



OHP

IT-Security in der Fernwirktechnik mit den OHP IT-Security Fernwirk-Steuerungen

© Copyright 1989 – 2026 – OHP Automation Systems GmbH

Urheberrechtshinweis: Alle Inhalte dieses Artikels, insbesondere Texte, Fotografien und Grafiken, sind urheberrechtlich geschützt. Das Urheberrecht liegt, soweit nicht ausdrücklich anders gekennzeichnet, bei OHP Automation Systems GmbH. Bitte fragen Sie uns, falls Sie diese Inhalte verwenden möchten. Unter der „Creative Commons“-Lizenz veröffentlichte Inhalte, sind als solche gekennzeichnet. Sie dürfen entsprechend den angegebenen Lizenzbedingungen verwendet werden. Wer gegen das Urheberrecht verstößt macht sich gem. §§ 106 ff UrhG strafbar, wird zudem kostenpflichtig abgemahnt und muss Schadensersatz leisten (§ 97 UrhG).

Allgemeine Hinweise: Die beschriebenen Sicherheitsfunktionen sind abhängig von Gerätetyp, Firmwarestand, Ausstattung und Konfiguration. Maßgeblich ist der für das jeweilige Produkt vereinbarte Leistungsumfang. Die Wirksamkeit der Schutzmaßnahmen setzt eine geeignete Systemintegration, sachgerechte Konfiguration sowie die regelmäßige Installation bereitgestellter Sicherheitsupdates voraus. Ein vollständiger Schutz vor sämtlichen Cyberbedrohungen kann nicht gewährleistet werden. Verweise auf Normen, Whitepaper und regulatorische Anforderungen beschreiben die Orientierung unseres Sicherheitskonzepts. Sie stellen keine pauschale Zusicherung vollständiger Konformität oder Zertifizierung dar. Bestehende Zertifizierungen werden ausdrücklich mit ihrem jeweiligen Geltungsbereich ausgewiesen. Stand der Informationen: 09/2026.

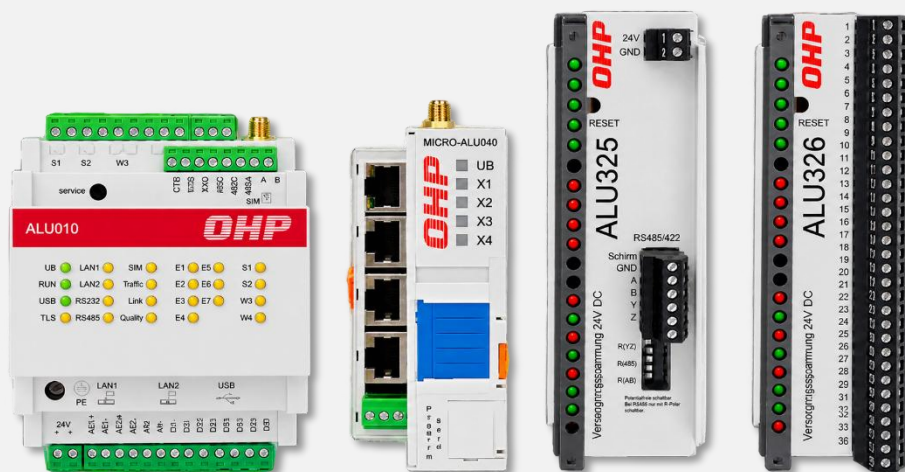
Geschützte Kommunikation. Kontrollierte Zugriffe. Zuverlässiger Betrieb.

Fernwerkstationen verbinden Anlagen mit übergeordneten Leitsystemen und übertragen wichtige Betriebsdaten. Ihre Sicherheit ist ein wesentlicher Baustein für den zuverlässigen Betrieb von Energie- und Infrastrukturanwendungen.

OHP Fernwerkstationen unterstützen Sie dabei, diese Verbindungen abzusichern, sensible Daten zu schützen und Zugriffe gezielt zu steuern. Unser mehrstufiges Sicherheitskonzept verbindet gehärtete Firmware mit verschlüsselter Kommunikation und individuell konfigurierbaren Schutzfunktionen.

Bei der Weiterentwicklung unseres Sicherheitskonzepts nutzen wir das BDEW-Whitepaper 3.0 sowie relevante Anforderungen der IEC 62443-4-1 und IEC 62443-4-2 als Orientierung. Die für unsere Produkte maßgeblichen Anforderungen des EU Cyber Resilience Act (CRA) berücksichtigen wir im Rahmen unserer Produktentwicklung und -pflege. OHP betreibt ein gemäß ISO/IEC 27001 zertifiziertes Informationssicherheits-Managementsystem (ISMS).

Verfügbarkeit und Umfang der Sicherheitsfunktionen hängen dabei von Gerätetyp, Firmwarestand und der Konfiguration ab.



Die IT-Security Fernwerk-Steuerungen
ALU010, ALU040, ALU325 und ALU326

Essentielle Sicherheits-Features auf einen Blick

- ✓ Patch- und Devicemanagement via OHP ControlManager
- ✓ Signierte Firmware
- ✓ Secure Boot
- ✓ Aktuelle, sichere Verschlüsselungs- und Hashalgorithmen
- ✓ IPsec (IKEv2) VPN-Tunnel direkt aus der Steuerung
- ✓ End-to-End Verschlüsselung via TLS
- ✓ Benutzerprofile mit individueller Rechtezuweisung
- ✓ Verschlüsselung der Projektdateien und Firmware
- ✓ Schutz der Integrität (Hashgruppe SHA2)
- ✓ Schutz vor Wiedereinspielen alter Nachrichten
- ✓ Authentisierung der Kommunikationspartner per Zertifikat
- ✓ Sicherer Filetransfer durch SFTP (Secure File Transfer) und FTPS (File Transfer Protocol über SSL)
- ✓ Deaktivierbarkeit von Zugängen
- ✓ Integrierte parametrierbare Firewall
- ✓ Perfect Forward Secrecy zur Unterbindung einer Rück-Entschlüsselung im Fall von abgehörter Kommunikation
- ✓ IT-Sicherheitskonzept der OHP Fernwerkstationen getestet durch das Security Analysis & Incident Response Team (CSIRT) eines großen Energieversorgers
- ✓ Gehärtete Firmware zur Reduzierung der Angriffsfläche
- ✓ Orientierung am Anforderungsprofil des BDEW-Whitepapers 3.0
- ✓ Orientierung an IEC 62443-4-1 für die sichere Produktentwicklung und -pflege
- ✓ Berücksichtigung der für unsere Produkte maßgeblichen Anforderungen des Cyber Resilience Act
- ✓ Kontinuierliche Weiterentwicklung des IT-Sicherheitskonzepts
- ✓ Anpassbare Netzwerkzugriffsregeln zur gezielten Begrenzung erlaubter Verbindungen
- ✓ Einschränkung von Benutzerberechtigungen auf die jeweils benötigten Funktionen
- ✓ Unterstützung einer automatisierten Zertifikatsverwaltung per SCEP
- ✓ Mehrstufiges Sicherheitskonzept aus Firmwarehärtung, Kommunikationsschutz und Zugriffskontrolle
- ✓ Interne Routingfunktion, in vielen Fällen kein externer Router notwendig.

Die essentiellen Sicherheits-Features im Detail

Linux-Echtzeitbetriebssystem

Die Steuerungen setzen Embedded Linux mit einer Echtzeit-Erweiterung als Betriebssystem ein. Dieses erlaubt eine stetige Weiterentwicklung der Firmware um die Anforderungen nach aktuellem Stand der Technik abzubilden.

Das Dateisystem des Embedded Linux ist dabei verschlüsselt. Der Schlüssel für das Dateisystem wird auf der Steuerung generiert und verlässt diese niemals.

Secure Boot

Auf der Fernwirksteuerung ALU010 kommt Secure Boot zum Einsatz. Dadurch wird sichergestellt, dass beim Start ausschließlich vertrauenswürdige und authentifizierte Softwarekomponenten ausgeführt werden. Manipulierte oder nicht autorisierte Software wird bereits während des Bootvorgangs erkannt und deren Ausführung verhindert.

Patch- und Devicemanagement

Mit dem OHP ControlManager steht ein webbasiertes Tool zur einfachen Überwachung und Aktualisierung der Firmwarestände im Feld zur Verfügung.

Firewall auf der Steuerung

Auf den Steuerungen kommt eine Firewall zum Einsatz, welche nach dem Whitelist-Verfahren („Es ist alles verboten was nicht explizit erlaubt ist“) arbeitet.

Das heißt für jeden Dienst oder jedes Paket, dass auf der Steuerung arbeitet und per Netzwerk kommuniziert, muss eine entsprechende Regel innerhalb der Firewall-Konfiguration gesetzt werden.

Um diese Konfiguration möglichst einfach zu gestalten, können die Firewall-Regeln per

OHP Toolbar oder Webserver in einer einfachen Konfigurationsmatrix aktiviert werden. Innerhalb dieser Konfigurationsmatrix befinden sich die Firewall-Zonen, sowie die Regeln.

VPN mittels IPsec IKEV2

Die Steuerungen unterstützen den Aufbau verschlüsselter und authentifizierter VPN-Verbindungen auf Basis von IPsec IKEV2 direkt auf der Steuerung ohne externen Router. So lässt sich die Kommunikation mit Leitsystemen und weiteren Kommunikationspartnern absichern. Flexible Konfigurationsmöglichkeiten ermöglichen die Anpassung an unterschiedliche Netzwerkinfrastrukturen und Sicherheitsanforderungen.

Sichere Übertragung der Konfigurationsdaten via TLS

Die Daten sowie die Anmeldung sind per TLS geschützt. Der Server auf der Steuerung lässt nur verschlüsselte Verbindungen zu, die dem TLS-Standard entsprechen.

Speicherung der Konfigurationsdaten im verschlüsselten Container auf der Steuerung

Dieser Container wird durch den Einsatz einer hybriden Verschlüsselung gesichert. Das kryptographische Verfahren RSA kommt für den asymmetrischen Teil zum Einsatz wobei AES für den symmetrischen Teil genutzt wird. Somit lassen sich die Systemressourcen (CPU und RAM) bei der Ver- bzw. Entschlüsselung optimal nutzen.

Doorman

Einsatz eines „Doormans“ als digitaler Türsteher für Firewall-Berechtigungen und Festlegung des Timeouts bis ein Dienst durch die Firewall wieder gesperrt wird, sobald keine weitere Übertragung stattfindet.

SSH Text Konsole

Es wird eine Konfigurationskonsole, die per SSH erreichbar ist, angeboten. SSH bietet den Vorteil gegenüber der Telnet Variante, dass diese nun nach dem aktuellen Stand der Technik abgesichert werden kann. Mit SSH wird ein marktübliches Werkzeug zum sicheren Fernzugriff bereitgestellt.

Zertifikats- und Schlüsselverwaltung

Die Unterstützung von SCEP erleichtert die automatisierte Bereitstellung und Erneuerung von Zertifikaten im laufenden Betrieb. Perfect Forward Secrecy schützt entsprechend abgesicherte Verbindungen

davor, dass aufgezeichnete Kommunikation durch eine spätere Kompromittierung langfristiger Schlüssel nachträglich entschlüsselt werden kann.

Passend zu Ihrer Intrastruktur

Wirksame IT-Sicherheit entsteht durch das Zusammenspiel von Technik, Konfiguration und Betrieb. Die Sicherheitsfunktionen unserer Fernwerkstationen lassen sich an Ihre Netzwerkstruktur, Berechtigungskonzepte und betrieblichen Anforderungen anpassen. Mit kontinuierlicher Firmwarepflege und technischer Unterstützung begleiten wir Sie bei der sicheren Einbindung Ihrer OHP Fernwerkstationen.

Das neueste Multi-Sicherheitstalent in der OHP Fernwirkfamilie – Die ALU010

- Integriertes 450 MHz/ LTE Dual-Sim-Modem
- IPsec VPN-Router sowie Firewall direkt auf der Steuerung
- Programmierung nach genormtem Standard IEC 61131-3
- Alternativ Parametrierung via Webserver

ALU010 – Der All-In-One Fernwirkcontroller

- Linux Realtime OS mit extended IT-Security
- 450 MHz/ LTE Dual-Sim-Modem
- IEC 61131-3
- 2x Ethernet, physikalisch getrennt
- 1x RS485
- 1x RS232
- 7 DE, 4 DA, 2 AE, 1 AA, 2x So on board



Über die OHP Firmengruppe

Die OHP Firmengruppe ist Ihr starker Partner für anspruchsvolle Aufgaben im Bereich digitaler Systemlösungen für Infrastruktur, Industrie und Verkehr. Unsere Mission ist es, durch Digitalisierung den Ressourceneinsatz zu optimieren.



Muttergesellschaft
Gründung 1989



> 2.200 Leittechnik-
Lizenzen verkauft



> 66.900 SPS/
FWT-Baugruppen
verkauft



90% Eigen-
entwicklungstiefe



Firmensitz in
Rodgau (Nähe
Frankfurt am Main)

- Hard- & Software Entwicklung
- Systemtest & Projektierung
- Steuer- und Schaltanlagenfertigung



Dipl.-Ing. Steffen Ott
Gründer und Geschäftsführer

- Elektrotechnik-Ingenieur
- seit mehr als 37 Jahren im Unternehmen



Dr.-Ing. Thorsten Fiedler
Geschäftsführer

- Elektrotechnik-Ingenieur
- seit mehr als 15 Jahren im Unternehmen



Sebastian Ott (M.Sc.)
Geschäftsführer

- Wirtschaftsingenieur
- seit mehr als 6 Jahren im Unternehmen



Als Familienunternehmen in zweiter Generation mit Sitz in Rodgau bei Frankfurt am Main stehen wir seit über 35 Jahren für Kompetenz und Zuverlässigkeit in der Automatisierungs-, Fernwirk- und Leittechnik. Wir sind Systemlieferant und bieten unseren Kunden innovative Produkte sowie umfassende Dienstleistungen für die Bereiche Infrastruktur, Industrie und Verkehr. Dabei setzen wir konsequent auf durchgängige Systemtechnik und offene Kommunikationsstandards. So schaffen wir die Grundlage für sichere, zukunftsfähige und wirtschaftliche Lösungen mit langfristigem Betrieb. Unsere Expertise und Leistungsfähigkeit spiegeln sich in einem langjährig gewachsenen und namhaften Kundenstamm wider, der auf unsere Lösungen und Partnerschaft vertraut.

Qualität „Made in Rhein-Main“ – seit 1989

Die Mitarbeiter von OHP bündeln das Know-how von über 35 Jahren Erfahrung. Hervorgegangen 1989 aus einer Entwicklungsabteilung der AEG in Seligenstadt greifen wir als eines der wenigen Unternehmen auf ein eigenentwickeltes Produktportfolio, vom Fernwirk-Automatisierungsgerät über offene Kommunikationstechnik bis hin zum Leitsystem, zurück. Unsere Lösungen stehen seit jeher für Investitionsschutz und Innovation. In jedem Fall erhalten unsere Kunden maßgeschneiderte Engineering- und Serviceleistungen.