WHITEPAPER

CHERNOBYL: ERRO HUMANO, FALHA DE PROJETO OU FALHA DE GOVERNANÇA?

Entenda por que Chernobyl não pode ser reduzido a erro humano e como falhas de projeto, regulação, comunicação, cultura de segurança e governança se combinaram.

A3A® Engenharia de Sistemas

SUMÁRIO

O acidente no **Reator 4 da usina nuclear de Chernobyl** costuma ser resumido em uma pergunta aparentemente simples: foi erro humano ou falha de projeto?

A resposta técnica é mais complexa. Chernobyl não cabe em uma única causa. A sequência que destruiu o Reator 4 envolveu decisões operacionais, características perigosas do projeto RBMK, cultura de segurança insuficiente, comunicação deficiente entre organizações técnicas, pressão por continuidade operacional e fragilidades de governança.

Por isso, talvez a pergunta mais adequada seja outra: **como um sistema crítico pôde permitir que tantas barreiras falhassem em sequência?**

Este artigo aprofunda o eixo de governança da série Chernobyl. Nos textos anteriores, explicamos o que aconteceu em Chernobyl, como funcionava o reator RBMK, a cronologia da noite do acidente, por que o AZ-5 não impediu a explosão e por que a queda de potência para 30 MWt continua tecnicamente inconclusiva.

Agora, vamos olhar para o acidente como um caso de engenharia, gestão de risco e governança técnica.

Uma análise sistêmica precisa distinguir pelo menos cinco camadas: **mecanismos físicos**, que explicam como o transiente se desenvolveu; **decisões operacionais**, que definiram o estado do reator; **decisões de projeto**, que determinaram margens e respostas de proteção; **controles organizacionais**, que deveriam impedir condições inaceitáveis; e **governança institucional**, responsável por transformar conhecimento técnico em requisitos, correções e autoridade de parada.

Governança, portanto, não é uma causa física concorrente ao coeficiente de vazio ou às hastes. É a camada que deveria garantir que riscos conhecidos fossem comunicados, registrados, tratados e impedidos de alcançar a operação.

Gestão de Requisitos, Evidências e Critérios de Aceite

Riscos críticos precisam ser convertidos em requisitos rastreáveis, limites verificáveis, evidências de atendimento e critérios formais de interrupção.

Conheça a solução de Gestão de Requisitos

1. A PERGUNTA CRUCIAL: FOI FALHA HUMANA?

Em grandes acidentes de engenharia, a busca por um culpado único costuma ser uma resposta emocionalmente satisfatória, mas tecnicamente pobre. Sistemas críticos raramente falham por um único ato isolado. Eles falham quando várias camadas de proteção deixam de cumprir sua função.

No caso de Chernobyl, houve ações operacionais inadequadas, violações de procedimentos e decisões tomadas em uma condição de risco crescente. Mas parar a análise nesse ponto distorce o problema.

O **INSAG-7**, relatório da Agência Internacional de Energia Atômica que atualizou a análise inicial do acidente, mudou o peso dessa interpretação. A narrativa inicial, fortemente concentrada em erro operacional, foi revisada para incorporar falhas de projeto, deficiências de comunicação, baixa cultura de segurança e limitações institucionais.

Essa mudança é essencial: Chernobyl não foi apenas a história de operadores conduzindo mal um teste. Foi a história de um sistema que permitiu que um teste crítico fosse conduzido com margens degradadas, informações incompletas e barreiras de segurança insuficientes.

2. A NARRATIVA INICIAL: O PESO COLOCADO NOS OPERADORES

Logo após o acidente, a explicação apresentada internacionalmente enfatizava uma combinação improvável de violações de instruções e regras operacionais. Essa leitura aparecia no contexto do INSAG-1, elaborado com base nas informações soviéticas disponíveis logo após o acidente.

O problema é que, naquele momento, muitas informações técnicas ainda eram incompletas, pouco acessíveis ou interpretadas dentro de uma narrativa institucional que favorecia a responsabilização operacional.

Com o avanço das análises, especialmente após novos dados soviéticos e estudos tridimensionais de física de reatores, ficou mais claro que o acidente não poderia ser explicado apenas pelas ações dos operadores. Havia características do RBMK que criavam riscos severos em determinadas condições, e algumas dessas características não eram plenamente compreendidas, comunicadas ou corrigidas.

Isso não elimina a responsabilidade operacional. Mas muda o enquadramento: operadores erraram dentro de um sistema que já carregava vulnerabilidades técnicas e institucionais profundas.

3. O QUE O INSAG-7 MUDOU NA INTERPRETAÇÃO DE CHERNOBYL?

O INSAG-7 é um documento central porque revisa a interpretação inicial do acidente. Ele reconhece que a explicação baseada apenas em violações operacionais era insuficiente e passa a dar mais peso a fatores de projeto e segurança.

Entre os pontos destacados estão:

- o coeficiente de vazio positivo do RBMK;
- as deficiências no projeto das hastes de controle e proteção;
- o efeito positivo inicial do desligamento emergencial;
- a baixa margem operacional de reatividade, a ORM;
- a importância de segurança da ORM mal compreendida;
- a falta de indicação conveniente da ORM para os operadores;
- a ausência de integração adequada da ORM ao sistema de proteção;
- falhas de comunicação entre projetistas, operadores, reguladores e organizações responsáveis.

O documento também é direto ao afirmar que a gravidade do acidente passou a ser associada por muitas análises aos defeitos no desenho das hastes de controle e segurança, combinados com as características físicas do RBMK que permitiam grandes coeficientes positivos de vazio.

Esse é um ponto de virada. A pergunta deixa de ser apenas “por que os operadores continuaram?” e passa a incluir: **por que o projeto permitia uma configuração tão perigosa e por que o sistema de proteção não impedia que ela fosse alcançada?**

A revisão também demonstra a importância da independência técnica. Investigações de acidentes precisam confrontar registros, modelos, procedimentos, decisões de projeto e responsabilidades institucionais sem assumir que a primeira explicação disponível é definitiva.

Auditoria Técnica

Auditorias independentes verificam aderência, evidências, interfaces, riscos e lacunas entre o que foi projetado, documentado, instalado e efetivamente operado.

Conheça o serviço de Auditoria Técnica

4. FALHA DE PROJETO: QUANDO PERFORMANCE E SEGURANÇA ENTRAM EM CONFLITO

O RBMK era um reator de grande potência, projetado para geração elétrica em larga escala. Do ponto de vista de performance, havia escolhas que faziam sentido dentro da lógica de eficiência neutrônica, operação em base load e produção de energia.

Mas algumas dessas escolhas criaram compromissos perigosos para a segurança. O exemplo mais conhecido é o projeto das hastes de controle, com deslocadores de grafite. Como discutimos no artigo sobre o AZ-5, esses deslocadores ajudavam a evitar absorção parasita de nêutrons pela água nos canais de controle quando as hastes estavam retiradas. Em operação normal, essa solução favorecia a eficiência do reator.

O problema é que, em certas condições, o primeiro movimento de inserção das hastes podia deslocar água por grafite antes que a parte absorvedora atuasse de forma eficaz. Como a água absorvia parte dos nêutrons e o grafite moderava nêutrons, essa substituição podia aumentar localmente a reatividade.

Na prática, uma solução de performance criou um comportamento transitório incompatível com a função de segurança. O “freio” não deveria depender de o sistema estar em uma condição favorável para começar a frear.

Essa é uma lição de engenharia aplicável a qualquer infraestrutura crítica: **otimização operacional nunca pode degradar a barreira de segurança em condição-limite**.

5. ORM: UMA VARIÁVEL CRÍTICA QUE NÃO ERA TRATADA COMO BARREIRA DE PROTEÇÃO

A **ORM**, margem operacional de reatividade, era uma variável fundamental no RBMK. Ela não representava simplesmente a quantidade física de hastes inseridas no núcleo, mas uma margem calculada de controle, expressa em número equivalente de hastes totalmente inseridas.

Segundo o INSAG-7, em potência nominal e regime estável, a ORM deveria estar entre 26 e 30 hastes equivalentes. Se caísse para 15, o reator deveria ser desligado imediatamente. Antes do início efetivo do teste, cálculos posteriores indicaram valores muito abaixo desse limite, na ordem de 6 a 8 hastes equivalentes, dependendo da reconstrução utilizada.

O ponto crítico é que a ORM não estava convenientemente disponível para o operador e não estava incorporada de forma adequada ao sistema de proteção. Além disso, sua importância para a segurança foi mal compreendida. Ela era vista principalmente como uma margem para manobra e controle da distribuição de potência, quando na verdade

influenciava fortemente o comportamento do reator frente ao coeficiente de vazio positivo e à inserção das hastes.

Do ponto de vista de governança técnica, isso é grave. Uma variável que define a segurança do sistema não pode ser apenas um parâmetro calculado com dificuldade, sem indicação clara e sem integração efetiva às proteções automáticas.

Em sistemas críticos modernos, a regra deveria ser clara: **se uma variável é crítica para a segurança, ela precisa ser visível, compreendida, registrada, auditável e capaz de acionar barreiras de proteção**.

Também precisa ser apresentada dentro de contexto. Um valor instantâneo sem histórico, qualidade de dado, tendência, estado operacional e relação com outras margens pode produzir falsa segurança. A governança da informação começa na instrumentação, passa pelo cálculo e termina na forma como o dado orienta decisão.

Sistemas SCADA

Historiadores, alarmes, tendências, qualidade de dados e sequência de eventos transformam variáveis dispersas em informação operacional rastreável.

Conheça a solução de Sistemas SCADA

6. PRESSÃO INSTITUCIONAL: ENERGIA, CRONOGRAMA E CULTURA DE METAS

Chernobyl também precisa ser entendido dentro do contexto da União Soviética, da Guerra Fria e de uma cultura institucional fortemente orientada por metas de produção, hierarquia e demonstração de capacidade tecnológica.

Isso não significa dizer que o contexto político, sozinho, causou o acidente. Não causou. Mas ele ajuda a entender o ambiente em que decisões técnicas eram tomadas.

Na noite do acidente, o teste foi adiado porque a rede elétrica ainda precisava da geração da unidade. A operação do Reator 4 não ocorria em um laboratório isolado; ocorria dentro de um sistema elétrico real, com demanda, despacho, pressão por disponibilidade e necessidade de continuidade energética.

Esse atraso é documentalmente verificável. Já a influência mais ampla da pressão política e da cultura de metas deve ser tratada como contexto institucional, não como uma ordem direta registrada para produzir o acidente. O rigor exige separar o que consta nos registros operacionais do que é inferido a partir da estrutura organizacional e do padrão posterior de comunicação.

Além disso, o ambiente soviético tornava mais difícil contestar hierarquias, expor falhas de projeto, interromper atividades críticas ou admitir publicamente limitações técnicas. O INSAG-7 destaca falhas de comunicação e ausência de linhas claras de responsabilidade entre projetistas, engenheiros, fabricantes, construtores, operadores e reguladores.

Esse é o ponto de governança: quando a organização valoriza entrega, produção ou cumprimento de plano acima da segurança técnica, as barreiras passam a depender da coragem individual de alguém dizer “pare”. Em sistemas críticos, isso é inaceitável.

7. OCULTAÇÃO, COMUNICAÇÃO DE RISCO E APRENDIZAGEM TARDIA

Outro elemento essencial é a comunicação. Depois do acidente, informações foram tratadas de forma lenta, incompleta e politicamente sensível. Isso afetou a resposta pública, a percepção internacional e a reconstrução técnica da sequência de eventos.

Mas a comunicação deficiente não começou depois da explosão. Ela já aparecia antes, na forma como informações críticas sobre o projeto do RBMK, o efeito positivo de desligamento emergencial e a importância da ORM foram transmitidas, compreendidas ou incorporadas à operação.

O INSAG-7 registra que o efeito positivo de inserção das hastes havia sido identificado anteriormente em outro RBMK, na usina de Ignalina, em 1983. Havia indicação de que mudanças de projeto seriam feitas para corrigir o problema, mas as medidas não foram implementadas de forma suficiente antes do acidente em Chernobyl.

Essa é uma das lições mais duras do caso: uma falha conhecida, quando não é tratada com prioridade, deixa de ser um problema técnico e se torna uma falha de governança.

8. HOUVE PUNIÇÃO? SIM, MAS A RESPONSABILIZAÇÃO FOI LIMITADA

É importante tratar esse ponto com cuidado. Após o acidente, houve responsabilização criminal de operadores e gestores locais. A narrativa pública inicial concentrou grande peso nas ações da equipe da usina.

Mas essa responsabilização não esgotava o problema. A análise técnica posterior mostrou que falhas de projeto, cultura de segurança, comunicação institucional e governança tiveram papel central. Em outras palavras, a punição de pessoas envolvidas na operação não significou que o sistema institucional responsável pelas vulnerabilidades tivesse sido plenamente responsabilizado desde o início.

Essa distinção é importante para qualquer análise de acidentes: responsabilizar indivíduos pode ser necessário, mas é insuficiente quando o sistema como um todo produziu as condições para a falha.

9. FALHA DE GOVERNANÇA: QUEM TINHA AUTORIDADE PARA PARAR?

A pergunta central em sistemas críticos não é apenas “quem fez?”, mas também “quem poderia interromper?”

Em Chernobyl, várias perguntas de governança aparecem:

- quem aprovou o programa do teste?
- quem avaliou suas implicações nucleares e não apenas elétricas?
- quem validou os critérios de segurança?
- quem tinha autoridade para abortar o teste quando a potência caiu para 30 MWt?
- quem garantia que a ORM estivesse dentro de limite seguro?
- quem comunicou aos operadores o risco do efeito positivo do AZ-5?
- quem deveria impedir a operação em uma configuração proibitiva?
- quem integrava projeto, operação, segurança e regulação?

Quando essas respostas não são claras, a segurança depende de improviso. E improviso é incompatível com sistemas críticos.

O PMBOK, em sua abordagem baseada em princípios, reforça a importância de governança, responsabilidade, partes interessadas, planejamento, qualidade, riscos, complexidade e adaptação ao contexto. Aplicado a sistemas críticos, isso significa que decisões técnicas precisam ter donos claros, critérios de aceitação, trilhas de aprovação, gestão de riscos e autoridade formal para interromper atividades inseguras.

Chernobyl mostra o que acontece quando engenharia, operação, política, regulação e gestão não formam um sistema de decisão seguro.

Em um arranjo robusto, a autoridade para interromper não pode depender apenas da hierarquia operacional imediata. Deve existir revisão independente, segregação entre quem produz e quem aceita a evidência, critérios de escalonamento e proteção institucional para decisões conservadoras de segurança.

Owner’s Engineering

A Engenharia do Proprietário cria uma camada independente entre contratantes, projetistas, fornecedores e operação para revisar premissas, riscos, interfaces e critérios de aceite.

Conheça o serviço de Owner’s Engineering

10. O TESTE NÃO ERA “APENAS ELÉTRICO”

Um dos pontos mais importantes do INSAG-7 é a crítica à classificação do teste como puramente elétrico. O teste de *rundown* envolvia a alimentação de bombas principais, circuitos de energia, sistemas de proteção e intertravamentos. Portanto, tinha implicações diretas sobre a segurança nuclear.

Essa é uma falha clássica de interface: uma atividade aparentemente pertencente a uma disciplina técnica afeta outra disciplina crítica. Em projetos complexos, muitos acidentes nascem justamente nas interfaces.

Em um projeto moderno, um teste desse tipo exigiria matriz de riscos, análise multidisciplinar, validação por segurança, critérios de abortagem, simulação de cenários, plano de comissionamento, aprovação formal e registro detalhado de pré-condições.

Quando uma atividade que afeta segurança nuclear é tratada como teste elétrico, a governança falhou antes do teste começar.

Além disso, uma aprovação não permanece válida indefinidamente. Mudança de turno, atraso de várias horas, alteração da potência, redução de margens ou indisponibilidade de sistemas exigem nova verificação das pré-condições. Prosseguir com base em uma autorização emitida para outro cenário transforma o plano de teste em formalidade.

Comissionamento e Aceite Técnico

Testes integrados precisam de pré-condições verificadas, matriz de responsabilidades, critérios de abortagem, registros sincronizados e aceite baseado em evidências.

Conheça o serviço de Comissionamento e Aceite Técnico

11. O QUE CHERNOBYL ENSINA SOBRE ENGENHARIA CONSULTIVA?

Chernobyl é um estudo extremo, mas suas lições valem para sistemas críticos modernos. Subestações, data centers, usinas, centros de operação, hospitais, redes industriais e sistemas de telecomunicações também dependem de projeto, operação, supervisão, testes, documentação e governança.

Em todos esses ambientes, não basta que o sistema funcione em operação normal. Ele precisa responder corretamente em transições, falhas parciais, perda de alimentação,

mudança de modo, operação degradada e emergência.

É nesse ponto que entram práticas de Owner's Engineering, FEL, EPCM, comissionamento, auditoria técnica e due diligence técnica.

Essas práticas ajudam o dono do ativo a fazer perguntas que precisam ser respondidas antes da operação:

- quais variáveis são críticas para segurança?
- essas variáveis são visíveis e registradas?
- os testes cobrem transições reais de operação?
- os sistemas de proteção foram validados em condição degradada?
- as interfaces entre disciplinas foram revisadas?
- quem pode interromper uma atividade insegura?
- os riscos estão documentados e aceitos formalmente?
- a operação recebeu treinamento suficiente?

Essas perguntas são tão importantes quanto o cálculo, o desenho ou o equipamento.

12. DE CHERNOBYL ÀS INFRAESTRUTURAS CRÍTICAS ATUAIS

A discussão sobre Chernobyl também dialoga com sistemas de supervisão e controle modernos. Em subestações e instalações críticas, soluções como SCADA no setor elétrico, teleassistência em subestações, monitoramento de chaves seccionadoras e projeto de telecomunicações para subestações existem justamente para ampliar visibilidade operacional, registrar eventos, permitir diagnóstico e apoiar decisões seguras.

Mas tecnologia de supervisão sozinha não resolve governança. Dados precisam ser interpretáveis. Alarmes precisam ter hierarquia. Proteções precisam atuar automaticamente quando limites críticos são violados. Operadores precisam entender o significado das variáveis. Gestores precisam respeitar critérios de parada.

A segurança de sistemas críticos é resultado de arquitetura técnica e cultura organizacional. Uma sem a outra é insuficiente.

13. ENTÃO, CHERNOBYL FOI ERRO HUMANO, FALHA DE PROJETO OU FALHA DE GOVERNANÇA?

Foi uma combinação dos três — mas a expressão "erro humano" precisa ser usada com cuidado.

Houve decisões operacionais inadequadas. Houve violação de limites. Houve continuidade do teste em condição perigosa. Mas também havia um reator com características de projeto perigosas, um sistema de proteção com comportamento inicial desfavorável em certas condições, uma variável crítica de segurança pouco visível, procedimentos insuficientes e falhas de comunicação entre organizações técnicas.

Acima de tudo, havia falha de governança: o sistema não impediu que uma condição perigosa fosse alcançada, não tornou variáveis críticas suficientemente visíveis, não corrigiu vulnerabilidades conhecidas com urgência e não estruturou autoridade clara para interromper o risco.

Por isso, o veredito técnico mais robusto é:

Chernobyl foi uma falha sistêmica de engenharia, operação e governança. O erro humano existiu, mas não explica sozinho o acidente. O projeto criou vulnerabilidades; a operação levou o reator a uma condição crítica; e as estruturas de governança não impediram que riscos conhecidos, margens degradadas e decisões de continuidade se combinassem.

14. CONCLUSÃO: A PRINCIPAL FALHA FOI SISTÊMICA

A grande lição de Chernobyl não é apenas que operadores podem errar. A lição é que sistemas críticos precisam ser projetados, testados, operados e governados considerando que pessoas erram, pressões existem, sinais são mal interpretados e condições degradadas acontecem.

Um sistema seguro não depende de perfeição humana. Ele cria barreiras para que erros não se transformem em catástrofes. Ele torna variáveis críticas visíveis. Ele impede configurações proibitivas. Ele testa transições. Ele registra decisões. Ele corrige vulnerabilidades conhecidas. Ele dá autoridade real para interromper atividades inseguras.

Chernobyl mostra o custo de quando isso não acontece.

Para a engenharia consultiva, esse é o ponto central: em projetos críticos, segurança não é um item a ser verificado no final. Segurança é uma arquitetura de decisões, requisitos, testes, responsabilidades e governança desde o início.

Para continuar a jornada, o leitor pode revisar a arquitetura do RBMK e avançar para as modificações implementadas nos reatores RBMK depois do acidente, quando os riscos reconhecidos foram finalmente convertidos em mudanças de projeto, proteção e regras operacionais.

[1] INTERNATIONAL ATOMIC ENERGY AGENCY. *The Chernobyl Accident: Updating of INSAG-1*. Safety Series No. 75-INSAG-7. Vienna: IAEA, 1992.

[2] SHTEYNBERG, N. A. et al. Causes and circumstances of the accident at Unit 4 of the Chernobyl Nuclear Power Plant. In: INTERNATIONAL ATOMIC ENERGY AGENCY. *INSAG-7*, Annex I. Vienna: IAEA, 1992.

[3] ABAGYAN, A. A. et al. Causes and circumstances of the accident and measures to improve the safety of plants with RBMK reactors. In: INTERNATIONAL ATOMIC ENERGY AGENCY. *INSAG-7*, Annex II. Vienna: IAEA, 1992.

[4] UNITED STATES NUCLEAR REGULATORY COMMISSION. *Report on the Accident at the Chernobyl Nuclear Power Station*. NUREG-1250. Washington, DC: NRC, 1987.

[5] UNITED STATES NUCLEAR REGULATORY COMMISSION. *Implications of the Accident at Chernobyl for Safety Regulation*. NUREG-1251. Washington, DC: NRC, 1987.

[6] INTERNATIONAL NUCLEAR SAFETY ADVISORY GROUP. *Safety Culture*. INSAG-4. Vienna: IAEA, 1991.

[7] INTERNATIONAL ATOMIC ENERGY AGENCY. *RBMK Reactors*. Technical description and safety characteristics of pressure-tube graphite-moderated reactors.

[8] CHERNOBYL NUCLEAR POWER PLANT. *Sequence of events at Unit 4 on 25–26 April 1986*. Technical chronology compiled from operating records.

[9] MUELLNER, Nikolaus. *Three Decades after Chernobyl: Technical and Institutional Lessons*. Vienna: University of Natural Resources and Life Sciences.

[10] PROJECT MANAGEMENT INSTITUTE. *A Guide to the Project Management Body of Knowledge — PMBOK Guide*. 7th ed. Newtown Square: PMI, 2021.

Chernobyl foi causado por erro humano?Houve decisões operacionais inadequadas, mas elas não explicam o acidente isoladamente. O INSAG-7 atribui peso relevante a falhas de projeto, comunicação, cultura de segurança e governança. **Qual foi o papel das falhas de projeto?**O coeficiente de vazio positivo, o desenho das hastes, a baixa visibilidade da ORM e proteções insuficientes permitiram que uma configuração vulnerável fosse alcançada. **O que o INSAG-7 mudou na interpretação do acidente?**O documento revisou a narrativa inicialmente concentrada nos operadores e passou a enfatizar deficiências de projeto, comunicação, regulação e cultura de segurança. **A pressão política causou Chernobyl?**Não como causa única. O contexto institucional influenciou prioridades, transparência, hierarquia e capacidade de contestação, mas o acidente resultou da

interação entre fatores técnicos e organizacionais. **O que caracteriza uma falha de governança técnica?**Responsabilidades pouco claras, riscos conhecidos sem tratamento, ausência de autoridade efetiva para interromper, critérios de aceite frágeis e comunicação deficiente entre projeto, operação e regulação. **Por que o teste não era apenas elétrico?**Porque alterava alimentação de bombas, intertravamentos, proteções e condições térmico-hidráulicas diretamente relacionadas à segurança do núcleo. **O efeito positivo das hastes era conhecido antes de 1986?**Sim. O fenômeno havia sido identificado em outro RBMK em 1983, mas não foi convertido a tempo em correções completas de projeto, proteção e procedimentos. **Qual é a principal lição para infraestruturas críticas atuais?**Segurança exige arquitetura técnica, governança, independência de revisão, dados confiáveis, critérios formais de interrupção e validação integrada das interfaces.

Soluções

- Gestão de Requisitos, Evidências e Critérios de Aceite
- Sistemas SCADA
- Sistemas Digitais de Supervisão e Controle

Serviços de engenharia

- Owner’s Engineering
- Auditoria Técnica
- Comissionamento e Aceite Técnico
- Front-End Loading

Jornada sobre Chernobyl

- Chernobyl: o que aconteceu e por que o Reator 4 explodiu
- Teste do Reator 4: cronologia dos segundos finais
- AZ-5 e desligamento emergencial
- ORM e margem de reatividade
- Coeficiente de vazio positivo
- O que mudou nos RBMK depois do acidente

Sobre a A3A Engenharia de Sistemas

Com 30 anos de história, a A3A Engenharia de Sistemas se consolidou como referência em serviços de Engenharia, oferecendo soluções integradas de Telecomunicações, Segurança Eletrônica, Segurança Digital e Instalações Elétricas.

A empresa atua em todas as etapas do ciclo de Engenharia, desde a elaboração de projetos e consultoria técnica até a implantação, manutenção e retrofit de sistemas, sempre em conformidade com as normas técnicas e melhores práticas do setor.

A3A® Engenharia de Sistemas