



smARTE **BY** **FLEX**
SOLUTIONS DIGITAL

SMARTE SPLICE

AUTOMOTIVE

"REAL-TIME OPERATIONAL EXCELLENCE"

FLEX SMARTER 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.



$$\frac{\text{Operating Income}}{\text{Average Operating Assets}} = \text{RETURN ON OPERATING ASSETS} \uparrow$$



OT CYBER SECURITY

BACKGROUND

Automakers and the automotive industry seem to be getting special attention from ransomware threat actors. One possible reason may be that attackers have identified the automotive segment as more vulnerable than others and they are exploiting it.

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 industrial and automotive stakeholders 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.

OT Cybersecurity is critical in asset-intensive industries such as the automotive manufacturing industry. Most of the manufacturing equipment, and related operational assets, are highly intelligent and connected. If this equipment were to be exposed to a cyber attack, the entire production line could come to a halt, resulting in huge financial losses, as well as company credibility to honour client delivery schedules and commitments.

It is therefore critical that an OT-focused cybersecurity intervention like smaRTE Splice be employed that does not merely detect, but also prevents all connected OT equipment from becoming vulnerable to cyber-attacks. smaRTE Splice will ensure the cyber-physical resilience of your automotive environment. It will also minimize the risk of production downtime and therefore, assist to maximize the return on all your automotive operational assets.





OT CYBER SECURITY

THE TYPICAL OPERATIONAL VULNERABILITIES:

The following are common operational vulnerabilities inherent in most automotive manufacturing environments:

- Unpatched (vulnerable) code running on Data Historians, Engineering and Operator Stations, HMI panels, and PLCs (for HMIs and PLCs there are likely no patches available)
- Insecure configurations aimed to ensure interoperability between different vendor equipment
- Fragmented and unprotected identities, sometimes unchangeable vendor defaults
- Unauthenticated and unencrypted Industrial Control Protocols

THE RESULTANT IMPLICATIONS:

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

- Take over normal operations
- Disrupt normal operations (this can be achieved without a deep understanding of the industrial process, with reusable attack tools, such as Pipedream)
- Hold the production line to ransom (Operating logic can be changed and Engineers can be locked out of the PLCs)
- Steal intellectual property, such as by exfiltrating confidential design and process documentation
- 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





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:

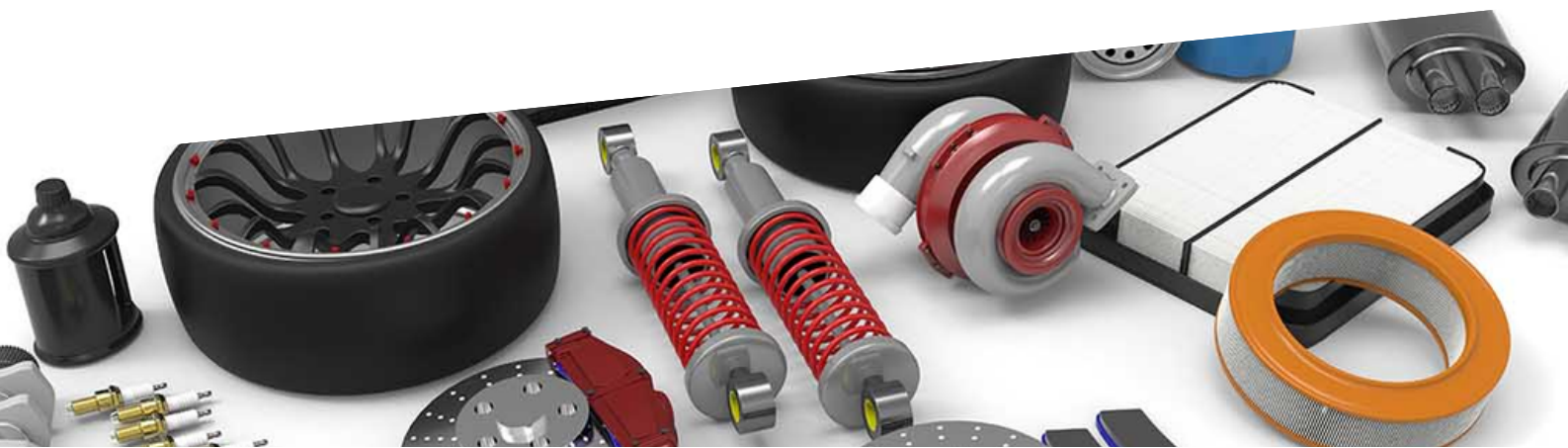
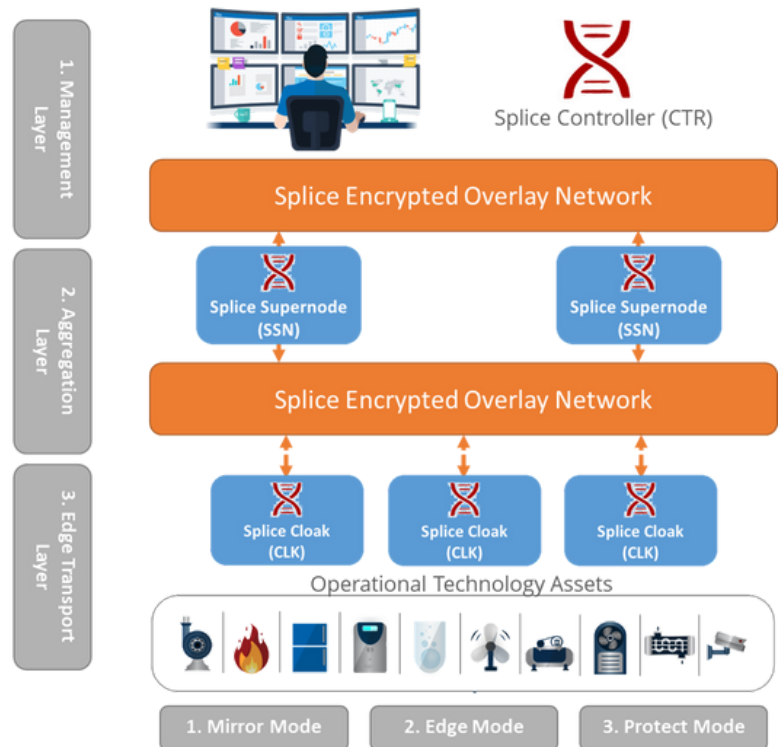
Simplicity & Flexibility!

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





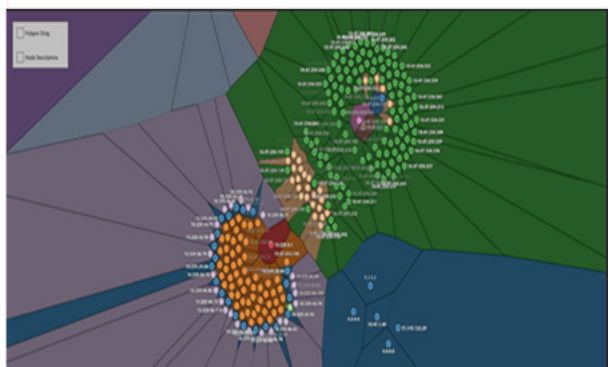
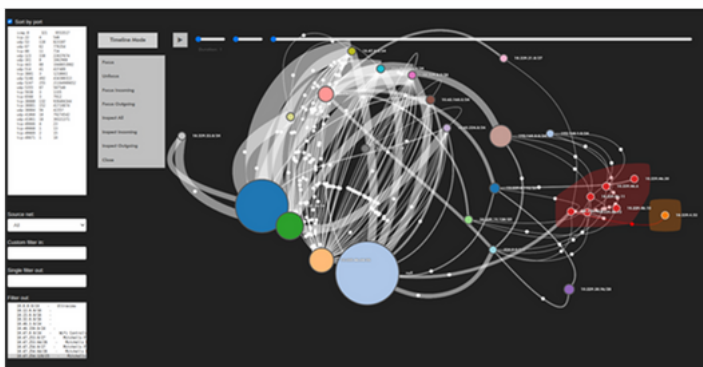
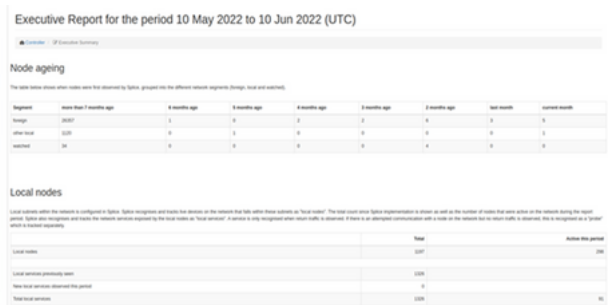
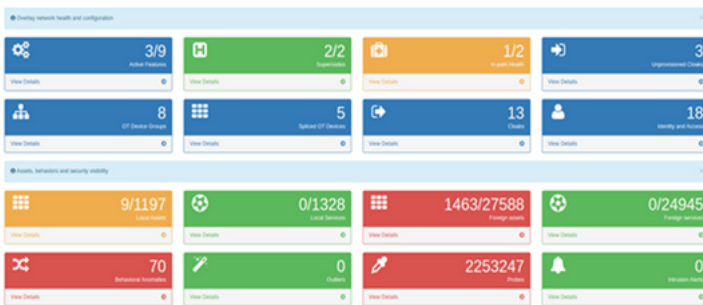
OT CYBER SECURITY

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

