# GESTÃO DA SEGURANÇA OPERACIONAL EM TEMPO REAL UTILIZANDO FERRAMENTAS DE ANALYTICS: A EXPERIÊNCIA DA ITAIPU BINACIONAL

**Juliano Couto Portela**
Itaipu Binacional
Av Tancredo Neves, 6731 – Foz do Iguaçu, PR, Brasil
jportela@itaipu.gov.br

**Paulo Zanelli Junior**
Itaipu Binacional
Av Tancredo Neves, 6731 – Foz do Iguaçu, PR, Brasil
zanelli@itaipu.gov.br

**Silver Gustavo Guerrero Ramirez**
Itaipu Binacional
Av. Monseñor Rodriguez, 150 – Ciudad del Este, Paraguay
silvergr@itaipu.gov.py

**Felipe Trevisan**
Itaipu Binacional
Av Tancredo Neves, 6731 – Foz do Iguaçu, PR, Brasil
ftrevisan@itaipu.gov.br

**Hugo Osvaldo Zarate Chávez**
Itaipu Binacional
Av. Monseñor Rodriguez, 150 – Ciudad del Este, Paraguay
silvergr@itaipu.gov.py

## RESUMO

Organizações são continuamente desafiadas a manter altos níveis de produtividade sem que sejam descuidados aspectos referentes à segurança das pessoas, instalações e meio ambiente. Paradoxalmente, em organizações cujas consequências socioeconômicas de eventuais falhas operacionais são elevadas, não raro o trade-off entre produção e segurança operacional é desafiado, uma vez que as características de redundância e sobredimensionamento de seus sistemas de segurança diminuem consideravelmente a probabilidade de falhas na operação. Esta realidade, no entanto, não as eximem de constantemente revisitar sua capacidade de monitorar, antecipar e responder a eventos de risco, tornando-as resilientes. Para lograr êxito em tal empreitada, é importante evoluir a gestão da segurança: de reativa, baseada na análise retrospectiva de eventos, para proativa, capaz de prover em tempo real a consciência situacional do estado das instalações e de eventuais vulnerabilidades não previstas. Este trabalho apresenta um dos caminhos que a Itaipu vem tomando no sentido de abordar proativamente sua segurança operacional: uma ferramenta de visualização em tempo real, de alto nível, de uma estrutura hierárquica de seis níveis, que capta mais de 15.000 pontos da instalação, desde o nível de processo, combinando-se através de pesos e cálculos estruturados até o nível de um indicador que representa a visão geral da segurança operacional da Itaipu Binacional, suas subestações, sistemas auxiliares, casa de força e barragem.

**Palavra-chave:** Segurança Operacional; Engenharia de Resiliência; Itaipu Binacional; Business Intelligence.

**ABSTRACT**

Organizations are continually challenged to maintain high levels of productivity without neglecting aspects of safety of people, facilities, and the environment. The trade-off between production and operational safety is often challenged, particularly in the case of organizations whose consequences of eventual operational failures are high. It happens mostly because of the redundancy and oversizing characteristics of their security systems as they considerably reduce the likelihood of operational failures. This reality, however, does not exempt them from constantly revisiting their ability to monitor, anticipate, and respond to risky events, making them resilient. To succeed in this endeavor, the evolution from reactive security management, based on retrospective event analysis, to proactive, capable of providing real-time situational awareness of facility status and potential unforeseen vulnerabilities, is essential. This paper presents one of the paths Itaipu has taken to address its operational safety proactively: a high-level, real-time visualization tool with a six-tiered hierarchical structure that captures more than 15,000 points from the installation. The combination of structured calculations from the process level, combined through weights, to the level of an indicator that represents Itaipu Binacional's operational safety overview, substations, auxiliary systems, powerhouse, and dam is the basis of the visualization.

**Keywords:** Operational Safety; Resilience Engineering; Itaipu Binacional; Business Intelligence.

**Como Citar:**
PORTELA, Juliano Couto *et al*. Gestão da Segurança Operacional em Tempo Real Utilizando Ferramentas de *Analytics*: a Experiência da Itaipu Binacional. *In*: SIMPÓSIO DE PESQUISA OPERACIONAL E LOGÍSTICA DA MARINHA, 19., 2019, Rio de Janeiro, RJ. **Anais** […]. Rio de Janeiro: Centro de Análises de Sistemas Navais, 2019.

## 1. INTRODUÇÃO

Infraestruturas Críticas (IC) – sistemas, serviços e bens vitais para o bem-estar da sociedade cuja perturbação ou destruição causa impactos graves sobre a saúde, segurança e bem-estar econômico dos cidadãos [1] – devem possuir pelo menos algumas das características das Organizações de Alta Confiabilidade (OAC), aquelas que, mesmo inseridas em um ambiente no qual uma taxa "normal" de acidentes seria esperada por conta dos altos fatores de risco e complexidade inerentes a sua operação, são bem-sucedidas em evitá-los ao longo de seu ciclo operacional [2].

Um exemplo de OAC é a Usina Hidrelétrica Itaipu Binacional, a maior geradora de energia do mundo, já tendo produzido mais de 2,6 bilhões de MWh em seus 34 anos de operação, e que apresenta em seu Modelo de Gestão da Operação o requisito básico de atender à produção de energia, subordinando-a à segurança das pessoas, das instalações e do meio ambiente no entorno da usina.

Para que estas infraestruturas continuem sua operação bem-sucedida em um contexto de aumento da complexidade operacional, é importante evoluir a gestão da segurança operacional: de reativa, baseada na análise retrospectiva de acidentes e "no que dá errado", para proativa, baseada na operação normal e "no que dá certo". Essa abordagem

suplementa as técnicas de análise de acidentes/incidentes, que normalmente apontam as causas-raiz destas ocorrências para falhas humanas, em componentes, equipamentos ou sistemas [3]. De fato, os estudos das causas-raiz de alguns dos mais graves acidentes de Instalações Críticas (Chernobyl, 1986; Three Mile Island, 1979; Sayano-Shushenskaya, 2009; Fukushima, 2011) concluíram que variáveis desconhecidas quando do design do projeto introduziram variabilidades nos sistemas enquanto em funcionamento normal, levando a situações desestruturadas.

Para prover novo rumo à investigação das condições que apontam vulnerabilidades na segurança operacional, e não somente ao estudo das causas que levam a acidentes, a abordagem de gestão de segurança denominada Engenharia de Resiliência (ER) vem sendo utilizada em ambientes de alto risco [4]. Aplicada a organizações, a resiliência apresenta capacidades que permitem gerenciar as atividades da organização para antecipar e evitar ameaças à sua existência e a seus objetivos [5]. Para a ER, a gestão de segurança operacional tradicional – denominada "Segurança-I" – foca em manter a taxa de acidentes em um nível o mais baixo possível, enquanto a nova gestão – "Segurança-II" – foca a probabilidade de sucesso levando em consideração a maior parte da operação normal, ou "o que normalmente dá certo", tornando a gestão mais proativa do que reativa [6].

De fato, a figura 1 mostra a quantidade de manobras operacionais na usina Itaipu Binacional de quatro manobras típicas selecionadas para um estudo [7] nos últimos dez anos e a quantidade de falhas de manobra que redundaram em perda de produção de energia, confiabilidade ou em danos em equipamentos. Nota-se que, no período de 2006 a 2015, as falhas representam 0,025% enquanto as manobras bem sucedidas somam 99,975% do total, uma forte sinalização de ser a gestão proativa de segurança, baseada na operação normal, uma bem-vinda forma de tratar Infraestruturas Críticas tais quais a Itaipu Binacional.

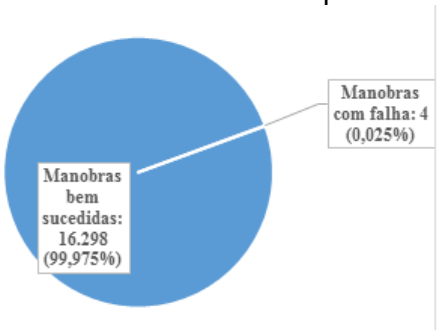


Fig. 1 Manobras bem-sucedidas x falhas na Itaipu Binacional, período 2006 a 2015

Portanto, conhecer a instalação, seu *modus operandi* e suas idiossincrasias é uma maneira fundamental de atender os requisitos proativos da abordagem de Segurança-II. Este artigo apresenta um dos passos tomados na direção de tornar proativa a abordagem de segurança operacional da Itaipu Binacional: a proposição de um indicador de tempo real, utilizando know-how e metodologia desenvolvidas internamente, capaz de prover especificamente o status da segurança operacional da planta industrial, em uma inovadora abordagem proativa. Este trabalho abordará as decisões que levaram à formação do indicador, com base nas opiniões estruturadas do staff técnico-operacional que desde 1984 opera a usina, e os preceitos, técnicas e heurísticas de business intelligence, considerando a integração entre várias fontes de dados – execução de serviços, Sistema de Supervisão e Controle (Scada), cadastro de estado de equipamentos –, definição de pesos, montagem do datawarehouse e seleção dos pontos a serem considerados na segurança operacional.

O resultado é uma estrutura hierárquica de seis níveis que capta mais de 15.000 pontos da instalação, desde o nível de processo, combinando-se entre si através de pesos e cálculos estruturados, até o nível do indicador SOP que representa a visão geral da segurança

operacional da Itaipu Binacional, suas subestações, sistemas auxiliares, casa de força e barragem.

## 2. DESENVOLVIMENTO DO PRODUTO

### 2.1. MODELO DE GESTÃO DA OPERAÇÃO

O Modelo de Gestão da Operação da Itaipu Binacional, apresentado na figura 2, livremente baseado em um modelo Balanced Scorecard, foi concebido de forma a apresentar quais seriam os atributos que, caso atendidos de maneira adequada, resultariam na "Excelência da Operação da Usina".


Fig. 2 Modelo de Gestão da Operação da Itaipu Binacional

O desempenho excelente da operação, por sua vez, garante o atendimento em alto nível da produção de energia – representada pelos altos índices de produção que vêm se verificando especialmente nos últimos anos –, da segurança das pessoas – adequadas taxas de gravidade e frequência de acidentes de trabalho – e do meio ambiente no entorno da instalação – por exemplo, resgate de peixes a cada parada longa de manutenção e inexistência de processos que derramam óleo no rio – e da segurança operacional dos equipamentos e do patrimônio da usina.

Com índices adequados que mapeiam a qualidade do atendimento à produção, à segurança das pessoas e ao meio ambiente, sentiu-se a necessidade de evoluir ainda mais em indicadores que pudessem mapear de maneira ágil, com resposta de tempo real e de fácil visualização aos diversos níveis gerenciais, a segurança operacional dos equipamentos e do patrimônio da usina. O indicador de Segurança Operacional (SOP) foi concebido com este fim.

### 2.2. FORMAÇÃO DA HIERARQUIA

Com base na opinião estruturada dos profissionais que operam a usina desde 1984 e nas documentações vigentes, o primeiro passo seria estabelecer a hierarquia de equipamentos e sistemas que daria forma ao indicador SOP, com as premissas de que: a) um só número pudesse identificar o status da segurança operacional da instalação; b) caso necessário, um simples clique no indicador macro abriria um detalhamento que pudesse facilmente encontrar o equipamento ou sistema que dá origem a eventual vulnerabilidade operacional

(drill down).

A solução encontrada foi a formação de uma estrutura hierárquica de certa forma análoga à de uma Árvore de Falhas (FTA), na qual o "Evento Topo" seria substituído pelo maior nível hierárquico (nível 1 – Itaipu Binacional) e os demais níveis seriam representados não por eventos, mas por equipamentos ou sistemas cuja condição de segurança operacional seja representada por um indicador, e o conjunto destes ajuda na formação do indicador do nível superior. Este procedimento foi seguido na formação dos indicadores dos níveis inferiores, até chegar no nível de processo.

A cada equipamento, condição ou sistema é atribuído um peso que representa sua importância para a formação do indicador do nível superior. A hierarquia geral pode ser visualizada na figura 3. Para fins de visualização da figura e entendimento, o único ramo de nível 2 que foi detalhado é o do "Sector 50Hz" e o único ramo de nível 4 que foi detalhado é o das unidades geradoras. Internamente ao sistema, no entanto, existem detalhamentos similares para todos os elementos.

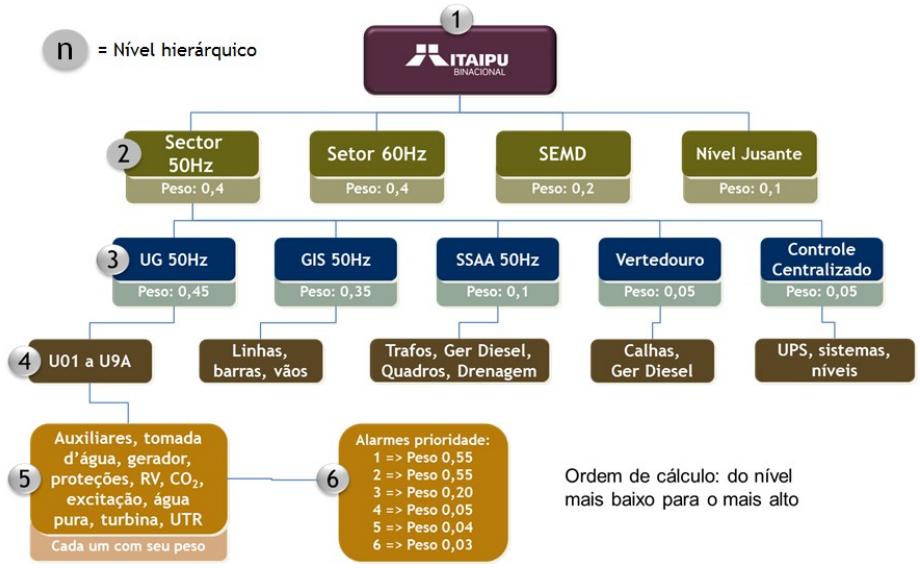


Fig. 3 Hierarquia para a formação dos indicadores de segurança operacional

## 2.3. INTEGRAÇÃO DE SISTEMAS E FERRAMENTA DE VISUALIZAÇÃO

A obtenção de dados de tempo real, entendendo "tempo real" como aquele factível tendo em vista o custo-benefício adequado entre recursos computacionais e necessidades de atualização dos indicadores, seria condição sine qua non para que se conhecesse a segurança operacional da instalação para análise e tomada de eventuais medidas operativas em tempo adequado. Para isso, precisou-se mapear quais tipos de dados teriam de ser obtidos e em quais sistemas eles estariam disponíveis. A característica dos dados necessários para o sistema levou à necessidade de buscar os bancos de dados dos seguintes sistemas:

a) Sistema de Controle de Estados de Equipamentos (SCE). Controla os estados de disponibilidade e indisponibilidade programada e forçada dos equipamentos principais da instalação, quais sejam: unidades geradoras, vertedouro, equipamentos principais dos serviços auxiliares, linhas de transmissão e transformadores.

b) Sistema Scada. Por meio do qual se obtém os dados do nível de processo, onde são buscados os alarmes relativos à segurança operacional. Para tal, é feita uma conexão por meio do Sistema Integrado de Redes Industriais (SIRI).

c) Sistema de Execução de Serviços (SES). Por onde tramitam as Autorizações de Trabalho (AT) e Pedidos de Desligamento (PD), que informam a indisponibilidade de equipamentos não principais (não contemplados pelo sistema SCE acima descrito) e o grau de atendimento do serviço a ser executado pela manutenção – programado ou urgente.

Os sistemas SCE, SES e SIRI – dados do Scada – alimentam um banco de dados no qual são armazenados, a cada 10 minutos, os dados destes sistemas.

Por meio de uma rotina de configuração, na qual estão definidos os elementos de cada nível hierárquivo e a configuração de vínculo dos pontos a serem consultados nos sistemas fonte, bem como os pesos atribuídos aos elementos que compõem a hierarquia, são feitas extrações para um data warehouse de onde o usuário final os captura por meio da ferramenta Tableau®, compondo os painéis de visualização do sistema.

Atualmente, a quantidade de pontos de cada sistema supracitado supervisionados pelo SOP é verificada na tabela 1.

Tab 1 Volume de pontos de acordo com o sistema fonte

| Nível Hierárquico | | Sistema Fonte | | |
|---|---|---|---|---|
| Nível 2 | Nível 3 | SCADA Pontos Aquisitados | SCE Equipamentos Impedidos | SES Trabalhos em Execução |
| NÍVEIS / NIVELES | Jusante / Aguas Abajo | 4 | 0 | 0 |
| SE-MD | Sector 66 kV | 16 | 5 | 54 |
| | Sector 220 kV | 189 | 10 | 180 |
| | Sector 500 kV | 556 | 19 | 288 |
| | Servicios Auxiliares SEMD | 54 | 0 | 78 |
| SECTOR 50HZ | Control Centralizado | 55 | 0 | 30 |
| | GIS 50Hz | 1.063 | 8 | 306 |
| | Servicios Auxiliares 50 Hz | 378 | 4 | 312 |
| | Unidades Generadoras 50Hz | 4.842 | 10 | 90 |
| | Vertedero | 74 | 3 | 66 |
| SETOR 60HZ | Controle Centralizado | 59 | 0 | 30 |
| | GIS 60Hz | 1.017 | 8 | 306 |
| | Serviços Auxiliares 60 Hz | 372 | 4 | 210 |
| | Unidades Geradoras 60 Hz | 4.813 | 10 | 90 |
| **Total geral** | | **13.492** | **77** | **1.992** |

A rotina de extração dos dados até a visualização para o usuário final é verificada na figura 4.

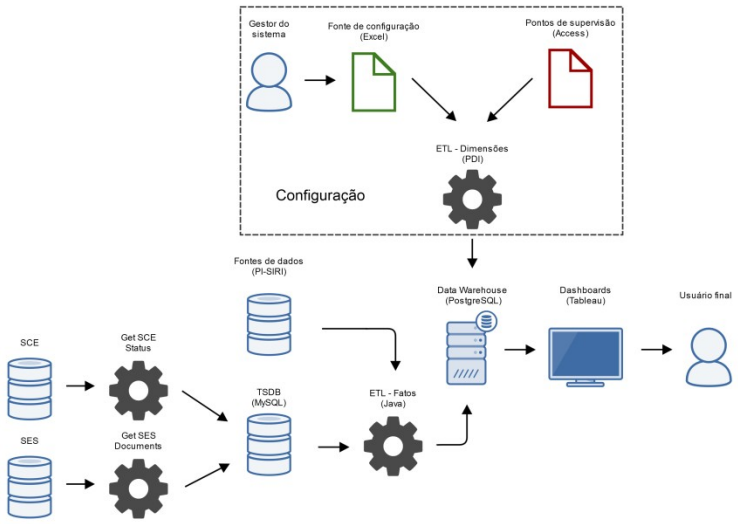


Fig. 4 Arquitetura do sistema SOP

## 2.4. PESOS E FORMAÇÃO DOS CÁLCULOS

### 2.4.1. Formação dos Indicadores de Nível Hierárquico 6

O valor do indicador dos elementos do nível 6 é calculado em função dos alarmes no sistema Scada. Cada elemento do nível 6 está associado a uma prioridade específica de alarmes, por exemplo: “Alarmes de Prioridade 3”.

O valor numérico atribuído ao indicador segue o seguinte critério:

- 100% caso não exista nenhuma indicação na respectiva prioridade;
- 0% caso exista alguma indicação na respectiva prioridade.

Cada prioridade de alarmes tem associado um peso, que é utilizado para compor uma média ponderada que resulta no valor do indicador dos elementos do nível hierárquico imediatamente acima (nível 5). Atualmente os pesos seguem a configuração abaixo:

- Alarmes de Prioridade 1 (bloqueios): 0,55
- Alarmes de Prioridade 2 (bloqueios não impeditivos): 0,50
- Alarmes de Prioridade 3 (alarmes impeditivos): 0,20
- Alarmes de Prioridade 4 (alarmes urgentes): 0,05
- Alarmes de Prioridade 5 (alarmes ordinários): 0,04
- Alarmes de Prioridade 6 (sistemas computacionais): 0,03

O acionamento de qualquer alarme em quaisquer das categorias acima penalizará o indicador de nível superior (5) no valor da respectiva prioridade. Por exemplo, um alarme urgente (prioridade 4) acionado no sistema de excitação de uma unidade penalizará o “sistema de excitação” no nível 5 em 0,05 pontos, tornando-o 0,95.

### 2.4.2. Formação dos Indicadores de Nível Hierárquico 1, 2, 3 e 5

O valor numérico do indicador para os níveis 1, 2, 3 e 5 (vide figura 3) é calculado proporcionalmente à média ponderada do valor dos indicadores associados aos elementos do nível hierárquico imediatamente abaixo deste, por meio da fórmula:

$$I_j^n = 1 - \sum_k P_k \times (1 - I_k^{n+1}) \quad (1)$$

Onde $I^n_j$ é o valor do indicador, $I_k^{n+1}$ é o valor do indicador para cada um dos elementos do nível inferior e $P_k$ é o peso atribuído a cada um destes.

Ou seja, um elemento qualquer do nível 5 tem seu indicador $I_5$ calculado em função do valor dos $k$ indicadores $I_6$ dos elementos de nível 6 configurados abaixo dele, ponderados pelos respectivos pesos ($P_k$).

### 2.4.3. Formação dos Indicadores de Nível Hierárquico 4

Uma vez que no nível hierárquico 4 estão localizados os equipamentos principais que possuem cadastro de disponibilidade/indisponibilidade, o valor do indicador para estes elementos é calculado levando-se em consideração, prioritariamente, a condição do respectivo elemento no sistema SCE e no sistema SES.

Cada elemento do nível 4 é associado, via configuração, com a respectiva unidade de manutenção utilizada para obter os dados da base do sistemas SCE e SES. O cálculo obedece a uma ordem de prioridades, conforme critérios abaixo:

Critério 1 - Caso o estado do equipamento no SCE indique indisponibilidade, ou unidade geradora parada por conveniência operativa, o valor numérico do indicador é atribuído conforme as seguintes referências:

a) 100% caso o elemento do nível 4 seja uma UG parada por conveniência operativa;
b) 65% caso o elemento do nível 4 esteja em um estado que indica indisponibilidade programada.
c) 35% caso o elemento do nível 4 esteja em um estado que indica indisponibilidade forçada.

Critério 2 – Não sendo atendido o critério 1 (não há cadastro para estado do equipamento) e existindo documentos registrados no sistema de execução de serviços, associados ao elemento do nível 4, o valor numérico do indicador é atribuído:

a) 35% caso exista algum PD urgente em andamento.
b) 65% caso exista algum PD programado em andamento.

Critério 3 - Não sendo atendidos nenhum dos critérios 1 e 2 acima, as indicações oriundas do sistema Scada são levadas em consideração, e o indicador assume valor de 35% caso exista algum alarme de prioridades 1 ou 2, oriundo de qualquer equipamento associado aos elementos hierarquicamente subordinados a este.

Critério 4 - Não sendo atendido nenhum dos critérios 1, 2 ou 3, o cálculo é definido conforme a equação aplicada aos demais níveis hierárquicos. Além disso, são aplicadas penalizações aos indicadores conforme as regras abaixo:

a) Aplica-se um fator de penalidade de 30% para cada serviço urgente em andamento no respectivo elemento do nível 4. O valor mínimo que o indicador do nível 4 atinge por este critério é 40% caso existam 2 ou mais serviços urgente para o equipamento.
b) Aplica-se um fator de penalidade de 10% para cada serviço programado em andamento no respectivo elemento do nível 4. O valor mínimo que o indicador do nível 4 atinge por este critério é 70% caso existam 3 ou mais serviços programados para o equipamento.

### 2.4.4. Interface de Visualização

A interface de visualização do sistema SOP é desenvolvida na ferramenta Tableau®, disponibilizada em plataforma *web*, *tablets* e celulares. A formação dos indicadores do nível mais baixo para o mais alto resulta na interface que pode ser vista na figura 5.

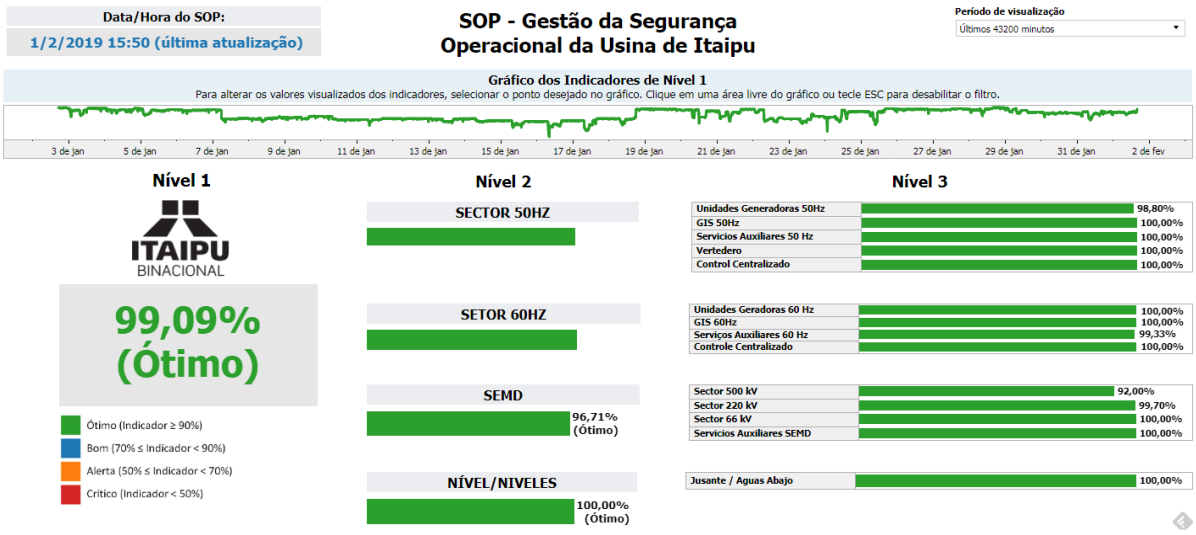


Fig. 5 Interface de visualização do SOP

O indicador também pode ser visualizado em gráfico do tipo polar, conforme figura 6, que representa o estado do indicador de nível 1. Esta visualização contempla os últimos 30 dias, em que é possível verificar o comportamento do indicador SOP, representado pela maneira na qual ele excursiona no gráfico. A cor verde (ótimo) representa a faixa de 90 a 100%, azul (bom) a faixa entre 70 e 90%, laranja (alerta) a faixa entre 50 e 70% e se o indicador excursionar no círculo vermelho o nível do indicador SOP de nível 1 está na condição crítica, entre 0 e 50%.

Tal gráfico é disponível em tablets, celulares e web, garantindo a transparência no processo. Cada vez que o indicador excursiona fora da "zona verde", um estudo específico é disparado para que sejam apontadas as causas do aumento da vulnerabilidade operacional, antes que um incidente ou acidente aconteça.


Fig. 6 Gráfico polar do SOP

## 3. CONCLUSÕES

A gestão proativa da segurança operacional, especialmente útil em Infraestruturas Críticas tais quais a Itaipu Binacional, a auxilia a evitar incidentes graves mesmo que altos fatores de risco e complexidade inerentes a sua operação estejam presentes durante seu ciclo operacional, tornando-a resiliente.

A ferramenta de gestão da Segurança Operacional da Itaipu Binacional (SOP) apresentada tem a intenção de prover uma abordagem proativa da segurança operacional da Itaipu Binacional, focada na operação normal e na análise em tempo real (atualizada a cada 10 minutos) de variáveis e elementos ligados à segurança operacional, de 3 (três) sistemas nos quais tramitam informações de processo e de produto. Além de apresentar vulnerabilidades operacionais que poderiam passar despercebidas cso não houvesse a integração entre os sistemas de execução de serviços, alarmes dos sistemas digitais e estados de equipamentos, provendo ao decisor informações valiosas a respeito da consciência situacional da planta.

Desenvolvida internamente à Itaipu Binacional, utilizou, para isso, a base de conhecimento de quem opera a usina desde 1984, a disponibilidade de mais de 15.000 pontos dos três sistemas citados (execução de serviços, estados de equipamentos e supervisão e controle) e ferramentas que representam o estado da arte em termos de apresentação de visualizações e painéis. Desta forma, cobre toda a instalação (casa de força, barragem principal, vertedouro, subestações, sistemas auxiliares), mostrando o quanto ela está operando de acordo com os requisitos de projeto. Sua metodologia e flexibilidade permitem que o trabalho aqui apresentado seja aplicado em qualquer planta industrial.

Foram analisadas as decisões e estratificações que levaram à formação do indicador, com base nas opiniões estruturadas do staff técnico-operacional e os preceitos, técnicas e heurísticas de business intelligence, considerando a integração entre várias fontes de dados.

Os próximos passos serão no sentido de aprimorar metodológica e cientificamente os estudos para aprimorar as definições dos pesos dos elementos que formam os indicadores e, à medida que sejam descobertas novas vulnerabilidades nos processos operacionais, inserirem-nas no processo de formação do indicador. Para isso, foi formado um comitê de estudos e decisão que se reúne regularmente para discutir assuntos pertinentes à segurança operacional da planta.

## 4. REFERÊNCIAS BIBLIOGRÁFICAS

LABAKA, L.; HERNANTES, J.; SARRIEGI, J. M. “Resilience framework for critical infrastructures: An empirical study in a nuclear plant”. *Reliability Engineering and System Safety*, v. 141, p. 92–105, 2015.

SÆTREN, G. B.; LAUMANN, K. “Effects of trust in high-risk organizations during technological changes”. *Cognition, Technology and Work*, v. 17, n. 1, p. 131–144, 2014.

HASSAN, J.; KHAN, F. “Risk-based asset integrity indicators”. *Journal of Loss Prevention in the Process Industries*, v. 25, n. 3, p. 544–554, 2012.

AZADEH, A. et al. “Assessment of resilience engineering factors in high-risk environments by fuzzy cognitive maps: A petrochemical plant”. *Safety Science*, v. 68, p. 99–107, out. 2014.

HALE, A.; HEIJER, T. “Defining Resilience”. In: HOLLNAGEL, E.; WOODS, D. D.; LEVESON, N. G. (Eds.). *Resilience Engineering: Concepts and Precepts*. 1. ed. Burlington: Ashgate, 2006. p. 35–40.

HOLLNAGEL, E.; WEARS, R. L.; BRAITHWAITE, J. “From Safety-I to Safety-II: A White Paper”. *Network Manager*, p. 43, 2015.

PORTELA J.C., DE MACEDO GUIMARÃES L.B. (2019) A Safety-II Approach on Operational Maneuvers of a Hydropower Plant. In: BAGNARA S., TARTAGLIA R., ALBOLINO S., ALEXANDER T., FUJITA Y. (eds). *Proceedings of the 20th Congress of the International Ergonomics Association (IEA 2018). Advances in Intelligent Systems and Computing*, vol 819. Springer.