Partners Universal International Innovation Journal (PUIIJ)
Volume: 04 Issue: 02 | March-April 2026 | ISSN: 2583-9675 | www.puiij.com

IEC 62443 Wireless Security: Deploying OT Wireless Controllers in Industrial Factory Networks

Dr.A.Shaji George

Independent Researcher, Chennai, Tamil Nadu, India.

Abstract - With the global manufacturing processes gaining momentum in their conversion to Industry 4.0, wireless connectivity has ceased to be a luxury and become a necessity to carry out its operations. All automated guided vehicles, IIoT sensors, SCADA terminals, and robotic systems rely on the constant secure wireless communication to maintain production. However, security infrastructures that regulate these networks are often copied off the enterprise IT models which were not created to operate in the operational technology environment. The paper is a technical guide to the protection of industrial wireless infrastructure by installing Prime (On-Premises) Wireless LAN Controllers in factories, which are supposed to be in line with the requirements of the ISA/IEC 62443 standard on cybersecurity. Based on the available standards of industrial security, patterns of deployment in the real world, and protocol-level analysis, the paper considers ten baseline security controls: CAPWAP DTLS tunnel encryption, placement of RADIUS in the on-premises, WPA2-PSK non-compliance at Level 2 of security, isolation of the management plane, Management Frame Protection (802.11w), command authorization by TAC The article postulates that the architecturally correct solution to the factory floor is the Prime Controller and offers a hybrid deployment framework that ensures OT resilience and allows flexibility in the management of the IT-layer.

Keywords: ISA/IEC 62443, CAPWAP DTLS, 802.1X EAP-TLS, Prime Controller, Wireless LAN Controller, OT wireless security, TACACS+, WPA2-PSK, Management Frame Protection, 802.11w, WIPS, SNMPv3, IDMZ, certificate revocation, OCSP, industrial cybersecurity, factory wireless architecture, Zone-Conduit model, NIST SP 800-82, IIoT security.

1. INTRODUCTION

Go to a factory today and the air over the machines is no less active than the production lines below. Robotic controllers, wireless signals by automated guided vehicles, IIoT sensors, handheld barcode scanners, wireless signals by SCADA terminals, and robotic controllers are constantly in motion around the facility. What most observers fail to notice is that there is a layer of protocols, encryption standards, authentication schemes, and access control policies that exist that make the difference between that wireless traffic being trustworthy or dangerously exposed. The wireless security of industries is at an awkward crossroad. It is too technical to be approached knowingly by generic enterprise IT teams, but too network-focused to be approached with confidence by many operational technology engineers who have made their careers off Modbus RTU on serial links. The outcome is a wireless infrastructure in the vast majority of manufacturing facilities that has been implemented under pressure in production, partially secured, and has never been in full compliance with the industrial cybersecurity guidelines that regulate the rest of the OT environment.

This paper is addressed to OT/IT security architects, network engineers and industrial cybersecurity practitioners who must go beyond checklists of surface compliance and go into the underlying engineering

Partners Universal International Innovation Journal (PUIIJ)
Volume: 04 Issue: 02 | March-April 2026 | ISSN: 2583-9675 | www.puiij.com

rationale of each security choice. Each of the controls below is based on a particular threat, a particular protocol vulnerability or a particular compliance requirement based on the ISA/IEC 62443, NIST SP 800-82 or a pattern of the established industrial network architecture. It is not aimed at presenting a product recommendation or a comparison of the vendors. It is to offer a technically sound, realistic action plan to any person in charge of designing, implementing, or auditing wireless security in a factory setting.

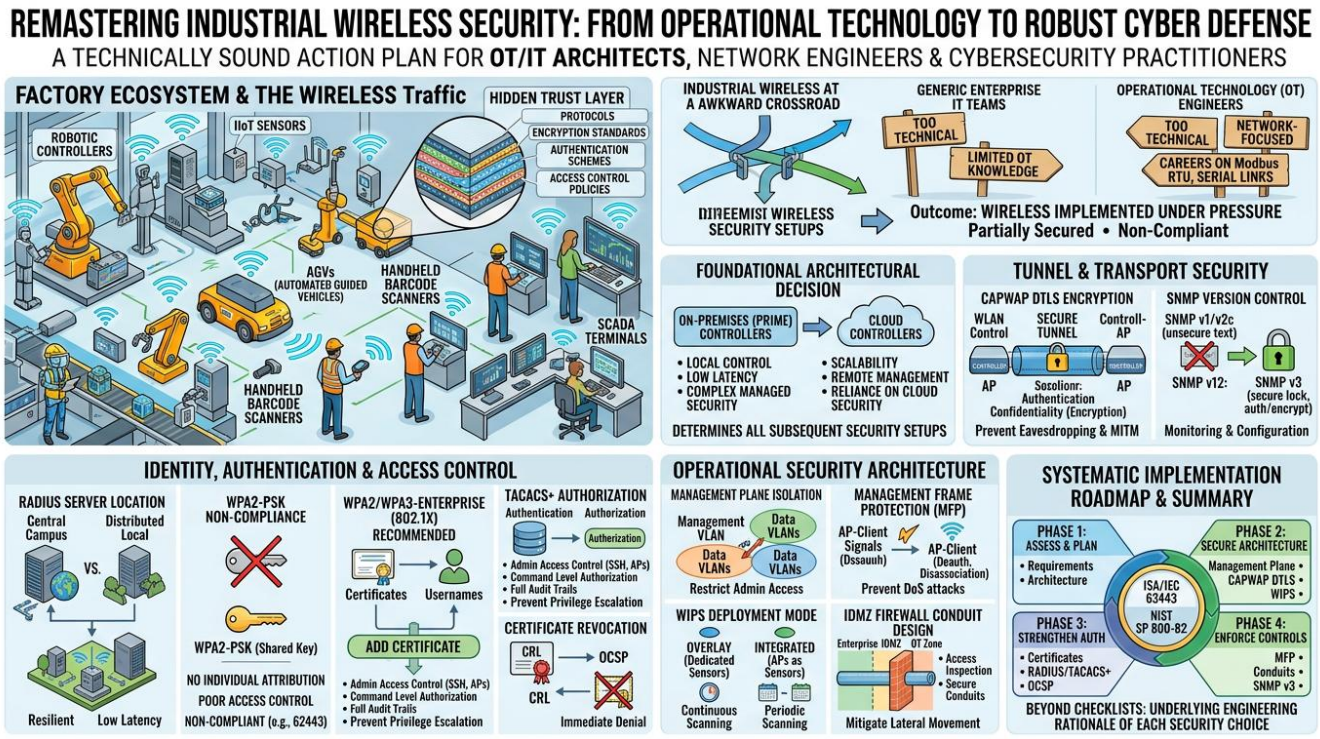

Fig -1: Remastering Industrial Wireless Security

The paper has five substantive parts. The architectural decision in Section 2 concerns the foundational architecture between the Prime (On-Premises) Controllers and Cloud Controllers since this decision will determine all of the subsequent security setups. Section 3 includes the security of tunnels and transport such as CAPWAP DTLS encryption, and SNMP version control. Section 4 is the identity, authentication and access control, which is about RADIUS server location, WPA2-PSK non-compliance, TACACS+ authorization, and certificate revocation. Section 5 is the discussion of operational security architecture, which includes management plane isolation, Management Frame Protection, WIPS deployment mode and IDMZ firewall conduit design. Section 6 summarizes all controls to a systematic implementation structure.

2. OBJECTIVES OF THE STUDY

The following are the key objectives of this article the development of a technically grounded, standards-compliant security architecture to wireless implementations in industry the discussion of the real threat vectors, protocol weaknesses and compliance requirements that underlie each security control the evaluation of the architectural trade-offs between on-premises and cloud-managed wireless controllers in the context of the needs of an OT network and the delivery of a workable implementation hierarchy

Partners Universal International Innovation Journal (PUIIJ)
Volume: 04 Issue: 02 | March-April 2026 | ISSN: 2583-9675 | www.puiij.com

3. HISTORICAL CONTEXT AND CURRENT TRENDS

3.1 The Evolution of Industrial Wireless Security

Industrial wireless networking was not initially a design with security in mind. The use of 802.11b and 802.11g was firstly implemented in factories at the beginning of the 2000s in order to provide mobility to handheld devices and avoid cabling expenses. The security settings of that time were often that of WEP encryption (when encryption was applied at all) and partitioning of the network was not an issue that was taken into account at the wireless layer. The OT network per se was presumed to be physically safe because it was within the factory grounds.

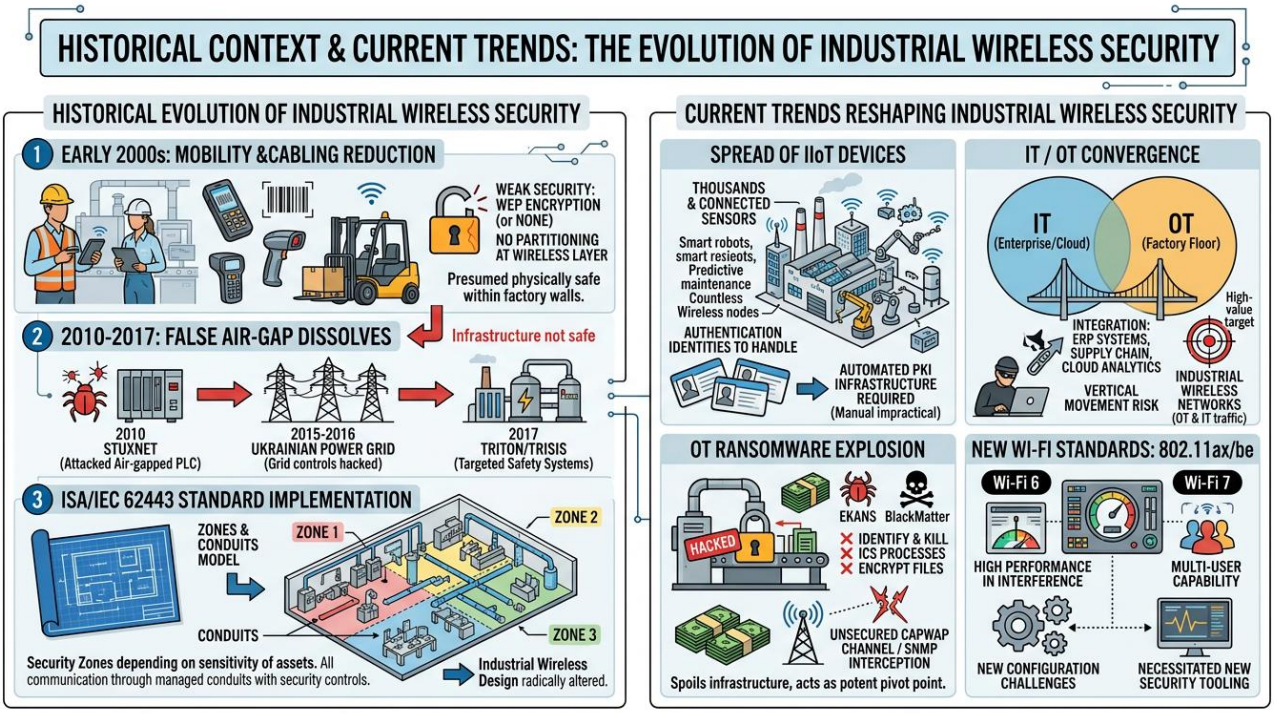

Fig -2: The Evolution of Industrial Wireless Security

That was the assumption that started to be disintegrated in front of our eyes in 2010. The case of Stuxnet showed that air-gapped industrial networks might be attacked, and later cases, such as the Ukrainian power grid attacks of 2015 and 2016 and the Triton/TRISIS attack on safety instrumented systems in 2017, proved that industrial infrastructure was not a mere possibility of attack, but a highly appealing one. The idea of physically isolated and hence safe was no longer believable. The release and gradual implementation of the ISA/IEC 62443 (originally in the form of ISA-99 at the beginning of the 2000s, which was subsequently developed into its present form) gave the industrial segment a detailed cybersecurity framework that was specially tailored to the conditions of an operational technology environment. The Zone-Conduit model of the standard brought about the idea of a security zone definition depending on the sensitivity of the assets in those zones, and that all communication between zones must pass through clearly defined, managed conduits with suitable security controls. This architecture radically altered the design that was required of industrial wireless network since all SSIDs, all authentication interactions and all management protocols were potential conduits that would have to be formally defined and controlled.

3.2 Current Trends Reshaping Industrial Wireless Security

A number of convergent forces are driving industrial wireless security into being increasingly significant as well as increasingly complex than it was even half a decade ago. The most evident trend is the spread of IIoT devices. Thousands of wireless sensors, controllers and monitoring devices are being implemented in manufacturing facilities in digital transformation efforts. All these devices offer an opportunity to the attackers, and each of them brings a new authentication identity that should be handled, provisioned, and revocable. The magnitude of the device populations in the contemporary factories renders the manual management of certificates to be impractical and requires the automated PKI infrastructure.

There is an intersection of IT and OT networks, which is generating new attack surfaces. The historical isolation between IT and OT is decreasing as factories integrate their production systems with enterprise resource planning (ERP) systems and supply chain platforms, and cloud analytics services. All the new links between these spheres are the possible ways of a vertical movement of an attacker who hacks either of the sides. A natural meeting point and, thus, a high-value target, is the industrial wireless networks which often have both OT device traffic and IT management traffic.

Cybercrime of operational technology in the form of ransomware has grown exponentially. Organizations like EKANS, BlackMatter and their predecessors have created malware that is targeted to identify and kill industrial control system processes and then encrypt files. An unsecured CAPWAP channel or an intercepted authentication traffic on an unsecured SNMP channel can allow an attacker to spoil a wireless infrastructure, and acts as a potent pivot point to these attacks. The shift to 802.11ax (Wi-Fi 6) and 802.11be (Wi-Fi 7) in industrial settings presents new features, such as better performance in high-interference settings and multi-user capability, but also presents new configuration challenges and necessitated new security tooling in order to effectively monitor it.

4. THE FOUNDATIONAL ARCHITECTURAL DECISION: ON PRIME CONTROLLER VERSUS CLOUD CONTROLLER

The most significant architectural choice in the industrial wireless design must be considered first before any single security control can be meaningfully considered; it is the location of the control plane.

4.1 Understanding the Two Architecture Models

An on-premises Wireless LAN Controller (WLC), also known as a Prime Controller, is a physical or virtual appliance that is implemented within the factory network boundary. Examples of these representative products are Cisco WLC 9800 series, Cisco Catalyst Center (previously known as DNA center), and Aruba Mobility Controllers. The controller handles all access points, traffic policy, authentication processes and security settings all within the plant boundary and without the need of a connection to the outside internet to function normally. Cloud Controller is an as a service software that is hosted in a data center run by the vendor. The most common that are deployed are Cisco Meraki, Aruba Central, and Juniper Mist. The administrators can control the access points and configurations using a web-based dashboard that can be accessed via any device that has an internet connection. The control plane is located in the cloud whereas the data plane in most architectures is located locally in the site by local forwarding. Periodically, access points cannot be configured by the cloud platform, providing a way to synchronize the configuration and update the firmware and policies.

Partners Universal International Innovation Journal (PUIIJ)
Volume: 04 Issue: 02 | March-April 2026 | ISSN: 2583-9675 | www.puiij.com

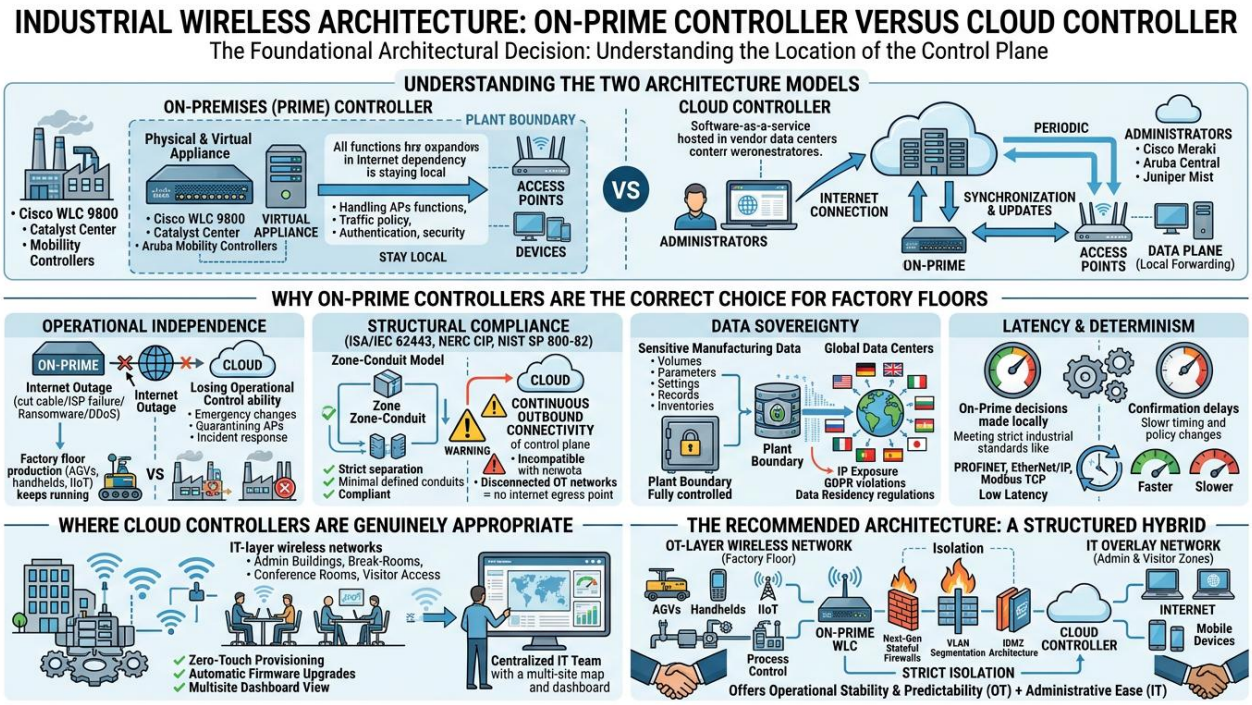

Fig -3: Industrial Wireless Architecture: On-Prime Controller Versus Cloud Controller

Both architectures can be considered as valid solutions in a particular case. The key issue is whether the conveniences of operation provided by the cloud model override the structural constraints in case the network under consideration controls a batch production line in a pharmaceutical company, an assembly robot in an automotive factory, or a control room in a power plant.

4.2 Why Prime Controllers (On-Prime Solutions) Are the Correct Choice for Factory Floors

The first difference is operational independence. A Prime Controller (On-Prime Solutions) is fully located within the local network. In case an internet connection is lost due to an ISP failure, cut of a physical cable, ransomware attack on the corporate IT network or a deliberate denial-of-service attack, the wireless network on the factory floor does not stop its operation. Access points remain in their configuration, devices keep on authenticating and roaming and the production wireless network behaves like the non-existent external internet.

This is not ensured in a cloud-managed architecture. Although the data plane of most cloud controller implementations is locally operational in the event of a cloud outage, the capacity to push emergency configuration, quarantine a compromised access point, react to an active security incident or bring on a replacement device is solely cloud reachable. A wireless management system that loses its operational control ability in the unfortunate event of an internet outage is a risk that the economics of production of the factory simply cannot afford.

The structural incompatibility of the cloud controllers and OT network requirements due to compliance alignment with ISA/IEC 62443 is incompatible with firewall exceptions. The Zone-Conduit model provided by the standard demands that OT networks should be disconnected with the public internet, and that any communication between zones should be clearly defined, reasoned, and regulated. Cloud controller needs continuous outbound internet connectivity of its control plane. This connectivity is also a conduit, which, in

turn, needs to be formally documented, risk-assessed, and approved in accordance with ISA/IEC 62443 rule. More to the point, NERC CIP and NIST SP 800-82 specifically outline designs in which the critical infrastructure OT networks do not have an internet egress point at all. This requirement is incompatible with a cloud controller.

The issue of data sovereignty is an increasing problem, depending on the sensitivity of the manufacturing process. Data on network telemetry, device inventories, traffic statistics, authentication logs, event records, and others contain data that can display volumes of production, process parameters, equipment settings, and patterns of operations. Having a On-Prime Controller, all these data are in the physical and logical boundaries of the facility, which are under the full control of the organization. Cloud controllers periodically send telemetry and metadata to vendor platforms in data centers which might be in other legal jurisdictions, and it is a valid concern that intellectual property is exposed, GDPR is violated, and data residency regulations in defence, aerospace and pharmaceutical manufacturing.

Latency and determinism are not just important as the majority of cloud controller marketing literature fails to admit. Industrial standards like PROFINET, EtherNet/IP and Modbus TCP are very strict in terms of timing. All the decisions on policy enforcement and management are done locally by a Prime Controller. Cloud controller makes a change in the latency of any management communication which needs cloud confirmation, and in certain designs, policy changes do not entirely reflect to access points until cloud synchronization is complete.

4.3 Where Cloud Controllers Are Genuinely Appropriate

The attack on cloud controllers in the context of OT does not mean that cloud controllers should be attacked in general. In the larger factory environment, they fit well in the management of IT-layer wireless networks that span administrative buildings, break-rooms, conference rooms and visitor access areas. These regions are devoid of OT resources, do not have latency sensitive processes and do not have air-gapping. Zero-touch provisioning, automatic firmware upgrades, and multisite dashboard view enable them to gain a great deal. A cloud controller can be used to give a centralized IT team of manufacturing organizations that operate dozens of geographically dispersed facilities a single, centralized view and configuration management without having to deploy individual, on-premises infrastructure to each geographic location. This architectural design is operationally viable in case of the corporate IT overlay network of a multi-site organization.

4.4 The Recommended Architecture: A Structured Hybrid

A layered hybrid architecture with a distinct and implemented separation is the most justifiable suggestion to a contemporary industrial facility. A Prime Controller (On-Prime) will handle all OT-layer wireless access points in the production floor which include AGVs, handheld devices, IIoT sensors, and any wireless component that is connected to process control infrastructure. Cloud Controller is used to control the IT overlay of administrative zones, visitor networks and mobile devices used by the corporation. VLAN segmentation, IDMZ architecture and next-generation stateful firewalls are used to keep the two networks strictly isolated. This model offers operational stability and predictability the factory floor needs at the same time offering the IT team administrative ease and remote maintainability which is appealing with cloud platforms to non-critical functions.

5. TUNNEL AND TRANSPORT SECURITY

5.1 DTLS Encryption on CAPWAP Tunnels

Partners Universal International Innovation Journal (PUIIJ)
Volume: 04 Issue: 02 | March-April 2026 | ISSN: 2583-9675 | www.puiij.com

The protocol with which a wireless controller talks to the access points that it manages is Control and Provisioning of Wireless Access Points (CAPWAP). It runs either over UDP and supports two types of traffic: the control channel, which transfers configuration commands, firmware updates, association tables and security policies, and the data channel, which transfers user traffic in centralized forwarding mode.

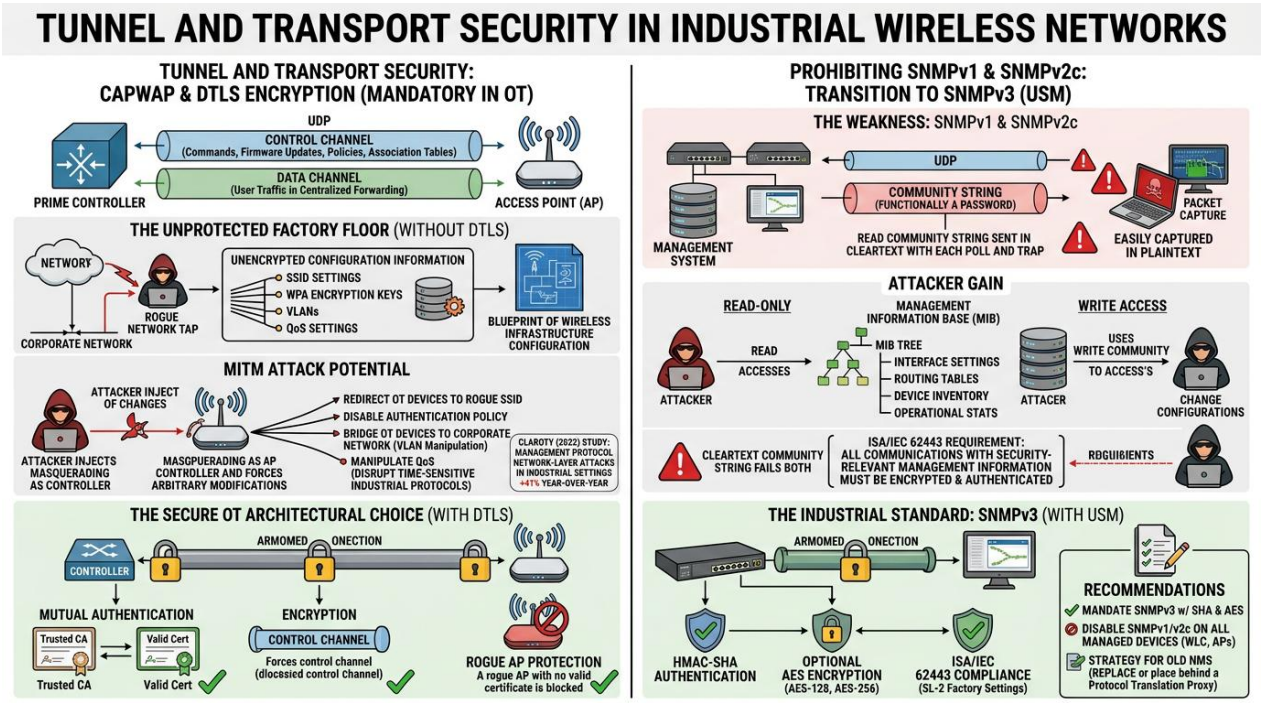

Fig -4: Tunnel And Transport Security in Industrial Wireless Networks

CAPWAP tunneling using DTLS (Datagram Transport Layer Security) encryption is not settable in an OT factory network. It is a security control that is mandatory. In the absence of DTLS on the CAPWAP control channel, an attacker who has gained access to the factory network via any mechanism, be it a rogue network tap, or a lateral movement pathway through the corporate network, can read all the configuration commands issued to each access point on the floor by the Prime Controller. These are SSID settings, authentication settings, WPA encryption keys, VLANs and QoS settings. Practically, when an attacker intercepts unencrypted CAPWAP traffic, he/she obtains the entire blueprint of the wireless infrastructure configuration. The more devastating potential that is opened by the lack of DTLS is man-in-the-middle injection. A compromiser between the controller and an access point may masquerade as the controller and force arbitrary changes in configuration upon the access point, such as configuration to redirect OT devices to a rogue SSID, configure VLANs to bridge OT devices to the corporate network, shut off authentication policy or manipulate QoS parameters to cause drops that disrupt time-sensitive industrial protocols. Claroty (2022) study of the pattern of industrial network attacks found that management protocol network-layer attacks on industrial settings were up 41 per cent year-over-year, making the argument that these attacks vectors are not only operational, but also exploited.

DTLS offers the mutual authentication between the controller and every access point via the X.509 certificates that also prohibit the entry of rogue access points into the managed infrastructure. An AP which

is unable to provide a valid certificate by the trusted CA of the facility is unable to initiate a DTLS session with the controller and hence cannot be provided with any configuration information.

5.2 SNMPv1 and SNMPv2c Prohibition

Simple Network Management Protocol is the protocol under which a management system receives reports of operational status, counters and alerts provided by network devices. The main weakness of SNMPv1 and SNMPv2c is that they both use community strings sent in cleartext in UDP to authenticate. A community string is considered to be functionally identical to a password. In these versions of the protocol this credential is transmitted across the network in plaintext with each poll request and trap message. Any intruder having access to the network and a packet capture software reads the community string instantly.

An attacker can use a captured community string to request the SNMP agent on the Prime Controller or any other managed access point to produce the entire management information base, including interface settings, routing tables, inventory of devices connected to it, and operational statistics. Using SNMP write community access, they are able to change configurations. ISA/IEC 62443 has that all the communications which contain security-relevant management information to be encrypted and authenticated to the level of security that the zone is. A cleartext community string meets neither of the two requirements. SNMPv3 can solve these vulnerabilities by the use of User-Based Security Model (USM), which offers HMAC-SHA authentication and optional AES encryption of the SNMP payload. The necessary settings to be used in SL-2 factory settings are SNMPv3 along with SHA authentication and either AES-128 or AES-256 encryption. SNMPv1 and SNMPv2c should be disabled in all the devices managed, the Prime Controller itself and all access points. The old network management systems which lack SNMPv3 functionality should be replaced or placed behind a protocol translation proxy.

6. IDENTITY, AUTHENTICATION, AND ACCESS CONTROL

6.1 On-Premises RADIUS Server Placement

In the ISA/IEC 62443-compliant deployments, the access of the wireless OT devices is authenticated by 802.1X EAP-TLS. It demands the authenticating device and RADIUS server to produce X.509 certificates and establishes a mutual authentication with no passwords or shared secrets being sent over the network. When an OT device is attached to factory SSID, it provides the RADIUS server with its device certificate, which is authenticated by the certificate authority chain and an access decision based on policy is returned.

The RADIUS server which will assist this process should be on-premise, both in terms of operation and architecture.

The operational argument is the same as the Prime Controller argument a cloud-based RADIUS server will go out of service as soon as the internet connectivity is disconnected. When the server is centralized and all new wireless associations are followed by a RADIUS authentication request, an unreachable server implies that devices which lose their wireless connection will not be able to re-authenticate. AGVs stop. Monitors of the safety systems are shut off. Sensors of IIoT lose SCADA connectivity. The effect that the failed authentication infrastructure will have on the production during the internet outage is just the same as the effect of the failed wireless infrastructure per se.

The architectural argument is based on the SIA/IEC 62443 Zone-Conduit model. OT wireless devices that are authenticated are part of OT security zone that is the most sensitive zone in the factory. Their authentication traffic should not leave the security boundary of the facility in terms of certificate

Partners Universal International Innovation Journal (PUIIJ)
Volume: 04 Issue: 02 | March-April 2026 | ISSN: 2583-9675 | www.puiij.com

transactions and access decisions. Sending RADIUS traffic to a cloud-based server will force it to go through the corporate IT network, through the public internet and then to a vendor data center, cutting across multiple conduit boundaries without the fine-grained control that the standard requires. It should be placed in the correct area, OT zone or the neighboring IDMZ, where the entire authentication interaction is kept within the controlled perimeter of the facility.

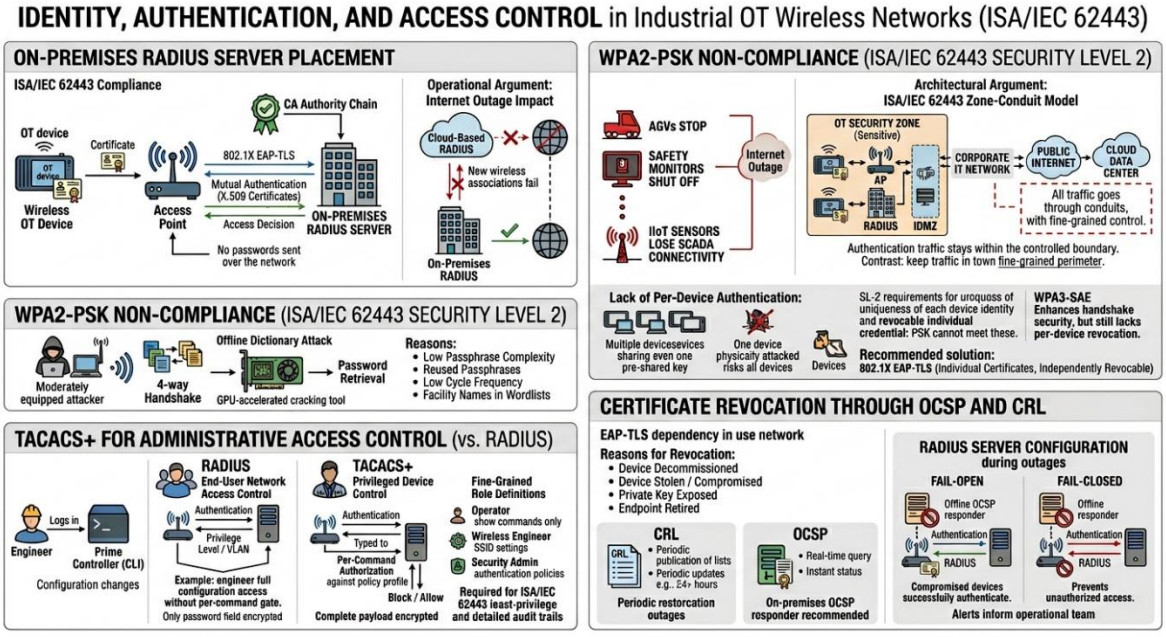

Fig -5: Identity Authentication and Access Control

6.2 WPA2-PSK Non-Compliance at ISA/IEC 62443 SL-2

WPA2-PSK is still popular in the industrial world since it is supported everywhere and easy to setup. WPA2-PSK is out of compliance with the structure of a factory where the ISA/IEC 62443 Security Level 2 is used, which involves protection against intentional attacks by moderately equipped adversaries with a specific motivation. These causes are protocol and specific.

WPA2-PSK relies on 4-way handshake to obtain session keys based on pre-shared key and two random nonces exchanged in the process of association. Any device within radio range can see this hand shake and it can be passively recorded without the attacker being the receiver of the communication. The intercepted handshake is offline brutally attacked and dictionaried. The attacker downloads the capture offline and cracks it with a GPU-accelerated cracking tool, and in case the passphrase is not sufficiently complex and entropic, retrieves it. This risk is increased by the industrial environment, which commonly reuses the same passphrase many times on large populations of embedded devices, has a low passphrase cycle frequency due to the operational interference of changing embedded controller passphrases and commonly uses passphrase based on the name of a facility, on a production line or an equipment identifier that can be added to an attacker target wordlist by an attacker with any knowledge of a specific site.

The second vulnerability is that it does not have per-device authentication. WPA2-PSK is a mutual credential. When one of the devices is physically attacked and its configuration is accessed, all other

devices within the same SSID are also attacked. No mechanism exists to revoke access to a single device without also every device changing its passphrase, which in an OT setting where hundreds of endpoints are operationally disruptive and changing them in a few seconds is hardly possible, is operationally disruptive and rarely can be executed with the speed needed to avoid an ongoing attack exploiting the window.

The ISO/IEC 62443 SL-2 demands the uniqueness of each device identity to be authenticated and the invalid credentials to be revocable without impacting other authorized entities. WPA2-PSK is not able to meet either of the requirements. WPA3-SAE enhances the security of WPA2-PSK by deterring passive handshake capture with simultaneous authentication of equals, but it does not offer any per-device revocable identity. The obedient solution to SL-2 factory settings is 802.1X EAP-TLS where individual devices are issued with a certificate which can be revoked independently without affecting any other device on the network.

6.3 TACACS+ for Administrative Access Control

An administrative session is needed to authenticate, authorize and audit when an engineer logs into the CLI of the Prime Controller to make changes to a configuration. Authentication is possible on both TACACS+ and RADIUS, however, TACACS+ is the appropriate protocol to use in the administration of a device in a factory setting and the explanation is an underlying architectural difference in the protocols at a fundamental level.

RADIUS was not made to be administered by device administrators, rather it is a network access control protocol created to be used by end users. It authenticates the user and issues a restricted amount of authorization attributes including a privilege level or a VLAN assignment. In an authentication by the administrator to a network device, the protocol sends back the information of whether the administrator is legitimate and what tier he/she belongs to, but cannot analyze and approve individual commands when typed in. When an authenticated administrator has been RADIUS authenticated into the level of privilege 15 on a Cisco device, such as, by default, they can fully configure the device with no additional per-command gate.

TACACS + was created to be used with privileged device control. It divides authentication, authorization and accounting in three different protocol interactions which can be managed separately. The outstanding feature is per-command authorization: once an administrator types a command on the CLI of the Prime Controller, that command string is sent to the TACACS+ server to make an authorization decision before the command is executed. The server does a check against the policy profile of the administrator and blocks or allows the execution of the command. This enables organizations to have fine-grained role definitions: a network operator is capable of issuing show commands but incapable of modifying interface settings; a wireless engineer is capable of changing SSID settings but incapable of changing management plane credentials; only a security administrator may change authentication policies.

TACACS+ also ciphers the complete payload of its message including the username using a common secret and MD5. The password field of an access request as sent by RADIUS is encrypted, with the remaining attributes (username) being left in cleartext. Per-command TACACS+ authorization is technically required in a factory setting in which ISA/IEC 62443 demands least-privilege access control and detailed audit trails of all configuration changes, and not a best practice.

6.4 Certificate Revocation Through OCSP and CRL

802.1X EAP-TLS offers a high level of mutual authentication, however, it also has a critical dependency, which is often poorly configured in industrial settings: certificate revocation checking. When EAP-TLS is used in a handshake, the RADIUS server should not only ensure that a presented certificate is issued by a trusted CA, and that the certificate has not expired. It should also ensure that the certificate is not explicitly revoked.

There are several reasons as to why certificates have to be revoked. One of the devices is decommissioned, a device is reported stolen or physically compromised, one of the private keys is suspected to have been exposed, or an endpoint is permanently retired to the production environment. In the absence of revocation checking, a certificate to a device that was decommissioned three years ago or in which the private key was leaked during a security incident will always be valid until its expiry date. Such a certificate can be used by an attacker to authenticate with the OT wireless network successfully as a trusted device.

There are two mechanisms of revocation checking. Periodically, Certificate Revocation Lists (CRLs) are published which are CA signed files containing a list of revoked certificate serial numbers. OCSP responder offers per-certificate revocation query in real time via HTTP. In the case of factory settings, on-premises OCSP responser is better than CRL distribution is due to instant revocation status as opposed to periodic CRL publication times, which can be 24 hours or more.

The security failure which is prevented by this control is when revocation checking is switched off or when the revocation infrastructure becomes unavailable and when the RADIUS server is set to fail open. The server in a fail- open setup allows authentication in case of inability to establish revocation status. This implies that on the event of the OCSP responder being offline in a period of maintenance, or a network route between the RADIUS server and the OCSP endpoint being lost, all devices with any certificate, even revoked and compromised ones, are successfully authenticated within that period. The appropriate setting is the fail-closed it is not possible to check the revocation status, it is denied. This should be accompanied by alerts in case the OCSP responder is not available and thus the operational team is notified immediately as opposed to the realization of the outage during a post-incident review.

7. OPERATIONAL SECURITY ARCHITECTURE

7.1 Dedicated Out-of-Band Management VLAN

A network infrastructure device has a management plane the administrative interface by which the engineers configure, monitor, and troubleshoot the device. This plane of management in a factory setting should be separated on a separate VLAN of production OT traffic and the justification is on both security and operational levels.

Security wise, an administrative control surface versus a production network is provided by a dedicated management VLAN. In case of an OT equipment being compromised, an infected process workstation is connected to the production VLAN, or an unauthorized device is connected to the production VLAN, the adversarial presence on that VLAN is unable to access directly the management interface of the Prime Controller. The production VLAN and management VLAN have to cross a firewall or layer-3 boundary, and access control lists may be used to restrict source IP addresses used, its traffic must be initiated by a specific jump host, use SSH and not Telnet, and all connection attempts should be logged. It is this type of firewall boundary that transforms the management plane into an open attack surface into a controlled access path that is audited.

In the absence of this separation, a single attacked OT endpoint on the production VLAN has direct layer-2 or layer-3 access to the management interface of the Prime Controller. An intruder who has breached a

Partners Universal International Innovation Journal (PUIIJ)
Volume: 04 Issue: 02 | March-April 2026 | ISSN: 2583-9675 | www.puiij.com

SCADA workstation may seek to compromise the controller by using brute-force through the credential of a workstation, by brute-forcing the known weaknesses in the controller management software or by creating malformed management traffic that slows the performance of the controller. Operationally, the management traffic and the production OT traffic will be in the same VLAN and will compete with each other in regard to bandwidth and switch queue priority. SNMP polling, ongoing syslog streams, SSH setups and firmware update file transfers all create severe bursts of traffic. This competing traffic can introduce queuing delays in a factory network with industrial protocols that have hard timing constraints which can be reflected as loss of packets or spikes in the process control communications. A special management VLAN with the right QoS policies will ensure that the administrative processes do not come in the way of production.

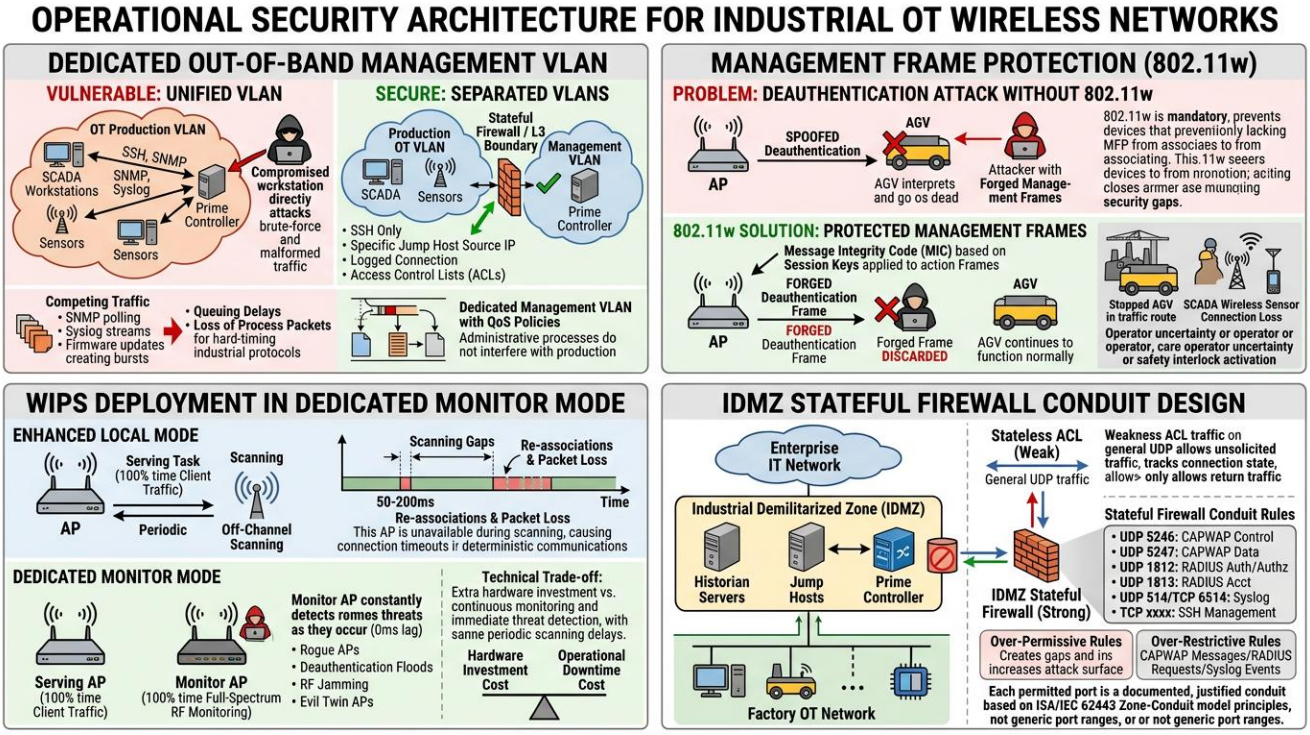

Fig -6: Operational Security Architercture for Industrial OT Wireless Networks

7.2 Management Frame Protection (802.11w)

Management Frame Protection is standardized in IEEE 802.11w and subsequently adopted into the 802.11 base standard, is a solution to a long-standing weakness of wireless protocol design management frames do not have cryptographic integrity protection. Prior to 802.11w, action frames, deauthentication frames and disassociation frames were not authenticated and integrity checks were not done. Any device that had a wireless interface had the capability of sending forged management frames on the network.

De-authentication flood attack is the attack which is prevented by 802.11w. An attacker sends spoofed deauthentication frame, in which the attacker is spoofed to look like it was sent by the legitimate access point, to a particular client or to the broadcast address to all clients at once. An OT receiving device interprets the deauthentication frame as a valid command by its access point and goes dead. A broadcast

deauthentication attack has the ability to disconnect all devices relating to a specific SSID at the same time.

The results on a factory floor are worse as compared to a normal enterprise setup. An AGV whose wireless connection is lost during transit undergoes its programmed fail-safe behavior, which is usually to stop immediately. An AGV that has stopped in a traffic route stalls other AGVs and needs to be corrected manually, which may interrupt the production process until the time when the AGV has been stopped. The wireless sensors of process parameters lose connection with the SCADA system which can lead to the activation of safety interlocks or the decision-making of operators with incomplete information. Work order management or quality inspections devices that are held in hand and fail to authenticate will not allow any more operations to be done.

OT-facing SSIDs with 802.11w enabled have the protection of management frames by a Message Integrity Code based on the session keys that were created during association. A received forged deauthentication frame which lacks a valid MIC is discarded by the receiving device prior to processing. The frame verification layer gets rid of the attack. Setting 802.11w as mandatory instead of optional on all OT SSIDs means that devices that cannot support MFP will never be able to associate and so the weakest devices will not be able to open an otherwise secured network to unprotected devices.

7.3 WIPS Deployment in Dedicated Monitor Mode

A Wireless Intrusion Prevention System searches the RF environment to identify rogue access points, unauthorized clients, ad -hoc networks, and active wireless attacks such as deauthentication floods, evil twin access points, and RF jamming. The On-Prime Controller is intended to assist WIPS in two different modes enhanced local mode, where access points serving do periodic off-channel scanning between their serving tasks, and dedicated monitor mode, where only a few access points are dedicated to RF monitoring without serving tasks.

Dedicated monitor mode is the necessary configuration in case of high-density OT factory deployments. There is the technical trade-off it involves extra hardware investment. However, the argument in favor of it is more significant than the argument against.

Enhanced local mode is desirable in that it does not need special hardware. Access points also scan the surrounding channels periodically to serve as a way of detecting a threat. The underlying issue is that when off-channel scanning is done, the access point cannot be used by its respective clients in the meantime. This short disconnect is not noticeable in a business office where there is a combined coverage between points of access and fault tolerant traffic of application. OT devices in factory floors frequently have continuous wireless connections with hard timeouts set to the deterministic communication needs of industrial protocols. Even a periodical unavailability of 50 to 200 milliseconds will cause connection timeouts, re-associations, and temporary loss of packets which is not acceptable in process control communications. Moreover, an access point that does serving and scanning offers poor quality in both modes, as it is unable to constantly scan any channel and at the same time provides traffic services on its main channel.

Specialized monitor access points make full-spectrum RF monitoring continuously and never carry client traffic. They detect the threats upon their occurrence instead of detecting them in the subsequent scan cycle. The cost of the hardware of deploying dedicated monitor access points should be compared to the cost of operation of the undetected rogue access point on the factory floor or a deauthentication attack that would halt the production even a few minutes.

7.4 IDMZ Stateful Firewall Conduit Design

The Industrial Demilitarized Zone (IDMZ) is an architecture buffer zone based on the principles of ISA/IEC 62443 and described in the Industrial Network Security reference architecture provided by Cisco which is between the corporate IT network and the OT production network. Services which need to be available in both domains such as historian servers, remote access gateways and authentication infrastructure are hosted in the IDMZ and not directly in either zone. There is no direct traffic between the IT network and the OT network or the other way round. The IDMZ brings to an end all inter-zone communication.

In the event of the deployment of a Prime Controller into or near the IDMZ, stateful firewall rules should explicitly allow the exact TCP and UDP ports needed by each protocol. UDP port 5246 is used in CAPWAP control traffic. UDP port 5247 is used in CAPWAP data traffic. UDP port 1812 is used in RADIUS authentication and authorization. UDP port 1813 is used in RADIUS accounting. UDP Syslog is transmitted over port 514 or TCP Syslog is transmitted over port 6514. These are not some generic ranges of port that should be guessed. They are protocol-defined values and are specific and each permitted port is a documented justified conduit in the ISA/IEC 62443 Zone-Conduit model.

The firewall should be set to stateful mode where the connection state of each flow is tracked and only the return traffic is allowed to pass to the direction that has been allowed. Stateless ACL that allows bi-directional UDP traffic on these ports is much weaker, as it grants the ability to any device on both sides of the firewall to make unsolicited traffic on these ports, whether there is a legitimate session on the ports or not. There are severe consequences of a misconfiguration in either direction. Excessively restrictive policies result in the Prime Controller being unable to provide CAPWAP control messages to access points, Authentication requests made by RADIUS being denied, and the syslog event history that is the main source of security visibility of the organization in the wireless environment being dropped silently. Rules that are over-permissive, like permitting all UDP traffic between zones so that it becomes easier to troubleshoot, are both unwarranted breaches of the minimization principle in the heart of the Zone-Conduit model and an increase in the attack surface the most sensitive point in the factory network design.

8. SYNTHESIZING THE FRAMEWORK A STRUCTURED IMPLEMENTATION HIERARCHY

To take these requirements into a consistent deployment, it is necessary to put them in the correct order. Technical controls which rely on lower-layer foundations being present before being implemented must be the latter implemented in the correct sequence.

The architectural background is the point of departure. Prime Controller should be installed in the OT network or IDMZ. The out-of-band management VLAN has to be configured as a dedicated VLAN prior to the configuration of management protocol. The controller should be authenticated all to administrative access, authorised to individual commands using TACACS+, limited to designated jump hosts and logged to an on-premise syslog server. NTP time synchronization should be tunning, and secured since all certificate validity checking, revocation timestamps checking and audit logs entries rely on proper time.

Secondly, the tunneling layer is applied. The entire access point CAPWAP tunnels between the controller and the access points must be encrypted with DTLS. Self-signed certificates that are defaulted on access points and the controller should be substituted with the facility internal PKI issued certificates. SNMPv1 and SNMPv2c should be turned off on the controller and all the access points and SNMPv3 with SHA authentication and AES-256 encryption should be set as the only enabled SNMP version.

The third one is the authentication layer which relies on the PKI infrastructure that is provided in the tunneling layer. On-premises RADIUS server will have to be installed onto the OT zone or IDMZ. The internal PKI of the facility should also issue devices certificates to every OT wireless endpoints. The RADIUS server should be set up to impose EAP-TLS with revocation verification to an on-premise OCSP responder that is set to be fail-closed when the revocation status is not accessible. WPA2-PSK should not be used in any SSID that is exposed to the OT.

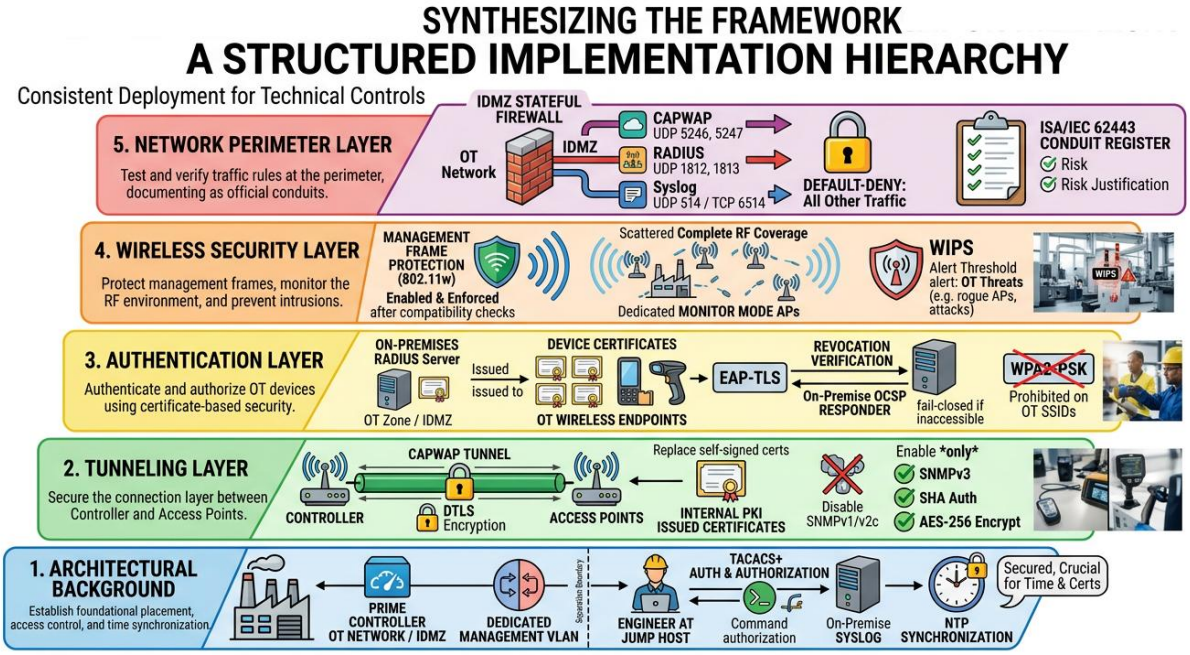

Fig -7: Synthesizing the Framework : A Structure Implementation Hierarchy

The fourth layer is the wireless security layer. Management Frame Protection (802.11w) should be enabled to necessary on all OT SSIDs and client compatibility should be verified first and then it should be enforced. Specially dedicated monitor mode access points should be installed at an adequate density to give complete RF coverage of the production floor on full channel. The classification rules and WIPS alert threshold should be set to indicate the threats that are important in the OT environment.

The last layer to be configured is the network perimeter layer which is tested by reviewing firewall rules and testing traffic capture. The IDMZ stateful firewall rules should clearly allow CAPWAP UDP 5246 and 5247, RADIUS UDP 1812 and 1813 and syslog UDP 514 or TCP 6514, all other traffic should default-deny. All of these rules should be recorded as a formal conduit in the organizations ISA/IEC 62443 conduit register and have a risk justification on all conducted by the change control procedure.

9. CHALLENGES AND GAPS IN CURRENT PRACTICE

Although all of the technical controls mentioned in this article are available, there is a big difference between what can be technically deployed and what is deployed in the majority of wireless industrial settings. The most prevalent operational obstacle is legacy device compatibility. Most OT endpoints, such as older barcode scanners, older handheld terminals, embedded wireless sensors, do not have support to

Partners Universal International Innovation Journal (PUIIJ)
Volume: 04 Issue: 02 | March-April 2026 | ISSN: 2583-9675 | www.puiij.com

802.1X EAP-TLS, SNMPv3 or 802.11w. Organizations have a hard decision to make between having a compliant security posture and continuing to produce with the current hardware. An interim solution is a practical one that would entail installing the non-compliant devices on separate VLANs with stringent network access control measures but would schedule hardware refresh cycles with security capability in mind as a first preference in the procurement requirements.

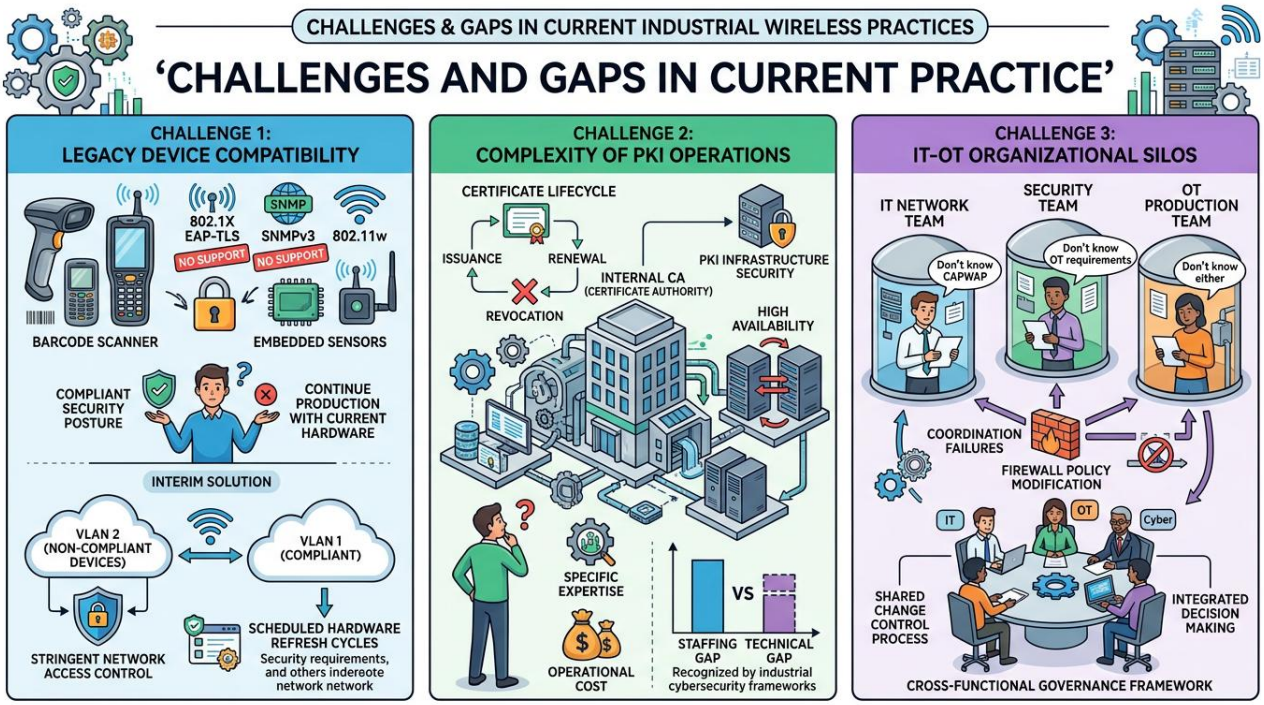

Fig -8: Challenges & Gaps in Current Industrial Wireless Practices

The complexity of PKI operations is always a challenge. Implementation and administration of internal certificate authority, certificate lifecycle, such as issuance, renewal, and revocation, and security of the PKI infrastructure itself and high availability imply a specific expertise and operational cost (which many manufacturing organizations have not historically required). This is becoming a staffing and organizational capability gap and not merely a technical capability gap as it is increasingly being recognized by the industrial cybersecurity frameworks.

IT-OT organizational silos cause coordination failures that sabotage technically correct designs. A firewall policy modification to allow a newly added CAPWAP conduit can require a network team, which does not know the CAPWAP, a security team, which does not know what is needed in OT, and a production team, which does not know either. The creation of cross-functional governance frameworks that involve the representatives of IT networking, OT engineering, and cybersecurity as a part of the same change control process is just as significant as the technical design.

Partners Universal International Innovation Journal (PUIIJ)
Volume: 04 Issue: 02 | March-April 2026 | ISSN: 2583-9675 | www.puiij.com

10. FUTURE PROSPECTS

The practice of industrial wireless security will also be influenced by a number of developments that are about to happen in the near future.

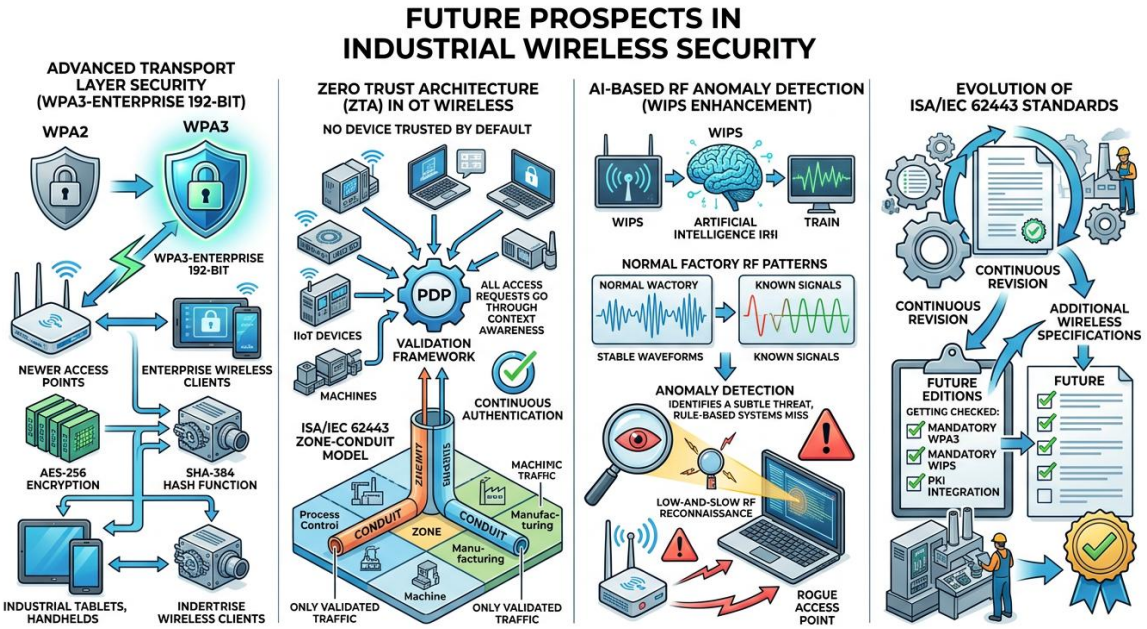

Fig -9: Future Prospects in Industrial Wireless Security

The 192-bit mode of WPA3-Enterprise offering AES-256 encryption and authentication with the use of the SHA-384 hash-function is gradually becoming a supported feature on newer access-points and more enterprise-level wireless clients. Its use in OT will enhance the transport layer of wireless security to greater levels than the present WPA2-Enterprise.

Application of the principles of Zero Trust Architecture (ZTA) to OT wireless networks is taken more seriously. The fundamental philosophy, which is no device is trusted by default, depending on the network location, and that all access requests should be actively validated, is a natural fit with the ISA/IEC 62443 Zone-Conduit model and offers an effective architectural guidance to the ever-increasing number of IIoT devices, which are connecting and disconnecting to factory wireless networks on a continuous basis.

The RF anomaly detector is AI-based and is directly built into the WIPS systems to enhance the speed and precision of the rogue access point or attack identification. Normal factory RF patterns trained by machine learning can detect anomalies that are not detected by rule-based detection systems such as low-and-slow RF reconnaissance, which is not detected by threshold-based notification.

The continuous revision of ISA/IEC 62443 is likely to add additional specifications on the wireless security controls within the operational technology setting that may require some of the controls described in this article to be mandatory in future editions of the standard.

Partners Universal International Innovation Journal (PUIIJ)
Volume: 04 Issue: 02 | March-April 2026 | ISSN: 2583-9675 | www.puiij.com

11. INCIDENT RESPONSE AND WIRELESS FORENSICS IN OT FACTORY ENVIRONMENTS

The implementation of the security measures outlined in this paper can go a long way towards minimizing the attack surface of an industrial wireless network. It never excludes the incidences. Rogue access points can be found. An unauthorized party may use a legitimate device certificate prior to the revocation being done. An active RF interference of an unknown source can be indicated by a WIPS alert. The speed and accuracy of the response is the same concern as the quality of the detection when these events take place.

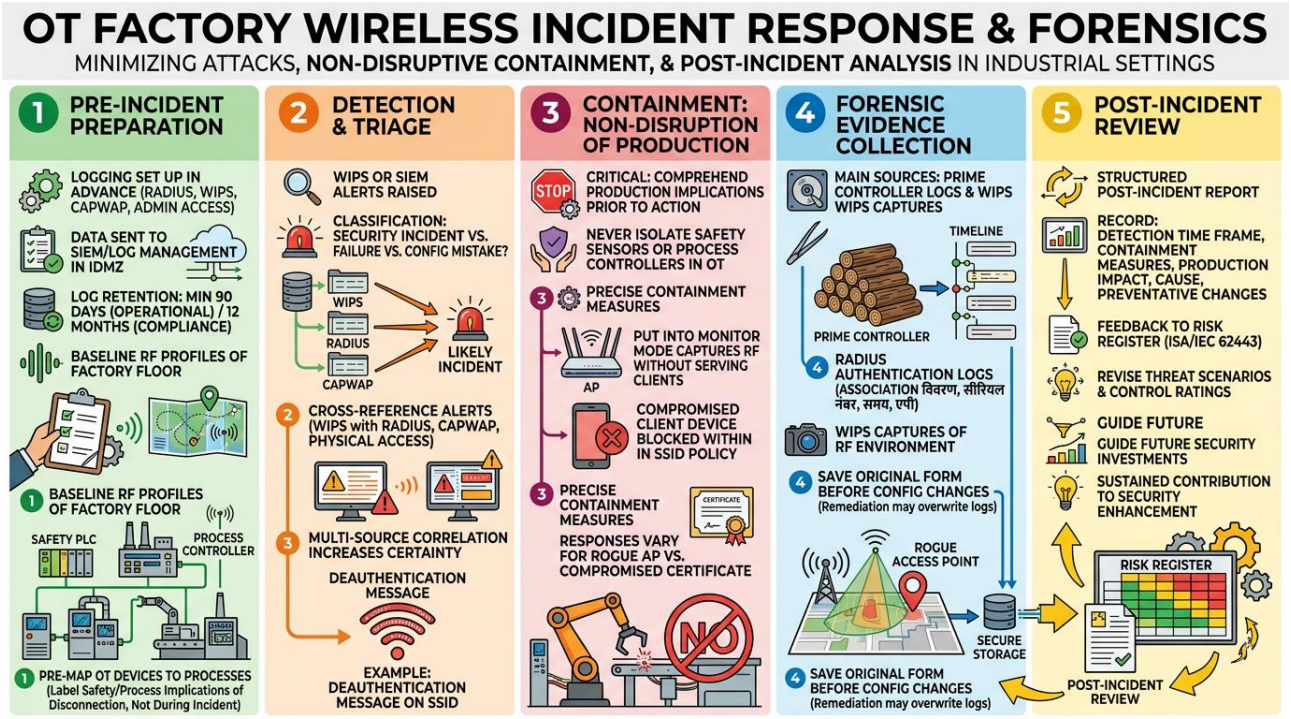

Fig -10: OT Factory Wireless Incident Response & Forensics

OT wireless incident response is not the same as IT incident response and it is a widespread and fallacious error to treat them as such. Seclusion of an endpoint that is compromised out of the network is the norm in an IT environment. Any wireless equipment which happens to be a sensor on a safety system or a process controller can present a greater danger in an OT environment when isolated than the actual incident. The initial principle of OT incident response is to comprehend the production implications of any course of action of containment prior to implementing it. All of the OT wireless devices are to be pre-mapped to the process functionality that it supports and the safety implications of its disconnection. This mapping should not be created when an incident takes place but prior to the occurrence of an incident.

Pre-Incident Preparation. The incident investigation needs the raw data which is the WIPS and authentication logs that are supplied by the Prime Controller but only when logging is properly set up in the first place. Events of RADIUS authentication, WIPS notification, CAPWAP control channel notification and administrative access session will be sent to on-premises Security Information and Event Management (SIEM) system or a dedicated log management service within the IDMZ. The log retention must be set to a minimum of 90 days to investigate the operations and 12 months to comply. RF profiles of the factory floor should be taken at baseline and documented capturing the projected access point and client population and characteristics of the signals so that in case of incident deviations can be detected instantly.

Detection and Triage. When WIPS or SIEM raises an alert the initial action is classification is this a real security incident, a hardware failure or a configuration mistake. An active RF attack or a broken radio on an access point may be indicated by a deauthentication message on a particular SSID, such as. The triage methodology is cross-referencing the WIPS alert with RADIUS logs of authentication failure and CAPWAP logs, and physical access to the facility. Multi-source alerts which have a correlation between the alerts of multiple log sources are more likely to be reflecting real incidents as compared to single-source alerts.

Containment Non-disruption of production. After a real incident has been established, the Prime Controller issues some containment equipment which can be used in a precise manner. The particular access point may be put into monitor mode so that it is not in active service but it is capable of being used to gather RF evidence. The SSID policy level can block a particular client device that does not affect the other devices in the same SSID. The compromised certificate can be revoked on the OCSP responder which will reject the subsequent authentication without necessitating any modification to the wireless infrastructure. Depending on the extent of the compromise confirmed, the action to be chosen is the containment action. A rogue access point on the factory floor is something that should be responded differently to a compromised device certificate.

Forensic Evidence Collection. The main sources of evidence to be used in the post-incident forensic analysis are the Prime Controller logs and WIPS captures. Authentication logs of the RADIUS give records of all the events of association of a device with the device certificate serial number applied, the time of the event and the access point which the device communicated with. WIPS captures leave a record on the RF environment over the incident window which may determine the physical location of a rogue access point through signal strength triangulation. Such logs should be exported and saved in their original form prior to any configuration being done to the wireless infrastructure as some remediation measures can overwrite log buffers.

Post-Incident Review. Any wireless security incident must produce a structured post-incident report that records the detection time frame, the containment measures implemented, the impact of production in case any, the cause and the exact measure or configuration modification that would have prevented the incident or minimized its effect. The review must be the direct input to the organization ISA/IEC 62443 risk register, which will revise the threat scenarios and control effectiveness ratings, which will be used to make future security investments. By so doing, incident response does not constitute an endpoint event but rather a sustained contribution to the security enhancement process.

12. CONCLUSION

Wireless infrastructure security in an OT factory is not achieved through implementing enterprise IT security practices with some slight modifications. It needs to be systematic, and technically based, with all controls being explained by a particular threat, a particular protocol weakness, or a particular compliance need. All ten controls analyzed in this paper are in place just because a given and consequential failure mode is absent without them.

CAPWAP tunnels using DTLS eliminates man-in-the-middle attacks that may re-configure all access points on the floor. On-premises RADIUS server avoids the reliance of authentication on external connectivity and maintains certificate transactions on the facility security perimeter. WPA2-PSK prohibition does not allow offline credential recovery, and does not have the shared credential revocation problem. A special management VLAN does not allow the access of the administrative interface of the controller by

compromised OT devices. 802.11w helps to avoid de authentication floods that may stop the production process. TACACS+ per-command authorization imposes the least-privilege control on the administrative actions. Specialized WIPS monitor mode offers a non-interruptive RF threat detection without interruption of the OT clients sessions. SNMPv3 gets rid of cleartext community string exposure. IDMZ stateful firewall conduits are used to control zone boundary but allow required protocol flows. OCSP and CRL revocation with the fail-close feature do not allow revoked device certificates to authenticate after compromise or decommissioning.

All these controls have their architecturally proper base in the Prime (On-Premises) Controller. It offers the operational autonomy, compliance congruence and data ownership that OT environments require. Practitioners applying this framework must also realize that the value of this framework lies not in the individual control but in all of the controls working together. Cleartext management protocols destroy an engineered authentication system. Any properly constructed IDMZ will be weakened by lax conduit regulations. The security of a factory wireless network can only be as good as the total of its properly installed, individually rationalized and continuously observed controls.

REFERENCES

[1] Byres, E., and Lowe, J. (2004). "The Myths and Facts Behind Cyber Security Risks for Industrial Control Systems." Proceedings of the VDE Kongress, pp. 213-218.
[2] Cisco Systems. (2020). Cisco SAFE: Industrial Network Security Architecture Reference Guide. San Jose: Cisco Press.
[3] George, D. A. S., George, A. S. H., & Baskar, D. T. (2023). Wi-Fi 7: The Next Frontier in Wireless Connectivity. Partners Universal International Innovation Journal, 1(4), 133–145. https://doi.org/10.5281/zenodo.8266217
[4] Claroty. (2022). Biannual ICS Risk and Vulnerability Report: 2H 2022. New York: Claroty Ltd.
[5] Dragos Inc. (2023). Year in Review: OT Cybersecurity Report 2023. Hanover: Dragos Inc.
[6] A. R. Research Publication. (2026, January 19). Securing Tomorrow: How 6G Networks and AI Are Reshaping the Cybersecurity Landscape. https://doi.org/10.5281/zenodo.18299699
[7] IEEE Standards Association. (2009). IEEE 802.11w-2009: Amendment to IEEE 802.11: Protected Management Frames. New York: IEEE.
[8] International Society of Automation. (2018). ISA/IEC 62443-3-3:2013: System Security Requirements and Security Levels. Research Triangle Park: ISA.
[9] George, D. A. S. (2024). Leveraging Industry 4.0 for Efficiency Gains in Food Production. Partners Universal International Research Journal (PUIRJ), 03(01), 86–108. https://doi.org/10.5281/zenodo.10823006
[10] International Society of Automation. (2020). ISA/IEC 62443-2-1:2010: Security Management System for IACS. Research Triangle Park: ISA.
[11] George, D. A. S. (2024). The Fourth Industrial Revolution: A Primer on Industry 4.0 and its Transformative Impact. Partners Universal Innovative Research Publication, 2(1), 16–40. https://doi.org/10.5281/zenodo.10671872
[12] National Institute of Standards and Technology. (2023). NIST Special Publication 800-82 Revision 3: Guide to Operational Technology (OT) Security. Gaithersburg: NIST.
[13] George, Dr. A. Shaji. (2025). The Critical Role of Data Science and Cybersecurity Innovations in Industry 4.0: A Handbook Review. Zenodo, 03(02). https://doi.org/10.5281/zenodo.15199362
[14] North American Electric Reliability Corporation. (2022). CIP Standards: Critical Infrastructure Protection Version 7. Atlanta: NERC.
[15] George, D. A. S., & George, A. S. H. (2023). Revolutionizing Manufacturing: Exploring the Promises and Challenges of Industry 5.0. Partners Universal International Innovation Journal, 1(2), 22–38. https://doi.org/10.5281/zenodo.7852124

[16] Stouffer, K., Lightman, S., Pillitteri, V., Abrams, M., and Hahn, A. (2023). NIST SP 800-82 Rev. 3: Guide to Operational Technology Security. Gaithersburg: NIST.
[17] George, D. A. S., George, A. S. H., & Baskar, D. T. (2023). The Evolution of Smart Factories: How Industry 5.0 is Revolutionizing Manufacturing. Partners Universal Innovative Research Publication, 1(1), 33–53. https://doi.org/10.5281/zenodo.10001380
[18] Wilhoit, K. (2013). "Who's Really Attacking Your ICS Equipment?" Trend Micro Research Paper. Tokyo: Trend Micro.
[19] George, Dr. A. Shaji. (2024). The Transformational Impact of AI Innovation on Financial Sectors in the Industry 5.0 Era. Zenodo, 02(06). https://doi.org/10.5281/zenodo.14626294
[20] Zetter, K. (2014). Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon. New York: Crown Publishers.
[21] Andia, L., & Morandini, Y. (2023). Building the path to ubiquitous wireless connectivity, from materials to systems. 2023 7th IEEE Electron Devices Technology & Manufacturing Conference (EDTM). https://doi.org/10.1109/edtm55494.2023.10103048
[22] Daousis, S., Peladarinos, N., Cheimaras, V., Papageorgas, P., Piromalis, D. D., & Munteanu, R. (2024). Overview of protocols and standards for wireless sensor networks in critical infrastructures. Future Internet, 16, 33. https://doi.org/10.3390/fi16010033
[23] Moldovan, L., & Gligor, A. (2018). Foreword global trends in manufacturing technologies which create a path to tomorrow's innovations. Procedia Manufacturing, 22, 1-3. https://doi.org/10.1016/j.promfg.2018.03.001
[24] Morin, A., & Moore, T. (2022). Towards cost-balanced intrusion detection in OT environments. 2022 IEEE Conference on Communications and Network Security (CNS). https://doi.org/10.1109/cns56114.2022.10091442
[25] O'Neill, O. (2006). Industrial wireless LAN applications, supplying solutions to industry demands. IEE Seminar on Industrial Networking and Wireless Communications for Control. https://doi.org/10.1049/ic:20060606
[26] Oualha, N. (2017). Network security in industrial wireless sensor networks. Industrial Wireless Sensor Networks. https://doi.org/10.1201/b14072-14
[27] Trsek, H. (2016). Isochronous wireless network for industrial automation. Isochronous Wireless Network for Real-time Communication in Industrial Automation. https://doi.org/10.1007/978-3-662-49158-4_4
[28] Willig, A. (2017). Wireless LAN technology for the factory floor: Challenges and approaches. Industrial Communication Technology Handbook. https://doi.org/10.1201/b17365-32
[29] (2007). Job description. Encyclopedia of Industrial and Organizational Psychology. https://doi.org/10.4135/9781412952651.n149
[30] (2016). KRI security baseline controls. Information Security. https://doi.org/10.1201/9781420013412-10
[31] (2019). NIST SP 800-82 security measures. Cybersecurity of Industrial Systems, 309-327. https://doi.org/10.1002/9781119644538.app3
[32] (2026). ISA/IEC 62443 security levels. Security PHA Review for Consequence-Based Cybersecurity, 117-138. https://doi.org/10.1002/9781394442447.app4
[33] Bellagente, P., Ferrari, P., Flammini, A., Rinaldi, S., & Sisinni, E. (2016). Enabling PROFINET devices to work in iot: Characterization and requirements. 2016 IEEE International Instrumentation and Measurement Technology Conference Proceedings. https://doi.org/10.1109/i2mtc.2016.7520417
[34] Buja, A. (2025). Threats and attacks to industrial internet of things (iiot). Cybersecurity of Industrial Internet of Things (IIoT). https://doi.org/10.1201/9781003383253-4
[35] CVEJIĆ, R., VASEV, A., & CVEJIĆ, S. (2013). INSECURITY OF WEP ENCRYPTION on WIRELESS NETWORKS. ANNALS OF THE ORADEA UNIVERSITY. Fascicle of Management and Technological Engineering., XXII (XII), 2013/2(2). https://doi.org/10.15660/auofmte.2013-2.2919
[36] Flügel, E. (2004). Basin analysis: Recognizing depositional settings. Microfacies of Carbonate Rocks. https://doi.org/10.1007/978-3-662-08726-8_15
[37] Hamada, R., & Kuzminykh, I. (2023). Exploitation techniques of iost vulnerabilities in air-gapped networks and security measures—a systematic review. Signals, 4(4), 687-707. https://doi.org/10.3390/signals4040038
[38] Jain, U., Tripathi, A., Kumar, S., & Kumar, G. (2025). Simple, secure and lightweight authentication protocol with session-key generation for iiot device in iiot networks. Microsystem Technologies, 31(2), 299-311. https://doi.org/10.1007/s00542-023-05566-y
[39] Paredes, I. (2020). IT/OT convergence – cybersecurity beyond technology. Abu Dhabi International Petroleum Exhibition & Conference. https://doi.org/10.2118/203093-ms

[40] Wang, Z., & Ierapetritou, M. (2018). Global sensitivity, feasibility, and flexibility analysis of continuous pharmaceutical manufacturing processes. Computer Aided Chemical Engineering. https://doi.org/10.1016/b978-0-444-63963-9.00008-7
[41] (2012). 11b sonderbehandlung von erhaltungsaufwand bei baudenkmalen. Einkommensteuergesetz. https://doi.org/10.9785/ovs.9783504381141.802
[42] (2019). NIST SP 800-82 security measures. Cybersecurity of Industrial Systems, 309-327. https://doi.org/10.1002/9781119644538.app3
[43] (2026). ISA/IEC 62443 security levels. Security PHA Review for Consequence-Based Cybersecurity, 117-138. https://doi.org/10.1002/9781394442447.app4
[44] (2026). Overview of the ISA/IEC 62443 series. Security PHA Review for Consequence-Based Cybersecurity, 19-24. https://doi.org/10.1002/9781394442447.ch2
[45] Музика, В. В. (2020). ANALYSIS OF CYBER-ATTACKS ON UKRAINIAN POWER GRID SYSTEMS IN THE CONTEXT OF ARMED CONFLICT IN DONBAS. Constitutional State, 0(39), 78-85. https://doi.org/10.18524/2411-2054.2020.39.212983
[46] Blumenthal, U., & Wijnen, B. (1998). User-based security model (USM) for version 3 of the simple network management protocol (snmpv3). https://doi.org/10.17487/rfc2264
[47] Chatzoglou, E., Kambourakis, G., & Kolias, C. (2022). How is your wi-fi connection today? dos attacks on WPA3-SAE. Journal of Information Security and Applications, 64, 103058. https://doi.org/10.1016/j.jisa.2021.103058
[48] Preuß Mattsson, J., & Sethi, M. (2022). EAP-TLS 1.3: Using the extensible authentication protocol with TLS 1.3. https://doi.org/10.17487/rfc9190
[49] Silva, M., Mocanu, S., Puys, M., & Thevenon, P. H. (2025). Safety-security convergence: Automation of IEC 62443-3-2. Comput. Secur., 156, 104477. https://doi.org/10.1016/j.cose.2025.104477
[50] Vulfin, A. M. (2022). Detection of network attacks in a heterogeneous industrial network based on machine learning. Programmnaya Ingeneria, 13(2), 68-80. https://doi.org/10.17587/prin.13.68-80
[51] Wright, P. (2014). Privileged access control foundations. Protecting Oracle Database 12c. https://doi.org/10.1007/978-1-4302-6212-1_12
[52] Unknown. (2026). ISA/IEC 62443 security levels. Security PHA Review for Consequence-Based Cybersecurity, 117-138. https://doi.org/10.1002/9781394442447.app4
[53] Blumenthal, U., Maino, F., & McCloghrie, K. (2004). The advanced encryption standard (AES) cipher algorithm in the SNMP user-based security model. https://doi.org/10.17487/rfc3826
[54] Jiang, N., Lin, H., Yin, Z., & Zheng, L. (2018). Performance research on industrial demilitarized zone in defense-in-depth architecture. 2018 IEEE International Conference on Information and Automation (ICIA). https://doi.org/10.1109/icinfa.2018.8812486
[55] Lounis, K. (2021). Cut it: Deauthentication attack on bluetooth. 2021 14th International Conference on Security of Information and Networks (SIN). https://doi.org/10.1109/sin54109.2021.9699265
[56] Polk, T., McKay, K., & Chokhani, S. (2014). Guidelines for the selection, configuration, and use of transport layer security (TLS) implementations. https://doi.org/10.6028/nist.sp.800-52r1
[57] Ryu, J. H., Lee, I. G., & Moon, J. H. (2023). OT industrial security enhancement focused on security-by-design. Korean Journal of Industry Security, 13, 91-118. https://doi.org/10.33388/kais.2023.13.s.091
[58] Shinder, T. W. (2007). ISA 2006 stateful inspection and application layer filtering. The Best Damn Firewall Book Period. https://doi.org/10.1016/b978-1-59749-218-8.00021-1
[59] Wright, D. (2018). The history of the IEEE 802 standard. IEEE Communications Standards Magazine, 2(2), 4-4. https://doi.org/10.1109/mcomstd.2018.8412452
[60] (2009). Control and provisioning of wireless access points (CAPWAP) protocol binding for IEEE 802.11. https://doi.org/10.17487/rfc5416
[61] Bartoli, A. (2020). Understanding server authentication in WPA3 enterprise. Applied Sciences, 10(21), 7879. https://doi.org/10.3390/app10217879
[62] Gwashy Young, R. (2025). AI and ML in endpoint security and zero trust models. Artificial Intelligence and Machine Learning in Cybersecurity. https://doi.org/10.4324/9781003615026-7
[63] Kumar, A., & Saini, M. (2026). Ai-based anomaly detection in air-gapped environments. International Journal of Science and Research (IJSR), 337-343. https://doi.org/10.21275/sr26308141537
[64] Madsen, T. (2023). OT zero-trust security. Zero-trust – An Introduction. https://doi.org/10.1201/9781003464587-8
[65] Radvanovsky, R., & Mustard, S. (2026). Incident response and recovery. Risk Management for Operational Technology (OT) Systems. https://doi.org/10.4324/9781003610557-9

[66] Serrat, O. (2017). Bridging organizational silos. Knowledge Solutions. https://doi.org/10.1007/978-981-10-0983-9_77
[67] Silva, H., Gonçalves, T., & Lippi, D. (2025). FIRM-OT: A methodology for cybersecurity forensics and incident response in OT. 2025 13th International Symposium on Digital Forensics and Security (ISDFS). https://doi.org/10.1109/isdfs65363.2025.11012047
[68] (2016). PKI management and security. Security without Obscurity. https://doi.org/10.1201/b19725-7
[69] (2026). ISA/IEC 62443 security levels. Security PHA Review for Consequence-Based Cybersecurity, 117-138. https://doi.org/10.1002/9781394442447.app4
[70] Bassill, P. (2013). The holistic approach to security. Network Security, 2013(3), 14-17. https://doi.org/10.1016/s1353-4858(13)70042-4
[71] Blumenthal, U., & Wijnen, B. (1998). User-based security model (USM) for version 3 of the simple network management protocol (snmpv3). https://doi.org/10.17487/rfc2264
[72] Byun, J. W. (2015). Privacy preserving smartcard-based authentication system with provable security. Security and Communication Networks, 8(17), 3028-3044. https://doi.org/10.1002/sec.1229
[73] Edwards, D. J. (2024). Threat landscape. Mastering Cybersecurity. https://doi.org/10.1007/979-8-8688-0297-3_2
[74] Hollerer, S., Kastner, W., & Sauter, T. (2021). Towards a threat modeling approach addressing security and safety in OT environments. 2021 17th IEEE International Conference on Factory Communication Systems (WFCS). https://doi.org/10.1109/wfcs46889.2021.9483591
[75] Megerman, J., & Abbott, W. M. (1989). Clinical importance of the compliant conduit. Vascular Dynamics. https://doi.org/10.1007/978-1-4684-7856-3_21
[76] Mutch, J., & Anderson, B. (2011). Final thoughts for least privilege best practices. Preventing Good People from doing Bad Things. https://doi.org/10.1007/978-1-4302-3922-2_11
[77] Nardone, M. (2025). Introduction of operational technology (OT) security and industrial control systems (ICS). Apress Pocket Guides. https://doi.org/10.1007/979-8-8688-2016-8_1
[78] Radivilova, T., & Hassan, H. A. (2017). Test for penetration in wi-fi network: Attacks on WPA2-PSK and wpa2-enterprise. 2017 International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo). https://doi.org/10.1109/ukrmico.2017.8095429
[79] Solinas, J., & Zieglar, L. (2010). Suite b certificate and certificate revocation list (CRL) profile. https://doi.org/10.17487/rfc5759
[80] Zhang, R., Pazhyannur, R., Gundavelli, S., Cao, Z., Deng, H., & Du, Z. (2018). Alternate tunnel encapsulation for data frames in control and provisioning of wireless access points (CAPWAP). https://doi.org/10.17487/rfc8350
[81] (2002). Centralized authentication services. Complete Book of Remote Access. https://doi.org/10.1201/9781420000429-23
[82] (2010). Stateful firewall model. Firewall Design and Analysis. https://doi.org/10.1142/9789814261661_0004
[83] (2020). Very relevant for flood prevention measures. https://doi.org/10.5194/hess-2020-605-rc1