WHITEPAPER

IEC 62351: SEGURANÇA PARA IEC 61850, IEC 104, DNP3 E SISTEMAS ELÉTRICOS

Entenda a IEC 62351, segurança para IEC 61850, IEC 104 e DNP3, TLS, certificados, gestão de chaves, RBAC, legados e interoperabilidade.

A3A® Engenharia de Sistemas

SUMÁRIO

IEC 62351 é uma série de normas de cibersegurança voltada às comunicações e aos sistemas de gestão de energia abrangidos pelo IEC TC 57. Ela define mecanismos para proteger protocolos e modelos utilizados em telecontrole, automação de subestações, centros de operação, intercâmbio entre sistemas e gestão de chaves e acessos.

A série não é um produto e não torna um sistema seguro apenas por ser citada em uma especificação. Sua aplicação exige arquitetura, certificados, chaves, perfis, interoperabilidade, desempenho, operação e testes. Equipamentos podem suportar apenas determinadas partes ou funções.

Em subestações, a IEC 62351 complementa protocolos como IEC 61850, IEC 60870-5-104 e DNP3. Ela também se relaciona com a IEC 62443, que aborda segurança de sistemas de automação e controle de forma mais ampla, incluindo zonas, conduítes e ciclo de vida.

1. O QUE É IEC 62351

A IEC 62351 foi desenvolvida para tratar segurança das comunicações e informações utilizadas em sistemas elétricos.

Os objetivos incluem autenticação, integridade, confidencialidade quando aplicável, controle de acesso, gestão de chaves e monitoramento.

A série reconhece que diferentes protocolos possuem requisitos de tempo, transporte e legado. Por isso, os mecanismos variam entre perfis TCP/IP, MMS, IEC 60870-5 e mensagens IEC 61850.

2. O QUE A IEC 62351 NÃO RESOLVE SOZINHA

A norma não substitui segmentação, hardening, inventário, controle de acesso remoto ou resposta a incidentes.

Criptografar uma sessão não impede uso indevido por uma conta autorizada. Certificados não corrigem uma regra de firewall ampla. Autenticação de mensagem não protege um equipamento sem suporte e sem gestão de chaves.

A IEC 62443 em subestações complementa a visão de arquitetura e ciclo de vida.

3. ESTRUTURA DA SÉRIE IEC 62351

A série é dividida em partes com escopos específicos. As primeiras partes apresentam visão geral e terminologia. Outras tratam segurança de perfis TCP/IP, MMS, telecontrole, IEC 61850, gestão de rede, controle de acesso e chaves.

O projeto deve identificar quais partes são aplicáveis a cada fluxo. Uma subestação pode utilizar vários mecanismos simultaneamente.

Exigir “conformidade IEC 62351” sem indicar partes, perfis e funções produz requisito ambíguo.

4. IEC 62351-1 E IEC 62351-2

A Parte 1 apresenta introdução, escopo e contexto. A Parte 2 define terminologia.

Essas partes ajudam a alinhar linguagem entre concessionária, integrador e fabricante.

Termos como entidade, associação, autenticação, autorização, chave e certificado precisam ser usados de forma consistente.

IEC 62351 precisa ser especificada por parte, perfil e mecanismo.

TLS, autenticação de mensagens, RBAC, certificados e gestão de chaves têm escopos diferentes e precisam ser associados a cada fluxo da arquitetura.

Conhecer a solução de Redes Industriais

5. IEC 62351-3: SEGURANÇA DE PERFIS TCP/IP

A Parte 3 trata proteção de perfis que utilizam TCP/IP. O uso de TLS fornece confidencialidade e integridade do transporte e autenticação por certificados conforme o perfil.

Esse mecanismo é relevante para IEC 60870-5-104, ICCP e outros serviços baseados em TCP.

A implantação exige compatibilidade de versões TLS, conjuntos criptográficos, certificados e nomes. Dois equipamentos podem anunciar suporte e ainda não negociar uma sessão comum.

O artigo sobre IEC 104 detalha a sessão de telecontrole e a porta 2404.

6. TLS EM SISTEMAS ELÉTRICOS

TLS cria um canal protegido entre entidades. Certificados identificam servidores e, em autenticação mútua, clientes.

O canal protege mensagens em trânsito, mas não valida a lógica operacional de um comando. A aplicação continua responsável por autorização e intertravamento.

Handshake, verificação de certificado e renovação precisam ser considerados em dispositivos com recursos limitados.

A inspeção de firewall pode ficar limitada quando o tráfego é criptografado. Monitoramento deve combinar logs dos endpoints e metadados de rede.

7. CERTIFICADOS X.509

Certificados associam uma chave pública a uma identidade. A confiança depende da autoridade certificadora e da validação da cadeia.

O projeto precisa definir nomes, finalidade, validade, algoritmos e armazenamento da chave privada.

Certificados compartilhados entre vários equipamentos reduzem capacidade de revogação e atribuição. Cada ativo deve possuir identidade própria quando suportado.

8. IEC 62351-4: MMS E PERFIS RELACIONADOS

A Parte 4 trata segurança de perfis que utilizam MMS, incluindo aplicações de IEC 61850 e intercâmbio entre centros conforme escopos aplicáveis.

MMS é usado na IEC 61850 para comunicação cliente-servidor, reports, leitura e controle.

A segurança pode envolver transporte protegido, autenticação e requisitos de associação. O suporte precisa ser verificado em IED, gateway e cliente.

O IED em subestações detalha MMS, reports e arquivos SCL.

9. IEC 62351-5: TELECONTROLE

A Parte 5 trata segurança de perfis da IEC 60870-5 e derivados, incluindo mecanismos aplicáveis a telecontrole.

Ela é relevante para IEC 101, IEC 104 e contextos associados ao DNP3.

Os requisitos variam entre comunicação serial e TCP/IP. Equipamentos legados podem exigir gateways ou controles compensatórios.

O DNP3 possui Secure Authentication como mecanismo relacionado à proteção de operações críticas.

10. AUTENTICAÇÃO DE MENSAGENS DE TELECONTROLE

Autenticação ajuda a verificar origem e integridade de mensagens.

Ela reduz risco de comandos forjados e replay quando corretamente implementada.

O sistema precisa gerenciar sequência, chaves, usuários e falhas. Uma mensagem rejeitada deve gerar diagnóstico e alarme sem bloquear indefinidamente a operação legítima.

11. IEC 62351-6: IEC 61850

A Parte 6 trata segurança de perfis IEC 61850, incluindo mensagens de alta criticidade como GOOSE e Sampled Values dentro do escopo aplicável.

Essas mensagens possuem requisitos de latência. A proteção precisa ser compatível com desempenho e capacidade dos IEDs.

A subestação digital e IEC 61850 deve ser projetada com VLANs, prioridade, sincronismo e redundância.

Criptografia e autenticação não devem ser habilitadas sem verificar interoperabilidade e tempo de entrega.

12. SEGURANÇA DE GOOSE

GOOSE utiliza multicast e repetição rápida. Um atacante com acesso à rede pode tentar publicar mensagens forjadas.

Mecanismos de autenticação de mensagem ajudam a verificar integridade e origem.

A gestão de chaves e o suporte dos subscribers são essenciais. Se apenas parte dos IEDs valida a proteção, a arquitetura precisa tratar os demais.

Testes devem medir latência, perda e comportamento diante de assinatura inválida.

13. SEGURANÇA DE SAMPLED VALUES

Sampled Values transportam amostras de corrente e tensão com alta taxa.

A proteção precisa atender capacidade e temporização. Processamento adicional não pode causar perda ou atraso incompatível com proteção.

A rede de processo permanece segmentada e fisicamente protegida. Segurança criptográfica complementa, não substitui, esses controles.

14. IEC 62351-7: GESTÃO DE REDE E SISTEMA

A Parte 7 define objetos de gestão para monitorar sistemas de energia e comunicação.

Ela permite representar condições de segurança, saúde, comunicação e ativos para plataformas de monitoramento.

O SNMP pode transportar informações de gestão quando suportado.

A coleta deve ser integrada ao SIEM ou monitoramento sem sobrecarregar dispositivos.

15. IEC 62351-8: CONTROLE DE ACESSO BASEADO EM PAPÉIS

A Parte 8 trata Role-Based Access Control, ou RBAC, para usuários e agentes.

Papéis representam funções como operador, engenheiro, mantenedor e auditor. Permissões são associadas ao papel em vez de concedidas individualmente de forma ad hoc.

O modelo precisa refletir menor privilégio e segregação de funções. Um operador pode comandar, mas não alterar ajustes; um engenheiro pode configurar dentro do escopo autorizado.

A integração com diretório, PAM e aplicações precisa ser testada.

16. RBAC E SISTEMAS LEGADOS

Equipamentos antigos podem possuir apenas administrador e usuário básico.

Nesse caso, PAM, jump server, segmentação e contas custodidas compensam a falta de granularidade.

O PAM e jump server pode atribuir uma sessão individual mesmo quando o destino usa conta compartilhada.

A limitação deve ser documentada e incluída no plano de modernização.

17. IEC 62351-9: GESTÃO DE CHAVES

A Parte 9 trata gestão de chaves criptográficas.

O ciclo inclui geração, distribuição, instalação, uso, armazenamento, renovação, revogação e destruição.

A segurança do mecanismo depende da proteção das chaves privadas e mestras. Distribuir chaves por e-mail ou arquivos compartilhados elimina a confiança.

Automação é necessária em ambientes com muitos IEDs, mas precisa ser compatível com disponibilidade.

18. AUTORIDADES CERTIFICADORAS

A PKI pode utilizar uma CA corporativa, dedicada a OT ou arquitetura hierárquica.

Separação reduz impacto e permite políticas próprias. Contudo, múltiplas CAs aumentam operação.

O projeto deve definir root offline, intermediárias, emissão, renovação e revogação.

Backups das chaves da CA exigem controles fortes e procedimentos documentados.

19. ENROLAMENTO DE DISPOSITIVOS

Enrolamento associa um certificado ao equipamento. Pode ocorrer na fábrica, comissionamento ou por protocolo automatizado.

A identidade inicial precisa ser confiável. Aceitar qualquer solicitação durante uma janela aberta permite inscrição indevida.

A equipe deve verificar serial, ativo, endereço e responsável antes da aprovação.

20. RENOVAÇÃO DE CERTIFICADOS

Certificados expiram. A renovação precisa ocorrer antes do vencimento e sem interromper a operação.

Equipamentos podem exigir reinicialização ou nova associação. Isso precisa ser conhecido.

Monitoramento deve alertar certificados próximos do vencimento. O servidor NTP é essencial para validação temporal.

21. REVOGAÇÃO

Certificados comprometidos ou de ativos removidos precisam ser revogados.

CRL e OCSP são mecanismos comuns, mas dispositivos OT podem ter suporte limitado ou conectividade restrita.

O comportamento quando a informação de revogação está indisponível deve ser definido. Falhar aberto reduz segurança; falhar fechado pode interromper operação.

22. ARMAZENAMENTO DE CHAVES PRIVADAS

Chaves podem ser armazenadas em software, TPM, HSM ou hardware embarcado.

A proteção depende de capacidade do dispositivo. Exportação deve ser proibida quando possível.

Backups de chaves de servidor precisam de controle. Chaves privadas de dispositivos não devem ser copiadas indiscriminadamente.

23. IEC 62351-10: ARQUITETURA DE SEGURANÇA

A Parte 10 trata diretrizes de arquitetura para sistemas abrangidos pelo TC 57.

Ela ajuda a posicionar mecanismos em centros, subestações, redes e interfaces.

A arquitetura deve ser combinada com zonas e conduítes da IEC 62443 e com a DMZ entre TI e OT.

O objetivo é defesa em profundidade, não depender de um único protocolo seguro.

24. IEC 62351-11: ARQUIVOS XML

A Parte 11 aborda segurança de arquivos XML utilizados no setor elétrico.

Arquivos podem conter modelos, configuração e intercâmbio de informações. Assinatura e proteção ajudam a verificar integridade e origem.

Na IEC 61850, arquivos SCL precisam de governança, versionamento e validação. Um arquivo assinado ainda precisa estar autorizado para o projeto correto.

25. RELAÇÃO COM IEC 62443

IEC 62351 foca comunicações e modelos do setor elétrico. IEC 62443 aborda segurança de sistemas de automação e controle, ciclo de vida, componentes, sistemas e operação.

As séries são complementares. Uma subestação pode aplicar IEC 62443 para arquitetura e requisitos e IEC 62351 para mecanismos dos protocolos elétricos.

Não é adequado escolher uma e ignorar a outra.

26. RELAÇÃO COM IEC 61850

IEC 61850 define comunicação e modelo de automação. IEC 62351 adiciona mecanismos de segurança.

A proteção precisa ser incluída na engenharia de sistema, SCD, certificados, chaves e configuração dos IEDs.

A mera presença de TLS em MMS não protege GOOSE ou Sampled Values; cada fluxo exige mecanismo apropriado.

27. RELAÇÃO COM IEC 104

IEC 104 utiliza TCP e pode ser protegida conforme perfis aplicáveis da IEC 62351.

TLS, certificados e autenticação precisam ser suportados em estação controladora e RTU.

Gateways podem adicionar proteção no transporte, mas o trecho legado continua exigindo controle.

28. RELAÇÃO COM DNP3

DNP3 Secure Authentication protege operações críticas. A IEC 62351-5 trata segurança de perfis de telecontrole relacionados.

A interoperabilidade depende de versão e perfil. O projeto precisa indicar mecanismo exato.

Comandos autenticados ainda precisam de autorização, logs e intertravamentos.

29. DESEMPENHO E LATÊNCIA

Criptografia e autenticação consomem processamento. Em servidores isso pode ser pequeno; em IEDs e tráfego rápido pode ser relevante.

O projeto deve definir latência máxima, taxa de mensagens e capacidade.

Ensaios precisam medir condições normais, pico, failover e renovação de chave.

Não se deve assumir que mecanismo seguro atende tempo crítico sem teste.

30. INTEROPERABILIDADE

Fabricantes podem suportar subconjuntos, versões e algoritmos diferentes.

Uma matriz de interoperabilidade registra parte IEC 62351, perfil, certificado, algoritmo, função e resultado.

FAT com equipamentos reais reduz risco. Declarações de conformidade precisam ser acompanhadas por evidências.

31. GATEWAYS DE SEGURANÇA

Gateways podem proteger um trecho legado ou terminar TLS.

Eles introduzem nova fronteira de confiança. O tráfego pode estar protegido de um lado e aberto do outro.

O diagrama deve mostrar onde criptografia começa e termina. O gateway precisa de hardening, redundância e logs.

32. EQUIPAMENTOS LEGADOS

Legados podem não suportar certificados ou autenticação.

Controles compensatórios incluem rede dedicada, firewall, jump server, monitoramento e proteção física.

A limitação deve ser registrada, com risco e plano de substituição.

Não se deve afirmar conformidade integral quando apenas o gateway suporta a norma.

33. GESTÃO DE PAPÉIS E IDENTIDADES

RBAC precisa ser integrado ao processo de admissão, mudança e desligamento.

Papéis temporários e fornecedores devem expirar.

O MFA em ambientes OT protege autenticação humana. Certificados identificam dispositivos.

Contas de serviço e agentes precisam de identidades próprias.

34. MONITORAMENTO DE SEGURANÇA

Eventos de certificado, falha de autenticação, chave, papel e sessão devem ser registrados.

O SIEM em ambientes OT correlaciona esses eventos com firewall, PAM e endpoints.

Falhas repetidas podem indicar configuração ou ataque. O playbook deve diferenciar.

35. RESPOSTA A FALHAS CRIPTOGRÁFICAS

Certificado expirado, chave comprometida ou CA indisponível podem interromper comunicação.

Procedimentos precisam indicar renovação, revogação, substituição e fallback.

Fallback para comunicação insegura não deve ocorrer automaticamente sem alerta e autorização.

Break-glass precisa ser limitado e auditado.

Criptografia sem arquitetura e ciclo de vida não sustenta a operação.

CA, enrolamento, renovação, revogação, papéis, legados, gateways, logs e contingência precisam ser definidos junto às zonas e conduítes OT.

Conhecer o serviço de Projeto de Telecomunicações

36. ARQUITETURA EM SUBESTAÇÕES

A subestação possui rede de processo, estação, gestão e telecontrole. Cada zona possui fluxos diferentes.

IEC 62351 pode proteger MMS, GOOSE, SV e telecontrole conforme suporte. Firewalls e PRP/HSR tratam outros requisitos.

Certificados e chaves precisam chegar aos IEDs sem criar acesso administrativo amplo.

37. PROJETO E DOCUMENTAÇÃO

O projeto deve produzir arquitetura de confiança, inventário de entidades, matriz de certificados, papéis, algoritmos, fluxos e partes aplicáveis.

Também deve definir CA, validade, renovação, revogação, armazenamento, monitoramento e contingência.

A lista de requisitos precisa indicar versão e perfil por equipamento.

38. FAT

O FAT deve verificar negociação, certificados, papéis, mensagens e desempenho.

Testes incluem certificado válido, expirado, revogado, não confiável e identidade incorreta.

Para GOOSE e SV, medir latência e comportamento diante de autenticação inválida.

Logs e alarmes precisam ser verificados.

39. SAT E COMISSIONAMENTO

No campo, o teste valida a arquitetura real, relógios, firewalls e redundância.

O roteiro mínimo inclui:

O Comissionamento e Aceite Técnico deve produzir evidências por mecanismo.

O aceite precisa testar confiança, desempenho e contingência.

Certificados válidos e inválidos, revogação, RBAC, assinatura, latência, failover, logs e recuperação devem ser comprovados com os equipamentos reais.

Conhecer o serviço de Comissionamento e Aceite Técnico

40. DIAGNÓSTICO DE FALHAS

Falha de TLS exige verificar cadeia, nome, validade, horário, algoritmo e confiança.

Autorização negada pode decorrer de papel, token ou mapeamento. Mensagem rejeitada pode indicar chave, sequência ou assinatura.

Latência elevada pode resultar de processamento, tamanho, rede ou carga.

Logs dos dois endpoints e captura de tráfego são necessários.

41. ERROS COMUNS

Erros frequentes incluem citar a IEC 62351 sem partes, usar o mesmo certificado em vários ativos e não monitorar vencimento.

Também são comuns algoritmos incompatíveis, chaves distribuídas manualmente sem controle, RBAC apenas formal e fallback inseguro.

Outro erro é proteger o protocolo e deixar interface de engenharia aberta.

42. CONCLUSÃO

IEC 62351 fornece mecanismos de segurança específicos para comunicações e sistemas elétricos. TLS, autenticação de mensagens, RBAC, gestão de chaves e monitoramento tratam necessidades que protocolos originais não cobriam.

A aplicação exige engenharia de confiança, interoperabilidade, desempenho e operação. Quando partes e perfis são definidos e testados, a série complementa IEC 61850, IEC 104, DNP3 e IEC 62443 em uma defesa em profundidade coerente.

[1] INTERNATIONAL ELECTROTECHNICAL COMMISSION. IEC 62351 series — Power systems management and associated information exchange — Data and communications security.

[2] INTERNATIONAL ELECTROTECHNICAL COMMISSION. IEC 62351-3 — Communication network and system security — Profiles including TCP/IP.

[3] INTERNATIONAL ELECTROTECHNICAL COMMISSION. IEC 62351-5 — Security for IEC 60870-5 and derivatives.

[4] INTERNATIONAL ELECTROTECHNICAL COMMISSION. IEC 62351-6 — Security for IEC 61850.

[5] INTERNATIONAL ELECTROTECHNICAL COMMISSION. IEC 62351-8 — Role-based access control for power system management.

[6] INTERNATIONAL ELECTROTECHNICAL COMMISSION. IEC 62351-9 — Cyber security key management for power system equipment.

[7] INTERNATIONAL ELECTROTECHNICAL COMMISSION. IEC 62443 series — Security for industrial automation and control systems.

[8] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. NIST SP 800-82 Rev. 3 — Guide to Operational Technology Security. Gaithersburg, 2023.

O que é IEC 62351? É uma série de normas de segurança para comunicações e sistemas de gestão de energia, incluindo IEC 61850 e IEC 60870.**IEC 62351 é a mesma coisa que IEC 62443?** Não. IEC 62351 foca protocolos e modelos de energia; IEC 62443 aborda segurança de automação e controle de forma mais ampla.**Qual parte trata TCP/IP?** IEC 62351-3 trata segurança de perfis que utilizam TCP/IP, incluindo TLS e autenticação por certificados.**Qual parte trata IEC 61850?** IEC 62351-6 trata segurança de perfis IEC 61850, incluindo mensagens rápidas dentro do escopo aplicável.**Qual parte trata RBAC?** IEC 62351-8 trata controle de acesso baseado em papéis.**Qual parte trata gestão de chaves?** IEC 62351-9 trata o ciclo de vida de chaves criptográficas.**IEC 62351 protege IEC 104?** Sim, partes aplicáveis tratam perfis TCP/IP e telecontrole, desde que equipamentos e sistemas suportem os mecanismos.**Equipamentos legados podem usar IEC 62351?** Muitos não suportam diretamente. Gateways e controles compensatórios podem proteger partes da arquitetura.**A norma elimina a necessidade de firewall?** Não. Segmentação, firewall, hardening, acesso remoto e monitoramento continuam necessários.**Como testar IEC 62351?** Devem ser testados certificados, chaves, papéis, mensagens, latência, revogação, failover, logs e contingência.

Soluções relacionadas

Serviços relacionados

Artigos e materiais técnicos relacionados

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