



# Zero Trust E2E Security & Resilience for Cyber-Physical & Autonomous Systems

**Sel4 Summit**

**Dr Shreekant (Ticky) Thakkar**  
**Chief Researcher**  
**Secure Systems Research Center**

**October 10th 2022**

Secure Systems  
Research Center

tii.ae

# TII is part of Advanced Technology Research Council (ARTC)



ARTC shapes research and development for transformative technology outcomes.

It is our responsibility to define Abu Dhabi's **research strategy across academia and industry** and to consolidate funds for efficient investment.

We are establishing Abu Dhabi and the wider UAE as a desired home for advanced technology talent and as a **global hub for innovation**.

## ARTC Board

ARTC Secretary General



ARTC Management



Program Management  
Business Development



Applied Research Centres



Venture Subsidiary

# ATRC Priority Areas



## Sectors



Healthcare



Food  
& Agriculture



Security  
& Defence



Sustainability,  
Environment & Energy



Aerospace  
& Space



Transport

## Technologies



Digital  
Science



Autonomous  
Robotics



Advanced  
Materials



Secure  
Systems



Directed  
Energy



Quantum



Cryptography



Alternative Energy  
& Renewables



Propulsion &  
Space



Biotech

# TII Research Centers



Quantum  
Research Center

Autonomous  
Robotics Research  
Center

Cryptography Research  
Center

Advanced Materials  
Research Center

AI and Digital Science  
Research Center

Directed Energy  
Research Center

Secure Systems  
Research Center

Renewable and  
Sustainable Energy  
Research Center

Biotechnology  
Research Center

Propulsion and Space  
Research Center

# SSRC Key Projects – Problem statement, End users & Solutions

## Secure Technologies

Current software and hardware stacks are monolithic and thus hard to build secure, resilient, scalable & maintainable systems

### End Users

- First responders e.g., Police, Firefighters
- Military & Defense
- Cyber security for enterprise
- Systems e.g., Secure UAS & Mesh

### Solutions



Android Virtualization in cloud



Thin Compute

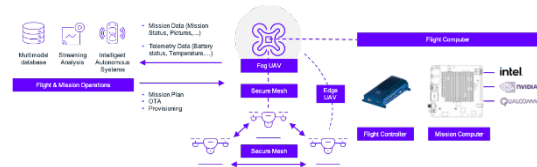
## Zero Trust Secure Autonomous UAS System

Limited E2E Secure and resilient Autonomous systems

### End Users

- First responders e.g., Police, Firefighters
- Military & Defense
- Logistics & service providers
- Smart Transportation
- Smart cities

### Solutions



E2E Secure & Resilient Stack

## Secure Mesh Shield

Current mesh based solutions does not support secure ad-hoc mobile peer to peer communication & scalability

### End Users

- First responders e.g., Police, Firefighters
- Military & Defense
- Logistics & service providers
- Smart Transportation
- Smart cities

### Solutions



Secure Mesh Shield SW Stack & Comms Module

A dark, monochromatic image of a river with a bridge and several drones flying in the sky. The scene is dimly lit, with the sky and water appearing in shades of blue and grey. In the foreground, a bridge spans across the river. Several drones of various sizes are scattered across the sky, some appearing to be in flight. The overall atmosphere is mysterious and technological.

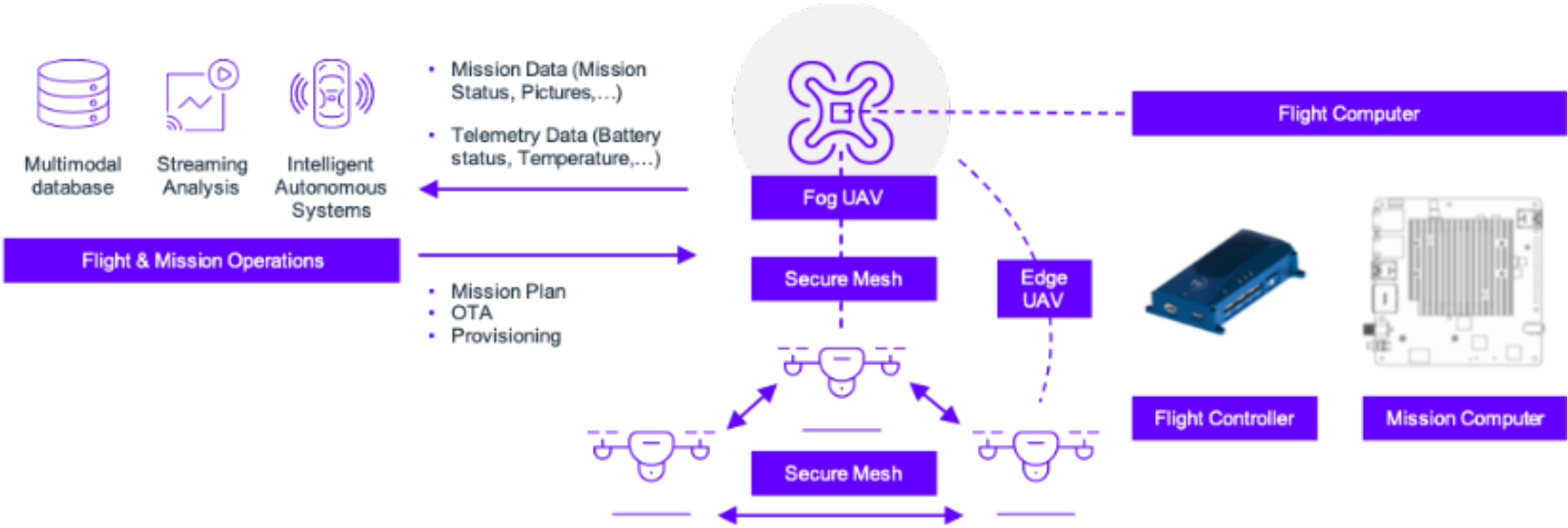
# Zero Trust Autonomous Systems

Secure Systems  
Research Center

# Future Connected Smart Cities will be managed by Autonomous Systems With Exponentially increasing Amount of Security Vulnerabilities



# Example: Secure and Resilient Autonomous Systems of fleet of Robot Drones

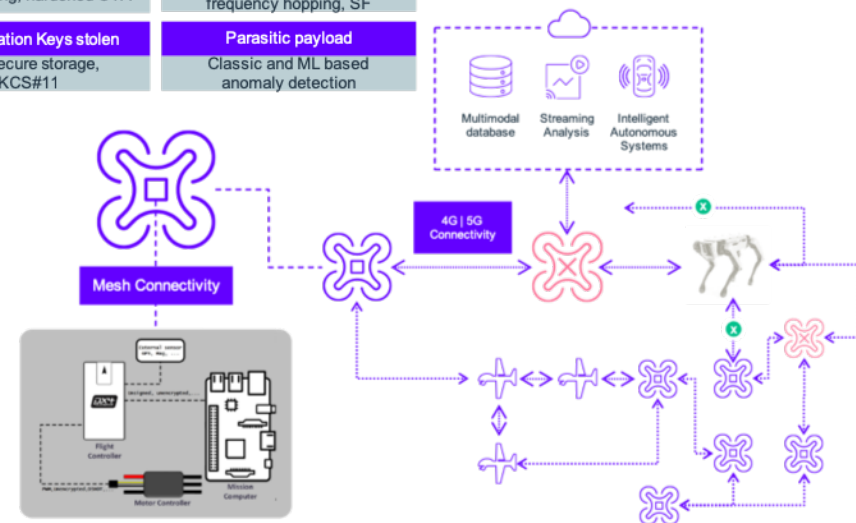




# What We Are Doing: Threats & Mitigation in Autonomous Flight and Mission Control System

<b>Injection malware to FW/SW updates, No secure boot loader</b>
Secure boot, hardened OTA
<b>Data exfiltration and infiltration (USB, SD card, SSD..)</b>
TEE, encrypted storage, digital signing and integrity checks
<b>Directed Energy (Acoustic attacks on IMU,...)</b>
Triple IMU with dissimilar acoustic resonant frequency
<b>UAV dismantled (Data and IP compromised)</b>
Encrypted DAR, Tamper protection and response
<b>Adversarial sensor data and spoofing ( GPS, camera,...)</b>
Redundancy and fusion, Classic and ML anomaly detection
<b>Absent HW Reset, no mitigation for HW exploits (BT, WiFi..)</b>
Dedicated power domains with reset and tamper protection

<b>SW Integrity (OS ROS, Autopilot...)</b>	<b>Jamming (GPS, Wifi, C2..)</b>
Digital signing, hardened OTA	VIO, Redundancy, frequency hopping, SF
<b>Authentication Keys stolen</b>	<b>Parasitic payload</b>
TEE, secure storage, PKCS#11	Classic and ML based anomaly detection



<b>Bug and access exploitation</b>
Hardened OS, VM split, containerization
<b>Single point of failure</b>
Sensor and flight controller redundancy

<b>Data infiltration / exfiltration</b>
RoT, MMU

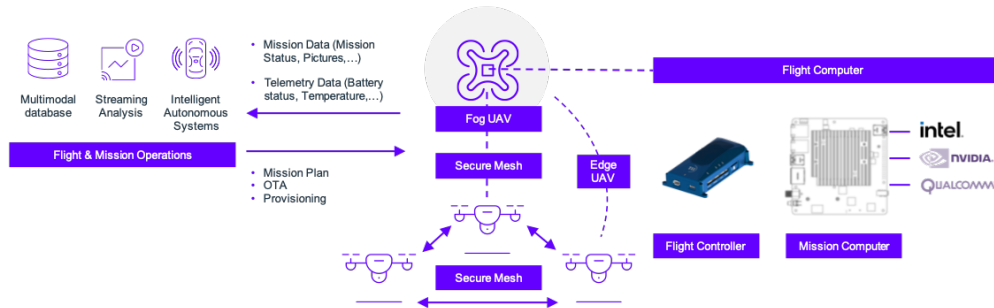
<b>Physical access to IC</b>
Tamper protection

<b>Data privacy compromised</b>
Functional encryption
<b>Adversarial mission upload</b>
Mission monitoring, M-of-N access control
<b>Link lost</b>
Fleet Autonomy Radio redundancy
<b>Alien UAV infiltrating swarm or protected space</b>
ROS2 security, mesh authentication
<b>Man in the middle</b>
Authentication, DIT encryption
<b>Data in transit hacked</b>
Authentication, DIT encryption

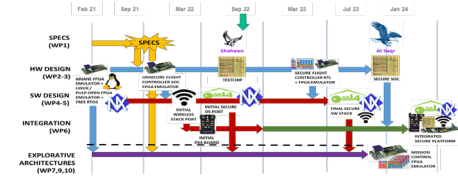
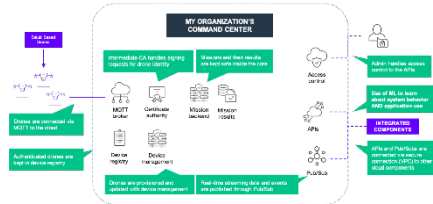
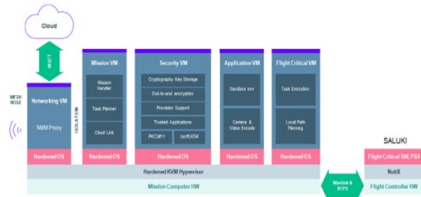
<b>Physical access to ports</b>
HW authentication

# Zero Trust End-2-End Secure and Resilient Autonomous Systems – Our Stack

- Secure Drone Flight Controller Stack
- Secure Mission Computer Stack
- Secure RISC-V based Hardware Stack
- Secure Flight and Mission Operations
- Secure Mesh Shield for communication
- Pentested for E2E operation



# ZT Autonomous UAS System Key Components



- E2E security and resilient solution from silicon to cloud
- Security solutions developed are HW agnostic
- Modular and scalable design
- Cloud mission & flight operations commanding a swarm with mesh communication between drones
- Autonomous mission planning & execution (OTA)

- COTS RISC-V: Microchip PolarFire SOC
- 10x performance & 1000x memory capacity + FPGA compared to commercial flight controllers
- Sensor board with redundancy (resilience)







- Secure and resilient Flight and mission operations
- Pilot for the swarm
- Secure Provisioning
- Secure OTA (over the air updates)
- Secure ML pipeline
- Data in Transit (DIT) protection

- Secure and Resilient flight & mission computer silicon
- Test chip taped out in July 2022
- Final version to tape out by min 2023
- Commercialization underway

# Partnerships



# SSRC Working with Ecosystems

Secure Autonomous Systems	Secure Platforms (RISC-V)	Secure ML	Secure Wireless	Secure Technologies
   				   

There is strong research community (**17 universities**) funded by SSRC to support each of areas above



**Visit [TII.ae](https://tii.ae) to learn more**

**Thank You**