smaRTE BY FLEX
SOLUTIONS DIGITAL

SMARTE SPLICE

# AVIATION

"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

**Aviation is facing a rising wave of cyber attacks**

Data shows that cyber attacks have increased by 530% year-on-year rise from 2019 to 2020 in reported incidents across the aviation industry. Airlines were targeted in 61% of all 2020 aviation cyber attacks - almost twice as much as the two next biggest affected market segments combined (16% for manufacturers and 15% for airports). The report goes on to highlight that the aviation industry faces a ransomware attack every week. Financial losses were reported in 55% of these attacks. This means that the entire aviation industry, which includes Air Traffic Management, Airport Management and Airlines, is at high risk of cyber attacks.

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 aviation industry 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 therefore critical in asset-intensive and highly regulated industries, like aviation, that has a significant dependency on safety, security and continued operations. Air Traffic Management, Airport Management and Airlines all have key operational assets that are critical for their profitability, as well as the safety and security of employees, contractors, visitors and passengers. Suppose any one of their systems or operational equipment were to be exposed to a cyber attack. In that case, the entire operation could come to a halt, resulting in huge financial losses, 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 Air Traffic Management, Airports, and Airlines and minimise the risk of downtime.

# OT CYBER SECURITY

## THE TYPICAL OPERATIONAL VULNERABILITIES:

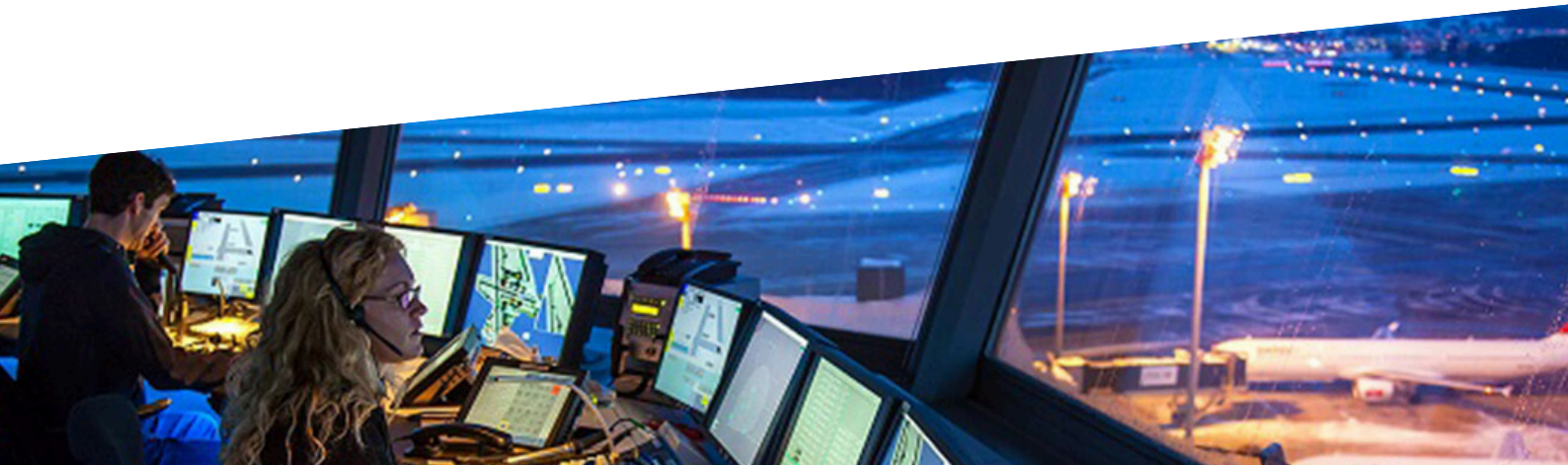
The following are common operational vulnerabilities inherent in most aviation environments:

- Siloed legacy systems make it very difficult to implement streamlined end-to-end security
- Physical assets, scanners, access and departure control, security cameras and many other operational devices are now connected to airport and airline systems, making it easier for cybercriminals to access operational equipment
- The inherent lack of security within existing devices makes it easier for threat actors to find access points
- A quickly evolving threat landscape where cybercriminals increasingly use more sophisticated tools that might challenge existing cybersecurity budgets

## 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 aviation industry)
- Holding the airport or airline to ransom and demanding exorbitant ransom amounts
- Steal confidential data and intellectual property and quickly sell it to their contacts
- Cause damage, destruction, unsafe conditions or even death to employees and passengers 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:

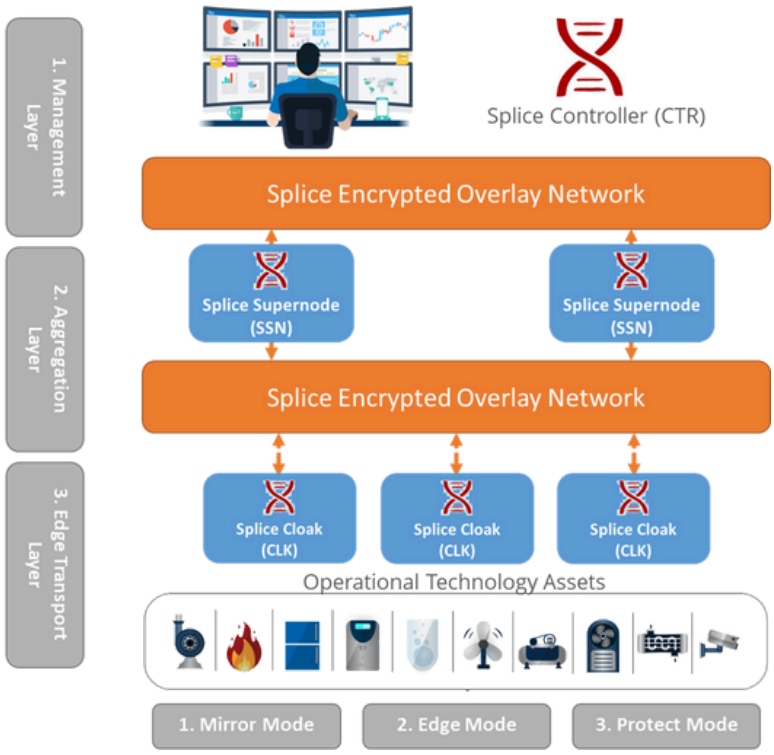
**Simplicity & Flexibility!**

**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



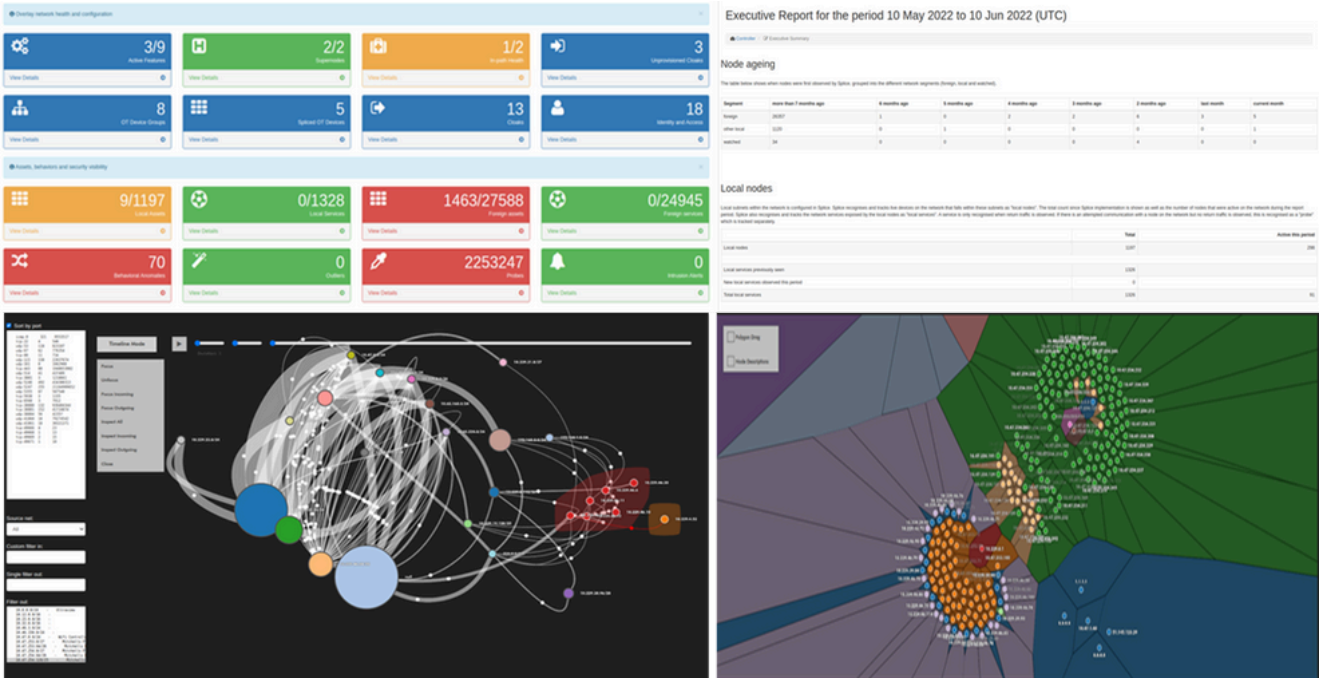

# OT CYBER SECURITY

## 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