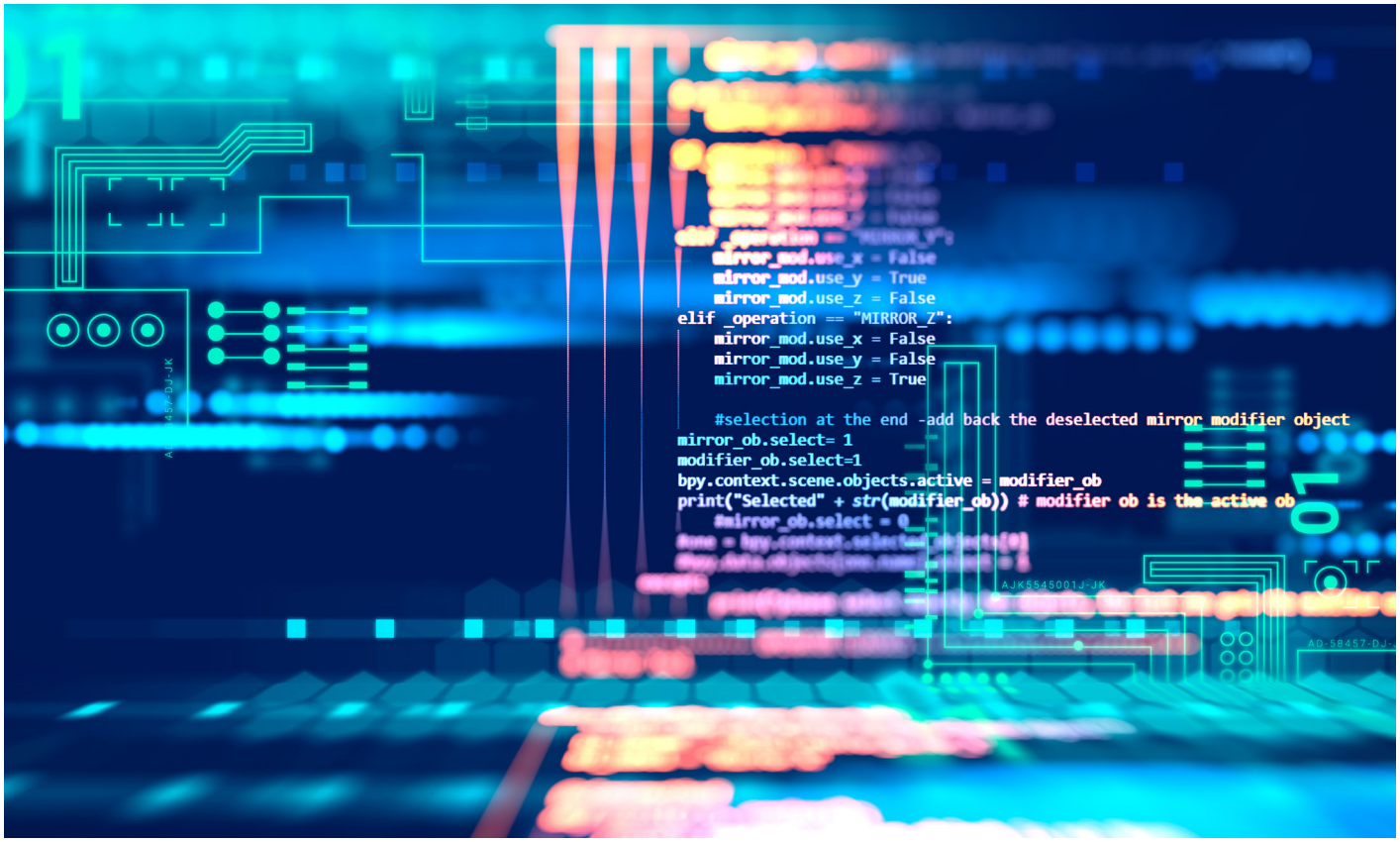
Itron

OpenWay® Riva Security

CONTENTS

WHITE PAPER



The cities of the future may be smart – but will they be cyber safe?

All together, the smart-city market is expected to exceed $1.7 trillion in the next 20 years. But the interconnectivity across the virtual and physical infrastructure that makes a smart city work also creates new and substantial cybersecurity risks. With each additional access point, sensitive data exposure vulnerabilities expand. Smart cities can be susceptible to numerous cyber attack techniques, such as remote execution and signal jamming, as well as traditional means, including malware, data manipulation and DDOS. To counter the risks, comprehensive smart-city plans designed to safeguard what is clearly "critical infrastructure" are needed on behalf of all parties involved, from the individual citizen to large public and private institutions.

- PwC, 'Smart cities: five smart steps to cybersecurity', March 3, 2017

THE CHANGING LANDSCAPE

Utility companies are being transformed, driven by advances in technology, business conditions and the need to manage resources more effectively. They are under increasing pressure to provide new services, develop new revenue streams and provide enhanced levels of customer service and interaction.

In addition, as migration toward urban centers increases, cities are being transformed into 'smart cities.' Smart cities are under pressure to increase economic growth, engage more effectively with their citizens and utilize new technologies to make the urban landscape more livable, sustainable and economically vibrant.

Some examples of the new technologies and services that utilities and smart cities will need to incorporate include:

- Network edge analytics
- Electric vehicle charging
- Distributed energy resource integration
- Energy and water efficiency programs
- Solar
- Prepayment
- Smart streetlights
- Environmental/gas/methane monitoring
- Traffic control

These new technologies and services present new opportunities for utilities and smart cities, but at the same time, they increase security challenges.

SECURING SMART UTILITIES AND SMART CITIES

As new ways to deliver, monitor and manage water, gas and electricity emerge and new capabilities, technologies and services are developed and introduced, new opportunities for security threats also arise. Those threats, combined with the challenges of maintaining grid security, securing the network against cyberattacks and malware, or maintaining compliance with government regulations and mandates can quickly overwhelm cities and utilities. They need a field area networking solution that will provide room for future expansion with new technologies and services, while at the same time providing the security necessary to counter evolving threats.

Itron's OpenWay® Riva solution, built for the Internet of Things (IoT) world, provides the answer.

OpenWay Riva is the solution built for the Internet of Things (IoT) world

For years, energy and utility organizations have been high-profile targets for hackers, cyberterrorists and foreign governments.

Infrastructure organizations are seen as vulnerable targets that can be used to cause mass disruption with a relatively few keystrokes pressed from a home located a few blocks away or from a foreign nation on the other side of the world. Because attacks on the energy and utility sector are often kept confidential—unlike data breaches suffered by retailers and healthcare organizations that are highly publicized to warn customers and patients whose information has been stolen—the public has little knowledge of infrastructure attacks, and even some cybersecurity professionals are unaware of a breach's true extent. New information, however, reveals that cyberattacks on utility and energy organizations are a serious and growing threat.

- Rishi Bhargava, 'The Energy and Utilities Sector Remains Vulnerable to Hackers', Electric Light & Power online, June 27, 2017

COMPREHENSIVE, END-TO-END SECURITY

Itron views security as the most critical and foundational concern in defining requirements of our smart grid-enabling architectures. Leveraging our breadth of experience in AMI deployments and projects across the globe, Itron and our strategic partner Cisco designed OpenWay Riva with an end-to-end integrated security solution using a defense-in-depth approach, where multiple layers of protection are strategically located throughout the multi-service architecture to provide the industry's most comprehensive, unified security available today.

This architecture delivers a true multi-purpose, secure communications platform for utilities and cities and protects the integrity of data, communications, and controls in an open, multi-service, multi-protocol network environment.

An iterative design process ensures that all possible threats have been addressed and mitigating measures are built into the OpenWay Riva solution. The benefit of this approach is the increased security of the system.

The OpenWay Riva solution was designed to support gas, water, electricity and smart cities by providing increased functionality, visibility and management, along with increased security. OpenWay Riva provides layered security controls and management to protect the multi-service IPv6 field area network (FAN) and all the devices and applications that run on it.

SECURITY AT THE NETWORK LAYER

The multi-service IPv6 network provides consistent security controls for all utility applications using the FAN. The FAN architecture provides unprecedented:

Access Control:

Strong authentication of nodes is achieved by taking full advantage of a set of open standards including IEEE 802.1x, Extensible Authentication Protocol (EAP) and Remote Authentication Dial-In User Service (RADIUS). This "white-listing" approach requires that every device joining the IPv6 network be authenticated before being allowed access to the network and smart metering system. Field area routers, along with intermediate meters, pass on a new device's credentials to the centralized Authentication, Authorization and Accounting (AAA) server. Once authenticated, the new device is then allowed to join the network, provided with an IPv6 address and mesh key, and will be authorized to communicate with other nodes.

Data Integrity, Confidentiality, Privacy:

The FAN employs network-layer encryption (IPsec with AES encryption) in the Wide Area Network (WAN) and link-layer encryption (AES on IEEE 802.15.4g or IEEE 1901.2) in the Neighborhood Area Network (NAN). This design choice preserves network visibility into the traffic at the router and enables use of IP-based techniques of multicast, network segmentation, and quality of service (QoS). It also allows smart meters and other endpoints to be low-cost constrained nodes that only do link-layer encryption while the field area router does both network-layer and link-layer encryption. Additional protection at the application-layer is provided by Itron's enhanced security architecture which provides confidentiality, message integrity and proof of origin (digitally signed firmware images or digitally signed commands as part of application protocols such as DLMS/COSEM) between the headend and the meter register itself.

Threat Detection and Mitigation:

The security architecture supports tools such as DDI and IPAM, VLANs, secure tunnels, Virtual Routing & Forwarding (VRFs), or Generic Routing Encapsulation (GRE) to achieve network segmentation of functional elements that should never communicate with each other. Additionally, access lists and firewall features can be configured on FAN and substation routers respectively, to filter and control access in the distribution and substation part of the grid.

Device and Platform Integrity:

Field area routers and meters are built with tamper resistant mechanical designs that generate alerts when physical tampering is detected. Additionally, each router motherboard is equipped with a dedicated security chip that provides secure unique device identifier (802.1AR), immutable identity, and certifiable cryptography, entropy source with true randomization, memory protection and image signing / validation.

Secure Field Tools:

Secure access is required of devices in the field using digitally signed time-based credentials and mutual authentication. In addition, the rule of least privilege can be applied to field access, preventing any contractor/field tech from being able to see device passwords or performing higher-privileged commands on devices.

SECURITY AT THE APPLICATION LAYER

At the application level, the OpenWay Riva solution provides an enhanced security architecture that emphasizes integrity of control, availability and confidentiality for the AMI application.

Commands and payloads are encrypted and digitally signed by OpenWay, supported by the Itron Security Manager (ISM), before they are transferred over the network. In this manner, the messages between the applications and endpoints are protected, regardless of the underlying network infrastructure. OpenWay Riva also provides auditing of both the security activities and the events being returned by the meter or device, managing the encryption keys and the larger set of security components deployed with the system. The OpenWay Riva solution protects information and commands from the headend system to the endpoint; therefore, the meter or device only operates on authenticated control commands.

OpenWay Riva application-layer security uses the following security appliances and applications:

Itron Security Manager (ISM):

Manages encryption, authentication, decryption and validation of data and commands to and from enabled endpoints. ISM also manages the key exchanges and security state for endpoints and repeaters in a cellular network.

Hardware Security Module (HSM):

Generates and secures asymmetric signing (command and revocation) keys (ECC, 256-bit). The HSM is connected over secure API to the ISM and is considered an integrated part of the ISM. No other devices or systems connect to the HSM.

SECURITY VALIDATION & VULNERABILITY TESTING

Security validation and vulnerability testing is conducted on the end-to-end system as part of Itron's overall ISO-compliant software development lifecycle process. This type of testing comprises security validation and vulnerability assessments, as well as penetration testing. Our assessment process not only accounts for the technical aspects of the solution, but strives to introduce technical controls that mitigate human vulnerabilities as well.

A dedicated team of internal security experts, as well as external, third-party organizations perform the testing. This testing is external to the product development and quality assurance organizations to help ensure the rigor of test cases and the independence of their findings.

Itron's solution security has also been tested independently by third parties at San Diego Gas & Electric, Southern California Edison, DTE Energy, National Grid, and BC Hydro. These assessments included penetration testing of the headend, field area routers, and meters as well as bench tests of physical attacks, port scanning, and system wide penetration attempts.

A COMPLETE SOLUTION

OpenWay Riva, the next generation IoT solution for utilities and smart cities, is a significant leap forward in technology. Built upon Itron's existing OpenWay IPv6 network, Itron has added a powerful distributed computing platform that uses distributed intelligence and adaptive communications technology to help solve business challenges and accelerate innovation. OpenWay Riva is the only solution that delivers both security and flexibility, allowing utilities and smart cities to expand the services offered to consumers while providing the security required to protect both data and the network.

Itron and our technology partners are working with global utilities and municipalities to develop and validate use cases that leverage these new capabilities to make real-time operational decisions at the edge of the network. This enables what we call the "active grid" or "active network," which is an active network that drives measurable valuable business outcomes.

Smart Cities Are Going to Be a Security Nightmare

The inevitability of cyberattacks is a lesson the private sector has learned the hard way. As cities adopt smart initiatives, they'd be wise to make data security a priority from the outset.

- Todd Thibodeaux, 'Smart Cities Are Going to Be a Security Nightmare', Harvard Business Review, April 28, 2017

What Threats Do Smart Cities Face?

Since cities account for the consumption of around 70% of the energy produced globally and the generation of 70% of the world's gross domestic product (GDP), any kind of intrusion, sabotage, and intelligence collection with malicious intent will have a great impact on smart cities.

- TrendMicro, 'Securing Smart Cities', May 30, 2017

SECURITY TODAY… AND TOMORROW

OpenWay Riva enables a wide variety of devices and assets to communicate and collaborate directly with each other. This means massive amounts of sensitive data will now traverse the network as these assets transmit, receive and share data, collaborate, analyze, decide and act in real time.

To put this in perspective, in 2016, the annual amount of global IP traffic (i.e., data across the Internet) was 1.2 ZB (zettabyte, or 10^{21} bytes) or 96 EB (exabyte, or 10^{18} bytes) per year. This is expected to grow to 3.3 ZB per year by 2021, or 278 EB per month. From 2016 to 2021 the Compound Annual Growth Rate (CAGR) for IP traffic will grow 24 percent.[1]

Obviously, security in this environment becomes even more critical.

The active grid requires state-of-the-art security capable of countering current and future threats, while being able to evolve and scale to support new use cases as they are developed. OpenWay Riva technology provides utilities and smart cities with that security.

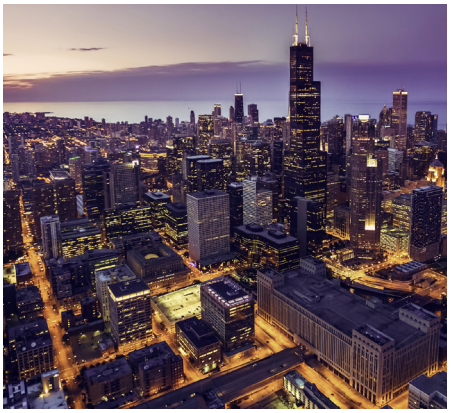
A few of the security-related outcomes the OpenWay Riva solution delivers include:

FOR SMART CITIES

Connected Infrastructure

Foundational to becoming a smart city are smart utility services, where energy and water use is being monitored and proactively managed for safety, waste reduction, conservation and sustainability goals. Through distributed applications and cloud services, Itron can help smart cities solve problems such as resource waste reduction, electrical distribution, streetlight management, water conservation and management of renewable power.

Itron helps smart cities accomplish these goals through an ecosystem of partners that utilize the interoperable OpenWay Riva environment to develop apps to run on the platform, or to embed Itron Riva technology into their devices. Commercially available chip set manufacturers are also putting the Itron Riva technology on their standard products, so hundreds of device manufacturers will have immediate access to join the network. Device and sensor manufacturers can also easily work together to bring new applications faster to market. Itron Riva technology ecosystem partners undergo a certification process



that includes the same security rigor and controls as Itron devices and applications, ensuring consistent security measures throughout the entire network. This partner ecosystem means utilities and smart cities are not reliant on one vendor for product innovations, providing them with access to new applications much faster than in the past.

However, to take advantage of these programs and realize the benefits, cities must be connected. Being connected allows smart cities to leverage data and technology in real time to drive real operational efficiencies and outcomes that matter to citizens and businesses.

Itron is a world leader in connecting infrastructure and managing data with over 150 million connected devices in cities throughout the world. Itron's next-generation solution for smart cities, OpenWay Riva, is built upon its proven OpenWay IPv6 network. The OpenWay Riva solution connects IoT devices through a powerful, fully standards-compliant distributed computing platform enabling endless possibilities for emerging city applications.

FOR ELECTRICITY

Diversion Detection:

With the OpenWay Riva platform, diversion detection can now be based on real-time, continuous, and localized analysis of changes in electricity current flows and voltage levels in the distribution network to distinguish legitimate metered loads versus those from theft. Through the meter's ability to communicate directly with other meters at different levels of the network, and knowing exactly where they are located on the distribution system, the system identifies when current is drawn on the secondary of a transformer that did not go through a meter, greatly increasing the accuracy and timeliness of diversion detection.

The Importance of Grid-wide Security Is Difficult to Overstate

To thwart attacks, utilities must deploy comprehensive security that spans field devices, the communications network and the cloud. In other words, utilities need an end-to-end approach that integrates both IT and operations technology (OT).

- Hugo Moreno, 'Staying On The Grid: Utilities Grapple With Security And The Internet Of Things', Forbes Insights, Nov. 15, 2016

Detection of Unsafe Grid Conditions:

High-impedance connections (HIC) or "hot spots" on the low-voltage distribution system represent a serious and ongoing safety risk, as well as causing customer voltage problems and utility energy losses. By continuously calculating and monitoring impedance throughout the lower voltage system, distributed intelligence changes the game for HIC detection. OpenWay Riva provides a practical and cost-effective solution for utilities to identify these losses, voltage anomalies and potential safety issues before they become a safety hazard or a costly liability.

FOR GAS

Safety:

The OpenWay Riva solution combines peer-to-peer communications and analysis of data throughout the gas distribution network to aid in pipeline safety. Utilities can pair methane sensors, seismic sensors, flood sensors and more with remote disconnect valves – enabling the utility to potentially alleviate dangerous situations and improve the safety of communities, employees and first responders.

System Integrity:

With OpenWay Riva, new applications are emerging to monitor pressure, temperature, pipeline stress via strain gauges and cathodic protection to aid in pipeline integrity management, to perform pressure studies, and to hit check-in dates for cathodic protection reports.

Methane Sensing:

OpenWay Riva's methane sensing application helps keep utility personnel and customers safe by monitoring for unsafe or changing levels of methane. Further, remote disconnect valves can be paired with the methane sensor to shut off gas service when elevated levels of methane are detected. By deploying methane sensors in highly-populated areas of a utility service territory, such as hospitals, schools, amusement parks, shopping centers and sports venues, methane gas leaks can be identified more quickly and gas service automatically shut-off immediately, alleviating potentially dangerous situations before they arise.

FOR WATER

Water Leak Detection:

The OpenWay Riva platform's leak detection solution includes an acoustic leak sensor and analysis and presentment software designed to be permanently installed, enabling the utility to continuously monitor its entire distribution network. The leak sensor is powered by the OpenWay Riva water module and supplies acoustic samples to the module for storage and transmission through the network to leak detection software. The leak detection software enables the utility to identify and prioritize potential distribution leaks for maintenance, reducing water loss and enabling the utility to address leaks prior to them becoming costly main breaks.

Remote Disconnect:

Itron has certified two third-party remote disconnect valves to operate within the OpenWay Riva solution. This advanced functionality enables utilities to remotely disconnect or limit water flow to an end customer. It reduces the need to roll a truck to perform this function, saving the utility a significant amount of money while enhancing the safety of field crews.

Advanced Sensing:

The OpenWay Riva platform enables the deployment of additional sensors on the water distribution system to monitor pressure and water quality. These sensors enable utilities to continuously monitor the distribution system pressure and water quality, while also correlating with other data, to enhance analysis and reporting.

EQUIPPED FOR THE FUTURE

Itron's OpenWay Riva is the only solution for utilities and smart cities that delivers scalable security while enabling support for new services, capabilities and business outcomes. The OpenWay Riva solution also provides true interoperability for an open ecosystem of grid devices and network sensors – delivering the active grid that utilities and smart cities demand.

Deploying a unified solution on one multi-purpose network provides well-defined points of interoperability between systems and greatly simplifies and reduces integration costs and difficulties. The OpenWay Riva solution allows utilities and smart cities to focus on creating business value through outcomes that improve services and enhance the lives of customers and citizens, without having to worry about security risks.

THE SOLUTION IS CLEAR

Utilities and smart cities need to deploy a solution that will not only provide robust security today, but will also provide the ability to secure and support new technologies and capabilities in the future.

Itron's OpenWay Riva is that solution.

To find out how OpenWay Riva solutions can help your utility or smart city, visit the OpenWay Riva website or contact your sales person.

[1] Cisco Systems, 'The Zettabyte Era: Trends and Analysis', updated June 7, 2017

Itron

Join us in creating a more **resourceful world**.
To learn more visit **itron.com**

CORPORATE HQ
2111 North Molter Road
Liberty Lake, WA 99019 USA
Phone: 1.800.635.5461
Fax: 1.509.891.3355