Interferência Eletromagnética Intencional: Análise de Riscos em Instalações Brasileiras

Rafael Venuto Bittencourt de Oliveira
PPGEE – Programa de Pós-Graduação em Engenharia Elétrica
UFMG – Universidade Federal de Minas Gerais
Belo Horizonte, Brasil
ravenuto.bittencourt@gmail.com

Alberto De Conti
LRC – Lightning Research Center
DEE – Departamento de Engenharia Elétrica
UFMG – Universidade Federal de Minas Gerais
Belo Horizonte, Brasil
conti@cpdee.ufmg.br

***Resumo*—Este artigo discute os riscos associados à interferência eletromagnética intencional, em especial as possíveis ameaças advindas da facilidade de acesso a informações e materiais para confecção de equipamentos *home made* que podem ser utilizados para fins maliciosos. Após a caracterização desta ameaça apresenta-se uma análise do contexto brasileiro (incluindo políticas de segurança específicas) ante a proximidade de eventos de vulto internacional e procede-se uma avaliação qualitativa da vulnerabilidade de instalações civis. Conclui-se que há evidências de vulnerabilidade e que é necessário investigar o desempenho dessas instalações frente a problemas de interferência eletromagnética intencional visando melhorar sua robustez frente a tais ameaças.**

***Palavras-chave*—Compatibilidade Eletromagnética, Instalações Civis, Interferência Eletromagnética Intencional.**

I. INTRODUÇÃO

A interferência eletromagnética intencional (IEMI - *Intentional Electromagnetic Interference*) vem se tornando, a cada dia, uma ameaça real à sociedade civil. A utilização crescente de sistemas eletrônicos e de redes de computadores (incluindo sistemas embarcados), que são altamente vulneráveis a fenômenos eletromagnéticos de alta potência, compõe um cenário preocupante, especialmente para instalações civis, que não foram projetadas para lidar com tais ameaças. A facilidade de se construir equipamentos *home made* de baixa tecnologia capazes de gerar IEMI, somada à realização sucessiva de eventos de grande porte (Copa do Mundo de 2014, Olimpíadas de 2016), aumentam a visibilidade do Brasil, tornando-o um alvo potencial de ameaças diversas.

Em [1] são apresentados casos documentados de ataques IEMI na Europa e no Japão, assim como as lições aprendidas a partir do estudo destes ataques. As motivações para ataques deste tipo incluem roubo, enfraquecimento de sistemas de comunicação com a finalidade de criar vulnerabilidade e/ou desativar sistemas de segurança (caso específico de situação envolvendo rebeldes chechenos e instalações russas), e vandalismo. Já no contexto brasileiro, foi recentemente noticiada a criação de um simulacro de um *pen drive* (USB *Killer 2.0*) capaz de aplicar uma descarga elétrica em portas USB e destruir os circuitos internos de um computador [2].

Neste cenário, é relevante estudar problemas de interferência eletromagnética intencional e analisar a sua inserção no contexto brasileiro, bem como investigar as contramedidas aplicáveis. Dado o espectro de incertezas associado a esses cenários, também se mostra importante a utilização de ferramentas que possibilitem lidar com eventos futuros incertos. Este trabalho lança mão de ferramentas clássicas de gestão de riscos combinadas com metodologias específicas para uma avaliação qualitativa de instalações civis em relação à sua vulnerabilidade.

II. ALGUMAS DEFINIÇÕES

A. Terrorismo

Existe uma grande dificuldade em se definir o que é terrorismo. As tentativas de defini-lo "... esbarram sempre na irredutibilidade da concepção que cada país possui" [3], sem contar, ainda, com a natureza mutável do que se considera terrorismo ao longo do tempo. A definição utilizada neste trabalho é a seguinte [4]:

> *"Ato de devastar, saquear, explodir bombas, sequestrar, incendiar, depredar ou praticar atentado pessoal ou sabotagem, causando perigo efetivo ou dano a pessoas ou bens, por indivíduos ou grupos, com emprego da força ou violência, física ou psicológica, por motivo de facciosismo político, religioso, étnico/racial ou ideológico, para infundir terror com o propósito de intimidar ou coagir um governo, a população civil ou um segmento da sociedade, a fim de alcançar objetivos políticos ou sociais. (...) Trata-se de ação premeditada, sistemática e imprevisível, de caráter transnacional ou não, (...), geralmente visando destruir a segurança social, intimidar a população ou influir em decisões governamentais".*

O presente trabalho foi realizado com o apoio financeiro da CAPES - Brasil. Alberto De Conti agradece o apoio financeiro da FAPEMIG e do CNPq.

O terrorismo tem por objetivo provocar o pânico; suas vítimas-alvo não são as diretamente afetadas, mas a sociedade, ao criar-se o sentimento de vulnerabilidade, impotência e desamparo ante o ato terrorista [5].

B. Interferência Eletromagnética Intencional

O termo *High Power Electromagnetics* (HPEM) descreve um conjunto de eventos capazes de gerar campos elétricos e/ou magnéticos com valores de pico intensos e/ou potência elevada. Casos típicos: os campos eletromagnéticos gerados por uma descarga atmosférica próxima, o pulso eletromagnético (EMP) gerado por uma detonação nuclear ou, ainda, os campos gerados por sistemas de radares [6,7].

Mais recentemente, o termo IEMI, descrito como "geração maliciosa de energia eletromagnética que introduz ruído ou sinais em sistemas elétricos ou eletrônicos e, com isso, perturba, confunde ou danifica estes sistemas para propósitos terroristas ou criminosos" [6] vem sendo apontado como uma ameaça à sociedade civil. Giri e Tesche [8] argumentam que dispositivos eletromagnéticos de alta potência podem ser utilizados intencionalmente para causar disrupção ou mau funcionamento em sistemas. Em particular, sinais na faixa de 200 MHz-5 GHz são mais propícios a causar perturbações em sistemas eletrônicos [9].

É possível agrupar as fontes de interferência eletromagnética intencional em duas categorias: fontes de efeitos conduzidos e fontes de efeitos radiados [10]. A fonte de efeitos conduzidos transfere energia eletromagnética para cabos (ou fios) por injeção direta. Já as fontes de efeitos radiados utilizam uma ou mais antenas para emitir campos eletromagnéticos a distâncias de vários comprimentos de onda em relação ao sistema ou equipamento vítima. Desta forma, fontes de efeitos radiados podem ser utilizadas remotamente, em contraste com fontes de efeitos conduzidos, que devem necessariamente estar próximas de um ponto de entrada ou cabo. Contudo, fontes de interferência que utilizem acoplamento conduzido podem representar maior ameaça do que fontes radiadas, uma vez que o campo eletromagnético gerado por fontes radiadas está sujeito a um decaimento proporcional ao inverso da distância entre fonte e vítima [9]. No contexto deste trabalho são consideradas exclusivamente as fontes de interferência conduzida.

Fontes que geram sinais com amplitude acima de 1 kV já podem ser consideradas parte de ambiente eletromagnético de potência [9]. Essas fontes podem ser classificadas quanto à sua portabilidade e disponibilidade, conforme indicado nas Tabelas I e II.

TABELA I – CLASSIFICAÇÃO: PORTABILIDADE [9].

Nível de Portabilidade	Descrição
PI	Tamanho de bolso ou "vestível"
PII	Tamanho de uma mochila ou pasta
PIII	Tamanho de um veículo a motor
PIV	Tamanho de um trailer

TABELA II - CLASSIFICAÇÃO: DISPONIBILIDADE [9].

Nível de Disponibilidade	Expertise requerida pelo usuário
AI	Consumidor
AII	Hobista
AIII	Profissional
AIV	"sob medida"

A Tabela III sintetiza algumas razões para o aumento da vulnerabilidade de sistemas a interferências eletromagnéticas intencionais [11] sob as perspectivas das "vítimas" e das fontes.

TABELA III - RAZÕES PARA O AUMENTO DA VULNERABILIDADE À IEMI [11].

Visão: Vítima	Visão: Fonte
Aumento do uso de tecnologias eletrônicas cada vez mais sofisticadas.	Maior disponibilidade de fontes de energia eletromagnéticas comerciais com potencial de utilização como armas e, ainda, de fontes comerciais utilizadas para testes de compatibilidade eletromagnética que também podem ser utilizadas para interferência eletromagnética intencional.
Miniaturização dos componentes e sinais de intensidade cada vez menores utilizados nos sistemas	Maior disponibilidade de componentes que podem ser utilizados para construção de fontes caseiras como, por exemplo, chaves, capacitores, magnetrons etc. Grande disponibilidade de informações disponíveis na internet.
Maior número de "pontos de acesso" que podem ser perturbados: antenas para sistemas wireless, tomadas de energia, conectores para cabeamento de dados e soquetes de lâmpadas para injeção de perturbações.	Ataques por interferência eletromagnética intencional, ao contrário de ataques terroristas tradicionais, podem ser executados de forma anônima e encoberta. Ao contrário de uma explosão, seu executor dispõe de maior tempo para encobrir seus "rastros".
As fronteiras físicas dos sistemas podem não coincidir com as fronteiras eletromagnéticas.	-

C. Instalações Civis

A crescente utilização de redes de computadores e sistemas eletrônicos, altamente vulneráveis a fenômenos eletromagnéticos de alta potência, juntamente com a observação de que instalações civis não são projetadas para lidar com tais ameaças, indicam o aumento da vulnerabilidade de tais instalações. Esse fato se soma à facilidade com que é possível produzir equipamentos de baixa tecnologia capazes de gerar tais interferências e também à acessibilidade de possíveis "pontos de injeção" (soquetes de lâmpadas ou tomadas elétricas, por exemplo) [12]-[15].

No contexto brasileiro, instalações elétricas civis são aquelas regidas pela norma ABNT NBR 5410 (instalações elétricas de baixa tensão) [16], cujo escopo abrange "instalações elétricas cujas tensões nominais são iguais ou

inferiores a 1000 V CA ou 1500 V CC", aplicando-se a "edificações residenciais e comerciais em geral, estabelecimentos institucionais e de uso público, estabelecimentos industriais, estabelecimentos agropecuários e hortigranjeiros, edificações pré-fabricadas, reboques de acampamento (trailers), locais de acampamento (campings), marinas e locais análogos, canteiro de obras, feiras, exposições e outras instalações temporárias" [16].

A Figura 1 apresenta um exemplo do aspecto de uma instalação elétrica civil. Para locais de grande afluência de público, existe uma norma específica [17] que determina que o acesso aos quadros de distribuição nesses locais só pode ser permitido a pessoas classificadas como BA4 ou BA5. A Tabela IV apresenta essa classificação.

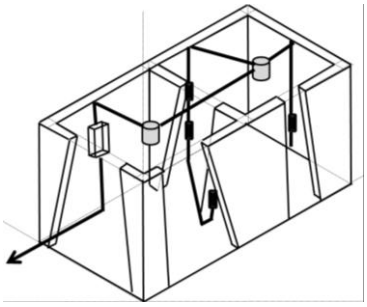

Figura 1. Exemplo simplificado de instalação elétrica.

TABELA IV – CLASSIFICAÇÃO: NÍVEIS DE COMPETÊNCIA [16]

Código	Classificação	Características	Aplicações e Exemplos
BA1	Comuns	Pessoas inadvertidas	-
BA2	Crianças	Crianças em locais a elas destinados	Creches, escolas
BA3	Incapacitadas	Pessoas que não dispõem de completa capacidade física ou intelectual (idosos, doentes)	Casas de repouso, unidades de saúde
BA4	Advertidas	Pessoas suficientemente informadas ou supervisionadas por pessoas qualificadas, de tal forma que lhes permite evitar os perigos da eletricidade (pessoal de manutenção e/ou operação).	Locais de serviço elétrico
BA5	Qualificadas	Pessoas com conhecimento técnico ou experiência tal que lhes permite evitar os perigos da eletricidade (engenheiros e técnicos)	Locais de serviço elétrico fechados

A análise de [16, 17] indica que ainda que exista um cuidado específico em relação à acessibilidade aos quadros de distribuição, não se identifica nas normas técnicas consultadas nenhuma outra preocupação com a acessibilidade de pontos de tomada e/ou soquetes de lâmpadas.

III. AVALIAÇÃO DE INSTALAÇÕES

Para proceder à avaliação de instalações é necessário lançar mão de modelos clássicos de gestão de riscos conjugados com metodologia específica para avaliação de instalações.

A. Metodologia para classificação de instalações

Uma metodologia para classificação de instalações com respeito à interferência eletromagnética intencional é apresentada em [18]. Esta metodologia tem como base três variáveis, que são definidas como: acessibilidade, consequência e susceptibilidade. Estas variáveis são associadas a uma escala qualitativa. A Tabela V apresenta a associação de cada variável e suas qualificações. Estas variáveis podem ser representadas graficamente e a combinação de suas graduações pode ser utilizada para se estimar a vulnerabilidade de uma instalação. A Figura 2 apresenta essa representação gráfica na forma de um cubo IEMI-ASC. De acordo com [18], a dimensão "acessibilidade" é definida em termos de quão fácil ou difícil é o acesso ao soquete de lâmpada, ao terminal de tomada ou ao quadro de distribuição. É expressa em função da presença (ou ausência) de barreiras físicas e/ou vigilância. A dimensão "consequência" é definida em termos dos impactos que um ataque à instalação teria em outros sistemas; um ataque a um sistema de energia, por exemplo, provavelmente seria mais impactante para a sociedade do que um ataque a uma agência de correios. Já a dimensão "susceptibilidade" pode ser definida como a "inabilidade de um dispositivo, equipamento ou sistema de funcionar sem degradação na presença de uma perturbação eletromagnética".

TABELA V – ESCALA QUALITATIVA ASSOCIADA A CADA VARIÁVEL

Acessibilidade	Consequência	Susceptibilidade
Muito Baixa	Muito Limitada	Muito Baixa
Baixa	Limitada	Baixa
Média	Severa	Média
Alta	Catastrófica	Alta
Muito Alta	-	Muito Alta

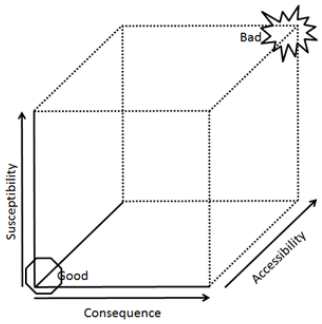

Figura 2. Cubo IEMI-ASC (*Intentional Electromagnetic Interference (IEMI) –Accessibility, Susceptibility , Consequence (ASC)*) (reprodução de [16]).

B. Teoria clássica de gestão de riscos

Atos de terrorismo possuem natureza não previsível. Na melhor das hipóteses, são eventos sobre os quais se possuem informações parciais [19, 20]. Risco pode ser definido como o produto da probabilidade P_i de ocorrência de um evento de risco R_i pelo impacto I_i deste evento, dado por

$$R_i = P_i . I_i \quad (1)$$

O risco total de um evento é dado pelo somatório de todos os *N* riscos conforme

$$R_T = \sum_{i=1}^{N} P_i.I_i \qquad (2)$$

Ainda segundo [19, 20], a análise qualitativa dos riscos pode ser feita criando-se faixas arbitrárias de valores, normalmente verbais, para se descrever a probabilidade e o impacto do risco como, por exemplo: Muito baixa(o), Baixa(o), Média(o), Alta(o) e Muito alta(o). Com isso, é possível construir um gráfico PxI com faixas de classificação de cada risco. Comparando-se a metodologia de classificação de instalações proposta em [18] com a teoria clássica de gestão de riscos [19, 20], é possível verificar que tais representações apresentam grandes semelhanças.

C. Avaliação de instalações brasileiras.

Nesta seção são apresentados dois estudos de caso em que se avalia o emprego da metodologia proposta em [18] na análise da vulnerabilidade de instalações civis brasileiras aos efeitos de interferências eletromagnéticas intencionais.

1) Estudo de Caso 1: Empresa do Setor Elétrico- COS

Avalia-se aqui, hipoteticamente, a vulnerabilidade do Centro de Operação do Sistema (COS) e do banco de servidores de uma empresa genérica do setor elétrico nacional. O COS coordena, em tempo real, as atividades de operação do sistema, integrando seus componentes de geração e transmissão. Tipicamente, localiza-se na sede da empresa e o acesso à suas instalações é normalmente restrito a funcionários previamente cadastrados. Em geral, suas portas podem ser bloqueadas por dentro, mediante o uso de barras metálicas, proporcionando maior segurança em caso de ameaças externas. Contudo após se ganhar acesso à instalação não há evidências de que existam maiores preocupações com a proteção dos equipamentos ali presentes. Isso corrobora com o apresentado em [9] sobre o fato de as fronteiras físicas dos sistemas críticos não coincidirem com suas fronteiras eletromagnéticas. A perda, ainda que parcial, das funcionalidades do centro de operação teria potencial para causar danos catastróficos para grandes regiões do país.

2) Estudo de Caso 2: Empresa do Setor Elétrico- Banco de Servidores

O banco de servidores localiza-se na sede da empresa e possui entrada controlada. Contudo, tipicamente há pontos de energia e dados acessíveis externamente que poderiam ser utilizados por indivíduos com intenções maliciosas. Contudo, ainda que a perda do banco de servidores possua efeitos danosos, é usual (e ideal) haver bancos em condição de redundância funcionando em localidades sigilosas. Desta forma, um ataque às instalações locais, ainda que causasse problemas, teria efeito temporário porque após um breve período de tempo a situação poderia ser regularizada. Caso os sistemas em redundância não estejam operando adequadamente ou simplesmente inexistam, os problemas causados poderiam ser catastróficos.

3) Estudo de Caso 3:Hospital

O hospital utilizado como referência para esta análise possui unidades cirúrgicas e laboratoriais, além de CTI e UTI. O acesso ao hospital é extremamente facilitado caso se entre pela portaria principal. Um ataque próximo a equipamentos sensíveis destas unidades tem potencial para causar inclusive óbitos. Uma vez mais, após se ultrapassar as fronteiras físicas da instalação normalmente não há evidências de que existam maiores preocupações com a proteção dos equipamentos ali presentes.

4) Aplicação da Metodologia

Ao aplicar-se a metodologia apresentada em [18] às condições citadas acima é possível obter o cubo IEMI-ASC apresentado na Figura 3. A Tabela VI apresenta os pares de pontos utilizados na elaboração deste cubo.

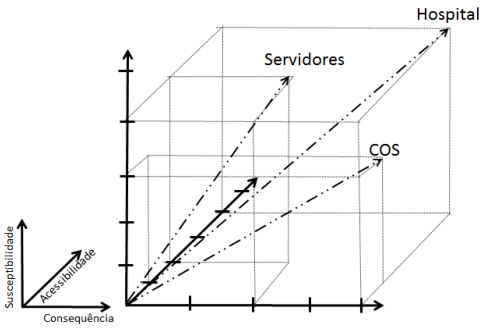

Figura 3. Classificação qualitativa das instalações analisadas.

TABELA VI - PARES DE PONTOS REFERENTES À FIGURA 3

Instalação	Consequência	Acessibilidade	Susceptibilidade
COS	*Catastrófica*	*Muito baixa*	*Média*
Servidores	*Limitada*	*Muito baixa*	*Alta*
Hospital	*Catastrófica*	*Alta*	*Alta*

5) Discussão dos Resultados

Os estudos de caso indicam que, ainda que exista interesse e investimento em termos de proteções elétricas e contra ameaças físicas tradicionais, existem vulnerabilidades consideráveis que poderiam ser exploradas por indivíduos motivados por interesses maliciosos.

É de especial preocupação a existência de hospitais que se enquadrem em tamanha exposição a tais riscos.

6) Contexto Brasileiro

O Brasil sediará, em 2016, os Jogos Olímpicos. Dadas as dimensões deste evento e a visibilidade por ele proporcionada, considerando-se a situação de crescente tensão internacional e o histórico, infeliz, de atentados como, por exemplo, os ocorridos em Munique 1972 [21], há de se precaver em relação a quaisquer possibilidades de ameaças à sociedade.

A preocupação oficial quanto à segurança deste evento (e do evento anterior – Copa do Mundo FIFA 2014) foi expressa pelo Decreto nº 7.538, de 1º de agosto de 2011, que criou a Secretaria Extraordinária de Segurança para Grandes Eventos (SESGE) [20]. Neste documento, são considerados quatro níveis de riscos, sendo os níveis III e IV de especial interesse: o primeiro trata de eventos "relativos à segurança setorizada, atuação de movimentos sociais, étnicos, religiosos, políticos, econômicos e organizações criminosas", enquanto o último trata de eventos que possam "vir a comprometer a continuidade do evento (ações terroristas graves, desastre de

massa)". Contudo o documento não dá indícios de considerar a possibilidade de ataques IEMI e os enquadra, genericamente, sob a égide de "outros crimes", que engloba "Crimes Cibernéticos e uso não autorizado de sistemas de TI; trotes e ameaças". Identifica-se, portanto, uma potencial fragilidade de sistemas elétricos brasileiros a ameaças associadas a problemas de interferência eletromagnética intencional.

IV. CONCLUSÕES

Diante de um cenário de crescente facilidade de acesso a informações que possibilitam a construção de equipamentos que podem ser utilizados em ataques de interferência eletromagnética intencional, a aplicação de metodologias para gerenciamento de riscos e classificação de instalações indica que o país pode estar vulnerável a tais ataques. Isso fica evidenciado pela ausência de políticas públicas de segurança específicas para lidar com tais situações. Neste contexto, existem diversas ações que podem ser realizadas para compreender melhor o desempenho de instalações elétricas nacionais frente a problemas de interferência eletromagnética intencional e também para melhorar a sua robustez frente a tais problemas. Essas ações estão sendo atualmente investigadas pelos autores.

REFERÊNCIAS BIBLIOGRÁFICAS

[1] F. Sabath, "What can be Learned from documented Intentional Electromagnetic Interference (IEMI) Attacks?", General Assembly and Scientific Symposium, 2011 XXXth URSI, Ago. 2011

[2] Jornal O GLOBO, "Pendrive assassino destrói seu computador em segundos" [online], reportagem de 15/10/2015 disponível em: http://oglobo.globo.com/sociedade/tecnologia/pendrive-assassino-destroi-seu-computador-em-segundos-17780060, consulta feita em 12/04/2016.

[3] A. M. Cardoso, "Terrorismo e segurança em um estado social democrático de direito", Revista CEJ n.18, pp.47-53, Brasília, Brasil, Set. 2002.

[4] P. T. R. Paniago, "Uma cartilha para melhor entender o Terrorismo Internacional – Conceitos e Definições", Revista Brasileira de Inteligência, v.3, n.4, pp. 13-22, Brasília, Brasil, Set. 2007.

[5] A. C. Raposo, "Terrorismo e contraterrorismo: desafio do século XXI", Revista Brasileira de Inteligência, v.3, n.4, pp. 39-54, Brasília, Brasil, Set. 2007.

[6] W. A. Radasky, C.E. Baum, M. W. Wiki, "Introduction to the Special Issue on High-Power Electromagnetics (HPEM) and Intentional Electromagnetic Interference (IEMI)", IEEE Trans. Eletromagn. Compat. vol. 46, No. 3, pp. 314-321, Aug. 2004.

[7] W. A. Radasky, "The Threat of Intentional Electromagnetic Interference (IEMI) to wired and wireless systens", 17th International Zurich Symposium on electromagnetic Compatibility, pp. 160-163, 2006.

[8] D. V. Giri, F. M. Tesche "Classification of Intentional Electromagnetic Enviromente (IEME)", IEEE Trans. Eletromagn. Compat. vol. 46, No. 3, pp. 322-328, Aug. 2004.

[9] G. Lungrin, et al., "Overview of IEMI Conducted and Radieted Sources: Characteristics and Trends", 2013 International Symposium on electromagnetic Compability (EMC Europe 2013), pp. 24-28, Sep. 2013.

[10] C. R. Paul, Introduction to Electromagnetic Compability, 2nd ed., Hoboken, New Jersey, Wiley-Interscience: 2006. 983 p.

[11] D. Månsson, M. Bäckström, R. Thottapillil "Classifying facilities with respect to Intentional EMI", 2010-Asia-Pacific International Symposium on Electromagnetic Compability, pp. 134-137, Apr. 2010.

[12] D. Månsson, T. Nilsson, R. Thottapillil, M. Bäckström, "Propagation of UWB Transient in Low-Voltage Intallation Power Cables", IEEE Trans. Eletromagn. Compat. vol. 49 , No. 3, pp. 585-592, Aug. 2007.

[13] R. Bansal, "Criminal Interference", IEEE Antennas and Propagation Magazine, vol. 43, No. 6, pp. 134-135, Dec. 2001.

[14] M. G. Bäckström, K. G. Lövstrand, "Suceptibility of Electronic Systens to High-Power Microwaves: Summary of Test Experience", IEEE Trans. Eletromagn. Compat. vol. 46, No. 3, pp. 314-321, Aug. 2004.

[15] D. Månsson, M. Bäckström, "Propagation of UWB Transient in Low-Voltage Power Intallation Networks", IEEE Trans. Eletromagn. Compat. vol. 50, No. 3, pp. 619-629, Aug. 2008.

[16] Associação Brasileira de Normas Técnicas – ABNT "NBR 5410 - Instalações Elétricas de Baixa Tensão", Rio de Janeiro, Brasil, 2004.

[17] Associação Brasileira de Normas Técnicas – ABNT "NBR 13570 - Instalações em Locais de Afluência de Público- Requisitos Específicos", Rio de Janeiro, Brasil, 1996.

[18] D. Månsson, R. Thottapillil, M. Bäckström,"Methodology for Classifying Facilities With Respect to Intentional EMI", IEEE Trans. Eletromagn. Compat. vol. 51, No. 1, pp. 322-328, Feb. 2009.

[19] C. A. C. Salles Júnior, A. M. Soler, J. A. S. Valle, R. Rabechini Júnior, Gerenciamento de Riscos em Projetos, Rio de Janeiro, Brasil, Editora FGV, 160p., 2006

[20] PMI Practice Starndart for Project Risk Management, Project Management Institute, Inc, Pennsylvania, 116p, 2009.

[21] M. V. Pinto, "Copa do Mundo de 2014: Um estudo sobre o risco de ocorrência de um atentado terrorista", [online], available: http://www.sotai.com.br/wp-content/uploads/Artigo-Terrorismo.pdf

[22] Ministério da Justiça: Secretaria Especial para a Segurança de Grandes Eventos, "Planejamento Estratégico De Segurança Para A Copa Do Mundo Fifa Brasil 2014", Brasília, Brasil, Jan. 2012.