MOGUĆNOSTI PRIMENE IIOT PLATFORME U ELEKTROENERGETSKIM SISTEMIMA

POSSIBILITIES OF IIOT APPLICATION PLATFORMS IN THE ELECTRICAL POWER SYSTEMS

Vojkan NIKOLIĆ*[1], Zoran STEVIĆ[2], Stefana JANIĆIJEVIĆ[3], Dragan KRECULJ[4]
[1] University of Criminal Investigation and Police Studies, Belgrade
[2] Technical Faculty Bor and School of Electrical Engineering Belgrade,
University of Belgrade, CIK Belgrade
[3] Comtrade SI, Belgrade
[4] Technical College of Vocational Studies Belgrade

https://doi.org/10.24094/mkoiee.020.8.1.255

Na tržištu postoje različiti internet inteligentni uredjaji (IoT) koji se primenjuju u elektroenergetskim sistemima. IoT uredjaji mogu biti fizički ili virtuelni, umreženi interoperabilnim komunikacionim protokolima i inteligentnim interfejsima. IoT tehnologije obezbedjuju njihovo povezivanje na internet, kao i povezivanje sa servisima i aplikacijama. Elektroenergetski sistemi imaju tradicionalno Sisteme za upravljanje resursima preduzeća (ERP), Sisteme za nadzor, praćenje, arhiviranje i kontrolu industrijskih sistema (SCADA), Distribuirane kontrolne sisteme (DCSs), kao i tradicionalnu industrijsku automatizaciju za postizanje integracije izmedju nivoa upravljanja kompanijom i nivoa proizvodnje. Industrijske IoT (IIoT) platforme treba da prevaziđu jaz između okruženja Informacionih tehnologija (IT) i Operativnih tehnologija (OT). Ove platforme pružaju pogodniju arhitekturu podataka za savremenu industrijsku automatiku. U radu je dat pregled savremenih rešenja.

Ključne reči: IIoT platforma, informacione tehnologije, operativna tehnologija, poslovna inteligencija

Nowadays ***i****n the market there are different Internet of Things (IoT) devices, that are used in electrical power systems. Such IoT devices can be physically, or virtually networked, with interoperable communication protocols and intelligent interfaces. IoT technologies provide their connection to the internet, as well as connection to special services and applications. Electrical power systems have traditional Enterprise resource planning (ERP), Supervisory control and data acquisition (SCADA), Distributed control systems (DCSs), as well as traditional industrial automation stack to achieve functional integration between the company management level and the production level. Industrial IoT (IIoT) platforms should overcome the gap between Information technology (IT) and Operational technology (OT) environments. These platforms providing a more suitable data architecture for the modern industrial automation stack. The paper presents the overview of one modern solution with the Claroty IIoT platform. Claroty delivers comprehensive and reduces the complexity of OT security.*

Key words: *IIoT platform, information technology, operational technology, business intelligence, claroty*

1 Introduction

Traditional IT are separate from OT. IT and OT have evolved independently for a long time. IT refers to the application of network, storage, and compute resources towards the generation, management, storage, and delivery of data throughout and between organizations, while OT refers to technology that monitors and controls specific devices and processes within industrial workflows. [1]

[*] Corresponding author, email: vojkan.nikolic@kpu.edu.rs

Recently, there has been an increasing convergence and integration of these two technologies. The convergence of IT and OT in IoT has been going on for a while and there isn’t a strict division between them in the real world. With IT and OT converging, the scope of CIO authority may cater to the needs of planning and coordinating a new generation of operational technologies alongside existing information- and administration-focused IT systems. [2]

In addition to the fact that IT and OT are increasingly converging with each other, they are also increasingly connecting to the internet. This integration provides IoT in such a way as to achieve a greater degree of integration, functionality and flexibility, as well as central management in accordance with the decisions that arise as a result of the complex algorithms of the Big Data concept. IoT is a global network infrastructure that provides connectivity of "smart" devices with interoperable communication protocols and intelligent interfaces.

IIOT represents the application of IoT in the industrial environment in order to increase industrial efficiency, productivity, safety and transparency. “…the industrial internet is an internet of things, machines, computers and people enabling intelligent industrial operations using advanced data analytics for transformational business outcomes, and it is redefining the landscape for business and individuals alike”. [3]

IoT platforms are a software and hardware platform for efficient development of IoT systems. With the number of connected IoT devices in a manufacturing facility, cyber security has become important to industrial companies and workers safety and productivity.

IIoT platforms are specialized IoT platforms for industrial environments. The development and implementation of the IIOT platform is a very dynamic area of the software and hardware environment. For the development of IIoT platforms used in electrical power systems, as well as for the development of any IoT platforms, it is necessary to consider the IoT devices to be used, communication components that will provide connectivity within the platform, services to perform, ways to manage platform functionality, security aspects of platforms and application components that allow end users to monitor, use functionality, and manage platforms.

With the development of mobile business technologies, the Internet of intelligent devices and social media, the amount of data stored in the company's information systems is increasing. [4]

Companies acquire a large amount of data every day that they cannot use by using traditional databases. Therefore, new approaches for storage, rapid retrieval and analysis of large amounts of data in real time, based on Big Data (BD) technology are being developed. [5]

In order for IIoT platforms to get their full functionality, it is necessary to apply BD analytics (BDA). Some studies showed that the adoption of BDA increase companies output and productivity; while IoT enables companies to have more information and control in physical resources, processes and environments. BDA is expected to provide operational and customer level intelligence in IIoT systems. Although many studies on IIoT and BDA exist, only a few of them have explored the convergence of these two paradigms. [6]

The paper presents the Claroty IIoT platform that provides deep integration between IT and OT, as well as BDA, and its implementation in electrical power systems significantly contributes to the quality of management and efficiency.

2 Information technology (IT) and Operational technology (OT) convergence

IT/OT convergence is the integration of information technology (IT) systems used for data-centric computing with operational technology (OT) systems used to monitor events, processes and devices and make adjustments in enterprise and industrial operations. A comparative analysis of these two technologies is presented in Table 1. [7]

IT/OT convergence improves automation and efficiency, provides interoperability conditions and accelerates innovation. In terms of business benefits, they are reflected in the reduction of risks due to the use of proven technologies and protocols, the reduction of costs due to the connection of distributed entities and the reduction of implementation time due to reduced complexity by introducing IoT technology.

Table 1. A comparative analysis between IT and OT [7]

	Information Technologies (IT)	**Operational Technologies (OT)**
Function	It refers to telecommunications equipment. Information Technology focuses on the storage, recovery, transmission, manipulation and protection of data	OT is more oriented to the control of processes or their change through the monitoring and control of devices
Use, area	Business-oriented	Industrial-oriented
Access	Connected with the outside world	Very restricted access. Limited to people with certain privileges
Assets Vs workers	The number of assets is usually equal (or close) to the number of professionals	More autonomous More devices than professionals
Frequency change	Constantly changing: new employees joining the company (=new devices connected) and former employees leaving the company (=devices that are disconnected)	Less changing environment (there may be no changes for months to years)
Environment	Controlled, stable and constant	OTs endure adverse weather conditions (extreme temperatures or humidity levels, among others)
Interface and Network	Web browser, keyboard, device	Sensors, coded or touch screens
Main priority	Data security (usually confidential data)	Uptime, the availability and integrity of the legacy and no longer system devices is essential
Updates	Constant due to software updates Service interruptions are tolerable and, in some cases, programmable outside of working hours	Updates must be tested carefully in advance and, usually involve restarting or stopping the machines Consequently legacy systems are very frequent
Life cycle	Shorter life cycles (3-5 years)	OT systems have longer life cycles (15-20 years) As a result, legacy systems and no longer supported ones are frequent
Processing requirements	Minutes-days	Milliseconds-Seconds
Objective	Logical security (no lives at risk) The objective is to protect confidential information from any potential risk (human error, natural disasters, cyberattacks, etc.)	The objective is to protect the environment, people and infrastructures
Operating System	Standard operating systems	Specific purpose equipment with proprietary Operating Systems (Custom-developed software)

Ready-made solutions can be used to implement IIoT platforms, or own platforms can be developed. IIoT platforms as ready-made solutions are commercial, ie. proprietary platforms and they represent complete and closed solutions that, immediately after purchase and installation, connect to IoT hardware and configure. After that, they are ready for the use. These platforms usually have APIs for connecting to other software solutions. Their main advantage is fast implementation and low price. On the other hand, like most proprietary software solutions, these platforms are closed to third-party devices and software components. Developing personal IIoT platform requires a significantly higher level of technical knowledge and a longer implementation time. The main advantages of one's own development are flexibility and openness.

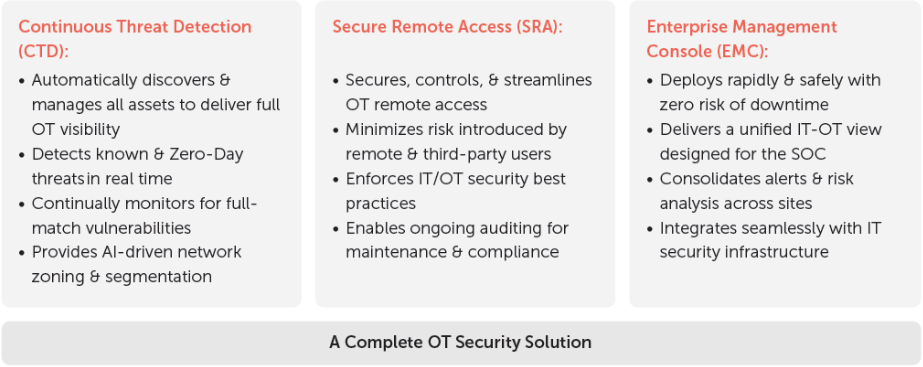
The quality of the IIoT platform also depends on the ability to provide the required flow of information in real time. In order to ensure that, the application of the Big Data concept is needed. BD has the ability to collect and store large amounts of data generated by IoT devices, as well as their processing.

3 Claroty IIoT platform

The Claroty platform bridges the gap and provides integration between information technology and operational technology environments. Claroty's converged IT/OT solutions, ensures the integration of an organizations IT solutions with OT critical infrastructure, where existing IT infrastructure and existing OT infrastructure can be used to a large extent. This platform provides the use of existing IT processes and security technology to improve the availability, safety, and reliability of their OT assets and networks seamlessly and without requiring downtime. The result is more uptime and greater efficiency across business and production operations. With Claroty product enterprises increase the utilization of IoT devices to drive digital transformation and increase the operation efficiency.

The Claroty Platform comprises Claroty's Continuous Threat Detection (CTD), Enterprise Management Console (EMC) and Secure Remote Access (SRA) systems. This single, agentless solution seamlessly integrates with existing IT security infrastructure. Also platform provides for the industry broadest range of OT security controls across four essential areas: visibility, threat detection, vulnerability management, and triage & mitigation. [8]

Claroty OT Security Solution is visible in the Figure 1.



Continuous Threat Detection (CTD):

- Automatically discovers & manages all assets to deliver full OT visibility
- Detects known & Zero-Day threatsin real time
- Continually monitors for full-match vulnerabilities
- Provides AI-driven network zoning & segmentation

Secure Remote Access (SRA):

- Secures, controls, & streamlines OT remote access
- Minimizes risk introduced by remote & third-party users
- Enforces IT/OT security best practices
- Enables ongoing auditing for maintenance & compliance

Enterprise Management Console (EMC):

- Deploys rapidly & safely with zero risk of downtime
- Delivers a unified IT-OT view designed for the SOC
- Consolidates alerts & risk analysis across sites
- Integrates seamlessly with IT security infrastructure

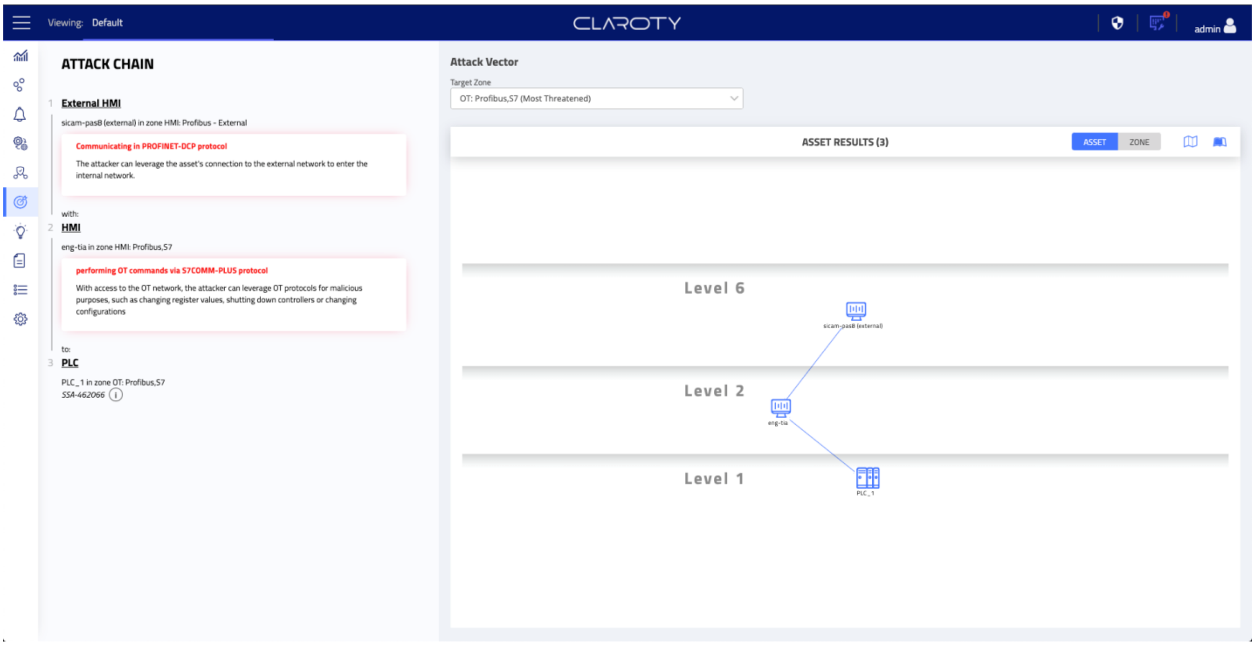
A Complete OT Security Solution

Figure 1. Claroty OT Security Solution [8]

Claroty CTD minimizes the considerable risks inherent to IT-OT convergence by extending fundamental security controls to OT environments. These controls can be implemented rapidly and safely, do not require downtime, or OT expertise, and span four key areas:

1. Asset Identification & Management;
2. Network Segmentation & Micro-segmentation;
3. Security Monitoring & Threat Detection;
4. Risk & Vulnerability Management. [9]

CTD provides complete OT visibility and asset management controls using OT protocols and passive, active, and AppDB scanning capabilities. One of the main advantages of the Claroty platform is that it provides visibility into all three variables of risk in OT environments: asset visibility, network visibility, and process visibility. CTDs intuitive interface offers a single-pane view into all assets, processes, sessions, and related risks & vulnerabilities in your OT environment (Figure 2).



ATTACK CHAIN

1 External HMI

sicam-pas8 (external) in zone HMI: Profibus - External

Communicating in PROFINET-DCP protocol

The attacker can leverage the asset's connection to the external network to enter the internal network.

with:

2 HMI

eng-tia in zone HMI: Profibus,S7

performing OT commands via S7COMM-PLUS protocol

With access to the OT network, the attacker can leverage OT protocols for malicious purposes, such as changing register values, shutting down controllers or changing configurations

to:

3 PLC

PLC_1 in zone OT: Profibus,S7

SSA-462066

Figure 2. Claroty Threat Detection [8]

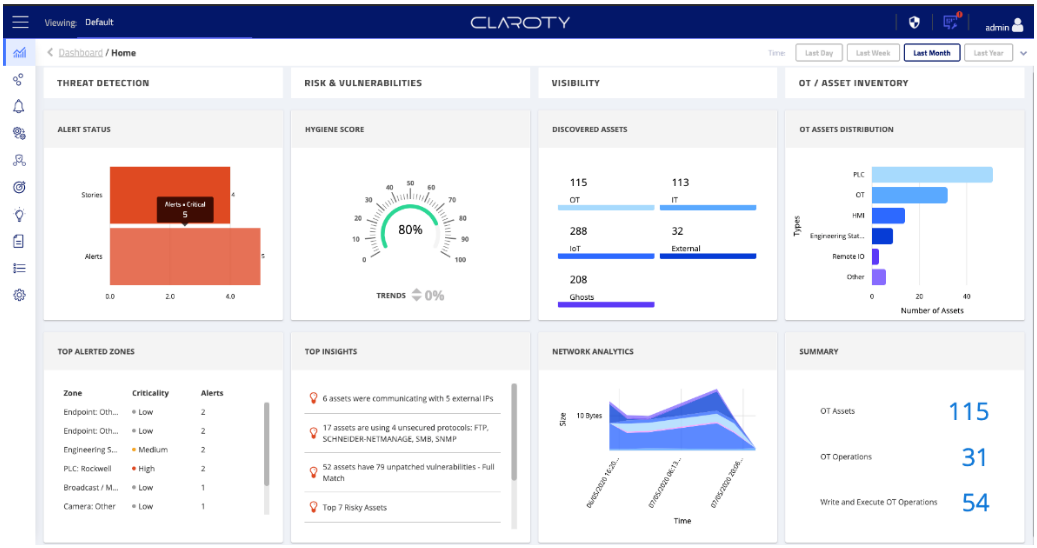
Claroty SRA provides simple, secure, highly controlled remote access to OT environments for both internal and third-party users. Key features and capabilities include:

– Automatic enforcement of granular role- and policy-based administrative controls in accordance with Least Privilege and Zero Trust principles;

– Over-the-shoulder monitoring and full recording of all remote sessions for live supervision and troubleshooting, painless audits, and streamlined investigations;

– A secure and clientless interface through which all remote users connect prior to performing software upgrades, periodic maintenance, and other support or auditing activities in OT environments. [9]

The unique Claroty platforms with the components are presented in Figure 3.



Zone	Criticality	Alerts
Endpoint: Oth...	• Low	2
Endpoint: Oth...	• Low	2
Engineering S...	• Medium	2
PLC: Rockwell	• High	2
Broadcast / M...	• Low	1
Camera: Other	• Low	1

6 assets were communicating with 5 external IPs

17 assets are using 4 unsecured protocols: FTP, SCHNEIDER-NETMANAGE, SMB, SNMP

52 assets have 79 unpatched vulnerabilities - Full Match

Top 7 Risky Assets

OT Assets	115
OT Operations	31
Write and Execute OT Operations	54

Figure 3. Claroty platform [9]

Then Claroty EMC is a centralized management interface that aggregates data from Claroty products deployed across multiple sites. It displays a unified view of all assets, activities, alerts, and access controls spanning the entirety of each customers OT environment. The key features include the following:

– Pre-built reports, customizable analytics dashboards, and contextualized risk scoring;

– Seamless integration with SIEM, SOAR, firewall, NAC, and other existing security infrastructure components;

– Single-pane-of-glass visibility and governance structure ideal for security operations center (SOC) deployments. [9]

4 Conclusion

The disagreement that exists between internet technologies and operating technologies is successfully bridging through the IoT. The IoT devices are increasingly appearing in electrical power systems, which on the one hand, need to be integrated into certain system; and on the other hand, to ensure the connection of this system with traditional IT solutions already owned by companies. This task is achieved by using IIoT platforms that can be proprietary solutions, or can be developed independently. With adequate platforms, after purchase and installation, they are connected to IoT hardware and configurations, so they can be completely used. The main advantages of these platforms are low prices and fast implementation. The independent development of the IIoT platform is reflected in the fact that a higher degree of technical knowledge and a longer implementation time are required, while the advantages of this approach are flexibility and openness.

With the advanced and cutting-edge technologies, the electric power industry has more options to control, monitor, analyze and utilize the collected data, in order to create intelligent decisions automatic. Through intelligence concept the IIoT allows this industry to evolve and to make its functions more efficient.

Claroty is supposed as high-quality commercial IIoT platform. It enhanced continuous threat detection and secure remote access. This platform is successfully applied in various electrical power systems. One of the main advantages of the Claroty platform is that it provides visibility into all three risk variables in OT environments: asset visibility, network visibility and process visibility. In addition, it ensures a high protection degree at all critical points of the complete system, as well as the necessary analytics for the data that collects and stores from IoT devices, and the processing of those data in real time.

Many energy companies in the electric industries rely on Claroty platform in order to enhance OT availability, integrity and safety. The Claroty platform comprehensive protects electric control systems and continuously monitors industrial networks to prevent dangerous cyber threats.

5 References

[1] *** https://www.coolfiresolutions.com/blog/difference-between-it-ot/ (Retrieved june 2020.).

[2] *** https://www.gartner.com (Retrieved june 2020.).

[3] **H. Boyes, B. Hallaq, J. Cunningham, T. Watson,** The industrial internet of things (IIoT): An analysis framework, Computers in Industry 101 1–12, 2018.

[4] **B. Radenković, M. Despotović-Zrakić, Z. Bogdanović, D. Barać, A. Labus,** Electronic Business, Faculty of Organizational Sciences Belgrade, 2015.

[5] **B. Radenković, M. Despotović-Zrakić, Z. Bogdanović, D. Barać, A. Labus, Ž. Bojović,** Internet of intelligent devices, Faculty of Organizational Sciences Belgrade, 2017.

[6] **M.H. Rehman, I.Yaqoob, K. Salah, M. Imran, P. P. Jayaraman, C. Perera:** The role of big data analytics in industrial Internet of Things, Future Generation Computer Systems, Volume 99, Pages 247-259, 2019.

[7] *** https://randed.com/information-technologies-it-vs-operational-technologies-ot/?lang=en (Retrieved june 2020.).

[8] *** claroty_platform_overview_april2020 (Retrieved june 2020.).

[9] *** https://claroty.com (Retrieved june 2020).