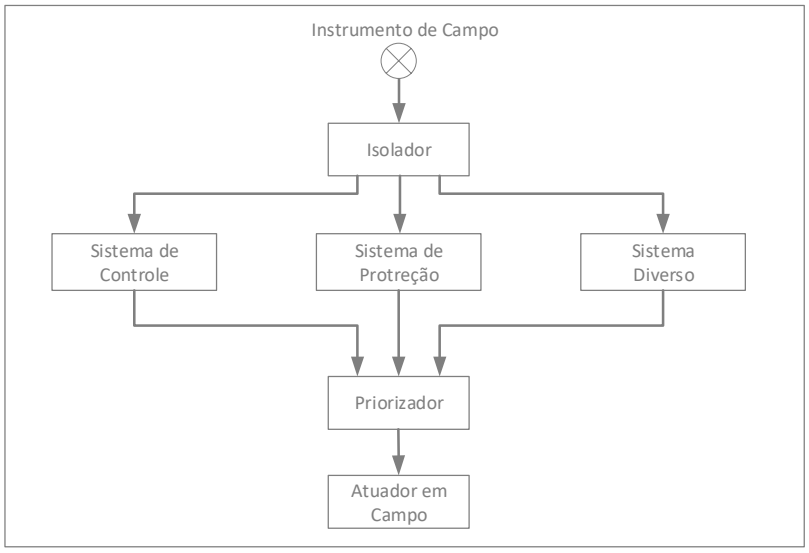


Os Sistemas de Controle da planta para operações normais devem ser segregados dos sistemas de proteção. O Sistema de Proteção do Reator executa as funções de segurança em uma situação de emergência, enquanto que o Sistema Diverso deve garantir, após um determinado período de tempo, a execução das

funções de segurança críticas caso o sistema de proteção seja afetado por uma Falha de Modo Comum (CMF - *Common Mode Failure*).

Uma NPP típica possui aproximadamente 10.000 sensores e detectores e 5.000 km de cabos de I&C. A massa total desses componentes de I&C pode chegar a ordem de 1.000 toneladas. Essas estimativas tornam os sistemas de I&C um dos mais pesados e o que possui as estruturas não construtivas mais extensas (IAEA, 2008). Dessa forma, para não estender ainda mais a quantidade de cabos e sensores, é comum o compartilhamento dos sinais dos sensores entre os Sistemas de Segurança, Sistema de Controle e com o Sistema Diverso. Contudo, para haver o compartilhamento, este deve ser realizado através de equipamentos que fazem a isolação do sinal de segurança e o sistema de controle, mantendo a segregação entre os sistemas, como pode ser observado na Figura 2.

Figura 2 – Compartilhamento de sensores em NPPs.



Sistemas de Controle

Os sistemas de controle são compostos por sensores, indicadores de status da planta, sistemas de lógica, sistemas de alarmes e sistemas de controle automático, incluindo as Interfaces Homem-Máquina (IHM). Esses sistemas têm como função o controle dos parâmetros da planta dentro dos limites normais, alertar ao operador os status da planta e subir alarmes quando os parâmetros normais forem excedidos (THOMSON, 2012).

Sistemas de Proteção

Os sistemas de proteção têm como função principal atuar para o desligamento do reator, evitando o superaquecimento, à deterioração do núcleo do reator e em última instância a liberação de material radioativo para o ambiente (LIMA, 2006). Eles são compostos basicamente por sensores, lógicas, atuadores e IHM dedicadas para os sistemas de proteção.

Os sistemas de proteção abrangem os seguintes sistemas: o Sistema de Proteção do Reator (RPS - *Reactor Protection System*) e o *Engineered Safety*

Features Actuation System (ESFAS) (THOMSON, 2012; SOUZA E MOREIRA, 2006). Tipicamente estes sistemas podem ser digitais, com o recebimento de sinais para o desligamento de emergência (*Trip signal* – termo em inglês para definir desligamento de emergência de uma planta industrial) processados e gerados por sistemas de software, ou analógicos (com sinais de desligamento de emergência gerados a partir de relés analógicos). As informações do campo podem vir tanto de forma digital (0 ou 1) como analógica (IAEA, 2007).

Sistema de Proteção do Reator (RPS)

O RPS é o sistema que inicia rapidamente o desligamento do reator quando os valores dos parâmetros importantes da planta excedem os níveis de segurança, esses parâmetros são configuráveis e característicos do projeto de cada planta (THOMSON, 2012). Esse sistema também inicia a ação do ESFAS.

Os parâmetros de *Trip* de um reator nuclear do tipo LWR (*Light Water Reactor*) pode variar conforme suas características técnicas e aplicações (um reator nuclear pode ter diferentes aplicações, como: propulsão, geração de potência elétrica, dessalinização e geração de calor). A título de exemplificação, seguem os parâmetros típicos para o *Trip* de um reator nuclear do tipo LWR são (IAEA, 2005):

1. Baixa pressão na saída do reator– limiar de detecção = 14,380 KPa;
2. Baixa geração de vapor - limiar de detecção = 11,94 m;
3. Alta pressão na saída do reator - limiar de detecção = 16,200 KPa;
4. Alto fluxo de nêutrons - limiar de detecção = 120 % do fluxo previsto em potência máxima;
5. Baixo tempo de dobramento - limiar de detecção = 8 %/s;
6. Baixa vazão do refrigerante - limiar de detecção = 2,00 Kg/s;
7. Baixo nível no pressurizador - limiar de detecção = 2,7 m;
8. Baixa pressão na descarga de água de alimentação - limiar de detecção = 5200 KPa;
9. *Trip* manual (desligamento manual).

Engineered Safety Features Actuation System (ESFAS)

ESFAS é o sistema de segurança que atua em diversas funções após o *Trip* do reator, com o objetivo de garantir o resfriamento e a integridade do reator após seu desligamento (THOMSON, 2012).

Tipicamente os sistemas que compõe o ESFAS são (NUREG, 2016):

A. Sistema de isolamento da contenção e do reator;
B. Sistema de resfriamento de emergência do núcleo;
C. Sistema de remoção de calor residual e despressurização;

D. Sistema de alimentação auxiliar do reator, para reatores do tipo PWR (*Pressurazed Water Reactor*);

E. Sistema de injeção de boro de emergência;

F. Sistema de tratamento de gás de espera, para reatores do tipo BWR (*Boiling Water Reactor*);

G. Sistema de purificação e limpeza de ar;

H. Sistema de controle de gás combustível da contenção;

I. Sistema de aquecimento, ventilação e ar condicionado e isolamento de emergência para a sala de controle.

Sistemas Diversos de Atuação (SDA ou DAS - *Diverse Actuation Systems*)

O objetivo dos sistemas diversos é de tentar eliminar a possibilidade de falhas de modo comum. O sistema diverso deve ser física e eletricamente independente do RPS e, na medida mais razoável possível, com princípios de operação diversos. A necessidade de sistemas diversos automatizado para a execução das ESFs (*Engineering Safety Functions*) deve ser avaliado em cada projeto. Em alguns casos uma ação manual de atuação das ESFs poderá ser suficiente (THOMSON, 2012).

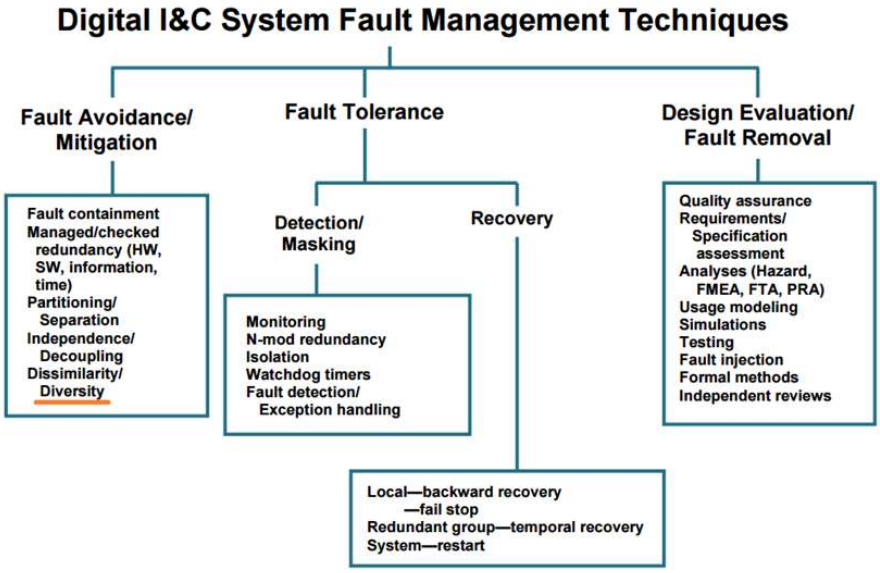
METODOLOGIA

Características de projeto do RPS

Existem diversas técnicas para gerenciar falhas um sistema de I&C digital que podem ser empregadas para funções de alta criticidade dentro de vários domínios de aplicação. Uma proposta de hierarquia para essas técnicas é apresentada na Figura 3. Essas técnicas são geralmente agrupadas em termos de avaliação de projeto e remoção de falha, tolerância a falha, e evasão e mitigação de falhas. As técnicas apresentadas envolvem abordagens de projeto, ações do ciclo de vida, escolhas de tecnologia, configuração de arquitetura, entre outros (NUREG, 2008).

Neste artigo vamos propor uma arquitetura de referência baseada nas técnicas de Tolerância a Falha apresentadas na Figura 3 (NUREG, 2008).

Figura 3 - Técnicas de Gerenciamento de Falhas para Sistemas de I&C digital



Fonte: NUREG (2008)

Essa hierarquia (Figura 3) de tolerância a falha representa técnicas específicas para acomodar a presença de falhas, evitando suas consequências. A detecção e a resiliência a falha (*masking*) referem-se à identificação da presença de falhas ou absorver seu potencial efeito. O diagnóstico e a votação de redundâncias são técnicas comuns. A recuperação está relacionada a resposta à uma falha ativa que permite a continua execução com a recuperação do estado antes da falha (NUREG, 2008).

Segurança de forma sistêmica e sustentável

Para avaliar a existência de condições efetivas de se garantir a segurança de forma sistêmica e sustentável de um reator nuclear é necessário considerar aspectos além do projeto e construção de um sistema de proteção. Para tal vamos utilizar o conceito de cultura de segurança que é abrangente e requer que as características apresentadas no Apêndice ocorram nas organizações (IAEA, 2002).

Assim, vamos caracterizar elementos de cultura importantes para a segurança em toda a cadeia produtiva e instituições envolvidas com a segurança do reator nuclear. Esta abrangência está de acordo com a visão das análises de sustentabilidade (MOREIRA et al., 2015). As questões ligadas a projeto construção foram estudadas anteriormente. Aqui se avaliam os elementos de cultura de segurança requeridos aos segmentos operação, monitoramento e fiscalização do reator nuclear para garantir a não ocorrência de acidentes e desastres.

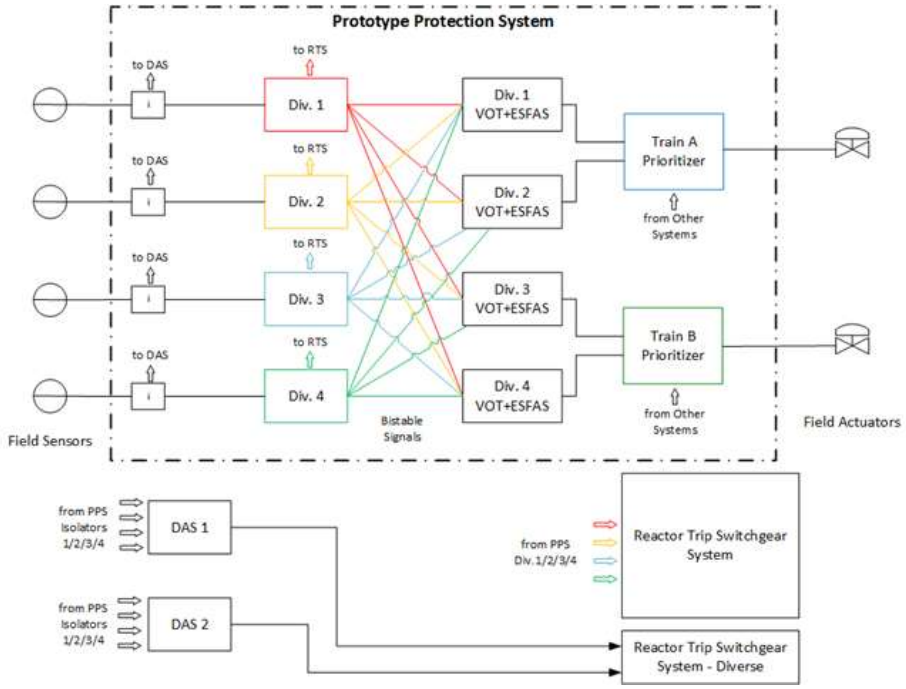
RESULTADOS E DISCUSSÕES

Tolerância a falha do modelo de referência para o Sistema de proteção

A Figura 4 apresenta a proposta de uma arquitetura de referência para o Sistema de Proteção do Reator e o Sistema Diverso de Atuação para uma planta nuclear. Seguindo os critérios tolerância a falha descritos na Figura 3.

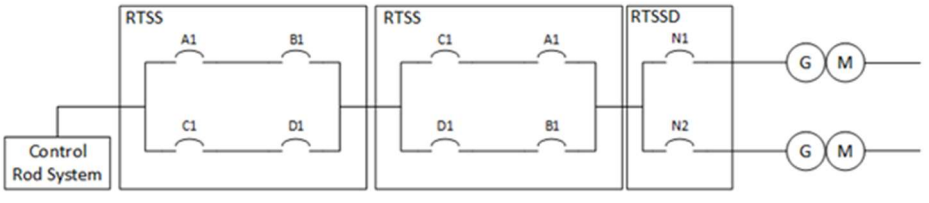
A seguir apresentam-se e avaliam-se as técnicas de gerenciamento de falha adotadas para tolerância a falha e uma análise da confiabilidade da arquitetura proposta por meio da técnica de RBD, incluindo o Sistema Diverso de Atuação.

Figura 4 – Arquitetura Proposta



A Figura 5 apresenta o detalhe dos disjuntores de desligamento de emergência apresentados na Figura 4.

Figura 5 – Disjuntores de desligamento do reator



RTSS – Reactor Trip Switchgear System

RTSSD – Reactor Trip Switchgear System Diverse

Monitoramento

A função de monitoramento é executada pelo Sistema de Controle da Planta que recebe os sinais críticos dos sensores do Sistema de Proteção através dos Isoladores. Dessa forma os operadores da planta podem analisar a tendência das variáveis de controle, realizar a comparação entre as variáveis redundantes e em

posse dessas informações tomar ações corretivas, evitando situações de emergência.

Redundância

A arquitetura proposta na Figura 4 apresenta 4 redundâncias para o Sistema de Proteção e realiza a votação 2oo4 (*2 out of 4*), ou seja, para realizar as ações de segurança pelo menos 2 divisões do Sistema de Proteção devem indicar a situação insegura.

A votação 2oo4 do *Trip* é realizada diretamente no *Switchgear* do Reator, tornando a ação de *Trip* mais rápida.

Isolação

A arquitetura proposta apresenta 4 redundâncias no Sistema de Proteção totalmente isoladas umas das outras. Além disso, o Sistema de Proteção também está isolado dos demais sistemas, como o Sistema de Controle e o Sistema Diverso de Atuação. Este isolamento garante a independência de cada sistema e reduz a possibilidade de a falha em um único sistema desencadear a falha nos demais sistemas da planta. Na isolação entre as divisões deve inclusive existir uma isolação física, como por exemplo salas distintas para cada divisão, evitando que causas externas provoquem efeitos comuns.

Watchdog timers e Fault Detection/Exception handling

Os equipamentos de controles a serem propostos para essa arquitetura devem incluir *watchdog timers* e auto-diagnóstico para detectar estados de falha e garantir um estado seguro e conhecido como uma ação para a recuperação de falhas.

Recuperação

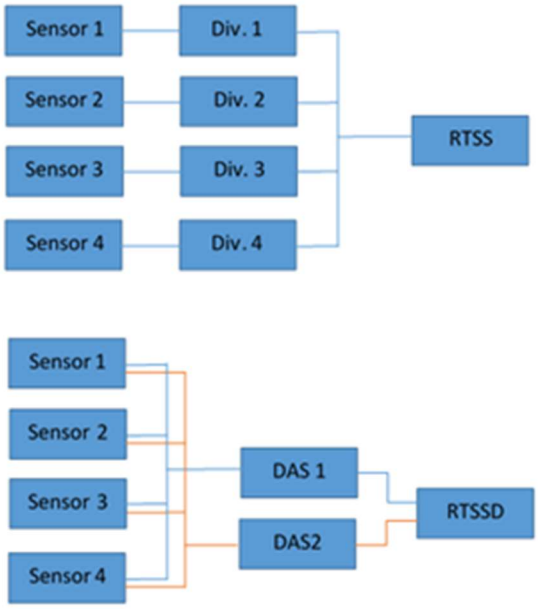
Os equipamentos de controles a serem propostos para essa arquitetura devem incluir requisitos de recuperação permitindo a retomada de um estado anterior seguro após uma falha.

Análise de confiabilidade

A confiabilidade é definida como a “Capacidade de um item desempenhar uma função requerida sob condições especificadas, durante um dado intervalo de tempo” (NBR, 1994). Portanto analisar a confiabilidade da arquitetura de segurança é mandatório para se certificar que as métricas de confiabilidade do sistema estão dentro da meta estabelecida pela planta nuclear em questão.

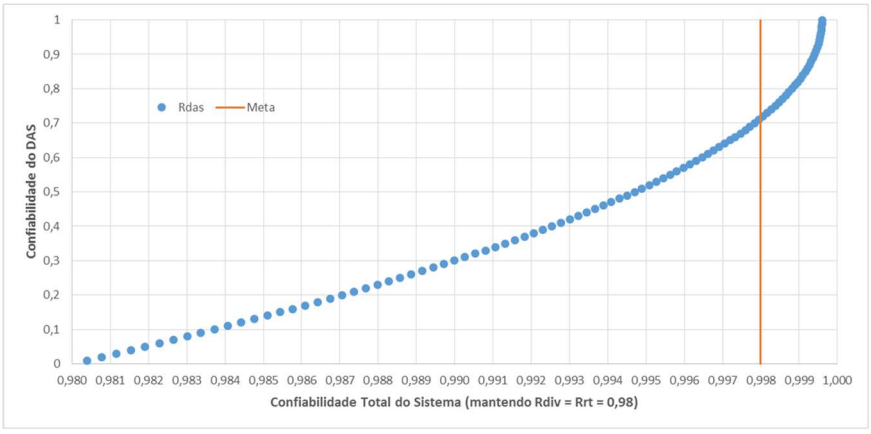
A Figura 6 apresenta os diagramas de RBD para o sistema de proteção e para o sistema diverso de atuação.

Figura 6 – Diagrama RBD para o RPS e para DAS



A Figura 7 apresenta o resultado de confiabilidade do sistema calculado conforme (BUSSE e OZEKI, 2018), onde o incremento de confiabilidade do sistema pela alocação no DAS é demonstrado. A Figura 7 apresenta também uma meta global estabelecida de 0,998 para o sistema.

Figura 7 – Alocação de confiabilidade do sistema pelo DAS



A Figura 4 apresenta uma arquitetura compatível com os requisitos de tolerância a falha esperado pela norma NUREG (2008). Podemos observar através da Figura 7 que a participação do sistema diverso de atuação para a confiabilidade global da planta, no que tange o desligamento do reator, é diretamente proporcional a confiabilidade do SDA. A Figura 7 apresenta também o valor necessário de confiabilidade do SDA para atingir uma meta global específica, assumindo-se uma meta de confiabilidade das divisões e dos disjuntores minimamente em 0,98.

Garantia de segurança de forma sistêmica e sustentável para a prevenção de acidentes

Para garantir a segurança não só durante a operação de um empreendimento, mas em todo o seu ciclo de vida deve-se pensar na segurança desde o projeto e construção e passar também pela operação, monitoramento e fiscalização (CORREA e CARDOSO JUNIOR, 2007; LU et al., 2015; YANG et al., 2018; WAHLSTROM, 2018; SILVA, 2017; ZOU et al., 2017). A ocorrência de acidentes nas indústrias que atuam com produtos ou ações perigosas depende de vários fatores, entre eles questões técnicas de segurança e também aqueles ligados à estrutura organizacional e gerencial das empresas e a correspondente cultura de segurança existente. Várias pesquisas demonstram que a cultura prevalecente nas empresas tem forte impacto no número de acidentes ocorridos (IAEA, 2002, WHALSTROM, 2018; SILVA, 2017). Todas as empresas envolvidas no processo devem estar imbuídas sobre as questões ligadas à segurança.

A IAEA identificou 30 características importantes relacionadas com a cultura de segurança para empresas e instituições do setor nuclear conforme apresentado no Apêndice. Estes pontos podem ser divididos em 4 grandes tópicos que são importantes para sua efetiva realização. A Tabela resume esta divisão.

Tabela 1 – Tópicos importantes para a cultura de segurança dentro de uma instituição e as características preconizadas segundo a IAEA

Tópicos	Características
1) Comprometimento da direção das instituições e empresas	2-6
2) Treinamento, aprendizagem e transparência dentro das instituições e empresas	1, 7, 9-12
3) Gerenciamento e confiança dos colaboradores	8, 13-20
4) Valores e sistema de cultura de segurança	21-30

Fonte: (IAEA, 2002)

Vamos analisar estas características e tópicos para a empresa responsável pela operação segura do reator nuclear e para as instituições responsáveis pelo monitoramento e fiscalização da segurança durante a operação. Para garantir que haja segurança não basta ter sistemas bem projetados e construídos conforme discutido na seção anterior. É necessário ter comprometimento da direção da empresa e instituições envolvidas nas atividades de operação, monitoramento e fiscalização.

O primeiro tópico importante é que as lideranças das instituições demonstrem compromisso pessoal com a segurança nuclear e que os assuntos de segurança sejam gerenciados e os conflitos efetivamente resolvidos.

Outro tópico importante está relacionado com o treinamento, aprendizagem e transparência dentro das instituições. Cumpre salientar que deve sempre haver procedimentos e que estes sejam observados. Educação e treinamento devem ser fornecidos frequentemente.

O tópico sobre gerenciamento e confiança dos colaboradores também é muito importante. Questões existentes e anormalidades devem ser reportadas livremente, de forma aberta e sem receios por parte dos trabalhadores, técnicos e gerentes. Melhorias devem ser continuamente implementadas.

Finalmente, a segurança deve ser considerada um valor importante e compartilhado por toda a organização. Como valor, consideram-se os compromissos assumidos pela organização e que a segurança seja uma prioridade. Cultura de segurança na organização significa que nela existe um sistema de normas de segurança e um sistema de gerenciamento funcional e efetivo. Esses sistemas devem ser construídos e mantidos.

A cultura de segurança não é uniforme em todas as etapas da cadeia produtiva do setor de energia e também entre todas as empresas. Em algumas delas há bastante informação enquanto para outras os dados são escassos. É necessário estabelecer uma governança específica para as atividades de monitoramento e fiscalização para garantir a segurança e gerenciamento adequado de desastres.

CONSIDERAÇÕES FINAIS

A sustentabilidade, em linhas gerais, é um conceito que se aplica à avaliação de projetos, empreendimentos e ações de governo ou de empresas que têm impactos nas dimensões ambiental, social e econômica. Ele foca naquelas variáveis que são importantes para garantir a sua manutenção e existência ao longo do tempo com capacidade de realizar suas funções ambientais, sociais e econômicas. O ponto importante é que a ocorrência de acidentes com um reator nuclear devido a falhas operacionais ou outras causas afeta a sustentabilidade da região onde ele está localizado.

Neste artigo, estabeleceu-se para os segmentos de projeto e construção, a título de exemplo, uma meta de confiabilidade total do sistema de proteção de 0,998. Assim consequentemente o SDA deverá possuir uma meta de confiabilidade mínima de 0,70. Este artigo estabeleceu uma metodologia para se determinar a confiabilidade mínima pra um sistema SDA respeitando as condições previamente declaradas para o atendimento dos critérios estabelecidos de tolerância a falha.

Nos segmentos de operação, monitoramento e fiscalização é evidente a necessidade de se ter viva nas instituições cultura de segurança. Notou-se a necessidade de uma governança específica para fiscalização e monitoramento ambiental e governança para o gerenciamento de desastres. É interessante notar que esta governança já existe no setor nuclear, que deve ser mantida e aprimorada continuamente e que se aplica a maioria dos projetos de infraestrutura que surgem todos os dias no Brasil!

Systemic fault tolerance evaluation in nuclear reactor protection systems

ABSTRACT

The concept of fault tolerance has become important in recent decades in the nuclear industry due to the use of digital Instrumentation and Control (I&C) systems. A fault is an unwanted anomaly in an item or system that can lead to an unsafe state and eventually generate incidents or accidents of socially undesirable consequences. Currently digital solutions are very attractive, though requiring software assessments for fault tolerance. Our paper intends to carry out a theoretical investigation on reliability and failure rate, based on a Reliability Block Diagram, in a digital protection system for nuclear reactors. In addition, it discusses the need for safety culture in the segments of reactor operation, monitoring and inspection to ensure that unwanted accidental events are avoided.

KEYWORDS: Fault Tolerance. Reliability block diagram. Nuclear Safety. Digital protection systems.

APÊNDICE

A International Atomic Energy Agency (IAEA) considera as características apresentadas abaixo como necessárias para uma organização ter uma boa cultura de segurança (IAEA, 2002):

1. Procedimentos e regulamentos de segurança do trabalho são observados
2. Os líderes demonstram compromisso pessoal com a segurança nuclear
3. Liderança e profissionalismo sobre a segurança nuclear são demonstrados
4. A comunicação vertical e horizontal é encorajada
5. Os líderes participam ativamente das atividades relacionadas à segurança nuclear
6. Assuntos relacionados a segurança nuclear são gerenciados e os conflitos são resolvidos
7. As opiniões são revisadas e consideradas na tomada de decisões
8. Questões existentes e as anormalidades são reportadas imediatamente
9. As atividades de aprendizagem e melhoramento são continuadas
10. Educação e treinamento especializado são oferecidos periodicamente
11. A educação e o treinamento relacionados com a segurança nuclear são oferecidos de acordo aos níveis pessoais
12. As experiências operacionais são oportunamente analisadas e utilizadas
13. Melhorias são continuamente executadas
14. Todos são responsáveis pela segurança nuclear
15. Os papeis e responsabilidades na segurança nuclear são claramente compreendidos
16. A consciência da segurança nuclear é estabelecida
17. A confiança permeia na organização
18. Os erros são reportados sem repressão e retaliação
19. Os assuntos relacionados a segurança são livremente levantados
20. Ações relacionadas a segurança nuclear são reconhecidas e os incentivos são fornecidos de acordo
21. Sistema de desenvolvimento da cultura de segurança nuclear é praticado
22. A política de segurança nuclear é estabelecida e seus valores são divididos entre os membros da organização
23. A segurança nuclear é considerada em primeiro lugar para os planos de negócio e distribuição de recursos humanos

24. A avaliação periódica de cultura de segurança nuclear é feita dependentemente ou independentemente
25. Vários resultados das avaliações de segurança nuclear para o processo de trabalho
26. Segurança nuclear é a primeira prioridade para toda a atividade de trabalho
27. O trabalho é realizado com propriedade
28. Os trabalhadores sempre têm uma atitude de questionamento de atitude no trabalho
29. A tecnologia nuclear é completamente compreendida e os trabalhos oferecidos são cuidadosamente desempenhados
30. A partir da percepção dos erros as piores situações são preparadas

REFERÊNCIAS

ABNT. Confiabilidade e Mantenabilidade, ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR 5462, 1994.

BUSSE, A. L; OZEKI, T. Y. B. Fault-tolerant design for protection systems. VIII SETI – Embraer technology and Innovation Seminar. Eugênio de Melo, 2018.

CARAJILESCOV, P; MOREIRA, J. M. L. Aspectos técnicos, econômicos e sociais do uso pacifico da energia nuclear. Revista Ciência e Cultura, 60: 33-36. 2008.

CORREA, C. R. P; CARDOSO JUNIOR, M. M. Análise e classificação dos fatores humanos nos acidentes industriais. Produção, 17, 186-198, 2007.

IAEA. Nuclear Technology Review: Instrumentation and Control Systems In Nuclear Power Plants: A Time of Transition. International Atomic Energy Agency. Annex V, Vienna, 2008.

_____. Self-assessment of safety culture in nuclear installations: highlights and good practices. International Atomic Energy Agency. Vienna: IAEA. 2002.

_____. Pressurized Water Reactor Simulator. Second Edition, Workshop Vienna, 2005. Disponível em: <http://www-pub.iaea.org/MTCD/Publications/PDF/TCS-22_2nd_web.pdf>. International Atomic Energy Agency. Acesso em 22/02/2019.

_____. Safety Glossary: Terminology Used iIn Nuclear Safety And and Radiation Protection. International Atomic Energy Agency. Vienna, 2016.

_____. TECDOC-1544: Nuclear Power Plant Design Characteristics. International Atomic Energy Agency. Vienna, 2007.

LAHTINEN, J., JOHANSSON, M., RANTA, J., Harju, H. and NEVAAINEN, R. Comparison between IEC 60880 and IEC 61508 for Certification Purposes in the

Nuclear Domain. Computer Safety, Reliability, and Security, 29th International Conference, SAFECOMP 2010 Vienna, Austria, September 14-17, 2010.

LIMA, F. J. e GARCIA, C. Uma Proposta de Arquitetura de Sistema de Proteção de Planta Nuclear do Tipo PWR. IEEE Latin America Transactions, Vol. 4, No. 6, December 2006.

LU, J. J., HSU, T. C., CHOU, H. P. System assessment of an FPGA-based RPS for ABWR nuclear power plant, Progress in Nuclear Energy, 85, 44-55, 2015.

MAIORINO, J. R, PERROTTA, J. A., YAMAGUCHI, M., MOREIRA, J. M. L., NAKATA, H., YORIYAZ, H., KOSAKA, N., COELHO, P. R. P., MENDONÇA, A. G., FANARO, L. C. C. B., Projeto nuclear da unidade critica IPEN/MB-01. In: Encontro Nacional de Física de Reatores e Termo-hidráulica - 1989, Recife, PE, Editora Universitária UFPE, v. 1. p. 311-323, 1989.

MOREIRA, J. M. L., GALLINARO, B., CARAJILESCOV, P. Construction time of PWRs, Energy Policy, 55, 531-542, 2013.

MOREIRA, J. M. L.; CESARETTI, M. A.; CARAJILESCOV, P.; MAIORINO, J. R. “Sustainability deterioration of electricity generation in Brazil”. Energy Policy, 87, 334-346, 2015.

RAOUF, A. Theory of accident causes. Accident Prevention. The ILO Encyclopaedia of Occupational Health and Safety, Fourth Edition. ILO Publications, Geneva, March 2011.

SAE INTERNATIONAL. ARP-4761:, Guidelines and methods for conducting the safety assessment process on civil airborne systems and equipment,1996.

SOUZA, R. G.P., MOREIRA, J. M. L. Power peak factor for protection systems–experimental data for developing a correlation, Annals of Nuclear Energy, 33, 609-621, 2006.

THOMSON, J. Nuclear Power Station Control and Instrumentation Safety Systems Architecture - An Overview. Safety In Engineering, March 2012IAEA - Nuclear Technology Review. Instrumentation And Control Systems In Nuclear Power Plants: A Time of Transition. Annex V, Vienna, 2008

USNRC. NUCLEAR REGULATORY COMMISSION. NUREG-0800:, 7.3 ENGINEERED SAFETY FEATURES SYSTEMS, Revision 6, August 2016.

_____. NUREG-CR-7007:. Diversity Strategies for Nuclear Power Plant Instrumentation and Control Systems. Oak Ridge National Laboratory, NRC job Code N6176, December 2008.

WAHLSTRÖM, B. Organisational learning – Reflections from the nuclear industry, Safety Science, 49, 65-74, 2011.

_____. Systemic thinking in support of safety management in nuclear power plants, Safety Science, 109, 201-218, 2018.

YANG, M., WANG, J., CHEN, S., CHEN, S., ZHANG, J. Development of NPP digital I&C system closed-loop online test system based on signal transmission array, Progress in Nuclear Energy, 108, 270-280, 2018.

ZOU, B., YANG, M., BENJAMIN, E. R., YOSHIKAWA, H. Reliability analysis of Digital Instrumentation and Control software system, Progress in Nuclear Energy, 98, 85-93, 2017.

Recebido: 09/03/2019
Aprovado: 23/12/2019
DOI: 10.3895/rts.v16n42.9780

Como citar: BUSSE, A.L.; et.al. Avaliação sistêmica de tolerância a falhas em sistemas de proteção de reatores nucleares. **R. Tecnol. Soc.**, Curitiba, v. 16, n. 42, p. 58-74. jul/set. 2020. Disponível em: https://periodicos.utfpr.edu.br/rts/article/view/9780. Acesso em: XXX.

Correspondência: