smaRTE BY FLEX
SOLUTIONS DIGITAL

SMARTE SPLICE

SMART BUILDINGS & CITIES

"REAL-TIME OPERATIONAL EXCELLENCE"

FLEX SMARTE SOLUTIONS

FLAWLESS EXECUTION THROUGH DIGITAL MASTERY

We will help you to maximise your organisation's Return on operational Assets (RooA). This means that we enable you to operate your assets as effectively and efficiently as possible, while also ensuring they are healthy and safe. In this way, you reduce your operational costs and risks, becoming far more profitable as a result.

We can achieve this through one or more of our six "smaRTE solutions" that have been built using a combination of our leading-edge, digital technologies and are focused around our "Real-Time Operational Excellence (RTE)" mantra.

OT CYBER SECURITY

BACKGROUND

Smart Buildings and Cities are tempting targets for Cyberattacks

The Internet of Things (IoT) is at the core of smart buildings and cities. More and more IoT devices are deployed in buildings, public works, and critical infrastructure to monitor, control, and provide better, and more efficient services. The IoT technology that is used to power smart buildings and cities however makes it a tempting target for cyberattacks. Building managers and city authorities must be aware of the risks they and their tenants or citizens could face if threat actors get unauthorised access to systems, infrastructure, or services.

Most organisations have Information Technology (IT) cybersecurity policies and systems in place believing that they are protected. Very few consider the vulnerabilities that are present in their Operational Technology (OT) environment. Savvy building managers and city authorities, however, understand that IT Cybersecurity and OT Cybersecurity are vastly different fields. The traditional "Air Gap" is difficult to maintain in an ever-increasing connected world, where OT-IT networks are converging. IT Cybersecurity solutions are also not designed to secure OT networks and assets.

An effective OT Cybersecurity strategy is critical to protect both smart buildings and cities against cyberattacks. Smart buildings and smart cities both use interconnected technology to monitor and control their environments. If a smart building or a smart city, or any of its operational assets were to be exposed to a cyber attack, the entire building or city could come to a halt, resulting in huge financial losses, health risks, serious injury, or even death.

It is therefore critical that an OT-focused cybersecurity intervention be employed that does not merely detect, but also prevents all connected OT equipment from becoming vulnerable to cyber-attacks. It must ensure the cyber-physical resilience of smart buildings and cities and minimise the risk of downtime.

OT CYBER SECURITY

THE TYPICAL OPERATIONAL VULNERABILITIES:

The following are common operational vulnerabilities inherent in most smart building and smart city environments:

- Digital transformation, growth of the Internet of Things (IoT), and interconnected technologies used in smart buildings and smart cities.
- The large quantity of IoT sensors and devices in buildings and in the field makes security harder
- Insecure configurations aimed to ensure interoperability between different vendor equipment
- Most IoT firmware does not have as many security protections in place as sophisticated systems running on computers and servers.

THE RESULTANT IMPLICATIONS:

An adversary with a foothold on the network can leverage any of these inherent weaknesses to:

- Take over or shutdown normal operations
- Disrupt normal operations or lock employees out (this can be achieved without a deep understanding of the smart building and smart city environment)
- Holding a smart building owner or city authority hostage and demanding exorbitant ransom amounts
- Steal confidential data or intellectual property and quickly sell it
- Cause damage, destruction, or unsafe working conditions by manipulating the state of the managed process and blinding operators to the real state of the process
- Cause health risks, serious injury, and even death to employees or citizens

OT CYBER SECURITY

THE SMARTE SOLUTION - SPLICE:

smaRTE Splice actively prevents cyber-physical attacks through proactive vulnerability shielding inside an encrypted overlay network. It, therefore, embraces connection and convergence. It is the logical alternative to air gaps, firewalls, data diodes, and old-school thinking. The Splice solution comprises three layers with three operating modes as can be seen below:

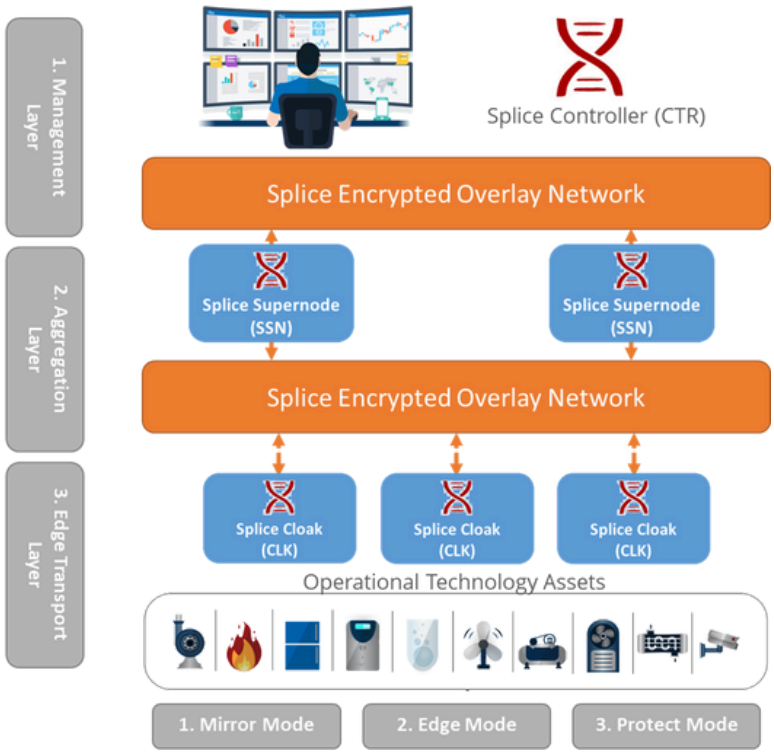
Simplicity & Flexibility!

3 Layers:

1. Management (Controller)
2. Aggregation (Supernode)
3. Edge Transport (Cloak)

3 Operating Modes:

1. Mirror - Observation
2. Edge – Manage access route to OT Equipment
3. Protect – All OT Equipment traffic via Splice



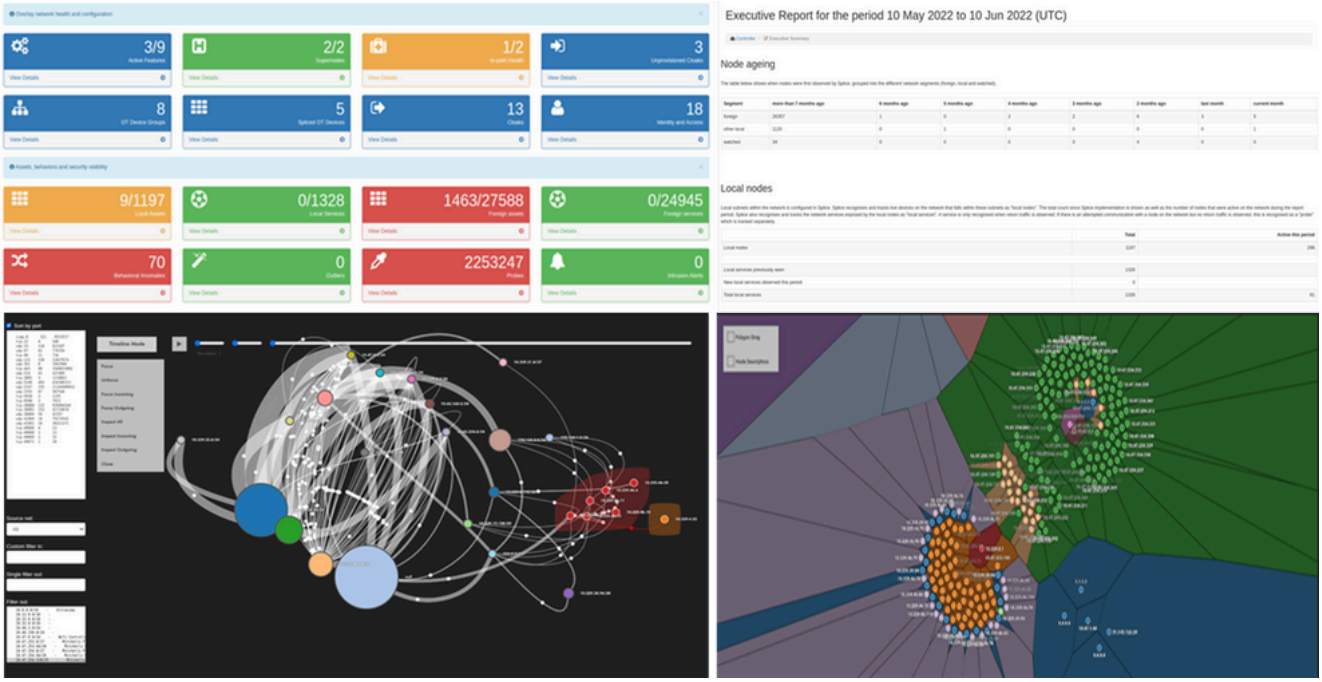
OT CYBER SECURITY

THE SMARTE SOLUTION - SPLICE:

smaRTE Splice actively prevents cyber-physical attacks by providing:

- Logical isolation within the control network core (rather than at the perimeter)
- Profiling of the entire control network traffic & full forensic audit trails (with visualisation of the “network universe”)
- Vulnerability shielding inside an encrypted overlay network
- Intrusion inspection
- Behavioural profiling & advanced machine learning-driven outlier & anomaly detection
- Passive node discovery & tracking
- Secure identity management
- Multi-factor authentication offloading
- Secure remote access for operators, engineers & support partners

Dashboard Examples:



OT CYBER SECURITY

THE BUSINESS BENEFITS:

- Actively reduces cyber exposure of all connected operational assets
- No rip-and-replace of existing network assets
- Continue operating with vulnerable equipment out in the field
- Enables passive asset management
- Increases asset uptime and production reliability

ROI < 1 YEAR!

INCREASE ROOA BY 10% OR MORE

CONTACT US TO FIND OUT MORE!

Website: www.flexdigitalsolutions.com

Email: info@flexdigitalsolutions.com

Phone: +27 (0)10 023 9044