# Adaptive Automation

**The SENECA Paradigm of Human-Centric, Interoperable, and Secure Automation**


**Paradigm Conceptualization**: Manuel Moschin

**Coordination**: Armando Martin

March 2026

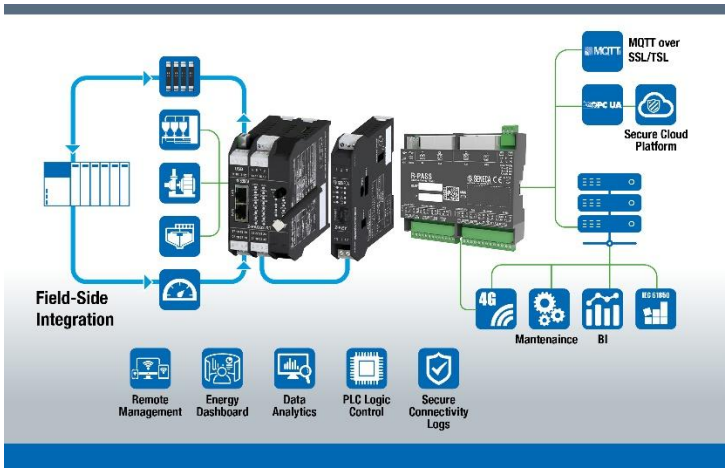
## Table of Contents

## 1. Introduction - From Complexity to Adaptive Automation

In recent years, industrial automation has undergone a profound transformation. Digitalization, IoT, remote assistance, energy management, cybersecurity, and Artificial Intelligence have progressively layered plant architectures. The result is growing complexity: heterogeneous protocols, dedicated gateways, separate PLCs, autonomous edge computers, and overlapping cloud systems. Historically, every new requirement generated a new device. Need connectivity? Add a gateway. Need remote access? A VPN router. Need data logging? A data logger. Innovation has been predominantly additive. This approach has produced more sophisticated plants, but also more rigid ones, more expensive to integrate and maintain, and more exposed to cyber vulnerabilities.

Digital transformation, intended to simplify, has often increased systemic complexity. This is the context for the **Adaptive Automation** paradigm, developed by **SENECA**, an Italian company that has been designing and manufacturing components and systems for industrial automation for nearly forty years. The paradigm emerged within the technological context **of Italian industrial manufacturing**, historically characterized by strong integration between electronic design, field applications, and the ability to adapt to the real needs of production plants. Adaptive Automation is not just another technology, but a shift in perspective. The goal is not to add functions, but to reduce the structural complexity of automation through four integrated pillars: **FLEX, Unified Firmware, Distributed Security, and EASY CLOUD**. The guiding principle is clear: automation must be configurable, not replaceable. Adaptive Automation integrates functions traditionally distributed across multiple systems into a single industrial node: programmable control according to IEC 61131-3, multi-protocol conversion, data logging, HMI/Remote Display, integrated web server, integrated IoT and mobile connectivity, industrial VPN, and secure communications management. This is not a generic convergence, but an integration designed for the field, featuring network segmentation, data encryption, and compliance with key security standards (IEC 62443-4-2).

Intelligence is placed **close-to-the-field**, near the machine or the electrical panel. This reduces latency, increases resilience, and allows control to be maintained even in the absence of external connectivity. The edge node becomes an active element of the plant, capable of executing logic, logging events, generating alarms, and communicating with higher-level systems autonomously. Alongside the technical dimension, there is an organizational dimension. Adaptive Automation is a **human-centric** model: technology should not multiply configuration points, but simplify them. When the operational context changes, adjustments are made to the software configuration, not the hardware. The system evolves without being rebuilt. Reducing devices, interfaces, and overlapping layers means reducing cabling, firmware, attack surfaces, and total cost of ownership. In a context where cybersecurity, operational continuity, and regulatory compliance are strategic factors, architectural simplification becomes a competitive advantage. Adaptive Automation is not a product, but a design model: a modular, configurable, secure, and architecturally scalable automation system capable of adapting to the plant without requiring constant technological replacements.




*IIoT architecture with SENECA Edge adaptive nodes that consolidate PLC, Energy Controller, IIoT Gateway, 4G Router, remote alarm unit, remote assistance, and data logger functionalities*

## 2. Architecture of the Adaptive Automation Paradigm

Adaptive Automation is not a product but a technical model structured around four integrated pillars: FLEX, Unified Firmware, Distributed Security, and EASY CLOUD. It is this coordinated architecture that transforms the industrial device from a static component into an adaptive network node.

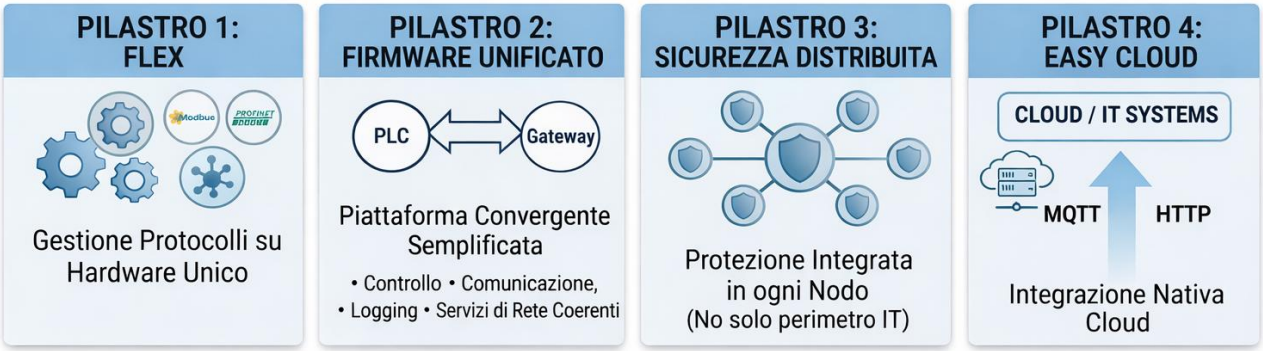
The first element is **FLEX**, which refers to the dynamic management and conversion of communication protocols on a single hardware platform. The principle is “configure, don’t replace”: the same device can function as a gateway, network analyzer, or multi-protocol I/O module simply by changing its configuration. The hardware remains the same; only its functional role changes.

The second pillar is **Unified Firmware,** a converged PLC/Gateway/Edge platform that simplifies updates, enables real-time configuration changes, and reduces management costs. Control, communication, logging, and network services coexist in a cohesive environment, featuring an integrated web server, centralized parameter management, and local diagnostics. Devices aren’t simply added; the platform evolves.

The third pillar is **Distributed Security**. Protection is not concentrated at the IT perimeter but integrated into every node of the architecture. LAN/WAN segmentation, industrial VPN, advanced authentication, SSL/TLS encryption, and adherence to standards such as IEC 62443 and NIS2 make security a structural property of the system. Each device actively contributes to overall resilience, reducing the risk of lateral threat propagation.

The fourth pillar is **EASY CLOUD**. Bidirectional connectivity with major cloud environments is made simple by preconfigured integration templates, primarily based on MQTT, which allow the device to be quickly adapted to the chosen platform. The operating principle is that the template connects the edge node to various clouds, and through configuration or advanced programming, the device adapts to the selected service without dedicated gateways or middleware, making the automation scalable and easily reconfigurable.

In this paradigm, the industrial device is no longer a passive element but an intelligent node capable of adapting to the application context. Innovation does not consist of adding functions, but rather of coordinating them within a unified, configurable, secure, and scalable platform, thereby reducing complexity, attack surfaces, and overall system costs.

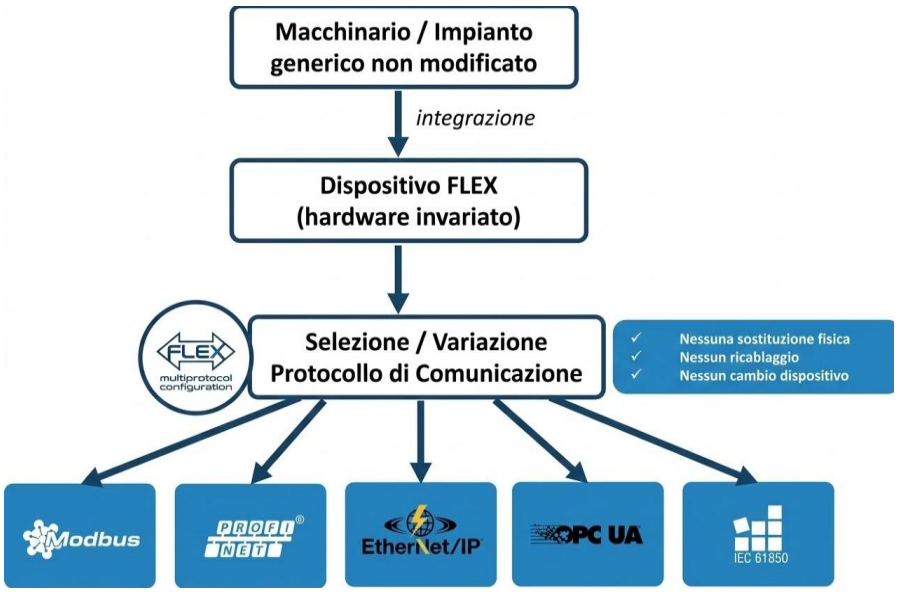



The Pillars of Adaptive Automation

## 4. Pillar 1. FLEX

The adaptive heart of the paradigm is the proprietary FLEX technology. FLEX is the solution developed by SENECA to permanently decouple the industrial communication function from the device's physical hardware. In traditional systems, each protocol requires a dedicated gateway, resulting in a proliferation of variants, firmware, and components. With FLEX, this limitation is overcome: a single multi-protocol hardware device manages Modbus RTU/TCP/ASCII, Profinet IO, Ethernet/IP, OPC UA, IEC 61850, and MQTT in real time, without the need to physically replace the device.

Platforms such as Z-KEY, R-KEY, R203, R204, and I/O modules integrate heterogeneous communication stacks on a common hardware base. FLEX acts as a logical orchestration layer above these stacks, allowing the node's operational role to be selected via software: Modbus RTU↔TCP gateway, OPC UA endpoint, Ethernet/IP bridge, Profinet node, IEC 61850 concentrator, or MQTT publisher to IIoT platforms with local logic (if-then-else rules). The principle is not merely the coexistence of multiple protocols, but their interchangeability without any physical impact on the system. The device retains the same hardware base while changing its logical role according to the architecture required by specifications or system evolution. This eliminates one of the main cost drivers in automation: architecture changes. It is no longer necessary to replace equipment when switching from one communication standard to another; a software reconfiguration via a web server or programming environment is sufficient.



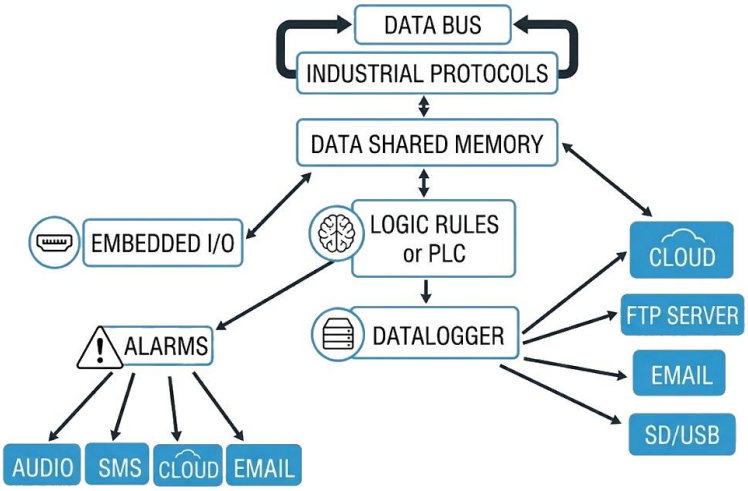

*FLEX: selection of the communication protocol without hardware modifications, rewiring, or device replacements.*

The technical impact is significant. FLEX enables the retrofitting of existing systems without a complete redesign, facilitates adaptation to different specifications across customers or markets, allows for inventory standardization by reducing the number of SKUs to manage, minimizes downtime associated with physical replacements, and enables a seamless migration toward IIoT architectures without technological disruption. Industrial communication becomes an adaptive function rather than a structural constraint.

Furthermore, the approach is not limited to protocol conversion. Edge and cloud are natively integrated. The devices support industrial multi-cloud, bidirectional MQTT, and secure remote configurations via VPN and HTTPS. Data acquired from buses or I/O is not merely collected and forwarded, but contextualized directly in the field thanks to shared memory and local logic. It can be processed, filtered, correlated, and then published to higher-level systems already enriched with operational meaning. FLEX thus transforms the gateway from a static object into a dynamic platform, consistent with Adaptive Automation: an infrastructure capable of evolving over time while keeping the hardware stable and adapting its communication identity via software.

**4. Pillar 2. Unified Firmware.**

In the Adaptive Automation paradigm, the convergence of functions does not result from a simple integration of heterogeneous products, but from a specific internal software architecture based on shared data memory and cooperating application services. In the latest generation of SENECA devices—such as the Z-PASS-RT, Z-TWS4-RT, R-PASS, and Smart Display families—data from industrial buses (ModBUS RTU/TCP, CAN), Ethernet LAN/WAN networks, or integrated I/O converge into a single central shared memory. This memory constitutes the common information model on which IEC 61131-3 PLC logic (Straton), multi-protocol gateway functions, data logging services, local If-Then-Else rules, alarm management, MQTT/OPC UA communication to the cloud and IIoT platforms, as well as VPN services for remote assistance and remote control, operate simultaneously. The key principle is operational simultaneity: control, acquisition, analysis, and transmission are no longer sequential functions entrusted to separate devices, but parallel processes that operate on the same operational data. A value read from an analog input or received via ModBUS can be used simultaneously by PLC logic, recorded to flash memory or a micro-SD card, published via MQTT to a remote broker, exposed via OPC UA, and made available on an integrated web server—all without duplication or intermediate conversions. Efficiency stems precisely from the unity of the data.

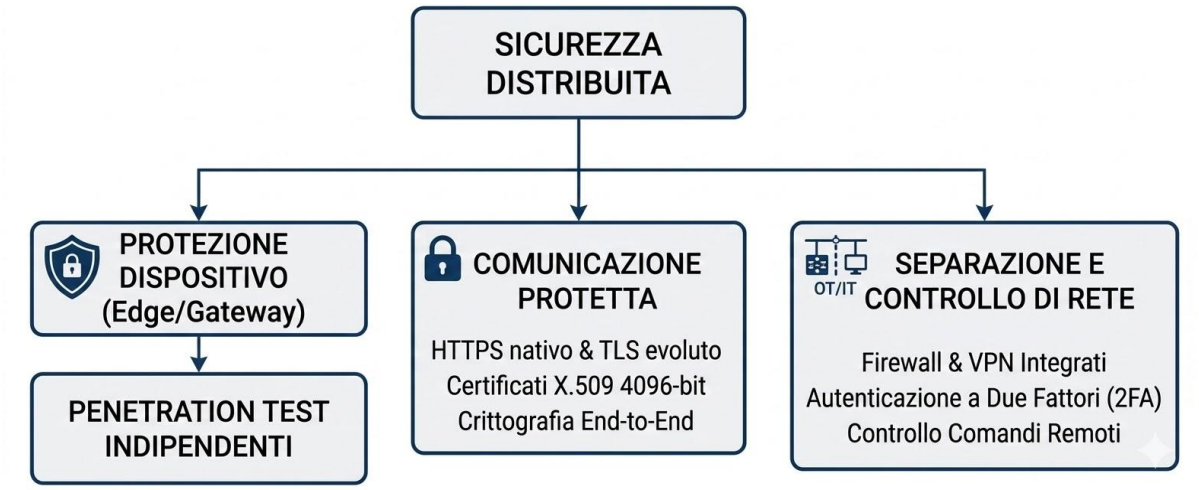



*Unified firmware architecture: communication, logic, data logging, and alarm management integrated into a single platform.*

Traditionally, system architecture involved distinct roles: the PLC controlled, the gateway converted, the data logger recorded, the edge computer processed, and the router ensured remote connectivity. In the Adaptive Automation model, these functions are no longer tied to hardware but to shared firmware. The unified SENECA platform, common to the RT, SSD, and R-PASS families, allows the same device to operate as a softPLC, multi-protocol gateway, LAN/WAN or 4G LTE router with VPN, advanced data logger, IIoT concentrator, or remote alarm unit. Behavior is determined by software configuration rather than physical replacement of the product. Security is not an add-on module but a native layer of the platform, as the device is developed according to IEC 61443-4-2 standards. The engineering benefits are significant. Reducing hardware variants simplifies design and inventory management; technological continuity ensures consistency throughout the plant's lifecycle; firmware updates enable new functions without replacing the device; maintenance focuses on a single software platform; interoperability between devices is intrinsic, as they share the same data model and configuration tools (Web Server, IEC 61131-3 environments, discovery and management tools). From this perspective, automation is no longer a collection of separate interconnected devices, but a software platform distributed across intelligent nodes, each capable of dynamically adapting its operational role. Adaptive Automation means exactly this: transforming the industrial device from a static component into an adaptive node, capable of evolving with the plant, with application requirements, and with the relevant digital ecosystem.

**5. Pillar 3. Distributed Security**

In the Adaptive Automation paradigm, cybersecurity is neither an additional layer nor a function delegated exclusively to the IT perimeter: it is an architectural requirement intrinsic to the device. The approach adopted is consistent with the principles of Security by Design and Security by Default, in which hardware, firmware, and communications protection are integrated from the design stage, in line with the technical references of IEC 62443 and the European regulatory framework NIS2 and the Cyber Resilience Act.




*Distributed security: device protection, encrypted communications, and secure OT/IT network control.*

IIoT Edge devices and industrial gateways implement advanced authentication with privilege management, protection against brute-force attacks, and granular access control for operators, maintenance personnel, and remote assistance systems.

Communication is secured via native HTTPS, advanced TLS, and X.509 certificates up to 4096 bits, ensuring end-to-end encryption of data in transit and protection of credentials.

The firmware is digitally signed to prevent unauthorized modification, reducing the risk of persistent device compromises.

In addition to software mechanisms, hardware access protections, remote command control, and structural separation between LAN/WAN environments and between OT and IT domains are provided, with integration of firewalls, VPNs, and two-factor authentication. Sensitive data is stored in encrypted partitions on the device. This segmentation drastically reduces the attack surface and limits the exposure of field systems to external networks. The devices are also subjected to independent penetration tests according to recognized methodologies (CWE, OWASP, CVSS, IEC 62443-4-2), with results integrated into the continuous improvement process.

The adopted model is one of distributed security. Instead of concentrating protection in the perimeter firewall or data center, each node is designed to be inherently secure. Advanced local logging, event monitoring (forensic audit logs), and controlled update management enable operational resilience to be maintained even in remote environments or with limited connectivity.

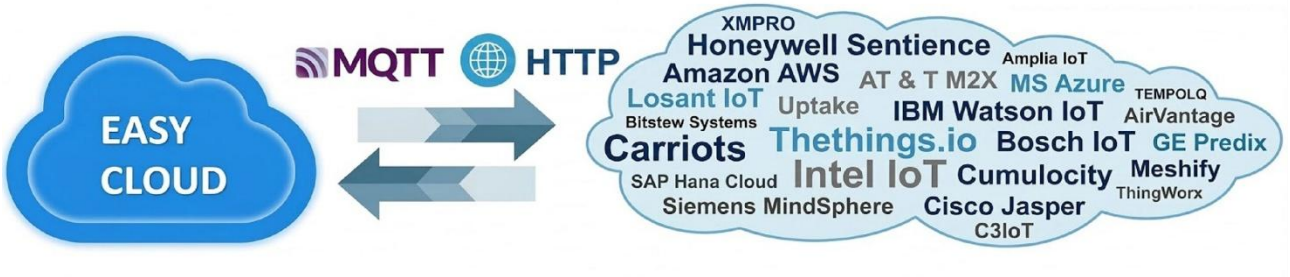
Firmware updates occur via secure and schedulable mechanisms, avoiding impacts on service continuity. This approach mitigates one of the typical risks in industrial plants: lateral attack propagation. If a node is compromised, segmentation and local controls prevent automatic spread to other OT devices. Security is therefore not only centralized (e.g., via a syslog server) but replicated and embedded in every element of the architecture.

In the Adaptive Automation paradigm, security thus becomes a structural property of the system: not an incidental cost, but a prerequisite for resilience, operational continuity, and regulatory compliance throughout the entire automation lifecycle.

## 6. Pillar 4. EASY CLOUD.

The fourth pillar of Adaptive Automation integrates connectivity, modularity, and application development into a single principle: automation must be able to evolve over time without being redesigned. This approach is realized through native integration between Edge and Cloud, the operational flexibility of devices, and an engineering model oriented toward real-world field requirements.

Connectivity is enabled by Easy Cloud technology, which allows for immediate bidirectional connection to major cloud services via preconfigured integration templates, primarily based on MQTT and HTTP. The edge node communicates directly with upper-level systems without requiring complex intermediate architectures or additional gateways. The devices feature a native web server, remote updates, and configuration functions via a web interface, enabling distributed infrastructure management. Models equipped with mobile connectivity include 4G modems, VPN management, and integrated network diagnostics, ensuring operational continuity even at remote or unmanned sites. Connectors and templates ready for integration with various cloud platforms are also available.




*Easy Cloud: simple integration with IoT platforms via standard protocols such as MQTT and HTTP.*

Operational flexibility extends not only to communication but to the entire system lifecycle. Devices such as gateways, RTUs, and HMIs integrate logging, PLC, VPN, and I/O functions into compact platforms. This approach reduces the number of separate components, wiring, and points of failure, simplifying retrofits, expansions, and adaptations to different specifications, with benefits in terms of energy consumption and efficiency as well. Hardware modularity also allows for the addition of optional modules or functional variants without replacing the base architecture, promoting standardization of inventory and maintenance.

Data is not merely collected and sent to the cloud: it is first contextualized in the field. Local processing on ARM processors with dedicated memory enables the execution of logic, scripts, signal normalization, and alarm management directly at the edge. This approach reduces latency, data traffic, and reliance on continuous connectivity, while maintaining decision-making autonomy in the field.

Thanks to Easy Cloud, connecting to major cloud environments is simplified by integration templates that allow the device to be quickly adapted to the chosen platform. The operating principle is that the template connects the edge node to various clouds, and through configuration or advanced programming, the device adapts to the selected service without requiring dedicated gateways or middleware.

In this way, Easy Cloud, modularity, and field engineering converge into a single concept: continuous operational evolution, from the sensor to the cloud, without architectural fractures and without disruptive replacements.

## 7. Industrial Impact and Benefits

The industrial impact of Adaptive Automation is not measured solely in terms of the features introduced, but in the structural transformation of how a plant is designed, managed, and evolved over time, and in the associated benefits.

1) **Reduced complexity**. Fewer devices mean fewer configurations, fewer hardware variants, fewer points of failure, and lower energy consumption. Concentrating multiple functions into a single adaptive platform reduces the architectural fragmentation typical of traditional plants, simplifies technical documentation, and decreases the risk of incompatibility between components. Complexity is not shifted elsewhere: it is absorbed by the architecture.
2) **Extended plant lifecycle**. In a static model, changing the protocol or supervisory system often requires the physical replacement of gateways or interface devices. In the adaptive paradigm, however, the hardware does not become obsolete as requirements change: it evolves through configuration. This decoupling of logical function from physical components preserves the initial investment and reduces the total cost of ownership.
3) **Operational resilience**. The architecture remains functional even as the IT infrastructure evolves, new standards are introduced, or the data collection system changes. The plant does not suffer structural disruptions: it adapts progressively. Continuity is not guaranteed by over-engineering, but by intrinsic flexibility.
4) **Cybersecurity.** The model goes beyond a purely perimeter-based approach. Protection is not concentrated at a single border point but distributed across the nodes. Each device becomes an active part of the defense, reducing the risk of lateral attack propagation. Security is not an external add-on but a structural property of the system.
5) **Technical sustainability**. Fewer replacements mean less electronic waste, less logistics, and fewer invasive interventions. The ability to update and reconfigure without dismantling contributes to an industrial model more consistent with the principles of durability and technological responsibility.

This set of effects defines the shift from the traditional paradigm to the adaptive one. Classic industrial automation is static: when the requirement changes, the device is changed. Adaptive automation is dynamic: when the requirement changes, the configuration is changed. It is a conceptual shift that introduces a new architectural level: from the programmable device to the adaptive system.

Adaptive Automation therefore represents not merely a functional evolution, but a change in the relationship between hardware, software, network, and operator. The plant is no longer a rigid structure to be replaced over time, but a configurable, evolving platform. Innovation is not merely technological: it is architectural.
This approach reflects an engineering tradition typical of Italian industrial manufacturing, where innovation stems from the ability to integrate electronics, software, and field applications. In this context, SENECA, an Italian manufacturer of automation components and systems for nearly forty years, has developed the Adaptive Automation paradigm as a synthesis of this application experience.
Automation ceases to impose constraints on the process and becomes capable of adapting to the process itself. And it is precisely this reversal of perspective that constitutes the distinctive technical value of Adaptive Automation.

## Glossary

**Adaptive Automation**

SENECA's architectural model based on configurability, interoperability, structural safety, and system evolution without hardware replacements.

**Close-to-the-Field Engineering**

A design approach based on real-world field requirements, incremental development, and application verticalization.

**Configurability vs. Replacement**

Guiding principle of the paradigm: when requirements change, the software configuration is modified, not the device.

**Cyber Resilience Act (CRA)**

A European regulation introducing mandatory cybersecurity requirements for connected digital products.

**CWE (Common Weakness Enumeration)**

A standardized catalog of software vulnerabilities used in security analysis processes.

**CVSS (Common Vulnerability Scoring System)**
A system for classifying and scoring IT vulnerabilities.

**EASY CLOUD**

Technology that allows edge devices to connect directly to cloud platforms via preconfigured MQTT/HTTP templates, without intermediate gateways.

**Industrial Edge Computing**

Local data processing on the field node before sending data to cloud systems or supervisory systems.

**Unified Firmware**

A converged software platform that integrates PLCs, gateways, logging, VPN, and IIoT services on shared memory.

**FLEX**
Proprietary technology enabling dynamic and interchangeable management of industrial protocols on a single hardware platform.

**Human-Centric Automation**

A model that simplifies configuration and management, reducing technical complexity and points of intervention.

**IEC 61131-3**

International standard for PLC programming.

**IEC 62443**

International standard for the security of industrial automation and control systems.

**Multi-protocol**

Ability to manage heterogeneous protocols (Modbus, Profinet, Ethernet/IP, OPC UA, IEC 61850, MQTT) on a single platform.

**NIS2**

European Directive on the cyber resilience of critical infrastructure and essential entities.

**Adaptive Industrial Node**

Edge device capable of modifying its operational role via software configuration.

**OWASP (Open Web Application Security Project)**

Framework and guidelines for application testing and security.

**Penetration Testing**

Independent vulnerability tests conducted according to structured methodologies.

**Evolving Retrofit**

Functional upgrades of existing systems without mass replacement of devices.

**Security by Default**

Active security configuration enabled by default.

**Security by Design**

Integration of security starting from the hardware and firmware design phases.

**OT/IT Segmentation**

Structural separation between the industrial operational network (OT) and the corporate IT network.

**Shared Memory**

Centralized data memory on which PLCs, gateways, logging, and cloud services operate simultaneously.

**Distributed Security**

A model in which every node in the architecture is inherently protected, reducing reliance on the IT perimeter alone.

**Bibliography and Resources**

**Product Technical Documentation**

- Multifunction IIoT Edge Devices: https://www.seneca.it/media/6849299/0099_seneca_edge_iiot-it-2025_it.pdf
- Industrial IoT Edge Devices (R-PASS): https://www.seneca.it/media/4151/0224-seneca_r-pass_it.pdf
- Multifunction HMI Gateway PLC (SSD): https://www.seneca.it/media/6848723/feb_25iiot-edge-hmi-multifunzione-it.pdf
- IIoT Edge Devices User Manual https://www.seneca.it/media/6849479/mi00557-26-it.pdf
- R-PASS – IIoT Edge Controllers https://www.seneca.it/media/6849366/flyer_r-pass-s-en-2210-ps.pdf
- IIoT Edge Gateway with VPN Support https://www.seneca.it/media/6849714/flyer_zpass1-rt_23070it.pdf
- IIoT Edge Gateway / 4G Router with VPN Support https://www.seneca.it/media/6849718/flyer_zpass2_rt_2307_it.pdf
- https://www.seneca.it/media/6849724/flyer_z-pass2-rt-s_2307it.pdf 4G IIoT Edge Controller

**Regulations and Technical Standards**

- IEC 62443 – Industrial Communication Networks – IT Security for Networks and Systems
- IEC 61131-3 – PLC Programming Languages
- NIS2 Directive (EU 2022/2555)
- Cyber Resilience Act (EU Regulation 2024)
- NIST SP 800-115 – Technical Guide to Information Security Testing
- OWASP Testing Guide
- CVSS – Common Vulnerability Scoring System
- CWE – Common Weakness Enumeration

**Institutional Web References**

- https://www.seneca.it
- https://www.iec.ch
- https://www.enisa.europa.eu
- https://digital-strategy.ec.europa.eu
- https://owasp.org
- https://nvd.nist.gov

SENECA s.r.l.
26 Via Austria - 35127 Padua
Tel. +39 049 8705359

Web: www.seneca.it
Email:info@seneca.it