Forum TERATEC 23

Unlock the future

31 MAI & 1er JUIN 2023 • Au Parc Floral, Paris

Un événement organisé par infoprodigital Teratec

Intrusion detection in embedded products: the challenges to overcome

Lionel Robin, CISSP

Chief Product Security Officer; Safran Electronics & Defense

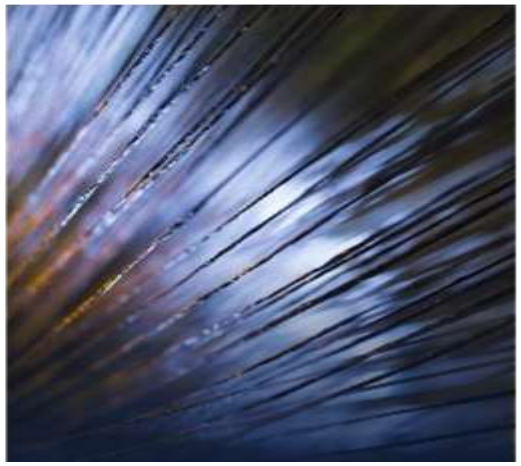
SAFRAN

Safran

An industrial high technology group

83,000
employees

€19.0
billion in revenues
in 2022



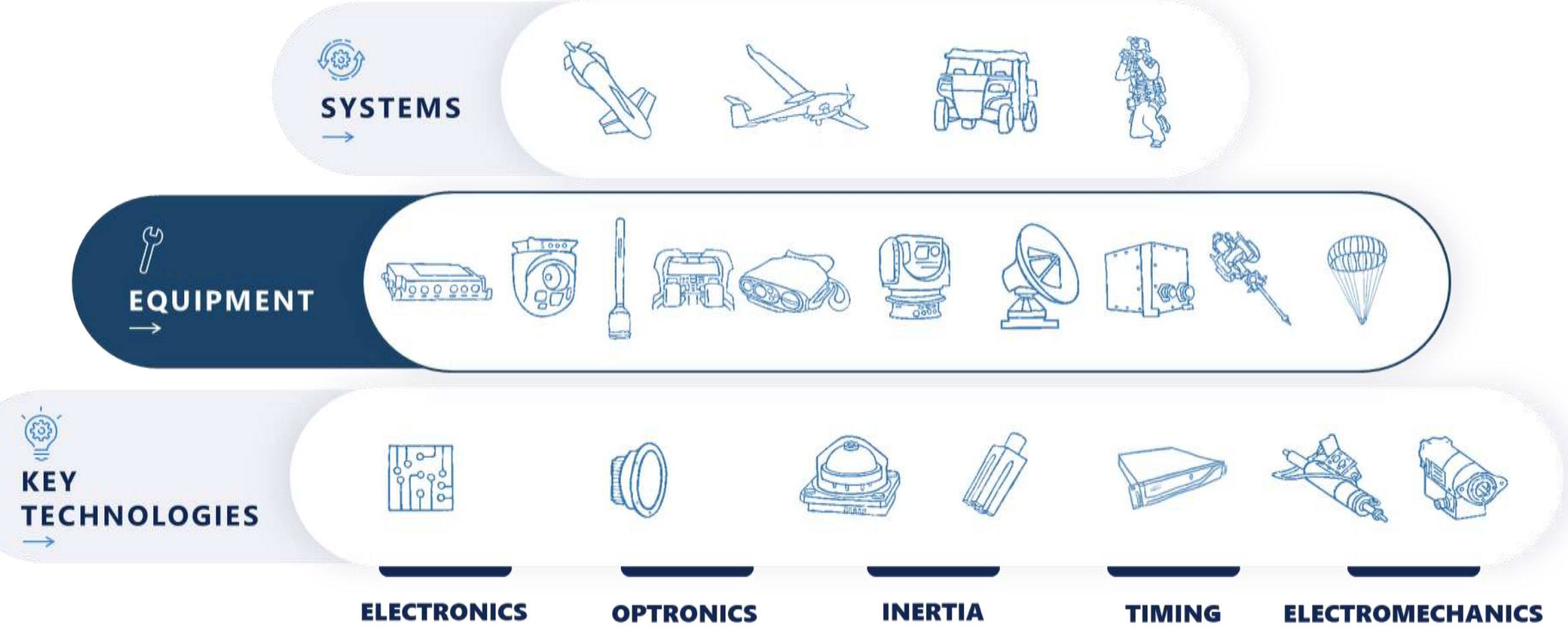
125 years
of history:
the oldest aerospace
manufacturer
in the world

No.3
aerospace company
worldwide (excluding
aircraft manufacturers)

Safran Electronics & Defense

A super-OEM with deep-rooted tech capabilities …

FOR DEFENSE, SPACE AND AVIATION MARKETS



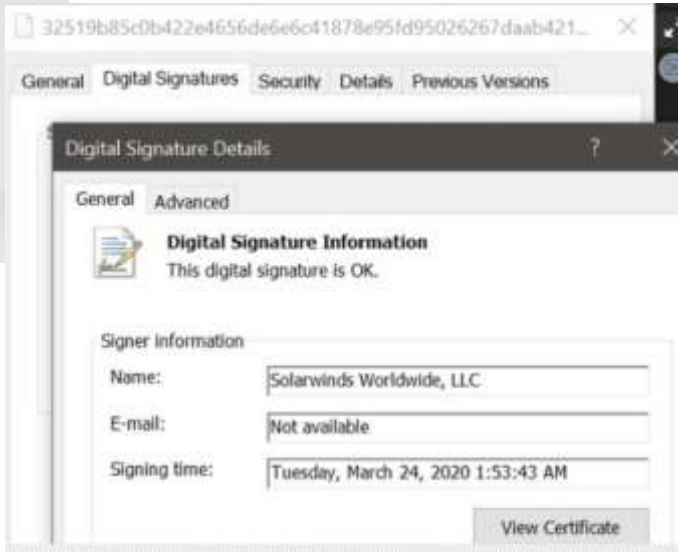
Overview

- Cyber: Everything is about trust
- Challenges around embedded functions
- The three ingredients to meet the challenge
  - Data, Algorithms and computational power
- Conclusion

Cyber, Everything is about trust

Cclearner Attack 2017 (source)

Asus live update Attack 2019 (source)



Solarwind 2020 (source)

We should be prepared against new types of attacks

Challenges for aeronautical embedded functions

- Maintain the airworthiness of on-board equipment
  - 1 plane takes off and lands every minute
  - 100,000 people in the sky every moment

- Contribute to reducing maintenance
  - Maximize the utilization rate of equipment
  - Reduce the time between two flights (Turnaround Time)

- Use new technologies and way to communicate

The surface of exposure increases more and more

How could the latest (AI-based) technology solutions help ?

Three ingredients to meet the challenges

Data

Algorithms

Computational power

The Data: coveted information

- Many sources of data onboard
  - Huge amount but the relevance is not always here
  - Large variety but very specifics protocols

DATABASE

- How is the owner ? Many stakeholders
  - Airlines (One or many) with its users (customers)
  - Maintenance and Repair operators (owned by Airline or not)
  - Manufacturer and the Supply chain (OEM, tiers 1, Tiers 2).

- How to collect the data
  - No one on board
  - how to ensure data integrity and origin ?

Get the data-set could be difficult and the assessment even more difficult

Algorithms: focus on development Lifecycle

- Based of Security Risks Analysis
  - Including cyber threats related to IA-related functions

- Deploy Secure Development LifeCycle (SDLC)
  - Standards ED202A, ED203A (AMC 20-42)
  - Coding standards
  - A lot of documentation, justification and evidence

- Auditing and Testing before releases
  - Functional Pre-use testing mandatory
  - Even truer if the functions reacts to the suspicious events
  - Verification and validations tools are part of the demonstration

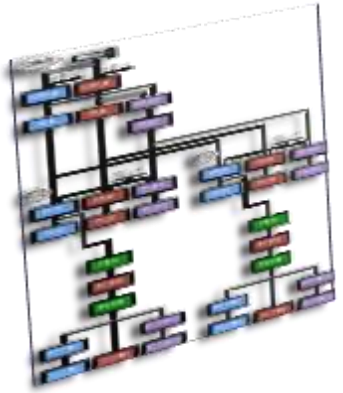
Airworthiness Authorities (EASA, FAA and others) has released rules (No creativity)

Need strict and supervised demonstration methods

Algorithms: keep in mind

- Be ready to demonstrate: Explainability of actions (XAI)
  - Transparency for the performance
  - Predictability in case of react capability

- Modifications and software updates
  - carried out with care
  - Closely monitored equipment update procedure

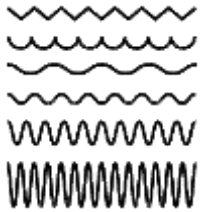


- An environment strict but under control
  - In operational use, very little change of systems

Computational power: Hardware-related challenges

- Standards from Airworthiness Authority
  - Rules about Multicore processing (AMC 20-193): partitioning

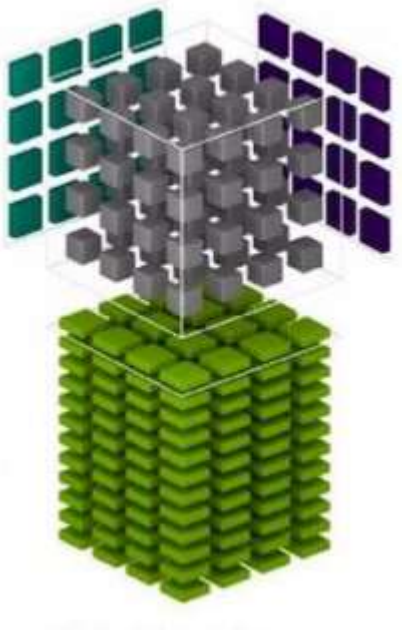
- Performance requirements
  - Capability to stay real-time,
  - low latency, Bandwidth efficient.



- Physical related requirements
  - Respect the limited housing dimensions,
  - Energy consumption,
  - vibration characteristics

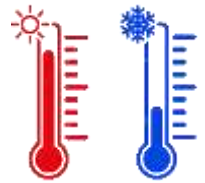
Computational power: Hardware-related challenges

- Technical solutions exist … but some concerns after a deep dive
  - Go behalf of marketing argument
    - Datasheet not crystal clear
    - Trade-off between performance & consumption
      - An example: 32 TOPs and 10W announced
      - yes but not a the same time…
  - Difficulty to assess the performance in the targeted context
    - Manufacturers characterize "standard" algorithms, different from our ones
    - Development and user support tools are not sufficiently covered



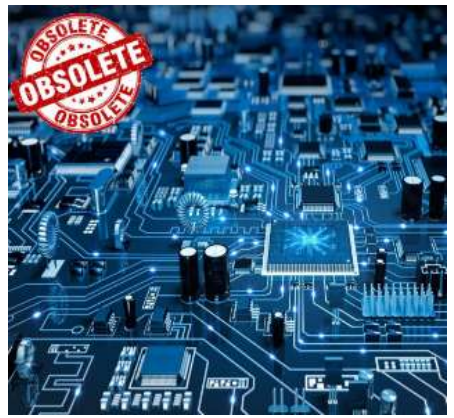
Other challenges about hardware

- Temperature and environmental constraints
  - needs [-40°C; 100°] or [-55°C; 125°C]
  - Large public consumer products [0°C; 70°C]



- Industrial challenge : Capability to buy components
  - Minimum Order Quantity (MOQ)
  - 100 k item by year for main suppliers (NVIDIA, Intel,…) large consumer products or for automotive

- Component Lifetime
  - Capability to buy the component
  - More 10/20 years versus 6 to 8 years



Conclusions

- Establishing Trust and reliability in the solution (Explainable AI)
- Take into account the embedded constraints at the heart of the solution
- Extend resilience and lifetime of the components

Be part of the challenge for the embedded world

Thanks for your attention

Questions

Lionel Robin

Lionel.robin@safrangroup.com