Cybersecurity for Energy and Utilities: Bringing trust and compliance in the age of digital transformation

Trusted partner for your **Digital Journey**

Atos

This document should be read in conjunction with the Atos publication "Tackling cybersecurity threats in the Utility industry" which discusses the utilities' digital transformation and the cyber threats targeting this industry.

How to tackle Utilities cyber threats and where to start?

The multiplicity of actors in the utilities' industry, combined with the digitalization of the production, transport and distribution infrastructures, are weakening the world of energy. This situation requires an increasing share of investment in cybersecurity.

Obviously, nobody wants to experience a cyberattack. However, the question is no more if they will happen but when and how to counter them? When fighting against cybersecurity attacks targeting utilities, the following exposures can lead to the creation of an entry point for hackers followed by a successful actualization of the attack itself:

1. Human error due to a lack of cybersecurity awareness
2. Use of off-the-shelf technology like Ethernet, TCP/IP and Windows in the OT sector introducing threats from the IT world
3. Difficulty to identify abnormal behaviors and detect advanced persistent threats
4. Risk of infections through unsafe mobile devices such smartphones and laptops (on-site and for remote working)
5. Insufficient access control for both physical and logical access
6. Lack of IIoT security for connected devices collecting data
7. Industrial control systems components such as HMI's (Human Machine Interface) and PLC's (Programmable Logical Controller) designed to be reliable and safe, often overlooking security

8 Older control systems units in facilities still prevalent and easy to exploit

9 Difficulty or impossibility to patch devices due to conflicting industry-specific regulations as well as configuration/warranty considerations

10 Remote maintenance of ICS components and entire systems is carried out without implementing security and access control measures by various operators (company maintenance team, third-party integrators or machine manufacturers)

To tackle these vulnerabilities and create a comprehensive security policy, utilities organizations must answer the following questions to know in which cybersecurity aspects they excel and in which they need to improve:

People

- Do you have cross-functional expertise to cover IT/OT/IoT & IIoT?
- Do you have a training plan to cover the knowledge gap?
- Do you have cross-functional security and safety knowledge exchange between IT/OT/IoT & IIoT experts?
- Did you define the required RACI structure?

Processes

- Do you have the right governance & security program?
- Do you know what are your legal obligations?
- Did you identify the right security standards/frameworks for your specific requirement?
- Did you identify how to manage your cyber risks and how to reduce the impact of a potential incident?
- Do you know the security posture of your suppliers?

Technology

- Do you have a clear view of your currents IT/OT/IoT & IIoT assets?
- Are you familiar with the industrial protocols in use in your environment?
- Are you conducting vulnerability scans and if the outcomes of such scans are dealt with?
- Are you aware of any patching processes actively maintained in your environment and if they actualized?
- Do you know who accesses the IT/OT systems and if the data is enough protected?
- Do you have a clear visibility and connectivity to your security tools in this environment?

Building a multi-layered cybersecurity approach is critical to address the specificities of the utilities sector. Protection of OT environments, whether it is ICS, DCS, SCADA & BMC has become a priority. For hackers, this environment is highly exposed today, can provide high revenue and allow them to "show-off" capabilities in an easy way. The Energy & Utility sector seats high on this list as it is also a main target for terror organizations and foreign entities wishing to have a big impact on a countries industry with very low effort.

This was observed during the Russian attack on the Ukrainian power grid, also known as **"Black Energy"**. Industrial organizations are required to be ready against the most common attacks, that can be blocked by antiviruses or even a patch in a regular IT environment, to most advanced ones. There is indeed a growing need to have the capability to provide continues monitoring for such environments based on advanced security operations center (SOC) which is a key element to detect and remove hidden attackers from the system.

How Atos can help you

With many years' experience in serving the world's energy and utilities companies, our sector specialists are working to ensure that our skills remain focused and relevant to the specific operational and commercial demands of our utility clients.

Atos in Utilities

In today's more interconnected world, companies need to adopt the right tools to get closer to the market and become more competitive. Atos has led hundreds of projects in the utility sector, each requiring specialist industry and IT knowledge.

Whether we are dealing with well-established heritage systems or with projects driven by digital transformation, we constantly seek to boost efficiency and enhance safety for our clients.

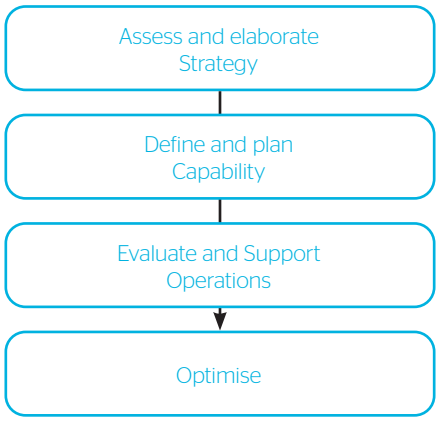
Here is just a taster of some activities in which we have taken the lead in recent years. Current engagements include:

- Centralized security for Gazpar and Linky smart metering
- Access control for IT/OT convergence to centrally control and monitor access to unconnected systems
- Security operations and consulting including Security Information and Event Management (SIEM), Data Loss Prevention, Security Foundation Services, Data Masking and Access Audit

Atos Utilities Security Services – end to end approach

Utilities security is considered a key area for digital transformation. At Atos, we believe that to achieve this digital transformation, it is critical to secure the business value of Utilities with sustainable security models.

Before beginning your journey to global security, it can be critical to set up a vulnerability management strategy on the connected assets to know how to secure, how to protect, and how to improve their integrity. Atos has the depth of technical expertise, the industry-specific knowledge and the depth of specialist partnerships to support you along this transformation. As business technologists with a special focus on utilities, we have designed the following methodology to have a clear picture of your people, processes and technologies across your different sites to define the most adapted cybersecurity posture:



- Process, people & organizational findings – Maturity risk assessment (CMMI)
- Discover IT/OT assets - get an Asset inventory & Network diagram
- Discover vulnerabilities and get a report of known common vulnerabilities and exposures (CVEs)
- Get visibility for OT behavior anomalies & malwares
- Automatically update Firewall policies to block suspicious traffic
- Generate appropriate incident into SIEM for monitoring and supporting integration into our Security operations capabilities (SOC)

Furthermore, we offer multiple innovative products and services to provide you with the best-of-breed security solutions.

IoT security suite for an end-to-end secured ecosystem

With Horus and IDnomic products and solutions, Atos delivers trust for the Internet of Everything (IoE) and ensures the security of the IoT on every level through its IoT Security Suite:

- **Embedded Security:** Protect devices and sensors without compromising performances with hardware trust anchors, secure elements, trusted identity and middleware for IoT devices.
- **Identity Lifecycle Management:** Provision and manage devices digital identities securely through a security server for device enrollment with IoT PKI & HSM for key and certificate management.
- **Secure Communication:** Encrypt private data at rest and in transit in IoT ecosystems with an end-to-end data encryption and privacy enforcement for message authenticity.
- **Firmware Update:** Improve integrity of sensitive operations such as device firmware updates of IoT devices to prevent malicious code execution.

Horus products also enable distribution system operators' standards to meet security requirements with a **"security by design approach"**. To meet regulatory requirements, the DSOs set up smart meters for the gas and electricity networks. These solutions integrate security provisions to protect the communication of metering data and meter settings. Any compromise of these data could indeed directly impact financial and brand aspects of the company.

The crypt2pay **hardware security module** functions for gas meters provide key management functions of Linky meters to meet the needs of all DSOs (gas and/or electricity).

The crypt2pay HSM also meets the G3-PLC, Gazpar and DLMS / COSEM standards. It is a scalable solution that can support millions of smart meters. Master keys are managed in HSMs deployed on the manufacturers' production lines, for the injection of the derived keys into the meters, and on the DSO's information system for the security of the frames exchanged with the deployed meters.

IDnomic offers identity management of the IoTs using a PKI (Public Key Infrastructure) in SaaS or On Premise. With its **ID-PKI solution**, the level of security of devices is increased by managing the lifecycle of digital identities. Thus, it is possible to massively and automatically deploy identities on all equipment and IoTs, even those with limited cryptography capabilities and limited energy power and energy-storage cap.

Secure Remote Access to bridge the air gap between IT and OT

Evidian is the Identity and Access Management (IAM) software suite of the Atos Group. It offers a dedicated Secure Remote Access solution to manage the shop-floor landscape. It is changed from isolated islands to highly complex networks, keep security at the forefront in configurations while maintaining availability and secure remote access credentials to avoid espionage or sabotage.

Utilities organizations need trusted secure Identities for Humans, Services and Things. With our Evidian solutions we bring strong authentication for utilities processes and enforce IAM for both IT and OT to interconnect both worlds and ensure integrity. Atos offers full transparency and control on the access you might wish to provide to your suppliers and partners for remote services. Our solution includes a detailed audit trail with ease of use.

We make sure you have the full sovereignty over your data.

How we bridged the Air gap on a smartphone:
A QR code scanned with the smartphone – in this way the smartphone connects to IT network and it is possible to see the person who is trying to connect to the OT system. If the person has the access, he receives a code to prove that he or she is properly authorized.

Federated Access for the Connected Industrial IoT Ecosystem - the Universal Identity Service Architecture

In a co-innovation project with Siemens AG Atos defined the Universal Identity Service Architecture as a blueprint for the next generation Identity and Access Management infrastructures for the Industrial Internet of Things (IIoT). The Atos Universal Identity Service Architecture (UISA) provides a framework for delivering secure identity and access management services for the industrial IT use cases in the extended enterprise. UISA defines a set of IAM services, functionalities, standard interfaces and protocols ready to be operated in the cloud or on premise. The IAM End User Services include identity assurance, dynamic risk analysis, risk tagging and risk-based authentication.

In a Utility environment, several identity name spaces must be integrated and managed for multiple tenants (customers, system vendors, IIoT service partners or external organizations, for example).

The UISA architecture defines a set of open standards and protocols for connectivity, identity management, authorization, authentication and identity federation, such as SCIM, OAuth, OpenID Connect, SAML and multi-factor authentication. The services are accessible via RESTful interfaces. Adapting the UMA standard supports the decentralized user-centric access control necessary for enhancing privacy and confidentiality.

In addition, UISA provides ancillary functions such as monitoring, analytics and reporting. The key design principle is externalization of IAM functionality on all layers of the IIoT architecture. We assume that both the Use Case Apps and the IIoT Services will not operate self-sufficiently but will require an open security layer to interact with each other and new third-party services.

The Evidian IAM suite is providing all key features of the UISA blueprint. New developments like Identity as a Service will complement the Atos offer for the extended enterprise and IoT.

Intrusion Detection System – Connect and protect industrial assets

Utilities critical infrastructure and associated operational technology are essential for providing services in safe and reliable way. To help maintain the health and security of all critical industrial infrastructure, Atos works with a network of leading partners, such as Intrusion Detection System (IDS) providers. The objective is to discover, decode, inventory, map and continually monitor both legacy and current ICS communications listening to the inputs and outputs from a variety of analog and digital sources like sensors, valves, relays and motors. A normal behavior baseline is established through machine learning and AI. It enables the rapid detection of cyber threats and anomalies.

In parallel, Atos Codex Analytics powered by BullSequanaS, high-performance computing, ingests the same data in real-time and on-premise where high-speed and low latency are critical for timely decision-making. This data is enriched with metadata from other sources like enterprise asset management tools, maintenance records, historical weather facts and much more for a wider view of all factors potentially affecting asset behavior. Atos applies machine learning models to quickly identify performance variability and to extend asset lifecycles and overall systems reliability and safety through smarter predictive and prescriptive maintenance.

For geographically dispersed assets or plants, a scalable cloud-based solution cost-effectively stores the same data but for multiple locations. Atos data scientists analyze data on a larger scale for comprehensive insights into the performance of the entire industrial asset ecosystem. This intelligence can provide enterprise-wide benefits such as prolonged asset lifecycles, smarter supply chain management and proactive threat identification.

OneSOC: our answer on how to align IT, IoT and OT SOC activities

Atos, as a global leader in digital transformation, has developed the concept of prescriptive security solution for customers to predict and remediate to security threats before they occur, the OneSOC. Combined with Atos Big Data analytics capabilities and powered by BullSequana S servers the detection and neutralization time is improved significantly compared to existing solutions.

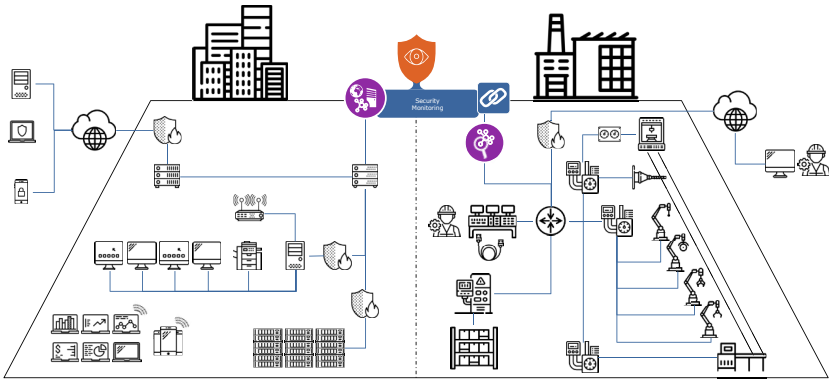
Based on Big Data analytics and Machine Learning technology, the SOC continuously learns from previous threats and orchestrates automated responses in real-time.

With Atos prescriptive next-generation Security Operations Centers, your IT and OT infrastructure will continuously be monitored, indicators from both environments correlated and when relevant, raw events will be merged and analyzed.

This will enable organizations to create visibility throughout their full surface and win the race against malware attacks, taking advantage of vulnerable, unpatched or highly proprietary systems, and propagating systemically and laterally into the rest of the Enterprise assets. Atos SOC orchestrates then the necessary actions, in real time, to protect the assets and stop the threats before the organizations critical processes are paralyzed.

360° Security Event and Incident Management for the whole Enterprise

- IT and OT environment
- Best in Class IT Security Expertise
- Best in Class OT Security Experts
- 24/7 Security Operation
- Global Presence
- Security Analytics
- Automated Response



Charter of Trust

The digital world is changing everything. Artificial intelligence and big data analytics are revolutionizing our decision-making process; billions of devices are being connected by the Internet of Things and interacting on an entirely new level and scale. As much as these are improving our lives and economies, the risk of exposure to malicious cyber-attacks is also growing dramatically. In this case, the security remains the most important key for a digital journey.

At Atos we believe in a collaborative approach of public and private entities to overcome all these new cybersecurity challenges of such digital world. Therefore, Atos is founder member of the Charter of Trust.

The Charter of Trust is a cybersecurity initiative that establishes three primary goals:

- to protect the data of individuals and business,
- to prevent harm to people, businesses, and infrastructure,
- to establish a reliable basis where confidence in a networked, digital world can take root and grow.

The Charter outlines ten principles to ensure companies and governments are acting to address cybersecurity at the highest levels:

Ownership of cyber and IT security - 1

Responsibility throughout the digital supply chain - 2

Security by default - 3

User-centricity - 4

Innovation and co-creation - 5

Charter of Trust

6 - Education

7 - Certification for critical infrastructure and solutions

8 - Transparency and response

9 - Regulatory framework

10 - Joint initiatives

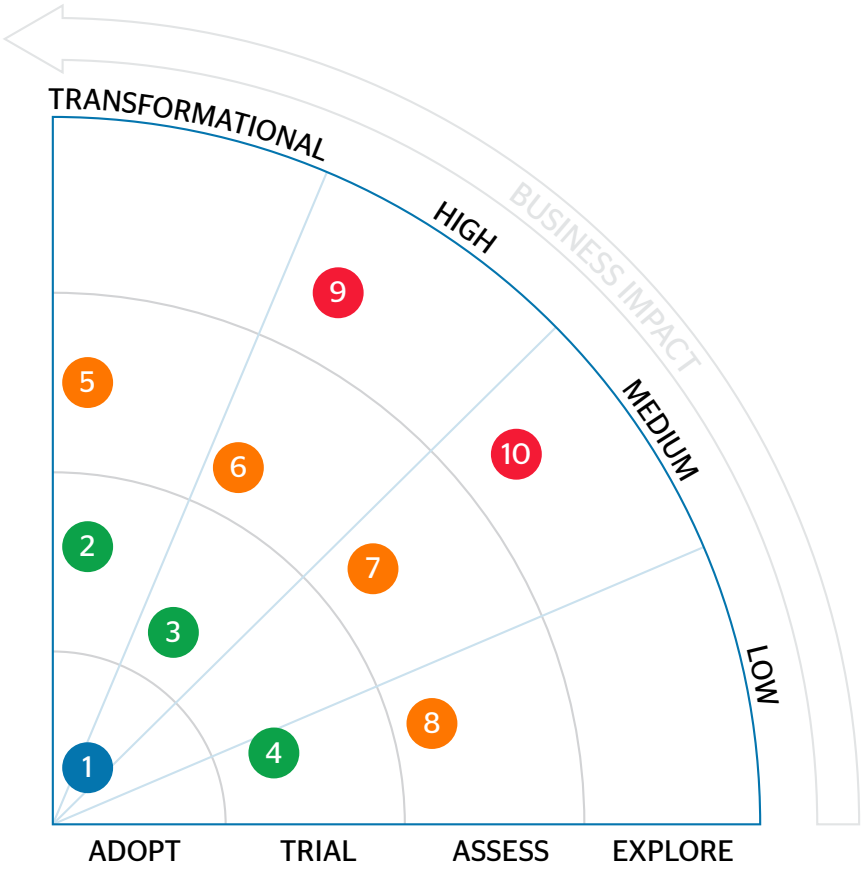
Other members are of the Charter of Trust are: AES, Airbus, Allianz, Cisco, Daimler, Dell Technologies, Deutsche Telekom, IBM, MHI, NTT, NXP, SGS, Total, TÜV Süd, German Federal Office for Information Security, the CCN National Cryptologic Center of Spain and the Graz University of Technology in Austria.

The digital journey can be compared to a sport. Both demanding determination, performance, reinvention and persistence. We can never complete this alone. Every progressive step is the result of constant challenge and collaboration. Every journey needs a partner.

Securing the future of Utilities

What technologies will power the utilities business of tomorrow and where will we need to implement new security approaches?

1. Hybrid Cloud
2. Real-Time Service Orchestration
3. API Platforms
4. Robotic Process Automation
5. Artificial Intelligence
6. Prescriptive Security
7. Drones & Robots
8. Augmented Reality
9. Blockchain
10. Quantum Computing



Source : Atos industry and technology experts

× Mainstream × Early Adoption × Adolescent × Emerging

Utilities will be faced with emerging cyberattacks as part of their digital transformation. Some threats still remain unknown as utilities companies are changing of paradigm and other will appear as new technologies will be adopted.

Security by design systems and processes will play a critical role in this digital transformation to better answer to unexpected cyberattacks, as well as an adaptive and flexible cybersecurity approach to react quickly and efficiently.

Disruption, by its nature, cannot be predicted. How utilities produce, store and distribute energy can be fundamentally changed by the use of Artificial Intelligence or the introduction of peer-to-peer (P2P) energy trading. Wherever the transformation comes from, utilities organizations must be ready to capture securely value where it is generated.

About Atos

Atos is a global leader in digital transformation with 110,000 employees in 73 countries and annual revenue of € 12 billion.

European number one in Cloud, Cybersecurity and High-Performance Computing, the Group provides end-to-end Orchestrated Hybrid Cloud, Big Data, Business Applications and Digital Workplace solutions. The Group is the Worldwide Information Technology Partner for the Olympic & Paralympic Games and operates under the brands Atos, Atos|Syntel, and Unify. Atos is a SE (Societas Europaea), listed on the CAC40 Paris stock index.

The purpose of Atos is to help design the future of the information technology space. Its expertise and services support the development of knowledge, education and research in a multicultural approach and contribute to the development of scientific and technological excellence. Across the world, the Group enables its customers and employees, and members of societies at large to live, work and develop sustainably, in a safe and secure information space.

Find out more about us
atos.net
atos.net/careers

atos.net/en/solutions/cyber-security
atos.net/en/industries/utilities

Let's start a discussion together

CT-200310-RY-J3662-ENERGY-WP-TRUSTAND