WHITEPAPER

SISTEMA DE DETECÇÃO DE INTRUSÃO EM SUBESTAÇÕES: SENSORES, ZONAS E ALARMES

Entenda como projetar detecção de intrusão em subestações: sensores, zonas, central, alimentação, integração, alarmes indesejados e comissionamento.

A3A® Engenharia de Sistemas

SUMÁRIO

Um **sistema de detecção de intrusão em subestações** precisa identificar acessos indevidos, violações e condições anormais com rapidez suficiente para apoiar uma resposta segura. Isso exige mais do que instalar sensores e conectar zonas a uma central: o projeto deve relacionar riscos, áreas supervisionadas, estados operacionais, alimentação, transmissão, integração e procedimentos.

Em uma subestação, o sistema pode supervisionar a casa de controle, salas técnicas, depósitos, acessos, portões e pontos vulneráveis associados ao perímetro. A arquitetura deve conviver com ambientes eletromagnéticos severos, instalações remotas, períodos sem presença permanente e atividades autorizadas de operação e manutenção.

O sistema de intrusão não substitui a barreira física, o controle de acesso ou o videomonitoramento. Sua função é acrescentar uma camada de detecção e sinalização, produzindo eventos rastreáveis para que a ocorrência seja verificada e tratada.

1. O QUE É UM SISTEMA DE DETECÇÃO DE INTRUSÃO

Um sistema de detecção de intrusão reúne detectores, contatos, interfaces, central de controle e sinalização, fontes de alimentação, meios de comunicação e dispositivos de aviso. Quando uma zona supervisionada muda de estado, o sistema processa o evento conforme sua programação e gera sinalizações locais ou remotas.

A arquitetura deve distinguir pelo menos quatro tipos de informação: intrusão, violação do próprio sistema, falha técnica e operação autorizada. Um contato de porta aberto durante uma janela de manutenção não possui o mesmo significado que a mesma abertura durante o período armado. Da mesma forma, a remoção de uma tampa, a perda de comunicação ou a baixa tensão da bateria não devem ser tratadas como simples alarmes de presença.

A série ABNT NBR IEC 62642 organiza requisitos para sistemas contra intrusão e roubo, incluindo funções, graus de segurança, classes ambientais, supervisão, registro de eventos e alimentação. A Parte 1 é voltada principalmente aos sistemas instalados em edificações; aplicações externas e perimetrais exigem critérios complementares de projeto e especificação.

2. ESTUDO DE RISCO, GRAU DE SEGURANÇA E CLASSE AMBIENTAL

A seleção do sistema começa pelo estudo da instalação. Devem ser avaliados os ativos, os caminhos de aproximação, a ocupação, o histórico de ocorrências, a presença de equipes, o tempo de resposta e as consequências de uma intrusão.

A ABNT NBR IEC 62642-1 estabelece quatro graus de segurança. Esses graus representam níveis crescentes de capacidade esperada do intruso e de resistência do sistema. Não existe um grau universal para toda subestação: a definição precisa ser documentada a partir do risco, das exigências do proprietário e das condições operacionais.

A mesma lógica vale para as classes ambientais. Equipamentos instalados em sala climatizada enfrentam condições diferentes daqueles montados em áreas abrigadas, fachadas, portões ou ambientes expostos. Temperatura, umidade, poeira, água, radiação solar, corrosão, vibração e interferência eletromagnética precisam ser considerados na especificação.

Um erro recorrente é selecionar o detector pelo alcance nominal e ignorar o ambiente. Em subestações, o desempenho pode ser afetado por superfícies metálicas, calor, vegetação, tráfego, animais, chuva, vento, estruturas vibrantes e campos eletromagnéticos. O equipamento deve ser adequado ao local e instalado conforme as limitações documentadas pelo fabricante.

3. ZONAS, ESTADOS E LÓGICA DE OPERAÇÃO

O sistema deve dividir a instalação em zonas coerentes com o risco e com os procedimentos. Casa de controle, sala de relés, sala de telecomunicações, banco de baterias, depósito, portão e acessos externos podem exigir tratamentos distintos.

A setorização permite identificar onde ocorreu o evento, aplicar horários diferentes e realizar manutenção sem desativar toda a proteção. Também facilita a apresentação automática de câmeras, a distribuição de responsabilidades e a análise de recorrências.

Os estados de ativação e desativação precisam ser definidos com clareza. Em locais remotos, determinadas áreas podem permanecer permanentemente supervisionadas, enquanto outras acompanham a presença de equipes. Funções de inibição, isolação ou sobreposição devem depender de autorização, motivo registrado e prazo controlado.

A lógica operacional deve responder a perguntas objetivas: quem pode armar ou desarmar, quais zonas podem ser isoladas, por quanto tempo, como a anormalidade será sinalizada e quem deve aprovar o retorno à condição normal. Sem essas regras, o sistema tende a acumular zonas anuladas e perder confiabilidade.

4. SENSORES DE INTRUSÃO E APLICAÇÕES

A tecnologia deve ser escolhida conforme o fenômeno que precisa ser detectado. Um único tipo de sensor raramente cobre portas, janelas, salas, corredores, fachadas e áreas externas com o mesmo desempenho.

TecnologiaAplicação típicaPontos de atençãoContato magnéticoportas, portões, tampas e janelasalinhamento, folgas, tipo de esquadria e proteção da fiaçãoInfravermelho passivomovimento em ambientes internosfontes de calor, incidência solar, correntes de ar e obstruçõesDupla tecnologiaáreas internas com maior risco de alarmes indesejadoslógica de confirmação, posicionamento e cobertura realQuebra de vidrofachadas e aberturas envidraçadastipo de vidro, acústica e distância de instalaçãoVibração ou sísmicoparedes, cofres, estruturas e pontos sujeitos a ataque mecânicovibrações normais da instalação e calibraçãoBarreira infravermelha ativacorredores, acessos e trechos linearesalinhamento, neblina, vegetação, animais e estabilidade das basesSensor de cerca ou cabointegração com o perímetrosetorização, condição da cerca, vento e manutenção da vegetação

Sensores internos devem considerar a atividade normal do local. Painéis, ventilação, portas técnicas, equipamentos móveis e equipes de manutenção podem alterar o ambiente. O projeto deve prever cobertura sem criar áreas cegas, mas também sem sobrepor detectores de forma indiscriminada.

Barreiras infravermelhas e sensores de cerca podem participar da solução, porém sua aplicação externa precisa ser coordenada com o projeto de **proteção perimetral em subestações**. Nesse caso, o foco deixa de ser somente o detector e passa a incluir terreno, barreiras físicas, setores, iluminação, verificação por vídeo e resposta.

5. CENTRAL, SUPERVISÃO E REGISTRO DE EVENTOS

A central recebe sinais, processa estados, controla partições, registra operações e inicia notificações. Sua capacidade deve ser analisada por número de zonas, áreas, usuários, interfaces, saídas, memória, comunicação e possibilidade de expansão.

A supervisão deve permitir diferenciar alarme, sabotagem, circuito aberto, curto, falha de comunicação, perda da fonte principal e problema na bateria. Linhas sem supervisão ou entradas programadas de forma genérica reduzem a capacidade de diagnóstico e podem ocultar falhas.

A proteção contra violação é relevante para detectores, caixas, fontes, módulos e central. Abertura de tampa, remoção da base ou intervenção na interconexão deve produzir evento

compatível com o grau e com a arquitetura adotados.

O registro precisa preservar data, hora, origem, usuário e ação realizada. Ativações, desativações, isolamentos, testes, falhas, reconhecimentos e restabelecimentos formam a trilha necessária para auditoria e manutenção.

6. ALIMENTAÇÃO, AUTONOMIA E DISPONIBILIDADE

A fonte de alimentação faz parte do desempenho do sistema. A ABNT NBR IEC 62642-6 trata de requisitos para fontes utilizadas em sistemas contra intrusão, incluindo monitoramento, armazenamento de energia, comutação, recarga e proteção.

O dimensionamento deve considerar a carga em condição normal e em alarme, módulos, interfaces, comunicadores, sirenes e dispositivos externos. A autonomia não deve ser definida apenas pela capacidade nominal da bateria: entram no cálculo consumo, envelhecimento, temperatura, margem, tempo de recarga e requisitos do grau de segurança.

Perda da alimentação principal, baixa tensão, falha do dispositivo de armazenamento e falha da unidade de alimentação precisam ser detectadas e sinalizadas. A simples presença de uma bateria dentro da caixa não comprova disponibilidade.

Em subestações, a solução deve ser coordenada com os serviços auxiliares, UPS, proteção contra surtos, aterramento e separação de circuitos. Interfaces longas e equipamentos externos exigem atenção especial a transitórios, diferenças de potencial e compatibilidade eletromagnética.

7. TRANSMISSÃO DE ALARMES E RESPOSTA OPERACIONAL

Um alarme somente produz valor quando chega ao responsável com contexto e dentro do tempo previsto. A arquitetura pode utilizar comunicação local, rede IP, enlace dedicado, rede móvel ou combinações, conforme disponibilidade e criticidade.

A perda do caminho de comunicação deve ser supervisionada. Para locais remotos, convém avaliar caminhos alternativos, armazenamento local, repetição de eventos e sincronização após recuperação. A redundância precisa ser real; dois serviços que compartilham a mesma infraestrutura física podem falhar juntos.

O evento deve indicar instalação, setor, zona, tipo, horário e estado. Alarmes genéricos obrigam o operador a investigar sem informação suficiente e aumentam o tempo de resposta.

O procedimento operacional define quem recebe, como confirma, quais imagens consulta, quando aciona uma equipe e como registra o encerramento. Sirenes podem integrar a solução, mas não substituem a transmissão, a verificação e a resposta organizada.

8. INTEGRAÇÃO COM CFTV, ACESSO E PROTEÇÃO PERIMETRAL

A integração deve conectar eventos relacionados sem misturar responsabilidades. Um alarme de porta pode apresentar a câmera do acesso, consultar o evento do controle de acesso e destacar a zona no mapa. Um disparo perimetral pode direcionar câmeras fixas ou PTZ para a área correspondente.

O videomonitoramento permite verificar contexto, mas não deve ser tratado como confirmação automática em qualquer condição. Iluminação, enquadramento, clima, vegetação, latência e indisponibilidade podem limitar a imagem.

O controle de acesso informa credencial, usuário, horário e decisão de liberação. A detecção de intrusão informa mudança de estado, violação ou falha. A correlação entre ambos permite diferenciar uma passagem autorizada de uma abertura forçada, mas depende de integração projetada e testada.

A matriz de causa e efeito deve documentar quais eventos geram vídeo, gravação prioritária, notificação, saída física, mensagem ao operador ou escalonamento. Automações sem limites podem produzir cascatas de eventos e dificultar a operação.

9. ALARMES INDESEJADOS E DESEMPENHO REAL

Alarmes indesejados reduzem a confiança do operador e levam à desativação informal de zonas. Por isso, a ABNT IEC/TS 62642-7 trata o estudo do local, as influências internas e externas, o planejamento, o comissionamento e a manutenção como partes do desempenho.

Em ambientes internos, as causas podem incluir correntes de ar, variações térmicas, equipamentos suspensos, vibração, insetos, animais, reflexos, portas com folga e alterações no layout. Em áreas externas, vegetação, chuva, neblina, vento, aves, tráfego, obras e incidência solar exigem atenção.

A resposta não deve ser simplesmente aumentar a sensibilidade ou acrescentar sensores. É necessário identificar o fenômeno, revisar localização, suporte, máscara, tecnologia, lógica de confirmação e condição ambiental.

Indicadores úteis incluem alarmes por zona, reincidência, falhas, tempo de indisponibilidade e quantidade de isolamentos. Esses dados ajudam a distinguir defeito, parametrização inadequada, mudança ambiental e problema de procedimento.

10. CIBERSEGURANÇA E SISTEMAS CONECTADOS

Centrais e comunicadores conectados à rede precisam ser tratados como ativos de tecnologia. Contas padrão, senhas compartilhadas, serviços desnecessários, acesso remoto permanente e firmware desatualizado ampliam a superfície de risco.

A arquitetura deve prever segmentação, autenticação individual, perfis mínimos, registros, backup de configuração, sincronismo de horário e processo controlado de atualização. O acesso remoto deve utilizar canais protegidos e ser limitado às funções necessárias.

Integrações com VMS, plataformas de gestão ou centros remotos devem ser documentadas. A indisponibilidade de uma integração não pode impedir as funções essenciais locais da central, quando a arquitetura exigir autonomia.

A cibersegurança também envolve fornecedores e ciclo de vida. É importante avaliar política de atualização, divulgação de vulnerabilidades, suporte, exportação de configurações e capacidade de substituir componentes sem perder rastreabilidade.

11. PROJETO, COMISSIONAMENTO E MANUTENÇÃO

A ABNT IEC/TS 62642-7 organiza o ciclo desde o estudo do local até operação e manutenção. O projeto deve produzir planta de zonas e detectores, diagrama de arquitetura, memória de alimentação, matriz de causa e efeito, descrição dos estados, lista de equipamentos, requisitos de comunicação e critérios de aceite.

No comissionamento, cada sensor deve ser testado na condição real de aplicação. Devem ser verificados alcance, direção, tempo de resposta, identificação da zona, violação, falha, transmissão, registro e integração.

Os testes também precisam simular perda da fonte principal, bateria baixa, interrupção de comunicação, abertura de caixa, isolamento autorizado e recuperação. A entrega deve incluir as-built, programação, backups, cadastro de usuários, instruções, registro de pendências e treinamento.

A manutenção precisa combinar inspeção física, testes funcionais, análise de eventos, limpeza, alinhamento, verificação de baterias, revisão de vegetação e atualização controlada. Mudanças na instalação podem invalidar uma cobertura que funcionava

corretamente no aceite inicial.

12. ERROS COMUNS EM PROJETOS DE DETECÇÃO DE INTRUSÃO

O primeiro erro é usar a solução perimetral como sinônimo de sistema de intrusão. A barreira externa é uma camada; portas, salas, equipamentos, central, alimentação e transmissão formam outras.

Outro problema é concentrar todas as áreas em poucas zonas. Isso reduz o contexto do evento e dificulta manutenção, correlação com câmeras e análise de recorrência.

Também é comum instalar detectores externos sem estudo ambiental, aceitar circuitos sem supervisão adequada, ignorar a alimentação de módulos remotos e cadastrar mensagens genéricas na central.

Por fim, sistemas tecnicamente funcionais podem falhar operacionalmente quando não há procedimento, responsável, teste periódico ou controle sobre zonas isoladas.

13. CONCLUSÃO

O sistema de detecção de intrusão em subestações deve ser projetado como uma cadeia: risco, zona, detector, central, alimentação, comunicação, integração e resposta. A qualidade do resultado depende da coerência entre essas etapas.

A série ABNT NBR IEC 62642 oferece uma base importante para requisitos, alimentação e diretrizes de aplicação. Entretanto, cada instalação precisa transformar essa base em critérios compatíveis com seus ambientes internos, interfaces externas, regime operacional e capacidade de resposta.

Quando o sistema registra eventos com precisão, supervisiona suas próprias falhas, mantém disponibilidade e entrega contexto ao operador, a detecção deixa de ser um conjunto de sensores e passa a funcionar como parte efetiva da proteção da subestação.

[1] ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR IEC 62642-1: Sistemas de alarme — Sistemas de alarme contra intrusão e roubo — Parte 1: Requisitos do sistema. Consultar edição vigente aplicável no Catálogo ABNT.

[2] ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR IEC 62642-6: Sistemas de alarme — Sistemas de alarme contra intrusão e roubo — Parte 6: Fontes de alimentação. Consultar edição vigente aplicável no Catálogo ABNT.

[3] ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT IEC/TS 62642-7: Sistemas de alarme — Sistemas contra intrusão e roubo — Parte 7: Diretrizes de aplicação. Consultar edição vigente aplicável no Catálogo ABNT.

O que é um sistema de detecção de intrusão? É o conjunto de detectores, central, fontes, comunicação e dispositivos de aviso que identifica intrusão, violação e falhas, processando e registrando os eventos conforme a lógica programada.**Detecção de intrusão e proteção perimetral são a mesma coisa?** Não. A proteção perimetral abrange barreiras físicas e eletrônicas externas. O sistema de intrusão também pode supervisionar portas, salas, janelas, equipamentos e áreas internas, além de integrar eventos do perímetro.**Qual grau de segurança deve ser usado em uma subestação?** Não existe um grau único para todas as instalações. A definição deve resultar do estudo de risco, das exigências do proprietário, do ambiente, do valor dos ativos e da capacidade esperada do intruso.**Quais sensores podem ser utilizados?** Contatos magnéticos, infravermelho passivo, dupla tecnologia, quebra de vidro, vibração, barreiras infravermelhas e sensores de cerca são exemplos. A escolha depende do fenômeno, do ambiente e da cobertura necessária.**Como reduzir alarmes falsos em áreas externas?** É necessário avaliar vegetação, animais, vento, chuva, neblina, incidência solar, estabilidade das bases e tráfego. Localização, tecnologia, parâmetros e manutenção devem ser validados no ambiente real.**O sistema precisa funcionar quando a comunicação remota falha?** Quando a arquitetura exige autonomia, a central local deve manter detecção, processamento e registro mesmo durante perda do enlace, transmitindo os eventos após a recuperação conforme a solução projetada.**Como integrar intrusão e CFTV?** Eventos podem apresentar câmeras relacionadas, destacar setores em mapas e iniciar gravação prioritária. A matriz de causa e efeito deve definir cada ação e os procedimentos do operador.**A bateria da central é suficiente para garantir autonomia?** Não necessariamente. A autonomia depende do consumo total, condição de alarme, envelhecimento, temperatura, margem, recarga e requisitos do sistema. O dimensionamento precisa abranger todos os dispositivos alimentados.**O que deve ser testado no comissionamento?** Detectores, zonas, violação, falhas, alimentação, bateria, comunicação, transmissão, registros, integrações, estados de ativação e desativação, recuperação e documentação final.**A ABNT NBR IEC 62642 cobre todo o perímetro externo?** A Parte 1 é voltada principalmente a sistemas instalados em edificações e componentes associados. Sistemas externos e perimetrais exigem especificações complementares de tecnologia, ambiente, infraestrutura e desempenho.

Soluções

- Alarme de Intrusão
- Proteção Perimetral
- Monitoramento Patrimonial

Serviços de engenharia

- Projeto de Sistema Integrado de Segurança Eletrônica

Materiais técnicos

- Cibersegurança em sistemas de CFTV
- Projeto e redução de riscos

Conteúdos correlatos

- Proteção perimetral em subestações
- CFTV patrimonial em subestações
- Controle de acesso em subestações

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