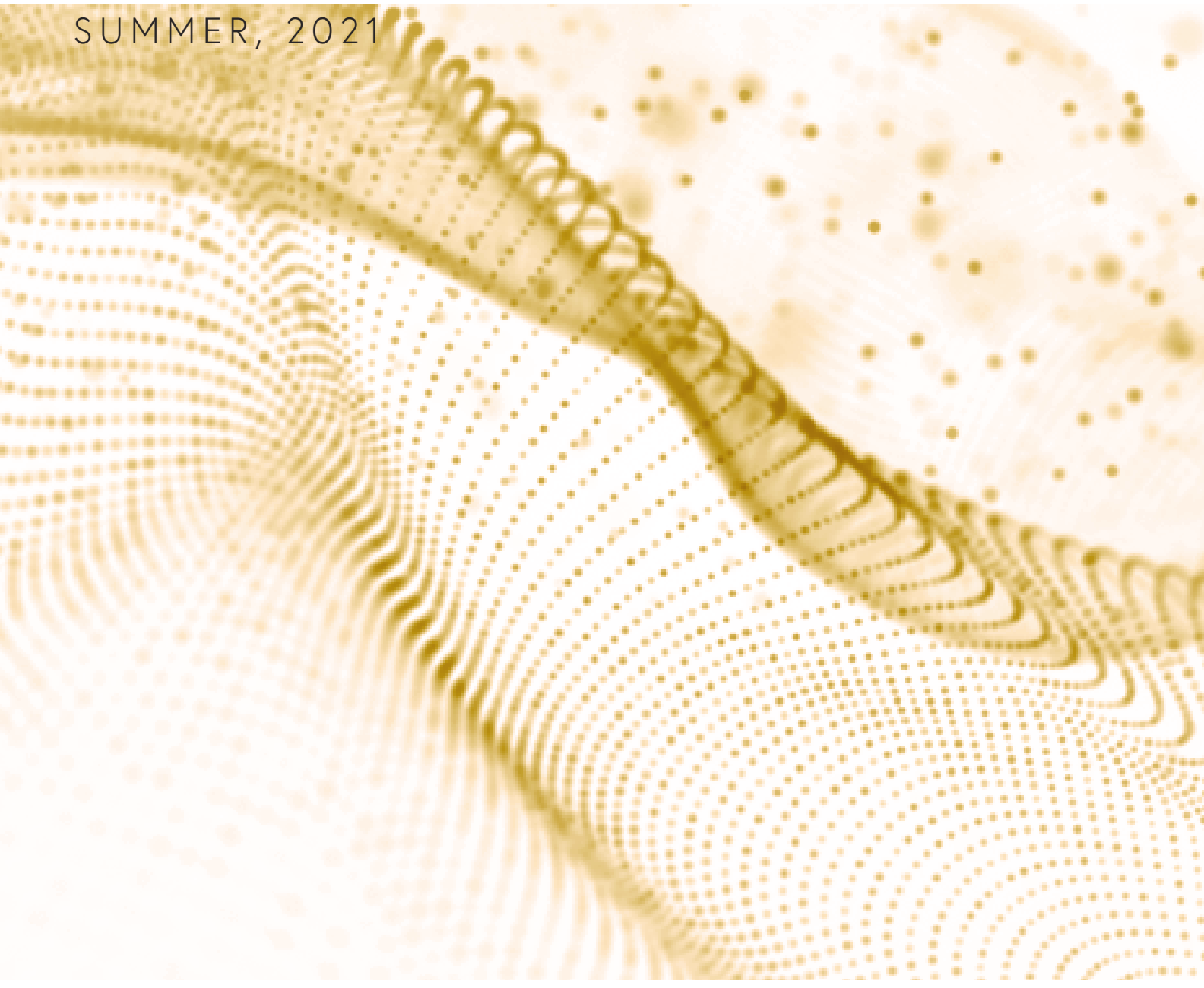
RUBIDEX SCADA INFRASTRUCTURE SOLUTIONS SERIES

SUMMER, 2021



AS CRIPPLING DATA BREACHES BECOME AN ALMOST DAILY OCCURRENCE, IT IS CRITICAL FOR INFRASTRUCTURE OPERATORS TO SECURE THEIR ASSETS AND BUSINESS PROCESSES

CYBER SECURITY FOR CRITICAL INFRASTRUCTURE

Cybersecurity threats exploit the increased complexity and connectivity of critical infrastructure systems, placing the nation's security, economy, public safety, and health at risk. Like financial and reputation risks, cybersecurity risk affects a company's bottom line. It can drive up costs and influence revenue, potentially harming an organization's ability to innovate, gain, and maintain customers. Cybersecurity is an important and amplifying component of an organization's overall risk management.

With utilities in the U.S. and around the world increasingly moving toward smart grid technology and other upgrades, correlative threats from malicious cyber-attacks on North American public infrastructure such as the electric grid continue to grow in frequency and sophistication. The potential for malicious actors to access and adversely affect US physical industrial assets in electricity generation, transmission and distribution systems, water supply and processing systems along with other public services is a primary concern.

With its innovative technologies and products, Rubidex is fundamentally changing the way data is collected, transmitted, processed, and stored by literally rewriting the concept of industrial sensing and control. The company's patented technology portfolio is designed to seamlessly integrate into existing industrial control networks, securing data collection and control from cyber espionage, regardless of attack vector. In phased implementations, Rubidex hardware and technology secures each layer as it is deployed, avoiding the costs of full scale replacement of sensors and controllers while dramatically improving security.

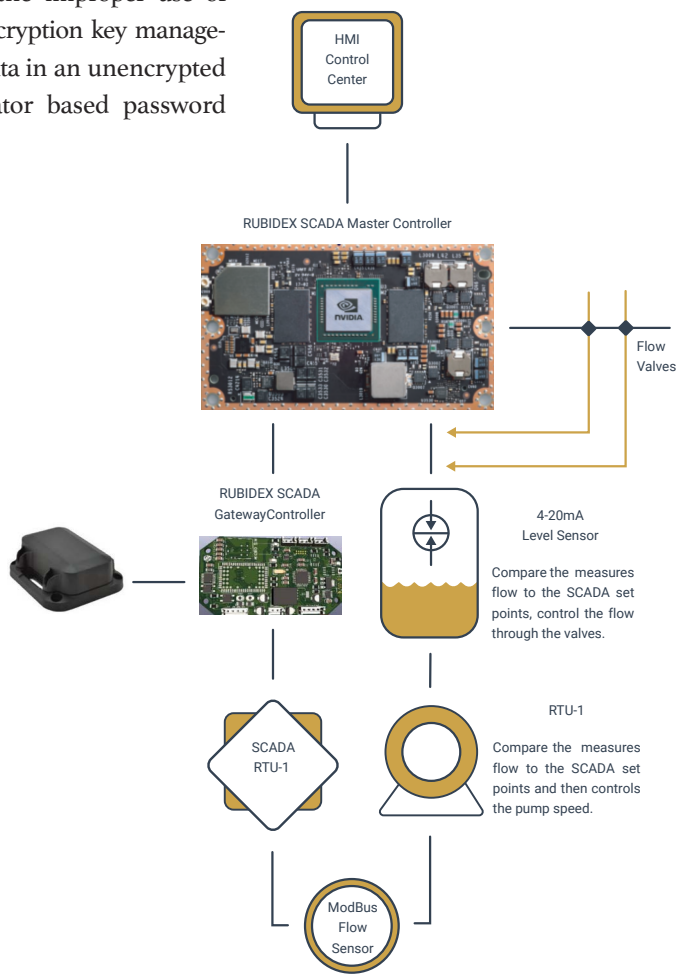
Supervisory control and data acquisition SCADA) is a control system architectu

CYBER RISK ASSESSMENT

Supervisory control and data acquisition (SCADA) is a control system architecture comprising computers, networked data communications and graphical user interfaces (GUI) for high-level process supervisory management. These systems also comprise of other peripheral devices like programmable logic controllers (PLC) and discrete proportional-integral-derivative (PID) controllers to interface with process plant or machinery. SCADA systems assist in the efficiency and safety of daily operations, maintenance, and play a keyrole in many sector facilities by monitoring and/or controlling physical processes.

In industrial utilities today, data acquisition and control equipment varies widely based on age and generation. These systems also vary greatly with respect to complexity and sophistication depending on the specific application. Some systems are closed systems, use isolated networks, and proprietary communication protocols, while others use open architectures, common communication paths, and may rely on the Internet forcommunications. As proven by numerous recent high profile hacking incidences, cyber risk represents a significant attack vector for infrastructure operators. Key cyber risks include attacks that target inadequate security controls, outdated patches, and other vulnerabilities; social engineering attempts designed to gain operator credentials, and intrusions from insider threats. All such attempts could allow attackers to access critical control systems and disrupt or control physical components and processes.

Historically, cyber threats were often mitigated by separating control system Operational Technologies (OT) from other networks and the Internet (known as air-gapping). As proven by some high profile cases such as StuxNet (2010), air-gapping is not a sufficient security practice to deter malicious actors. As industrial control systems begin to be attached to the Internet for cloud-based data analytics the threat of unauthorized access increases exponentially. Common threads in many of these threats are linked directly to the improper use of encryption, poor encryption key management, and storing data in an unencrypted form behind operator based password schemas.



RUBIDEX SCADA/PLC SECURE INFRASTRUCTURE

At the heart of the Rubidex SCADA/PLC Secure infrastructure are two important technologies that are used in tandem to resolve security challenges in industrial control systems. The first is the use of 256 bit encryption technology beginning at the sensor level to ensure that at no time, the data resides in an unencrypted state; the second, is a block-chain based consensus algorithm to used for identity attestation and data integrity validation that is executed at every stage of the data collection and control processes.

DEVICE LAYER:

Many SCADA deployments in use today deploy no encryption within the communication protocols and use only operator based password controls to set parameters and read data registers. Analog voltage & current based inputs such as 4-20mA and 0-5VDC cannot be digitally encrypted but all other types of data communicating on a bus using communications protocols can. The attack vector for these analog devices rely on physical access as these layers are analog in nature, thus not vulnerable to remote attack. It is also not cost effective in most cases to replace analog sensing devices to address vulnerabilities at this level thus Rubidex solutions begin with focusing on the digital communication layer between device and controllers.

In order to secure the sensing and control device layer, Rubidex has created new low level firmware drivers for many SCADA devices that provide data encryption on communications buses using common protocols such as ModBus, BACNet, PROFINET and others. Encrypting data in the sensing/collection process combined with on-site block-chain based identity attestation guarantees that data cannot be modified or altered while in transit from sensor transducers to controllers and connected gateways.

CONTROL LAYER:

SCADA controllers collect and transmit information on their analog and digital ports, along with communications buses. These controllers use preprogrammed internal logic to control external devices based input data. These controllers are typically expensive, are difficult to program, and require significant training to set up and operate, so much so, that many industrial companies rely on third party vendors for setup and monitoring. Controller logic programming as well as and viewing current activity is commonly implemented on PC computer platforms installed locally and/or via dial in or continuous network/Internet connectivity. The local computing platforms notoriously add significant vulnerability due to their use of common operating systems such as Microsoft Windows. As many IT professionals concur, continuous security upgrades and software patches are necessary to reduce unauthorized access; in industrial control applications it is common to find legacy systems that have never been upgraded since they were installed.

In addition to unpatched computing platforms attached to industrial control systems, data collected, transmitted and stored within these networks and SCADA controllers is rarely encrypted. Inter-device control commands, databases and data queries with other controllers are therefore critical attack vectors. Similarly, device identity also represents a potential attack vector as attestation would to prevent a foreign device added to the network from accessing the network. Device identity attestation is poorly implemented in most industrial control implementations.

To resolve critical attack vectors in industrial network control systems, Rubidex has developed new SCADA controllers that implement 256bit encryption and block-chain based identity consensus. Whether running on air-gapped internal networks or connected to the Internet, these devices act together to provide a consensus network ensuring that at all times, all devices and data packet transiting the network remain encrypted at all times and can be identity attested. RUBIDEX encrypts all data packets, both command/control and sensing data registers using 256 bit encryption. Any local storage remains in an encrypted form and utilizes block-chain based data structures to validate authenticity.

PRESENTATION LAYER:

Automated data collection, command and control are primary functions of a SCADA installation. Many of these processes are also complemented by PC computer screens for operator viewing and controls. At best, most of these systems in use today are protected by basic user passwords that are rarely changed, and are often communicated to others operating these systems within the plant. These PC's add significant vulnerability as they typically run common operating systems such as Microsoft Windows and in many cases are not regularly security patched. Additionally, data stored within databases on these PC's is rarely encrypted and can be accessed with anyone that has a valid username and password to log in.

RUBIDEX has developed new presentation processes that implements block-chain based consensus and full 256 bit encryption techniques that ensure that all stored data remains in its fully encrypted form at all times. Data decryption and visualization occurs only in computer memory thus never at risk from unauthorized view or modification whether in motion nor at rest.

RUBIDEX SCADA/PLC SECURE DEVICES

Rubidex hardware devices were designed for ease of placement within existing SCADA implementations as well as new industrial control system deployments. To address cloud-based connectivity and data collection in existing SCADA networks, the Rubidex Controller Gateway was engineered. This gateway provides secure remote read and write capabilities with existing SCADA controllers via Modbus protocol. Other communications bus protocols such as BACNet and ProfiNet are in active development. Rubidex is also developing a series of flexible hardware based SCADA Master Controllers that add port expandability, edge processing and machine learning capabilities. These Controller Gateways and Master Controllers can be deployed individually or in multiples, and can co-exist with legacy SCADA controllers as desired.

IT DATA PROTECTION PLANS

COMPATIBILITY MATRIX	RUBI WARE	RUBI CORE	RUBI PRO	RUBI PLATINUM
Mac Compatible	✓	✓	✓	✓
Linux Compatible	✓	✓	✓	✓
Windows Compatible	✓	✓	✓	✓
IOS Compatible	✓	✓	✓	✓
Android Compatible	✓	✓	✓	✓
Web Enabled	✓	✓		✓
FEATURE MATRIX				
256bit Encrypted Data at all times ensuring no unauthorized access to your data	✓	✓	✓	✓
Distributed Blockchain-Fully recover data in minutes against ransomware	✓	✓	✓	✓
Application Development using common IDEs (MS Vis. Studio, Delphi, Lararus, C++ and others to ensure end to end data protection.		✓	✓	✓
Turnkey Customized Solutions by the Rubidex expert team			✓	✓
Drag & Drop Customization, Core, text Editor, Visual Editor, GUI Dev Editor, Web Editor and Compiler (* Avail 2022)				✓

IT DATA PROTECTION PLANS

The RUBIDEX™ System is a true database replacement technology that utilizes blockchain functionality. The RUBIDEX™ System is efficient and flexible. It can be used for almost any use-case with minimal adjustments. It is, at its core, an API command set so any possible use case can be created. Anywhere a database is used, the RUBIDEX™ System can replace it with 100% security, scalability, expandability and efficiency.

Servers are centralized, meaning one server controls all the data. In a centralized system, if the administrator forgets to apply patches and updates, the system can be vulnerable to security exploits by hackers. This makes databases prone to breaches. The concept of database has not changed since it was first written. The SQL programming language was first developed in the 1970s by IBM researchers Raymond Boyce and Donald Chamberlin. Apache is the most commonly used web server on the internet. Apache attacks are common and include "directory traversal attacks", Denial of ServiceAttacks, Domain Name System Hijacking, Sniffing, Phishing, Pharming, and Defacement.

Most databases are of the SQL variety (Oracle, MySQL, SQL, Postgresse, CouchDB, MariaDB, Microsoft SQL Server, etc). Others, like FoxPro, Access, FileMaker, etc are not immune. Since "web databases use the structured query language, or SQL, the attack is known as a SQL injection," the cause of database infiltration. Blockchains are equally problematic. Browsers, the main front-end for blockchain, are known to have many security issues of their own. A blockchain is actually a database because it is a digital ledger that stores information in data structures called blocks. A database likewise stores information in data structures called tables. IBM Hyper-ledger Fabric stores its data to a database. As outlined in their manual: "The data is stored in a private, separate database on the peer".

The RUBIDEX™ System was written to be a blockchain for business use. It can handle any size data, any file type and is infinitely scalable. Like a blockchain, all nodes maintain a copy of all blocks and is a true ledger, building trust and accountability. Unlike other blockchains, RUBIDEX™ does not require synchronization to function and can even work offline if need be. The RUBIDEX™ software was built to be secure. It is encrypted itself and will not work outside a small perimeter around the location it was meant for, eliminating software piracy. It renders malware and ransomware useless and spoofing will not work. We utilize SSH end-to-end encrypted tunnels for all communications between nodes and servers for the most secure possible transmission.

RUBIDEX SECURE INFRASTRUCTURE PLATFORMS

COMPATIBILITY MATRIX	IOT Devices (1)	SCADA Device (2)	SCADA Edge (3)	SCADA Cloud (4)
Custom Industrial Sensing Hardware Development	✓	✓	✓	✓
256bit Encryption on Device	✓	✓	✓	✓
256bit Encrypted Communications	✓	✓	✓	✓
Cellular, LPWAN, Satellite, Drone Communications	✓	✓	✓	✓
AI/Machine Learning Data Analytics			✓	✓
Locally Distributed Database Architecture			✓	✓
Cloud Geo-Distributed Database Architecture				✓

RUBIDEX IoT solutions capture industrial and commercial data, encrypt the data and distribute the data in a distributed blockchain format. These solutions can work alongside or replace industrial SCADA command and control hardware bypassing the use of traditional databases, allowing for secure ML/AI and predictive data analytics both locally and in the Cloud. Telemetry solutions can be custom designed to be used in challenging telecom environments, drones, satellites and radio telematics. Rubidex SCADA appliances and controllers embed the encrypted Rubidex database replacement functionality delivering systemwide protection of industrial grids building HVAC systems and other command and control environments. The solution allows for system protection and enhanced protection while not requiring complete replacement of existing SCADA hardware. Traditional SCADA protocols such as ModBus, BACNet and others supported over wired and wireless networks.