

Universidade Federal de Uberlândia
Faculdade de Engenharia Elétrica

ANA JULIA COSTA SANTANA

**Soluções de Segurança Eletrônica em Usinas Fotovoltaicas: Tecnologias e Estratégias
para Proteção de Infraestruturas Críticas**

Uberlândia – MG
2025

ANA JULIA COSTA SANTANA

Soluções de Segurança Eletrônica em Usinas Fotovoltaicas: Tecnologias e Estratégias para
Proteção de Infraestruturas Críticas

Trabalho de Conclusão de Curso apresentado
à Faculdade de Engenharia Elétrica da
Universidade Federal de Uberlândia, Minas
Gerais, como requisito parcial exigido para
obtenção do título de bacharel em Engenharia
Eletrônica e de Telecomunicações.

Orientador(a): Prof^a.Dr^a. Milena Bueno Pereira
Carneiro

ANA JULIA COSTA SANTANA

Soluções de Segurança Eletrônica em Usinas Fotovoltaicas: Tecnologias e Estratégias para Proteção de Infraestruturas Críticas

Trabalho de Conclusão de Curso apresentado à Faculdade de Engenharia Elétrica da Universidade Federal de Uberlândia, Minas Gerais, como requisito parcial exigido para obtenção do título de bacharel em Engenharia Eletrônica e de Telecomunicações;

Trabalho aprovado em 6 de Maio de 2025.

COMISSÃO EXAMINADORA

Prof.^a Dr.^a Milena Bueno Pereira Carneiro
Orientadora

Prof. Dr. Carlos Eduardo Tavares
Membro Avaliador

Prof. Me. Éder Alves de Moura
Membro Avaliador

Uberlândia – MG
2025

AGRADECIMENTOS

Inicialmente, agradeço profundamente a Deus pela minha vida e assim pela maravilhosa oportunidade de estudar um curso que escolhi e aprendi a apreciar ainda mais.

Agradeço ainda minha família, meus pais Aida Santana e Rosivaldo S. Santana e aos meus irmãos Rosivaldo C. Santana e Davi Santana, que sempre me auxiliaram durante a minha jornada, oferecendo todo o suporte para a minha formação como pessoa e acadêmica.

Estou muito grata por todos os amigos que pude conhecer, todas as histórias, sorrisos e choros que pudemos compartilhar. Sem vocês esses anos teriam sido sem cor.

E por fim, não posso deixar de agradecer a todos os professores que compartilharam um pouco de conhecimento comigo, em especial a minha orientadora Milena Bueno, que esteve comigo em momentos variados da minha trajetória e me proporcionou muitos ensinamentos.

”E a paz de Deus, que está além de toda compreensão, guardará o seu coração e a sua mente por meio de Cristo Jesus.”

(Filipenses 4:7)

RESUMO

O crescimento da demanda por fontes de energia limpa e renovável tem impulsionado a expansão das usinas fotovoltaicas (UFVs) em todo o território nacional. No entanto, essas infraestruturas críticas enfrentam diversos desafios operacionais e de segurança, principalmente devido à sua localização — seja em áreas urbanas, com maior risco de furtos e vandalismo, ou em zonas rurais, onde há exposição a queimadas, descargas atmosféricas e dificuldades logísticas. Diante disso, a segurança eletrônica surge como uma aliada estratégica para garantir a continuidade da geração de energia e a integridade dos equipamentos. Este trabalho tem como objetivo analisar e comparar diferentes estratégias de segurança eletrônica utilizadas em UFVs, com foco em três tecnologias: sensores de barreira, câmeras com analítico de vídeo e fibra óptica sensível. A metodologia inclui pesquisa bibliográfica sobre os conceitos de segurança perimetral e sistemas fotovoltaicos, além da simulação prática de cenários urbanos e rurais por meio das ferramentas AutoCAD e *IP Video System Design Tool*, com o intuito de avaliar a aplicação, cobertura e desempenho das soluções em ambientes reais. Os resultados permitem identificar as vantagens, limitações e condições ideais de uso de cada tecnologia, oferecendo subsídios técnicos para a escolha de soluções mais eficazes e economicamente viáveis. Dessa forma, o estudo contribui para o desenvolvimento de projetos de segurança mais robustos, adaptados às particularidades de cada tipo de usina e alinhados com a crescente demanda por confiabilidade e proteção no setor de energia solar.

Palavras-chave: usinas fotovoltaicas, segurança eletrônica, sensores, câmeras, fibra óptica, infraestrutura crítica.

ABSTRACT

The growing demand for clean and renewable energy sources has driven the expansion of photovoltaic power plants (UFVs) across Brazil. However, these critical infrastructures face various operational and security challenges, especially due to their locations — whether in urban areas, where the risk of theft and vandalism is higher, or in rural zones, which are more exposed to wildfires, lightning strikes, and logistical difficulties. In this context, electronic security systems emerge as a strategic tool to ensure the continuity of energy generation and the protection of equipment. This study aims to analyze and compare different electronic security strategies used in UFVs, focusing on three technologies: barrier sensors, video analytics cameras, and sensitive fiber optics. The methodology involves a theoretical review of perimeter security and photovoltaic generation concepts, along with the simulation of real application scenarios using AutoCAD and *IP Video System Design Tool* to assess the implementation of the proposed systems in different environments. The results identify the advantages, limitations, and ideal application conditions of each technology, providing technical insights for selecting more effective and cost-efficient solutions. Thus, this study contributes to the development of more robust security projects tailored to the specific characteristics of each type of plant, in line with the growing demand for reliability and protection in the solar energy sector.

Keywords: photovoltaic power plants, electronic security, sensors, cameras, fiber optics, critical infrastructure.

LISTA DE FIGURAS

Figura 1 – Infográfico de Geração no Brasil - Abril 2025	15
Figura 2 – Esquema de Instalação do Sensor	18
Figura 3 – Parâmetros de Instalação	19
Figura 4 – Representação DORI	21
Figura 5 – Câmera PTZ	22
Figura 6 – Elevação do Terreno Escolhido	27
Figura 7 – Caso 1 - Usina com Perímetro Regular	28
Figura 8 – Caso 2 - Usina com Perímetro Irregular	28
Figura 9 – Conexão do Sensor	29
Figura 10 – Simulação do FOV da câmera	31
Figura 11 – Distribuição das Câmeras no Caso 1	31
Figura 12 – Distribuição das Câmeras no Caso 2	32
Figura 13 – Topologia Fence Lite	34
Figura 14 – Fibra Óptica fixada com abraçadeiras	35

LISTA DE TABELAS

Tabela 1 – Quantidade de Fibra Dimensionada	35
Tabela 2 – Comparativo de Tecnologias	39

LISTA DE ABREVIATURAS E SIGLAS

CFTV	Circuito Fechado de Televisão
IEEE	INSTITUTE OF ELECTRICAL ELECTRONICS ENGINEERS
IEEE	Instituto de Engenheiros Eletricistas e Eletrônicos
NBR	NORMA BRASILEIRA
PPM	Pixels por metro
PTZ	pan - tilt - zoom
QCC	Quadro Concentrador CFTV
QDC	Quadro Derivador CFTV
TCC	TRABALHO DE CONCLUSÃO DE CURSO
UFV	Usina Fotovoltaica
VCA	Video Content Analysis
VMS	Video Management System

SUMÁRIO

1	Introdução	11
1.1	Objetivo Geral	12
1.1.1	Objetivos Específicos	12
1.2	Metodologia e Organização	13
2	Referencial Teórico	14
2.1	Usinas Fotovoltaicas	14
2.2	Ameaças à Segurança em Usinas Fotovoltaicas	15
2.3	Soluções de Segurança Eletrônica	17
2.3.1	Sensores de Barreira	17
2.3.2	Câmeras Perimetrais e Monitoramento por Imagem	19
2.3.3	Fibra Óptica Sensível	23
3	Estudo de Caso	27
3.1	Sensores de Barreira	29
3.2	CFTV	30
3.3	Fibra Sensível	33
4	Análise Comparativa das Tecnologias de Segurança	37
5	Conclusão e Considerações Finais	41
	REFERÊNCIAS	42

1 Introdução

Com os novos patamares de tecnologia alcançados pela humanidade, cada dia se torna mais difícil viver num mundo desconectado, e assim uso de energia elétrica é um aspecto essencial da vida moderna. Para suprir o aumento constante dessa demanda, as usinas fotovoltaicas (UFVs) tem sido uma solução bastante popular, levando em conta aspectos sustentáveis e econômicos.

As usinas variam em tamanho e configuração, desde pequenas instalações até complexos que ocupam milhares de hectares. Além das tradicionais usinas terrestres, há inovações como usinas flutuantes, que aproveitam superfícies de reservatórios para otimizar o uso de recursos hídricos e reduzir a evaporação.

Conforme Absolar (2025), os infográficos mostram que explorar o potencial energético do Brasil quando se trata da geração de energia solar, tem sido bastante rentável nos modelos de sistemas de Geração distribuída (GD) e de Geração Centralizada (GC). Por isso, houve um aumento no investimento dessa área e consequentemente, na quantidade de usinas construídas.

A maior parte dessas usinas é considerada nova, baseando-se na vida útil estimada de 25 anos, porém para garantir a funcionalidade delas é necessário que sejam respeitados os aspectos de: acompanhamento, monitoramento e manutenção. Um dos desafios para que isso ocorra é a localização das usinas, que podem ser construídas em áreas urbanas ou rurais (KLEIN, 2025). No meio urbano, manutenções e acompanhamentos são facilitados pelo acesso mais fácil à mão de obra especializada, porém isso pode facilitar o acesso de elementos mal intencionados, que possam vir a vandalizar ou furtar equipamentos e cabos que compõem o sistema. E nos locais mais remotos, além dos riscos já citados, podem ser incluídos: queimadas e incêndios e descargas atmosféricas.

Em ambos os casos existe a possibilidade de reparo e/ou substituição para retomada da geração normal da UFV, mas até que um desses problemas seja identificado e corrigido, a geração de energia pode ser muito impactada. Desse modo, para auxiliar no monitoramentos das usinas a aplicação de sistemas de segurança eletrônica é uma ferramenta muito poderosa.

Diversas tecnologias podem ser aplicadas para reforçar a segurança das usinas. Sensores e radares são capazes de monitorar áreas extensas, câmeras permitem uma análise em tempo real e registro de eventos, controle de acesso e cercamentos físicos ajudam a reduzir invasões. Entretanto, a eficácia dessas soluções pode ser comprometida por falsos alarmes e aumentar a

quantidade de componentes com necessidade de manutenção contínua.

A integração de tecnologias mais novas, como fibras óptica sensorial e análise avançada de vídeo, tem se mostrado uma alternativa promissora para aprimorar a segurança e a resposta a ameaças. (BADRA, 2025)

Conhecer diferentes sistemas de segurança eletrônica e seus potenciais riscos e benefícios é muito importante ao elaborar o projeto de uma UFV, já que mesmo um sistema avançado, ao ser aplicado de forma incorreta se torna ineficaz.

Neste contexto, este trabalho propõe uma análise comparativa entre três tecnologias principais aplicadas à segurança perimetral de usinas fotovoltaicas: sensores de barreira, câmeras com analítico de vídeo e fibra óptica sensível, que combinam inovação tecnológica, eficácia e viabilidade. Levando em conta aspectos como alcance, precisão e aplicabilidade em diferentes cenários presentes nessas infraestruturas críticas em um momento de crescente demanda por energia renovável.

1.1 Objetivo Geral

Este trabalho tem por objetivo analisar três diferentes estratégias de segurança eletrônica adotadas no mercado, utilizadas em usinas fotovoltaicas e como podem ser adaptadas para atender às necessidades específicas desse tipo de infraestrutura, considerando seus riscos e vulnerabilidades únicas.

Foram selecionados três tipos de sistemas diferentes: sensores de barreira, câmeras com analítico de vídeo e fibra óptica sensível para que, o TCC venha a ser um material auxiliar na escolha de sistemas, baseado no cenário de aplicação. Para alcançar esse objetivo foram utilizadas a ferramenta Autocad, um software *Computer Aided Design* (CAD), criado pela Autodesk, Inc., além do *IP Video System Design Tool*, para simular a aplicação das câmeras que compõem um sistema de Circuito Fechado de Televisão (CFTV).

1.1.1 Objetivos Específicos

Os objetivos específicos deste trabalho são:

- Abordar as Usinas Fotovoltaicas como Infraestrutura Críticas;
- Levantar referencial sobre Projetos de Segurança Eletrônica;
- Identificar e comparar as principais estratégias de segurança eletrônica utilizadas no

mercado atual;

- Investigar fatores que influenciam na escolha e adoção de uma estratégia específica de segurança eletrônica, como o tipo de infraestrutura, o nível de risco e a legislação vigente, a fim de fornecer recomendações para a tomada de decisão em relação à implementação de um sistema de segurança.

1.2 Metodologia e Organização

Este trabalho está dividido em cinco capítulos, abordando aspectos teóricos ou análise de estudos de caso obtidos.

No Capítulo 2, está incluída a fundamentação teórica do trabalho, apresentando conceitos, como as diferenças entre tipos e localizações de Usinas, ameaças e desafios para o monitoramento das UFVs e sistemas de segurança e seus princípios de funcionamento.

O Capítulo 3 aborda diretamente, dois cenários de aplicação para cada um dos sistemas definidos neste trabalho, simulando componentes e quantidades baseados em estudos de casos e referenciais para elaboração de projetos de segurança perimetral.

No Capítulo 4, é feita comparação das soluções com base em critérios como eficácia, manutenção e integração com outros sistemas, e a discussão sobre quais combinações tecnológicas oferecem maior proteção dependendo do tipo e localização da usina.

Por último, o Capítulo 5, resume as recomendações para implementação de sistemas de segurança eficientes e levanta sugestões de novas pesquisas na área.

2 Referencial Teórico

Para compreender a aplicabilidade e o desempenho dessas soluções, é essencial estabelecer um embasamento teórico que aborde tanto os conceitos fundamentais da segurança perimetral quanto os aspectos técnicos da geração de energia solar. A partir dessa base, torna-se possível avaliar de forma criteriosa as vantagens, limitações e adequações de diferentes tecnologias às particularidades dos ambientes urbano e rural.

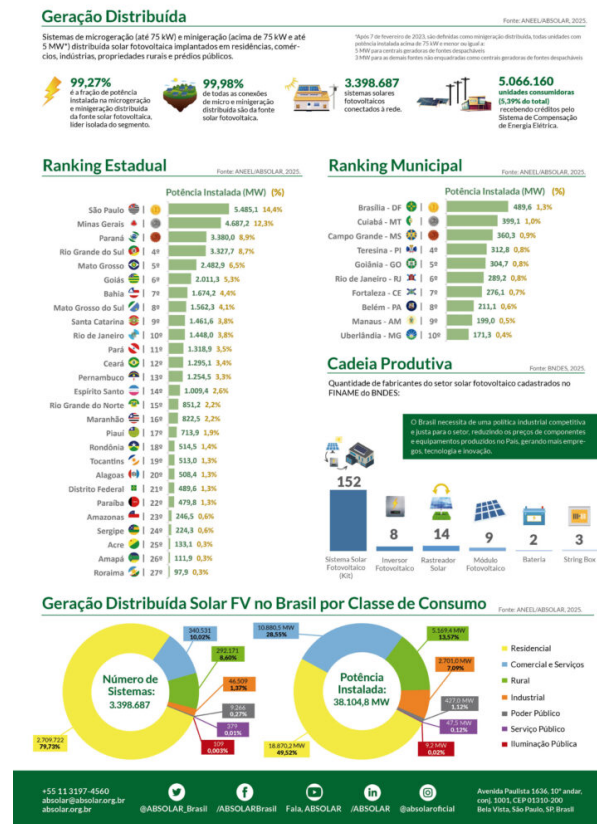
Dessa forma, este capítulo apresenta os principais fundamentos que sustentam o uso de tecnologias eletrônicas em sistemas de segurança de UFVs, servindo como suporte para a análise detalhada, nos tópicos seguintes, de três soluções específicas: sensores de barreira, câmeras com analítico de vídeo e fibra óptica sensível.

2.1 Usinas Fotovoltaicas

A energia solar ou fotovoltaica é uma forma de transformar a luz do sol diretamente em eletricidade. Isso é feito com o uso de placas solares, chamadas de células fotovoltaicas, que são feitas com materiais semicondutores — o mais comum é o silício. Quando a luz do sol bate nessas células, ela agita os elétrons que existem dentro do material, fazendo com que eles se movimentem. Esse movimento dos elétrons é o que gera a eletricidade. Esse processo é conhecido como efeito fotovoltaico e é o que faz os sistemas de energia solar funcionarem. (KLEIN, 2025)

O nome usina fotovoltaica (UFV), é dado de forma popular ao conjunto das placas, transformadores, inversores, e outros componentes do sistema de geração, com conexão na rede feita em média tensão (PINHO; GALDINO, 2014).

Figura 1 – Infográfico de Geração no Brasil - Abril 2025



Fonte: Adaptado de Absolar

As usinas com maior número de crescimento são as GDs, geralmente instaladas em regiões com recursos solares uniformes, e sem elementos de sombreamento ou superfícies reflexivas próximas. A Lei nº 14.300/2022 da ANEEL, estabelece que usinas de geração distribuída (GD) possuem central geradora com potência até 5MW, acima deste valor são consideradas centralizadas.

Conforme Pinho e Galdino (2014), é mais provável encontrar superfícies livres e com fácil circulação de ar em regiões isoladas, e a recomendação de segurança é que sejam instaladas cercas para que pessoas não autorizadas não possam acessar o local facilmente.

Essa cerca, é o foco de interesse quando se fala sobre segurança eletrônica pois dá referência do perímetro e área de proteção necessários.

2.2 Ameaças à Segurança em Usinas Fotovoltaicas

Como infraestruturas críticas de geração de energia, as ameaças comprometem não apenas o desempenho operacional, mas também a viabilidade econômica desses empreendimentos. Infelizmente tais ameaças são particularmente desafiadoras em países que

possuem perfil similar ao Brasil onde muitas instalações estão localizadas em regiões remotas e suscetíveis à ação criminosa.

Os roubos em usinas solares têm se tornado cada vez mais frequentes, motivados, sobretudo, pelo alto valor comercial dos equipamentos utilizados. Módulos fotovoltaicos, inversores, controladores de carga e cabos são os principais alvos. Esses componentes, além de possuírem elevado custo de reposição, são facilmente revendidos no mercado paralelo, o que dificulta sua rastreabilidade.

O cobre em especial, é um material altamente valorizado no mercado de sucata devido à sua ampla aplicação industrial e seu preço relativamente alto (HEIN, 2024). Nas usinas fotovoltaicas, cabos de cobre são utilizados em grande quantidade para interligação dos módulos, aterramento e conexões com inversores e painéis de distribuição. A remoção desses cabos compromete seriamente a operação da planta e pode causar falhas elétricas generalizadas. Além disso, a substituição dos cabos exige interrupções na geração e um alto custo de mão de obra e materiais.

Até em tentativas malsucedidas, ocorrem impactos na operação, já que a invasão de perímetros por pessoas não autorizadas, seja com fins criminosos ou por curiosidade, representa uma ameaça séria à segurança física da instalação. O vandalismo pode incluir a destruição proposital de painéis, danos a cabos, pichações e até incêndios criminosos. Tais ações não apenas deterioram os equipamentos e instalações, como também aumentam os riscos de acidentes com choques elétricos ou curtos-circuitos. Além disso, a simples presença de intrusos pode gerar paradas preventivas nos sistemas, impactando diretamente a produção energética e os indicadores de desempenho da usina.

Um dos desafios para a segurança de usinas fotovoltaicas está relacionado à sua localização geográfica e à extensão territorial. Muitas dessas usinas estão situadas em zonas rurais afastadas de centros urbanos, com pouco ou nenhum apoio policial nas imediações. Esse cenário dificulta a resposta rápida a incidentes de segurança e favorece a ação de criminosos. Além disso, o grande perímetro das usinas torna o monitoramento convencional — vigilância física — ineficiente e custoso. A falta de iluminação noturna e a topografia acidentada também dificultam a detecção de movimentos suspeitos.

Em conjunto, o impacto financeiro de todas essas ocorrências pode ser significativo, refletindo em prejuízos diretos, interrupções no fornecimento de energia e aumento nos custos de seguros e manutenção. Em casos extremos, comprometem a continuidade da operação da

usina, prejudicando investidores, serviços públicos essenciais e consumidores (NAWAZ; KAYANI; AYSAN, 2024).

2.3 Soluções de Segurança Eletrônica

A segurança é um item essencial ao ser humano, para proteção de sua integridade e a de suas posses, impactando em sua saúde e bem-estar. Um sistema de segurança eletrônica bem implementado pode significar grandes economias, já que pode auxiliar na identificação de um infrator no caso de incidentes ou até diminuir a ocorrência deles através da dissuasão. Conforme a Associação Brasileira das Empresas de Sistemas Eletrônicos de Segurança:

A Segurança Eletrônica engloba uma gama abrangente de tecnologias e serviços integrados, projetados para o monitoramento e proteção de espaços e pessoas. Este termo não se limita apenas ao uso de câmeras de monitoramento e sistemas de alarme, mas também inclui controle de acesso, sensores de movimento, barreiras físicas eletrônicas, intercomunicação e videomonitoramento (ABESE, 2025).

Neste trabalho serão abordados apenas três sistemas devido a gama gigante de cenários onde podem ser aplicados, muitas vezes sendo utilizados até em conjunto, para criar soluções consonantes.

2.3.1 Sensores de Barreira

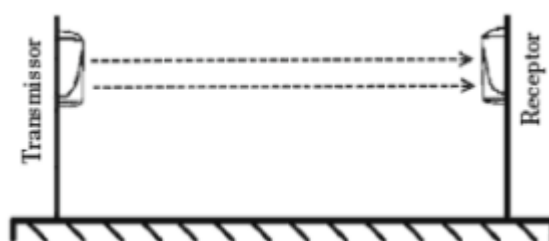
Um sensor, é um dispositivo que recebe e responde sinais ou estímulos, em geral, são uma tecnologia mais econômica para realizar a detecção de movimento em um ambiente, pois conseguem identificar se há alguém (ou algo) no local onde são instalados, através da detecção de movimentos, variação de temperatura, micro-ondas ou pela interrupção de feixes infravermelhos. Dispositivos mais recentes podem até mesclar duas formas de detecção para diminuir as chances de ocorrerem alarmes falsos. Os sensores podem ser instalados a fio ou sem fio, se comunicando com uma central de alarme.

Os sensores infravermelhos passivos IVP, operam pela detecção da variação do calor gerada quando há a movimentação no ambiente, e podem ser configurados para ignorar movimentações “menores” que se referem a animais, por exemplo ao ajustar sua sensibilidade e alcance (SOBRINHO, 2008).

Os sensores de barreira, também conhecidos como sensores IVA ou barreira infravermelha foram uma das primeiras tecnologias a surgirem no ramo de segurança

eletrônica, e no mercado atual se consolidaram como uma solução econômica eficiente para segurança patrimonial. Consistem em um conjunto de emissor x receptor de luz infravermelha, que é invisível a olho nu e quando ocorre a interrupção desse feixe de luz que transita entre ambos se detectar uma intrusão e o sensor ativa seu sinal de saída. O emissor, emite um sinal na faixa infravermelha em rajadas ou pulsos organizados, de forma que saem e chegam no receptor que irá fazer a comparação do sinal, e assim informar se houve a interrupção e o intervalo de tempo da mesma.

Figura 2 – Esquema de Instalação do Sensor



Fonte: Intelbras (2024)

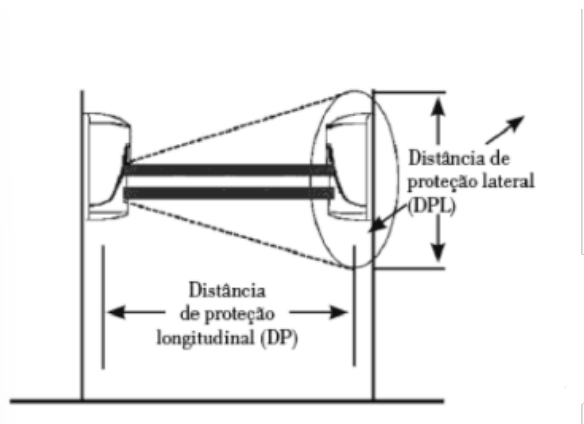
Para infraestruturas maiores, como é o caso das usinas, geralmente opta-se por utilizar modelos de múltiplos feixes, que são mais precisos devido a maior quantidade de luz que é emitida. Neste caso são aplicados na forma de cercas virtuais, mas é necessário observar bem as distâncias de instalação recomendadas.

Os sensores de micro-ondas captam os movimentos através da variação de massa. Ou seja, mesmo que ocorra a camuflagem da variação de calor identificada por infravermelho, a detecção por micro-ondas garante a identificação da intrusão e a comunicação com a central de monitoramento.

Os sensores magnéticos são utilizados para detectar abertura e fechamento indevidos de janelas e portas e para evitar invasões. Funcionam através de um contato elétrico e um ímã. A função do ímã é manter o sensor acionado e, no caso de abertura de porta ou janela, há afastamento dos contatos, enviando imediatamente um sinal para a central de alarme. Pode ser encontrado com fio ou sem fio. No caso de ser sem a fiação, o sensor emite sinais de radiofrequência quando houver abertura da porta ou janela, que são captados pelo receptor conectado diretamente à central de alarme. Sensores desse tipo podem ser de feixe único, de feixe duplo, feixe duplo e/ou quádruplo sincronizados, e os multifeixes. Em usinas mais antigas é comum ver sensores IVA instalados, esse tipo de sensor funciona em pares ou com

refletores.

Figura 3 – Parâmetros de Instalação



Fonte: Adaptado de Intelbras (2024)

Os sensores possuem dois parâmetros principais, sua distância de proteção longitudinal (DP), a distância máxima permitida entre o receptor e o emissor e a distância de proteção lateral (DPL) que é o diâmetro do cone que forma o feixe infravermelho ao longo do percurso.

$$DPL = DP \times 0,1 \quad (1)$$

Os sensores são concentrados com um feixe direcional, e para melhor operação é necessário que estejam devidamente instalados e alinhados, o que pode ser complicado em distâncias superiores a 50m, sem o auxílio de uma mira laser ou uma pontaria virtual. Além disso, são dispositivos muito suscetíveis às variações climáticas, já que neblina ou chuva intensa podem dispersar os feixes infravermelhos gerando alarmes falsos, e atrapalhando a operação normal.

Em usinas localizadas em zonas isoladas, é vital que seja realizada a poda, já que a grama cresce de forma rápida e pode também gerar interferência nos feixes gerando ainda mais alarmes falsos. Isso gera um custo operacional maior já que essa poda deve ser feita com constância. Terrenos com uma inclinação muito elevada, ou perímetros muito irregulares não são ambientes favoráveis para a instalação desse sistema de segurança.

2.3.2 Câmeras Perimetrais e Monitoramento por Imagem

Um Circuito Fechado de Televisão (CFTV) consiste em um sistema de monitoramento de ambientes e objetos por meio de câmeras. As imagens captadas são transmitidas diretamente, via

cabo ou rede, para um centro de supervisão, onde os operadores utilizam softwares específicos para acompanhar em tempo real o que ocorre em determinada UFV. A instalação de CFTV em fazendas solares visa reforçar a segurança física da instalação e permitir o monitoramento contínuo das condições ambientais.

Todas essas câmeras são conectadas a um algum ponto principal de concentração, podendo ser o quadro concentrador dentro de um gabinete de CFTV, em uma sala de Operação Local ou um os quadros derivadores localizados em algum dos Postes, conforme dimensionamentos que respeitem a tecnologia aplicada como o cabeamento com cabos UTP Cat.6 ou puramente fibra óptica.

Na arquitetura de CFTV mais comum, a conexão das câmeras aos pontos de concentração é feita com cabos UTP quando a distância entre eles não compromete o desempenho do sistema de transmissão. Para a interligação entre os pontos muito distantes entre si, é necessário empregar cabo de fibra óptica, que assegure uma transmissão de dados sem perdas(MURDAN; CAREMBEN, 2018).

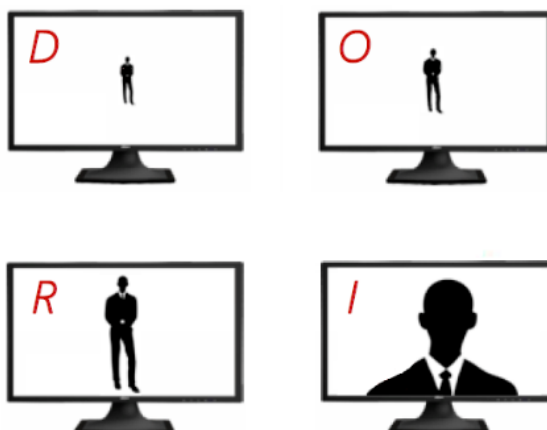
O layout típico do sistema de CFTV em uma usina solar consiste na instalação de cada câmera em um poste, de forma que cada equipamento visualize o seguinte, criando uma estrutura em anel. Atendendo as recomendações estabelecidas por (ALMEIDA, 2017).

O campo de visão de cada câmera forma um setor triangular, onde um dos vértices corresponde à posição da câmera. Essa configuração é essencial para a aplicação de algoritmos de análise de vídeo, e o espaçamento entre as câmeras varia conforme o nível de detalhamento exigido pelas análises visuais automatizadas.

Sendo recomendado que as operações ocorram nas áreas de Identificação ou Reconhecimento, conforme a tabela DORI, proveniente da norma IEC EN62676-4: 2015 International Standard, que se baseia em pixels por metro (PPM).

A diferença na perspectiva da imagem e o impacto das distâncias pode ser observado na ilustração a seguir, ela demonstra o critério DORI, com cada painel demonstrando uma etapa do processo, onde as letras representam Detecção (apenas perceber que um alvo está presente), Observação (distinguir características gerais do alvo), Reconhecimento (ser capaz de reconhecer o alvo como familiar) e Identificação (confirmar a identidade do alvo sem margem para dúvidas). A progressão visual, que vai de uma figura distante até um close-up, exemplifica como a qualidade e o zoom da imagem determinam o nível de informação que pode ser obtido em uma cena vigiada.

Figura 4 – Representação DORI



Fonte: Dahua (2025)

Os valores PPM são conforme:

Detecção: 25 ppm

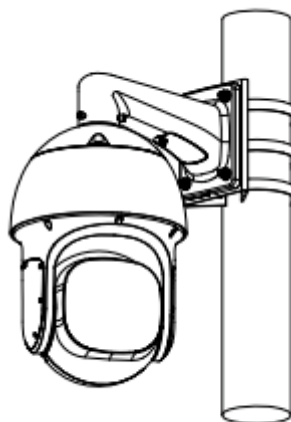
Observação: 63 ppm

Reconhecimento: 125 ppm

Identificação: 250 ppm

A característica principal no projeto de CFTV são a câmera, seu conjunto e lentes, pois a partir disso é possível determinar o consumo de banda, o espaço de armazenamento, a distribuição ao longo do perímetro etc. Existem diversos modelos de câmeras a tradicional com a lente óptica, que possui um sensor de imagens que realiza a captação de pixels organizado em linhas (H) e colunas (V) formando um quadro HxV que nos dá a resolução. Esse sensor pode ser fixo ou motorizado.

Figura 5 – Câmera PTZ



Fonte: Dahua (2025)

As câmeras PTZ (pan - tilt - zoom) são do tipo motorizado e conseguem captar imagens em até 360° horizontalmente. Normalmente possuem um conjunto de lentes que permite fazer zoom óptico entre 10x e 50x. Mas não são indicadas para a proteção sozinhas já que podem perder um sincronismo e deixar pontos cegos em trechos do alambrado, por exemplo, costuma-se utilizar estes dispositivos como uma apoio operacional de visualização geral ou para buscar um local / evento específico.

As câmeras, com a funcionalidade de Video Content Analysis (VCA) ou seja, analíticos de vídeo aplicadas ao sistema CFTV, ganharam muito espaço e destaque na aplicação de segurança patrimonial. São uma solução bastante flexível, que permite a criação de regras específicas que quando quebradas geram alarmes a depender da regra quebrada.

As soluções baseadas em inteligência artificial conseguem identificar padrões e prever possíveis riscos, alertando equipes de segurança antes mesmo que incidentes ocorram. Esta capacidade preditiva transforma a segurança perimetral de uma abordagem reativa para uma estratégia proativa de prevenção.

Os softwares modernos de análise preditiva processam grandes volumes de dados capturados por câmeras, identificando comportamentos suspeitos e gerando alertas automáticos. Esta tecnologia é particularmente valiosa em instalações críticas como usinas, centros de dados e complexos industriais, onde falhas de segurança podem ter consequências graves.

As câmeras modernas permitem armazenar registros de vídeo que podem ser consultados posteriormente, facilitando investigações de incidentes e fornecendo evidências

visuais. Alguns modelos até oferecem recursos de armazenamento local em cartão micro-SD, garantindo a preservação dos registros mesmo em caso de falha na conexão de rede.

Os sistemas de monitoramento perimetral por imagem, embora avançados, apresentam desafios significativos que devem ser considerados durante o planejamento. Um dos principais obstáculos está relacionado às limitações físicas das câmeras, como linhas de visão restritas e sensibilidade a condições climáticas adversas. Neblina, chuva intensa ou reflexos de luz podem comprometer a qualidade das imagens e a eficácia das análises inteligentes, especialmente em câmeras térmicas, que, apesar de superarem problemas de iluminação, ainda enfrentam dificuldades em ambientes com interferências térmicas.

Além disso, a necessidade de infraestrutura robusta, incluindo largura de banda estável para transmissão de vídeo em alta resolução e sistemas de armazenamento de dados, eleva os custos operacionais e exige manutenção especializada, tornando a implementação complexa para pequenas empresas ou residências.

Outro ponto crítico é o risco de falsos alarmes, que persiste mesmo em sistemas com inteligência artificial. Embora tecnologias analíticas reduzam erros ao diferenciar pessoas, veículos e animais, fenômenos naturais como ventos fortes ou mudanças bruscas de iluminação ainda podem disparar alertas indevidos, sobrecarregando equipes de segurança. A integração entre diferentes componentes do sistema, como câmeras PTZ, sensores de cerca e softwares de análise, também exige compatibilidade técnica, muitas vezes dificultada pela diversidade de fabricantes e protocolos. Questões éticas e legais, como o uso de reconhecimento facial e gravação contínua, adicionam camadas de complexidade, exigindo conformidade com regulamentações de privacidade e proteção de dados.

Por fim, a dependência de energia elétrica e redes estáveis cria vulnerabilidades, já que falhas nesses sistemas podem paralisar completamente o monitoramento, deixando áreas críticas desprotegidas. Esses fatores destacam a importância de uma avaliação criteriosa das necessidades específicas de cada projeto antes da implementação.

2.3.3 Fibra Óptica Sensível

O funcionamento da fibra óptica sensível baseia-se na capacidade de detectar mínimas alterações nas propriedades da luz que percorre o interior da fibra quando esta sofre perturbações externas. Uma das principais tecnologias empregadas é a Distributed Acoustic Sensing (DAS), variante que monitora a assinatura coerente do ruído de retrodifusão em um cabo de fibra óptica

à medida que pulsos de luz são enviados através dele (OZKAN T ERKORKMAZ, 2020).

O sistema analisa cuidadosamente as mudanças no padrão de retroespalhamento, que gera uma "impressão digital" única na assinatura de retrodifusão do cabo de fibra, permitindo a detecção de alterações mínimas ao longo de toda a extensão do cabo. Qualquer perturbação física externa, como pressão, vibração ou movimento próximo à fibra, altera esse padrão, possibilitando não apenas a detecção do evento, mas também sua localização precisa.

Existe também a Distributed Vibration Sensing (DVS), empregada em diferentes aplicações de monitoramento por fibra óptica. Estas tecnologias transformam o cabo de fibra óptica em um elemento extremamente sensível a pressão, acústica e movimento, capaz de detectar vibrações diminutas transmitidas através de vedações, solo ou superfícies diversas. Em sua implementação mais simples, o princípio pode ser demonstrado focalizando um feixe de luz através de uma fibra óptica para que incida sobre um fotossensor, onde qualquer movimento da fibra modifica a transmissão da luz e pode ser detectado pelo receptor.

Em sistemas mais avançados, um cabo de fibra óptica monomodo típico se transforma em um poderoso sensor de vibração que pode monitorar grandes extensões, detectando e localizando eventos específicos com precisão notável (BADRA, 2025).

A tecnologia também permite classificar assinaturas específicas de eventos com base em algoritmos de detecção, diferenciando, por exemplo, entre passos humanos, veículos, tentativas de escavação ou corte em cercas. Os sistemas modernos incorporam inteligência artificial para melhorar a classificação dos eventos detectados, reduzindo significativamente a ocorrência de falsos alarmes e aumentando a confiabilidade da detecção. A fibra óptica monomodo é a mais comumente utilizada nessas aplicações, oferecendo diferentes níveis de sensibilidade física que podem ser otimizados para diversas condições ambientais e de solo. Os sistemas atuais permitem o monitoramento contínuo em tempo real, com resolução de localização tipicamente entre 3 e 20 metros em toda a extensão do perímetro protegido.

Uma das principais vantagens da fibra óptica sensível é sua excepcional capacidade de cobertura de longas distâncias, permitindo o monitoramento de até 100 quilômetros com uma única unidade de processamento, a depender do sistema, tornando-a a solução economicamente mais competitiva disponível atualmente para segurança perimetral de grandes áreas. Esta característica elimina a necessidade de múltiplos equipamentos eletrônicos distribuídos pelo perímetro, simplificando a infraestrutura e reduzindo os custos de instalação e manutenção.

Como nenhum componente eletrônico ou fonte de energia é necessário ao longo do perímetro monitorado, apenas o cabo de fibra óptica, o sistema apresenta excepcional robustez e confiabilidade operacional, especialmente em ambientes hostis ou remotos. Esta simplificação também reduz significativamente os requisitos de manutenção e praticamente elimina os pontos de falha ao longo do perímetro.

A imunidade da fibra óptica a interferências eletromagnéticas (EMI) e descargas elétricas como raios representa outra vantagem crucial, tornando o sistema intrinsecamente seguro mesmo em atmosferas explosivas ou em ambientes com alta interferência eletromagnética. Esta característica é particularmente valiosa para aplicações em indústrias químicas, plataformas de petróleo, mineração e outras instalações onde a segurança intrínseca é um requisito crítico (SHAH; PARMAR; PANDYA, 2015).

O sistema também oferece grande flexibilidade na configuração de zoneamento, permitindo ajustes via software sem necessidade de modificações físicas na instalação, possibilitando diferentes níveis de sensibilidade para cada zona de acordo com requisitos específicos de segurança.

A capacidade de monitoramento em tempo real proporciona detecção precoce de potenciais problemas ou mudanças nas condições monitoradas, permitindo respostas rápidas a eventos de segurança ou anomalias operacionais. Comparada aos sensores tradicionais, a fibra óptica sensível oferece maior precisão, menor susceptibilidade a interferências e capacidade de monitorar grandes áreas com um único sistema integrado, simplificando a infraestrutura de monitoramento e reduzindo os custos operacionais. A natureza distribuída da detecção significa que cada metro da fibra funciona como um sensor independente, proporcionando informações detalhadas sobre a localização e natureza dos eventos detectados ao longo de toda a sua extensão.

Apesar das numerosas vantagens, a implementação da tecnologia de fibra óptica sensível apresenta alguns desafios significativos que precisam ser adequadamente abordados para garantir seu desempenho ótimo. A instalação requer conhecimento especializado e técnicas específicas para maximizar a sensibilidade do sistema sem comprometer sua confiabilidade ou durabilidade. O manuseio e instalação inadequados podem resultar em atenuação excessiva do sinal óptico ou pontos de estresse na fibra que poderiam gerar falsas alarmes ou pontos cegos no sistema de detecção. O correto dimensionamento do sistema, seleção apropriada do tipo de cabo e determinação do posicionamento ideal representam

aspectos críticos que exigem planejamento cuidadoso e conhecimento técnico especializado.

O investimento inicial relativamente elevado constitui outro desafio, embora seja geralmente compensado pelos menores custos operacionais e pela extensa cobertura proporcionada por um único sistema. A análise adequada de custo-benefício deve considerar não apenas o investimento inicial, mas também os custos reduzidos de manutenção, a maior durabilidade e a escalabilidade da solução em comparação com alternativas convencionais.

A calibração adequada do sistema representa um aspecto crítico para equilibrar a sensibilidade desejada com a minimização de falsos alarmes, especialmente em ambientes variáveis ou com condições climatológicas extremas. Sistemas excessivamente sensíveis podem gerar numerosos falsos positivos, enquanto configurações muito conservadoras podem deixar passar eventos relevantes.

A interpretação dos dados gerados pelos sistemas de fibra óptica sensível exige software sofisticado e, idealmente, algoritmos de inteligência artificial capazes de distinguir entre diferentes tipos de eventos e filtrar perturbações ambientais normais. O desenvolvimento e refinamento desses algoritmos representam um desafio contínuo, particularmente para aplicações em ambientes complexos com múltiplas fontes de vibração ou interferência.

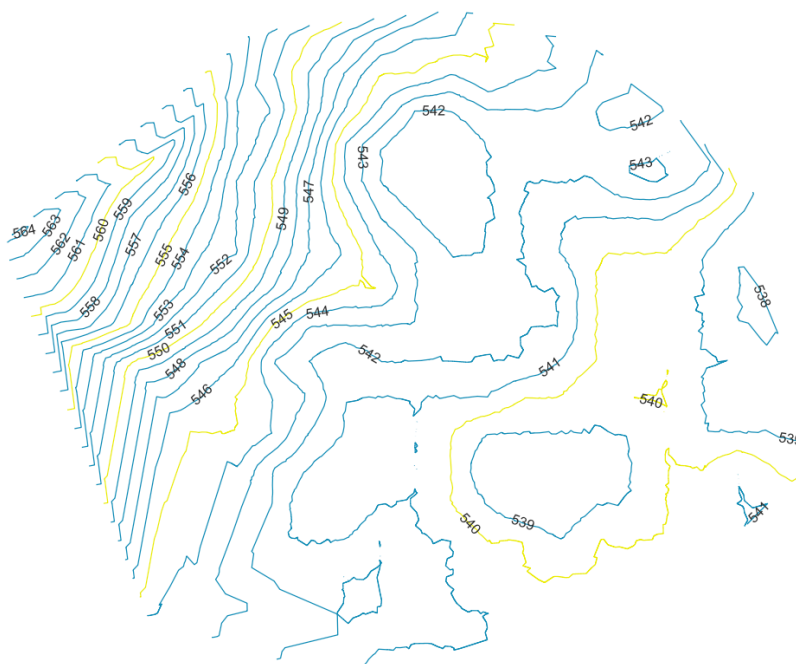
Adicionalmente, a integração com sistemas existentes de segurança ou monitoramento pode apresentar complexidades, especialmente quando se busca uma abordagem unificada para gerenciamento de segurança e resposta a incidentes. Esta integração frequentemente requer desenvolvimento de interfaces personalizadas e protocolos de comunicação para garantir o funcionamento harmônico de todos os componentes do sistema de segurança.

3 Estudo de Caso

Para os estudos e análises comparativas, foram elaborados dois leiautes de usinas, utilizando um mesmo terreno hipotético, para minimizar os efeitos que o relevo tem em relação a escolha de um sistema, neste caso é feito um comparativo de aplicação de um cenário complexo versus um cenário mais simples.

A imagem abaixo representa o espaço geográfico onde os diferentes leiautes das usinas serão aplicados. A localização será mantida a mesma, e a localidade escolhida foi feita com base na presença de outras usinas localizadas nas regiões próximas, observada com auxílio de imagens de satélite, indicando que o local atende aos critérios contidos no Manual de Engenharia Para Sistemas Fotovoltaicos (2014) para locais otimizados para a geração de energia.

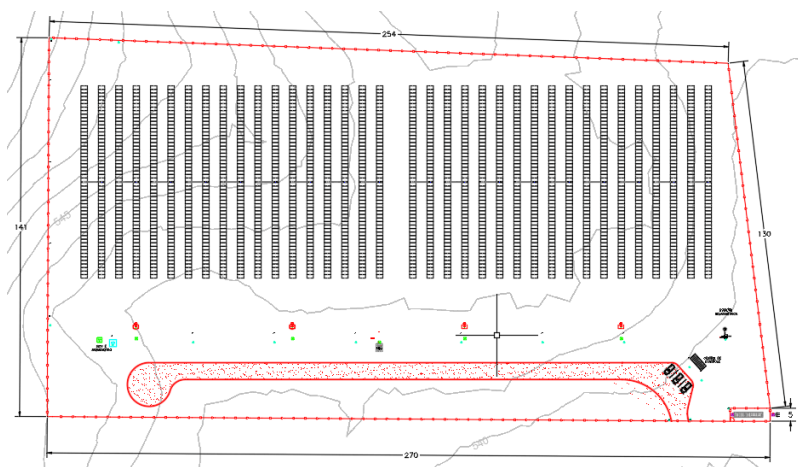
Figura 6 – Elevação do Terreno Escolhido



Fonte: A Autora (2025)

Com o auxílio das ferramentas QGis e as coordenadas extraídas do *Google Earth*, foi selecionado um terreno com declividade suave, com inclinação média de terreno de 2,2%. Ambas as usinas foram desenhadas para possuir 800 metros de perímetro, similar a outras usinas GD implantadas.

Figura 7 – Caso 1 - Usina com Perímetro Regular



Fonte: A Autora (2025)

A Usina nomeada como Caso 1, possui um contorno regular, com cantos fechados em ângulos retos. As cercas se encontram distantes das placas, procurando evitar quaisquer tipos de sombreamento que possam ocorrer.

Figura 8 – Caso 2 - Usina com Perímetro Irregular



Fonte: A Autora (2025)

E o Caso 2, possui um formato mais irregular, simulando os desvios e adaptações feitos em situações como áreas alagadas ou zonas de proteção ambiental que precisam ser evitadas.

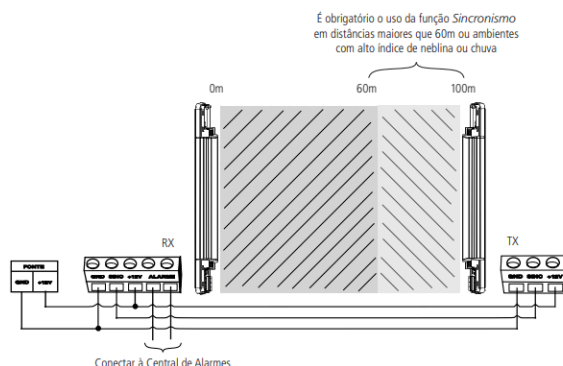
3.1 Sensores de Barreira

Considerando a tecnologia de Sensores de Barreira, são levantados pontos críticos para um sistema eficaz (INTELBRAS, 2024) :

- Alinhamento preciso: Requer instalação em linha reta, com verificação de reflexões em superfícies claras.
- Distância máxima por sensor: Até 100 metros de cobertura por unidade, manual para aplicações com cabo de sincronismo.
- Dimensione corretamente a fonte e o cabo de alimentação;

Utilizando o limite recomendado, sem a utilização de um cabo de sincronismo, o que tornaria necessário um uso maior de infraestrutura e materiais. E levando em conta o pior cenário para ambos os casos, que é um ambiente com altos índices de chuva e neblina, define-se que instalação dos sensores está ideal de 60 em 60 metros.

Figura 9 – Conexão do Sensor



Fonte: Intelbras (2024)

Considerando essa distância, aplica-se a equação (1) para saber qual a distância correta entre sensores operando no mesmo canal.

$$DPL = 60 \times 0,1 = 6m \quad (2)$$

Isto indica, que é necessário se observar curvas onde são necessários a aplicação de mais pares de sensores, para que não gerem interferência um no outro. Para reduzir as chances de interferências, os sensores são dispostos de forma oposta, com dois pares do mesmo tipo receptor-receptor ou transmissor-transmissor juntos num mesmo poste ou estrutura de instalação.

Pensando apenas no perímetro, vale estimar a quantidade mínima de sensores a serem utilizados.

$$Sensores = P \div DP = 800 \div 60 = 13,33 \cong 14 \quad (3)$$

Saindo um pouco fora da estimativa, houve a necessidade de 16 pares de sensores, conforme os 60m estimados, e levando em conta um distanciamento de até 30m entre as caixas de passagem conforme ABNT 5410.

Para o caso irregular este valor sobe para 19 unidades, compensando os obstáculos e irregularidades encontradas no caminho.

É importante observar que, caso o alambrado interfira na sincronização dos sensores pode ser necessário adicionar sensores a mais para fazer a cobertura de áreas que possuam mais cercas, como a subestação de energia, ou trechos que devem permitir o acesso da concessionária.

3.2 CFTV

Para estabelecer um sistema confiável, Saver (2013) define alguns parâmetros a serem avaliados:

- Projetar distâncias baseando-se na altura de um humano, em geral 1,8m;
- A câmera deve ser instalada entre 3-5m para detecção de humanos, ou em caso da presença de alambrado deve ser no mínimo maior que o mesmo;
- A zona de interesse deve cobrir mais que 1/4 da imagem;
- Selecionar câmeras que operem bem em baixa luminosidade, ou providenciar iluminação adequada;
- Configurar a distância focal para melhor visualizar a área de interesse.

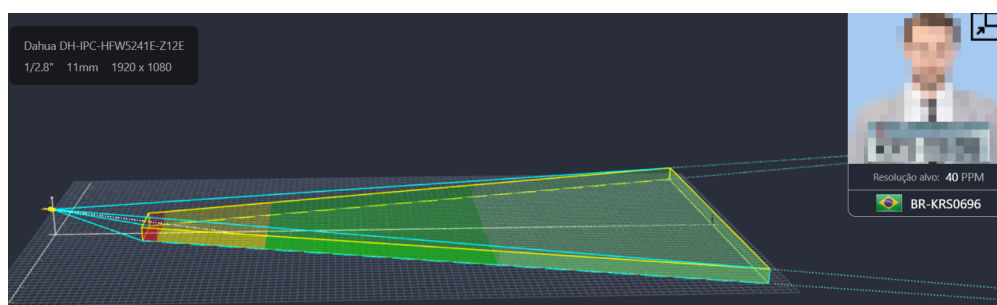
Existem vários modelos de arquitetura CFTV, o adotado consiste de um Quadro Concentrador, onde fica localizado o Gravador de Vídeo, ou o servidor onde serão registradas as imagens e Quadros Derivadores, fixados em postes ao longo da Usina, para distâncias maiores que o raio de coberturado do QCC.

Neste caso, utilizando câmeras com IR maior ou igual a 100m, garante-se a visualização mesmo em ambientes com baixa luminosidade, para uso de cabos Cat.6,

respeitando uma distância menor que 100m para aplicação da tecnologia PoE, conforme o padrão IEEE 802.3af/at/bt.

Utilizando a ferramenta IP Video System Design Tool e uma câmera com as configurações: Zoom Óptico de 12X, 2MP, 25/30 FPS@1080P, IR = 150m, IP67, IK10, Codificação H.265, Lentes Motorizadas, considerando o ajuste da lente em 11mm, o FOV abaixo é simulado, para uma distância de 100m, e uma instalação em 4m de altura.

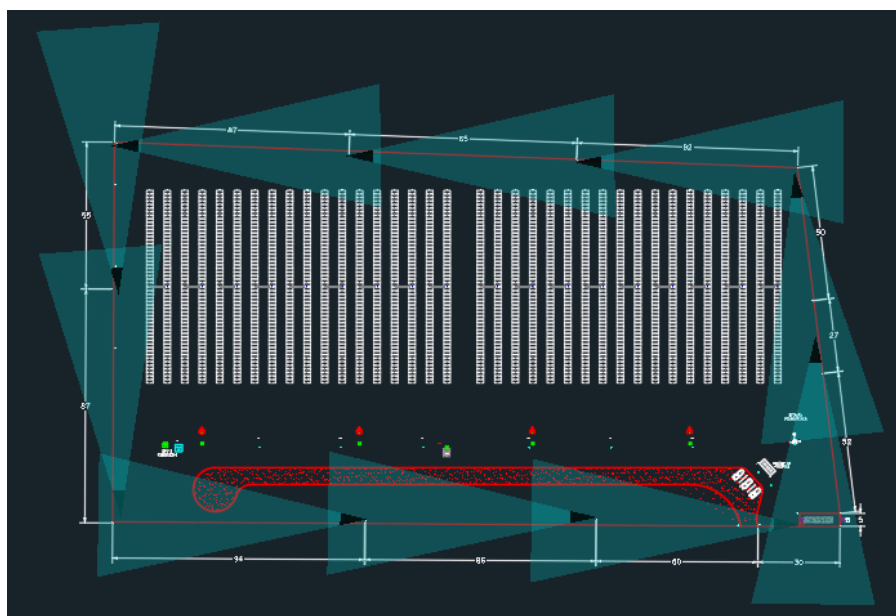
Figura 10 – Simulação do FOV da câmera



Fonte: A Autora (2025)

Os equipamentos utilizados para proteção perimetral precisam ser instalados de forma correta, com uma câmera cobrindo o ponto cego da posterior.

Figura 11 – Distribuição das Câmeras no Caso 1



Fonte: A Autora (2025)

Fazendo essa distribuição, com a câmera selecionada, para o Caso 1 o número de

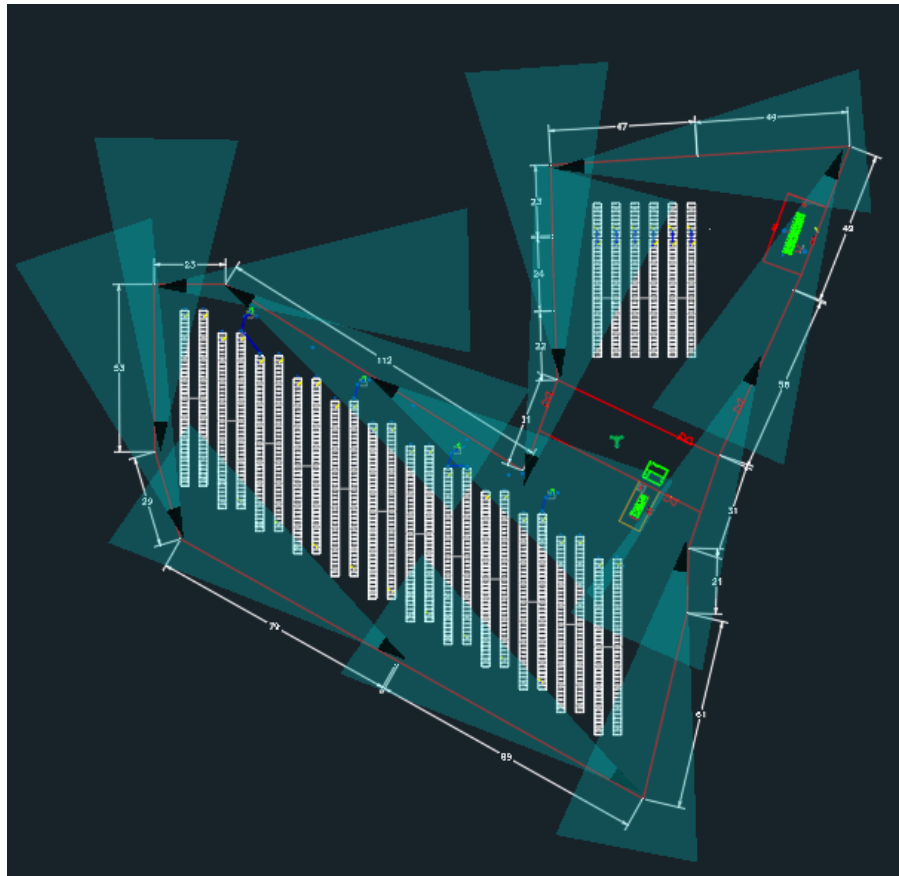
câmeras é 10.

Ao realizar o cálculo para a distribuição dos quadros, tem-se que um QDC "alimenta" também as câmeras nos Postes anterior e Posterior. Descontando as que são conectadas ao QCC.

$$N_{QDC} = \frac{Postes - Postes_{QCC}}{3} = \frac{10 - 3}{3} = 2,333 \cong 3 \quad (4)$$

Isso indica que devem ser montados 3 quadros externos, onde deve se chegar fibra óptica, numa distribuição em anel, para que se um dos lados tiver um problema como um rompimento, o outro lado continua realizando o tráfego das imagens e alarmes.

Figura 12 – Distribuição das Câmeras no Caso 2



Fonte: A Autora (2025)

Já no caso 2 é necessário prestar atenção aos cantos da Usina. Apesar de serem trechos curtos, por serem irregulares tornam necessários a instalação de câmeras a mais, ficando 13.

De forma similar ao calculado acima, tem-se:

$$N_{QDC} = \frac{Postes - Postes_{QCC}}{3} = \frac{13 - 3}{3} = 3,333 \cong 4 \quad (5)$$

Esse caso, aumenta um QDC, logo um custo maior de mão de obra, para realizar a

montagem dele além dos materiais.

Para ambos os cenários 2 PTZs com IR250 são suficiente para cobertura de apoio de áreas críticas.

Com a instalação realizada, existe o último passo para garantir que o sistema esteja operando, que são as linhas virtuais de barreira. Essas linhas são zonas de detecção configuradas via software nas câmeras ou no sistema de gerenciamento de vídeo (VMS), permitindo identificar movimentações indevidas em pontos estratégicos — como acessos não autorizados ou aproximações em perímetro externo.

A calibração adequada dessas linhas virtuais é essencial para reduzir alarmes falsos e garantir que apenas eventos relevantes sejam notificados à central de monitoramento. Dessa forma, o sistema CFTV atua não só como elemento reativo, mas também como ferramenta preventiva de segurança.

As câmeras IP possuem uma interface web integrada, acessível por navegador, através da qual é possível configurar todos os parâmetros operacionais. Nessa interface, o instalador ou operador pode ajustar a qualidade da imagem, selecionar o padrão de compressão (como H.264, H.265 ou Smart Codec), definir resoluções, taxa de quadros (FPS), além de configurar perfis de vídeo distintos para gravação e transmissão ao vivo.

Também é nesse ambiente que se realizam as configurações de rede, como o endereço IP fixo, porta de acesso, gateway e DNS, além da integração com o sistema de gerenciamento de vídeo (VMS) ou NVRs.

Além disso, a página web das câmeras IP permite a ativação e ajuste dos recursos analíticos embarcados, como detecção de movimento, cruzamento de linha, intrusão em área, e agendamento de alarmes com base em horário ou eventos.

Essa capacidade de configuração individualizada é essencial para garantir o desempenho ideal do sistema, adaptando cada câmera ao cenário específico em que está instalada — como áreas externas, ambientes noturnos ou zonas com grande movimentação.

3.3 Fibra Sensível

Ao trabalhar com a fibra óptica sensível, é necessário levar em conta:

- Tipo de instalação: Enterrada (solos tratados) ou em alambrados.
- Sensibilidade: Detecta vibrações ou pressão ao longo de todo o cabo.

- Processamento: Quantas controladoras cobrem o perímetro analisado.

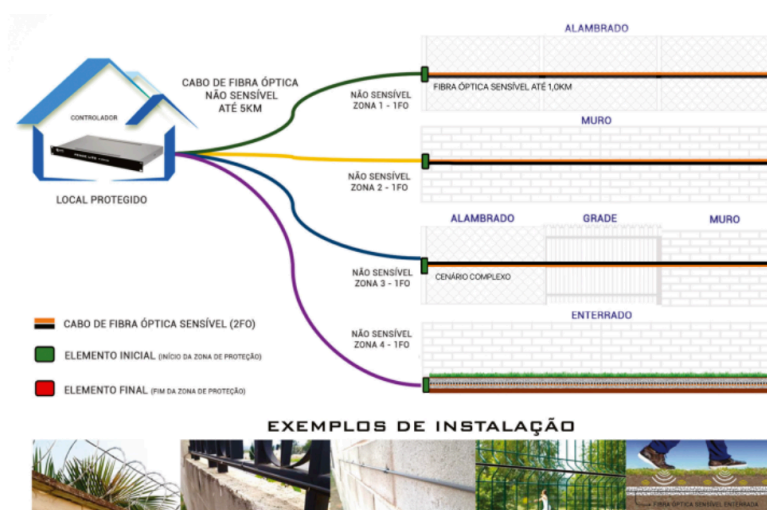
A tecnologia do Sensoreamento Óptico possui vários níveis assim como as câmeras com analítico ou os sensores de barreira.

Dando um passo para trás e analisando melhor os cenários de aplicação, temos dois perímetros de 800 metros cada. Em ambos os casos, os alambrados possuem cerca de 2,4m de altura.

Existem opções de controladoras que projetegem até 100km, com precisão de 3-20m, mas esses modelos tem um custo bem mais elevado.

É interessante notar que existem soluções que funcionam com o mesmo princípio, de detecção por variação na fibra óptica, mas para escalas menores. Como é o caso da Solução Fence Lite, de proteção até 4000m, distribuídos em 4 zonas de 1000m.

Figura 13 – Topologia Fence Lite



Fonte: Alfa Sense

Para essa tecnologia a instalação no alambrado é um jeito mais rápido e fácil de ser implantado, a fixação deve ser feita a cada 30cm com o uso de abraçadeiras, mantendo a Fibra anexada ao alambrado mas não prensada contra ele. Esse tipo de fixação pode ser observado na imagem a seguir, quanto maior a superfície de contato da fibra com o alambrado, melhor funcionará a solução, já que as vibrações provocadas por tentativas de escalada ou corte no alambrado irão disparar um alarme na controladora.

Figura 14 – Fibra Óptica fixada com abraçadeiras



Fonte: A Autora (2025)

Para saber quanta fibra é necessária, é feita uma relação entre a metragem linear da Fibra e a dela montada no Painel entre os mourões.

Considerando cercas de alturas diferentes, é possível obter a tabela abaixo, com a proporção de fibra óptica necessária para cada metro linear.

Tabela 1 – Quantidade de Fibra Dimensionada

ALTURA DA CERCA	FIBRA / METRAGEM LINEAR	FIBRA / PAINEL 2,9M
1,8m	1,62:1	4,7m
2,4m	1,83:1	5,3m
3,0m	2,03:1	5,9m

Fonte: Adaptado de Alfa Sense (2024)

Considerando os 800m e a cerca de 2,4m,

$$Fibra = 800 \times 1,83 = 1464m \quad (6)$$

A arquitetura do sistema de detecção de intrusão perimetral será baseada em uma configuração mínima de duas zonas de detecção independentes. Conforme as especificações

de performance do sistema, cada zona de detecção ativa (cabo sensor) é limitada a uma extensão máxima de 1.000 metros. Esta limitação garante a resolução e sensibilidade adequadas para a detecção de perturbações. Para os cenários propostos, uma única Unidade de Processamento de Alarme (controladora) com capacidade para, no mínimo, dois canais (zonas) é suficiente para cobrir o perímetro designado.

A instalação da controladora deve ser executada em um ambiente controlado e seguro, preferencialmente em um rack de 19 polegadas localizado na Sala de Controle da Usina ou em um gabinete de telecomunicações climatizado. É mandatório que o equipamento seja conectado a um sistema de aterramento elétrico de baixa impedância (resistência inferior a 5 Ohms), seguindo as premissas da norma NBR 5410, a fim de assegurar a proteção contra descargas atmosféricas, surtos de tensão e mitigar os efeitos de interferência eletromagnética (EMI).

Uma zona de detecção é efetivamente estabelecida entre dois pontos demarcadores passivos. O ponto de ativação, conhecido como elemento inicial, pode estar instalado a uma distância de até 5 km de distância da controladora, utilizando um cabo de fibra óptica de *lead-in*. O elemento final delimita o término da zona sensível e deve estar posicionado no máximo 1 km após o elemento inicial correspondente, formando assim o trecho monitorado por intrusão via fibra.

Esses elementos — inicial e final — devem ser instalados em invólucros com grau de proteção adequado (mínimo IP66), podendo ser inseridos em Caixas de Terminação Óptica (CTO), quadros de comando ou caixas de emenda óptica, desde que sejam observadas boas práticas de instalação. A fibra deve ser acomodada sem tensionamentos mecânicos, com curvaturas suaves e respeitando o raio mínimo de curvatura recomendado pelo fabricante, evitando atenuações excessivas ou danos à estrutura óptica.

As sobras técnicas de fibra devem ser acondicionadas em formato de espiral suave dentro das caixas de terminação, ou próximas delas, garantindo que não haja pontos de esmagamento ou dobras agudas.

O manuseio e a instalação criteriosa do cabo sensor são fatores críticos que impactam diretamente a sensibilidade, a confiabilidade e a vida útil do sistema, especialmente em ambientes externos como usinas fotovoltaicas, que estão sujeitas a constantes variações térmicas e estresse mecânico.

4 Análise Comparativa das Tecnologias de Segurança

A comparação das soluções de segurança perimetral para usinas deve considerar quatro critérios principais: custo, eficácia, manutenção e integração com outros sistemas.

O custo envolve não apenas o investimento inicial para aquisição e instalação dos equipamentos, mas também os custos operacionais e de manutenção ao longo da vida útil do sistema. Entre as soluções comparadas — sensores de barreira, câmeras com analítico de vídeo e fibra óptica sensorial — observa-se uma variação significativa nos investimentos necessários, tanto em infraestrutura quanto em manutenção. Os valores apresentados foram estimados com base em catálogos técnicos de fornecedores como Intelbras, Optex, Hikvision, Dahua, Axis, VETTI e Furukawa e bases de dados de projetos reais em usinas fotovoltaicas, datando dos meses de evolução deste trabalho.

A eficácia está relacionada à capacidade de detectar intrusões com baixa taxa de falsos alarmes, garantindo cobertura total do perímetro e adaptabilidade a diferentes tipos de terreno.

A manutenção refere-se à frequência e complexidade das intervenções necessárias para manter o sistema operacional, enquanto a integração avalia a compatibilidade dos equipamentos com sistemas de monitoramento existentes, como CFTV, alarmes e controle de acesso, além da facilidade para expansão futura.

No caso dos sensores de barreira, o custo é moderado, pois exige múltiplas unidades distribuídas ao longo do perímetro. Eles apresentam eficácia em perímetros retos, mas são sensíveis a desalinhamentos e interferências ambientais, o que pode demandar manutenção frequente para ajustes e limpeza. A integração desses sensores com sistemas de alarme e CFTV é geralmente boa, permitindo respostas rápidas a eventos detectados. Apresentam um custo médio de R\$ 2.500 por par de sensores, considerando modelos com alcance de até 100 metros, resistentes à intempérie e dotados de funções anti-mascaramento.

Em cenários com 16 a 19 pares, o custo de aquisição gira em torno de R\$ 48.000. A esse valor, soma-se a infraestrutura de postes, energia elétrica e eletrodutos, com custo médio estimado de R\$ 15.000. A instalação especializada, que exige alinhamento preciso dos feixes e testes operacionais, pode alcançar R\$ 8.000. Já a manutenção anual — geralmente preventiva e corretiva — inclui verificação do alinhamento, limpeza das lentes e testes de disparo,

representando um custo aproximado de R\$ 5.000 por ano. O total estimado de implantação dessa solução gira em torno de R\$ 71.000, sendo indicada para perímetros segmentados e acessos controlados.

Sistemas de CFTV, especialmente quando compostos por muitas câmeras fixas ou PTZ, possuem custo mais elevado devido à infraestrutura necessária e à manutenção periódica das câmeras, como limpeza das lentes e ajustes técnicos. Modelos de câmeras fixas com inteligência artificial, capazes de identificar pessoas, veículos e movimentos suspeitos, custam entre R\$ 8.000 e R\$ 10.000 por unidade, incluindo licenciamento de software e armazenamento em NVRs ou servidores. Considerando um sistema com 10 a 13 câmeras, o custo médio de equipamentos é de R\$ 120.000. A infraestrutura associada — cabos de rede (Cat6 ou fibra), switches PoE, caixas de passagem e energia elétrica — representa um adicional de R\$ 25.000. A instalação, envolvendo configuração de rede, ajuste de zonas de detecção e testes integrados, pode chegar a R\$ 15.000. A manutenção anual, que inclui limpeza de lentes, troca de HDs, atualizações de firmware e reconfigurações, está estimada em R\$ 10.000.

O custo total de implantação de um sistema de videomonitoramento inteligente fica próximo de R\$ 160.000, sendo a opção mais cara, mas com maior valor agregado em termos de verificação visual e evidência de ocorrências. Contudo, oferecem alta eficácia pela cobertura visual detalhada, especialmente quando equipados com tecnologia infravermelha para baixa luminosidade, e se integram muito bem com sistemas digitais de monitoramento e gravação.

A fibra óptica sensível apresenta um custo inicial moderado a alto, por ser uma solução inovadora e altamente eficaz para grandes perímetros. Baseada em tecnologias de detecção distribuída (DAS ou DTS), essa solução utiliza o próprio cabo de fibra óptica como sensor, permitindo identificar e localizar tentativas de invasão, cortes, escavações ou escaladas. Uma controladora sensorial com capacidade para até 2 km de cobertura custa em média R\$ 80.000 a R\$ 100.000, dependendo da tecnologia (Rayleigh, Brillouin, interferometria, etc).

Estima-se um custo de R\$ 90.000 em 2 km de cabo sensível, acessórios e equipamentos principais. A infraestrutura necessária — incluindo dutos subterrâneos, canaletas, caixas de emenda e proteção mecânica — representa um custo de cerca de R\$ 30.000. A instalação técnica envolve fusões ópticas, testes OTDR e calibração do sistema, totalizando aproximadamente R\$ 10.000. Como a fibra é passiva, a manutenção anual é baixa, girando em torno de R\$ 3.000, geralmente dedicada ao monitoramento da controladora e atualizações de software. O custo total de implantação da solução fica em torno de R\$ 130.000, com destaque para alta escalabilidade

e baixo custo por metro protegido, ideal para usinas solares, áreas industriais e propriedades rurais.

Considerando o equipamento e a instalação especializada, mas compensa com alta eficácia em perímetros complexos e irregulares, onde outras tecnologias podem apresentar falhas ou alarmes falsos frequentes. Sua durabilidade é elevada, com baixa necessidade de manutenção por até 25 anos, o que reduz os custos operacionais no médio e longo prazo.

Tabela 2 – Comparativo de Tecnologias

Tecnologia	Aplicação Ideal	Vantagens para Perímetro Regular	Vantagens para Perímetro Irregular
Sensores de Barreira	Detecção de intrusão por feixes IR	Fácil instalação baixo custo em perímetros retos	Pode exigir ajustes frequentes em perímetros irregulares
CFTV	Monitoramento Visual Contínuo	Boa Cobertura com Posicionamento ideal	Número maior de câmeras e ajustes de campo de visão
Fibra Óptica Sensível	Detecção contínua e precisa	Alta durabilidade, imune a interferências Eletromagnéticas	Excelente para perímetros complexos e com obstáculos

Fonte: A Autora (2025)

Estudos de casos reais mostram que usinas fotovoltaicas localizadas em terrenos regulares tendem a adotar a combinação de sensores de barreira com câmeras fixas, pois essa estratégia oferece um bom equilíbrio entre custo e eficácia, aproveitando a geometria simples para uma instalação otimizada. Já usinas situadas em áreas com obstáculos naturais, como zonas alagadas ou áreas de proteção ambiental, têm preferido a fibra óptica sensível para garantir uma cobertura contínua e precisa, minimizando alarmes falsos causados por animais ou fatores ambientais. Nesses casos, a fibra é frequentemente complementada por câmeras PTZ, que proporcionam monitoramento visual flexível e detalhado em pontos críticos.

Para perímetros regulares, a combinação de sensores de barreira com câmeras fixas é recomendada, pois o sistema de segurança, pois sua instalação pode contornar obstáculos físicos e garantir detecção contínua e precisa.

A complementação com câmeras PTZ traz flexibilidade para monitorar áreas específicas com maior detalhamento. Embora o custo inicial seja maior, a redução significativa de alarmes falsos e a menor necessidade de manutenção tornam essa solução mais vantajosa a médio e longo prazo.

No entanto, uma desvantagem importante a ser considerada no uso da fibra óptica sensível é a vulnerabilidade em caso de rompimento físico do cabo. Diferente de sensores ponto a ponto, que podem isolar falhas apenas na zona afetada, o rompimento da fibra pode interromper completamente a detecção ao longo de toda a zona, comprometendo a cobertura do perímetro monitorado.

Essa falha pode ser causada por ações acidentais — como escavações, manutenção não autorizada ou impacto mecânico — ou ainda por tentativa deliberada de sabotagem. Em locais onde não há redundância de anel ou sistema de bypass, o rompimento pode exigir o reposicionamento e fusão de fibra, o que demanda tempo, mão de obra especializada e, muitas vezes, acesso restrito à infraestrutura física. Pode ser evitado com a instalação enterrada, mas essa necessita de um maior preparo da infraestrutura .

5 Conclusão e Considerações Finais

Após analisar diversos cenários de aplicação, casos de sucesso reportados e as simulações executadas, nota-se que a escolha da tecnologia ideal deve sempre levar em conta o perfil do terreno, o tipo de usina e o orçamento disponível.

Todos os sistemas, quando bem projetados e executados, são capazes de suprir a demanda por proteção que possa mandar alertas de forma remota. É fundamental que o projeto considere as características do terreno e as particularidades da usina, como áreas alagadas ou zonas de proteção ambiental, para escolher a melhor configuração e localização dos sensores e câmeras.

A escolha final varia conforme o objetivo com os alertas. No caso dos sensores e da fibra óptica sensível, caso não haja uma implementação híbrida com câmeras, dificulta-se a identificação visual de intrusos. Os sensores são mais baratos, mas exigem manutenções constantes. Já a fibra óptica sensível oferece o melhor custo-benefício para perímetros complexos e extensos. Sistemas híbridos — que unem sensores, câmeras e fibra — combinam detecção precisa e confirmação visual, sendo recomendados para áreas críticas e estratégicas.

Entre os desafios futuros estão a redução de alarmes falsos, especialmente em ambientes com alta interferência ambiental, e a adaptação das tecnologias para novos formatos de usinas, como as solares flutuantes, que demandam monitoramento sob lâminas d'água. Tecnologias sustentáveis, como radares alimentados por energia solar, também estão em desenvolvimento para garantir segurança com baixo impacto ambiental.

Apesar de não existir uma fórmula concreta que garanta a proteção total e a garantia de não haver mais intrusões, sistemas híbridos de proteção perimetral baseada em fibra óptica, integrada a sistemas de alarme e CFTV, representam o estado da arte em segurança para usinas de energia, garantindo proteção total e confiabilidade operacional. Investir em tecnologias integradas não só melhora a proteção, mas também pode reduzir custos operacionais e riscos, contribuindo para a operação segura e eficiente da usina e minimizar custos e riscos futuros.

REFERÊNCIAS

- ABESE. **Entendendo a Segurança Eletrônica: objetivos e benefícios**. 2025. Disponível em: <<https://www.abese.org.br/conteudos/entendendo-a-seguranca-eletronica-objetivos-e-beneficios>>. Acesso em: 28 mar. 2025.
- ABSOLAR. **Infográfico ABSOLAR**. 2025. Disponível em: <<https://www.absolar.org.br/mercado/infografico/>>. Acesso em: 21 abr. 2025.
- ALMEIDA, C. de. **Tecnologias aplicadas à segurança:: um guia prático**. Editora Intersaberes, 2017. Disponível em: <<https://books.google.com.br/books?id=mS0yEQAAQBAJ>>.
- Usina bifacial utiliza detecção por fibra óptica sensível para mitigar roubos e furtos. **Revista Canal Solar**, 2025. Disponível em: <<https://canalsolar.com.br/usina-bifacial-fibra-optica-mitigar-roubos-furtos/>>. Acesso em: 13 mar. 2025.
- HEIN, H. (org.). **Como evitar furtos de cabos em usinas solares?** Canal Solar, 2024. Disponível em: <<https://canalsolar.com.br/furtos-cabos-usinas-solares-como-evitar/>>. Acesso em: 26 mar. 2025.
- INTELBRAS. **Manual do usuário: IVA 7100 Dual, Quad/Black, Hexa e Octa**. 2024. Disponível em: <https://backend.intelbras.com/sites/default/files/2024-12/Manual_IVA_7100_Dual_Quad_Hexa_Octa_portugues_01_24_site.pdf>. Acesso em: 19 mar. 2025.
- KLEIN, A. L. Análise operacional da usina solar fotovoltaica ‘mulheres na energia solar’ do campus litoral norte da ufrgs. 2025.
- MURDAN, A. P.; CAREMBEN, S. An autonomous solar powered wireless monitoring and surveillance system. In: . [S.l.: s.n.], 2018. p. 784–789. 10.1109/ICIEA.2018.8397820.
- NAWAZ, F.; KAYANI, U.; AYSAN, A. F. Unraveling the hidden costs: how cable theft and vandalism fuel soaring energy tariffs in emerging economies. **International misc of Management and Marketing**, v. 14, p. 255–262, 2024.
- OZKAN T ERKORKMAZ, B. C. E. Fotas (fiber optic based acoustic sensing system): requirements, design, implementation, tests and results. Periódico, 2020. Disponível em: <<https://www.spiedigitallibrary.org/conference-proceedings-of-spie/11525/115250B/FOTAS-Fiber-Optic-Based-Acoustic-Sensing-System--requirements-design/10.1117/12.2581713.short>>.
- PINHO, J.; GALDINO, M. **Manual De Engenharia Para Sistemas Fotovoltaicos, CEPIL-CRESEB**. 2014.
- SAVER. **CCTV Technology Handbook**. [S.l.: s.n.], 2013.
- SHAH, A. P.; PARMAR, A. A.; PANDYA, N. N. Fiber optic applications in solar power plant. **Periódico**, 2015.
- SOBRINHO, A. F. D. P. Princípio de funcionamento de sensores. Universidade Federal de Campina Grande, 2008.