Case Study

SEcube™

Addressing the security challenges posed by Cyber-Physical Smart Water Systems

Background

The issues that the water distribution systems is experiencing such as climate change, rapid urbanisation and ageing infrastructure, urge the integration of on-line systems for continuous monitoring to improve investments, operating efficiencies and environmental sustainability. Digital transformation in the water supply sector is on-going. Smart grids are the new paradigm, which rely on the integration and interaction of the power network infrastructure (physical systems) and the ICT network (cyber system). Cyber-Physical-System (CPS) platforms are the enabler of this integration whereby sensing, computation, control, networking and analytics are orchestrated to interact with the physical world.

Challenge

Cyber-physical systems (CPS) rely on the interconnectivity of devices thus exposing the whole system to a wider attack surface due to its reach and complexity. The process control systems used to control Cyber-Physical Energy Systems were developed for a non-networked world and without a security requirement in mind. Hardware and software components that are highly dependable, reconfigurable, certifiable and trustworthy are therefore required.

Industry

Critical Infrastructure
Water Supply

Challenges

- engineering challenges related to the integration of physical and computational elements (integration and interoperability)
- security and privacy issues of emerging smart CPS to fulfil stringent data protection regulations

Goals

- addressing operation goals along with security goals

Solution

- SEcube™ is a System-on-Chip focused on security in support of Cyber-physical Systems for the management and protection of data to preserve ownership rights as well as beneficial use of data

Solution

While smart grids grant modern water distribution systems reliability, autonomy, and efficiency, through a complex cyber-physical interconnected systems (CPS), they are exposing both the physical and cyber infrastructures to attacks. These attacks usually target the supervisory control and data acquisition (SCADA) system, supervising the whole infrastructure, or the programmable logic controllers (PLCs) that locally operate pumps and valves. Attacks can range from the accessing consumer or operational information to intentional damage to the physical water assets (pumps, valves, tanks) such as a decrease in the water supply or water contamination. CPS operates in mission-critical environments that prioritise safety, availability, security, reliability, resilience and adaptability.

Within a water distribution system, SEcube™ is used to guarantee the integrity, availability and confidentiality of the recorded and retrieved data acting as a controller that reads and protects information, both at rest and in motion, sent or received from sensors, commands actuators and controller throughout the water distribution infrastructure. From the water resource, through the treatment plant to the distribution system, SEcube provides not only high computational power but above all security features to achieve operational integrity against system resources and shared data manipulations, and confidentiality by keeping the status of the physical system and other sensitive information secret from unauthorised access.

Benefits

- System-on-Chip (ARM - SC - FPGA)
- Small Size and reduced PCB footprint (9x9mm)
- Multi-factor authentication
- Data encryption (at rest and in motion)
- Forward error correction
- High reliability
- Low power
- Efficient parallel programming
- Adaptive and reconfigurable for reuse
- Established development environment
- Open-source

> “The Integration of SEdesk in Cyber-Physical interconnected Systems represents an opportunity to address CPS vulnerabilities and prevent attacks across IT, OT and IoT.”
>
> Prof. Paolo Prinetto
> President of CINI

CINI coordinates research and training activities in the field of Information Security on a national and international scale with the ultimate objective to support the National Italian Authorities to thwart cyber threats, making it a more resilient Country. CINI is committed to improving the protection measures of the Public Administration and Enterprises from cyberattacks and is actively involved in the definition of the National standards and methodologies. https://www.consorzio-cini.it

Blu5 Group
info@blu5group.com
www.blu5group.com