A Cyber-Resilient IoT Certification Framework for Aviation Systems

Roland Atoui

Managing Director

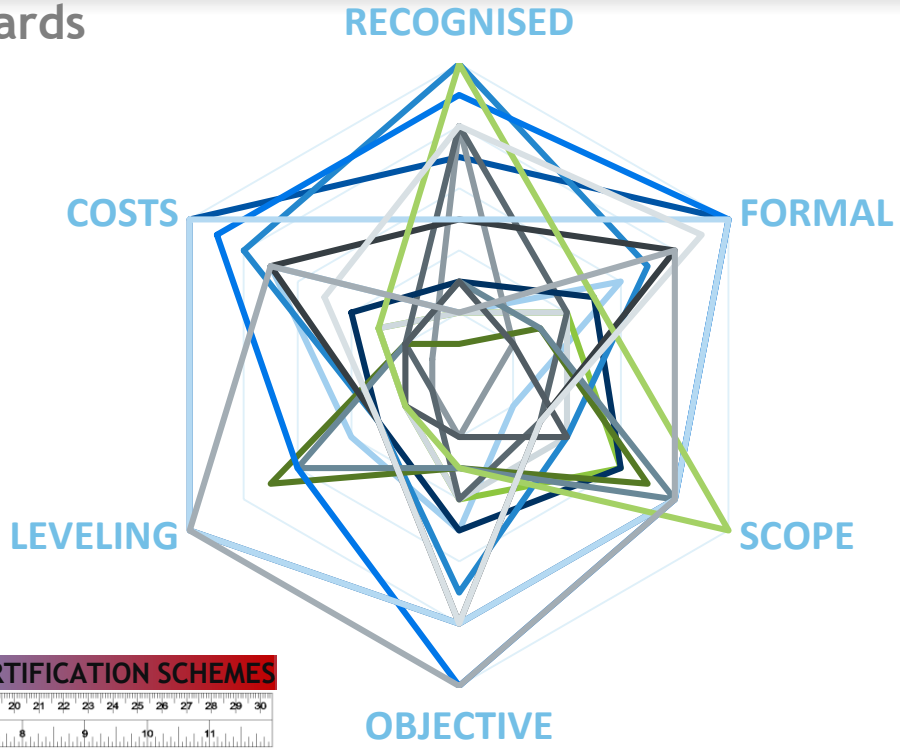
@Roritto

linkedin.com/in/rolandatoui

RED ALERT LABS
IoT Security

HOW DO WE MEASURE SECURITY ?

Certification Standards
what metrics ?

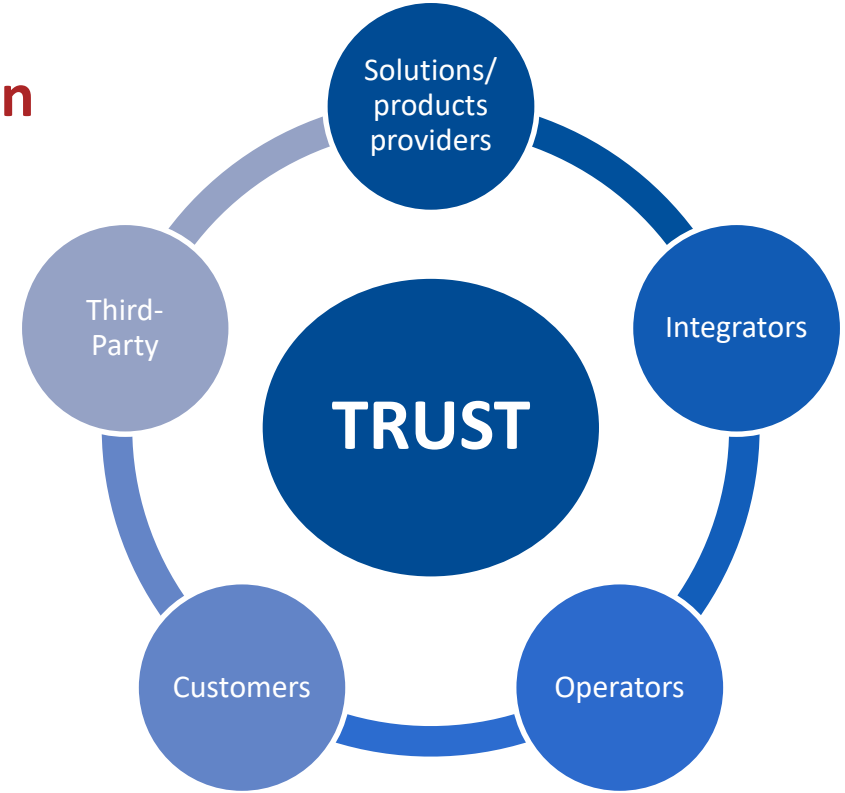


METRICS defined by STANDARDS/CERTIFICATION SCHEMES

HOW DO WE TRUST THESE MEASURES ?

Trust

Definition



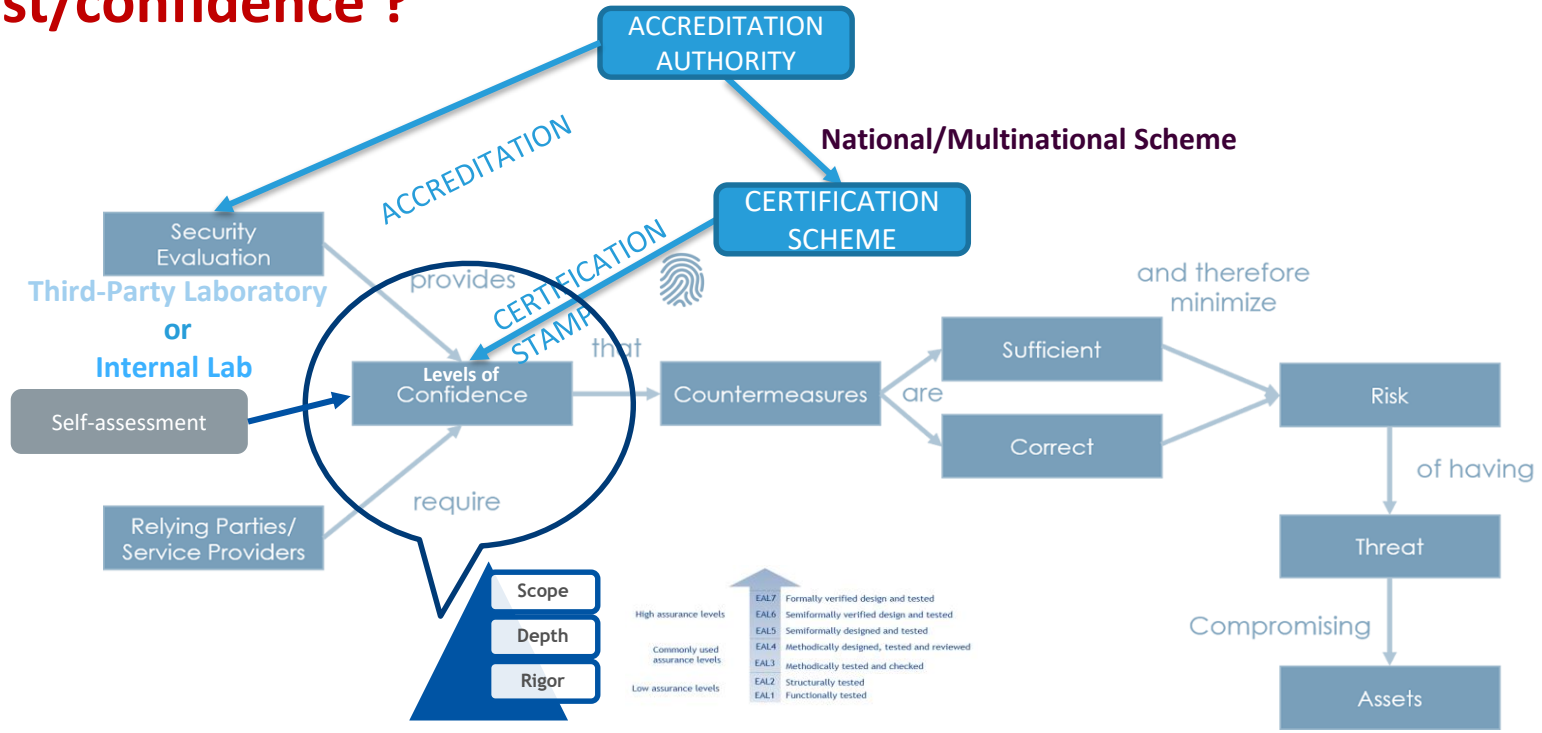
TECHNICAL
(assessment, review, validation)

LEGAL
(regulations, contracts, commitments, liabilities)

SOCIAL
(reputation, transparency)

Security Evaluation

What trust/confidence ?



WHAT IS THE PROBLEM WITH EXISTING IT PRODUCTS CERTIFICATION ?

Internet of Things

Problems in Certification Practices

- Evaluation Lab
- CC consultancy (optional)
- In-house Evidence development
- Site visit expenses (optional)
- Travel Expenses (optional)
- Equipment Costs
- Lost opportunity
- Certification Scheme (ANSSI -> FREE, BSI -> 2,5K€ to 12K€)

➔ Evaluation Lab Examples of Fees:

- **EAL 2**: 80K€ → 150 K€
- **EAL 3**: 120K€ → 200 K€
- **EAL 4+**: 150K€ → 300 K€

"Objective" IT Products Certifications cost a considerable amount of MONEY, Takes TIME and is more often VALID for only a short time

EAL Level	Evaluation Times
EAL 2	4 – 6 months
EAL 3	6 – 9 months
EAL 4	7 – 12 months
>EAL 4	12 – 24 months

SO WHY NOT REUSE EXISTING EVALUATION TECHNIQUES FOR IoT ?

IoT Product Security

Why Not Reusing Existing Certification Techniques ?

Cost, time, validity

- Can't be applied to the 50 Billion IoT product market ! Not enough resources to do that…

Subjective

- What is the credibility of the evaluation lab/pentester/etc. ?What does secure mean? Can we compare more or less secure products?

Scope

- Silo Approach - they often cover part of the problem, specific to an industry (banking, ID) but security & privacy is now a concern of every business and citizen.

Poor Security Definition

- There is no common and holistic approach to define security requirements per profile taking into account the threat model & risks due to the intended usage

WHAT SOLUTION ?

AN IOT SECURITY CERTIFICATION FRAMEWORK FOR AVIATION SYSTEMS

A Risk-Based Approach
Operational Environments

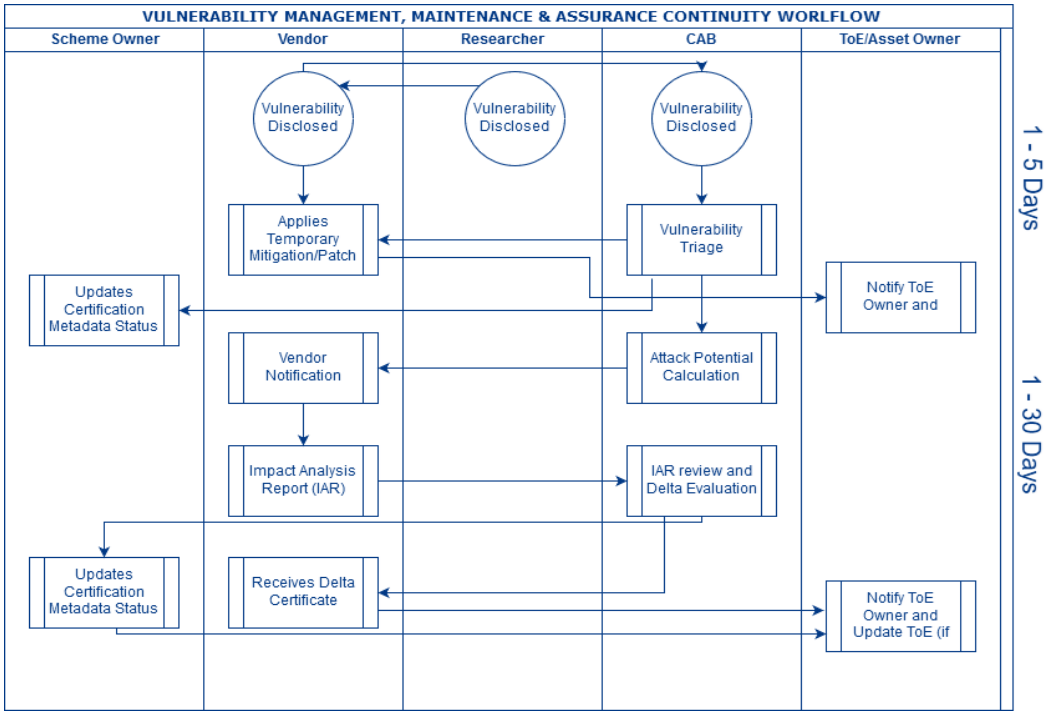
Risk-Based Security Assurance Activities

SUBSTANTIAL

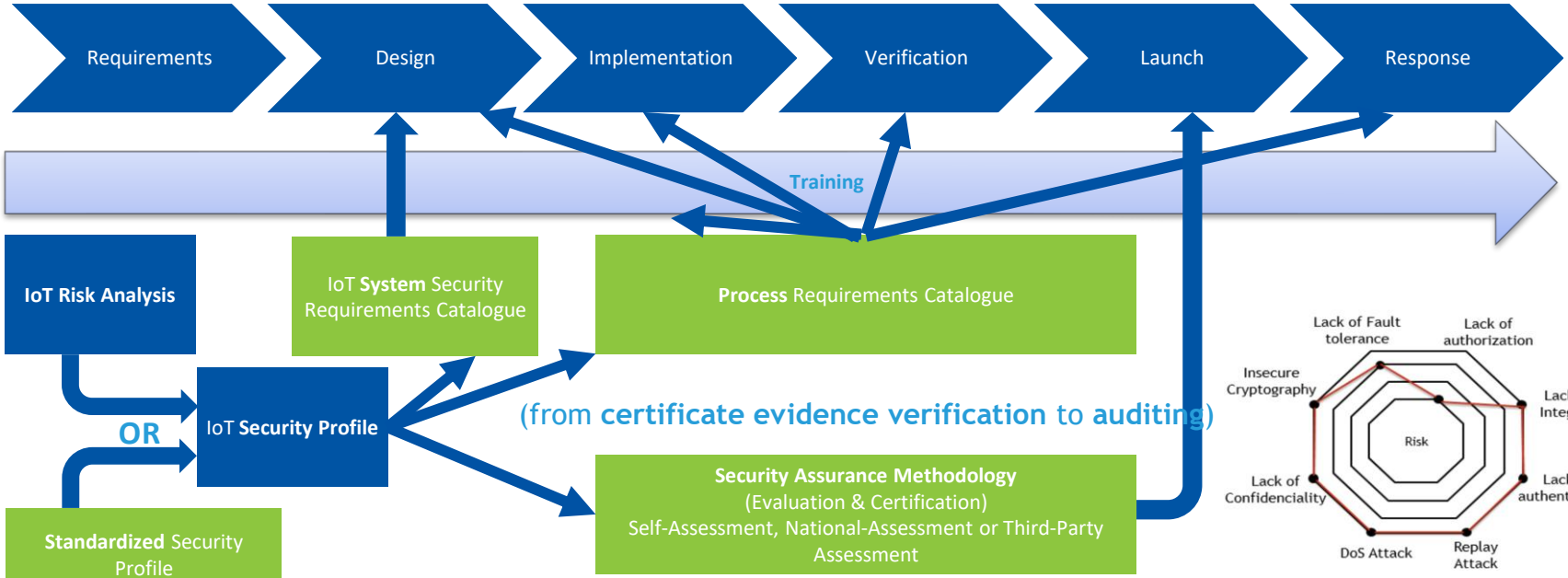
IMPACT VS LIKELIHOOD	UNLIKELY (1)	LIKELY (2)	VERY LIKELY (3)	ALMOST CERTAIN (4)
SEVERE (4)	CA.DocumentationReview CA.SourceCodeReview CA.CompositionAnalysis (if applicable) VA.VulnerabilityScanning	CA.DocumentationReview CA.SourceCodeReview CA.FunctionalSecurityTesting CA.CompositionAnalysis (if applicable) VA.VulnerabilityScanning VA.BasicRobustnessTesting	CA.DocumentationReview CA.SourceCodeReview CA.FunctionalSecurityTesting CA.CompositionAnalysis (if applicable) VA.VulnerabilityScanning VA.BasicRobustnessTesting VA.AdvancedRobustnessTesting	CA.DocumentationReview CA.SourceCodeReview CA.FunctionalSecurityTesting CA.CompositionAnalysis (if applicable) VA.VulnerabilityScanning VA.BasicRobustnessTesting VA.AdvancedRobustnessTesting
MODERATE (3)				
MINOR (2)			VA.VulnerabilityScanning VA.BasicRobustnessTesting	CA.CompositionAnalysis (if applicable) VA.VulnerabilityScanning VA.BasicRobustnessTesting
LOW (1)	CA.DocumentationReview CA.CompositionAnalysis (if applicable)	CA.DocumentationReview CA.CompositionAnalysis (if applicable)	CA.DocumentationReview CA.CompositionAnalysis (if applicable) VA.VulnerabilityScanning	CA.DocumentationReview CA.SourceCodeReview CA.CompositionAnalysis (if applicable) VA.VulnerabilityScanning

- **Conformity Analysis** (Doc Review, Source Code Review, Composition Analysis, Security Functional Testing)
- **Vulnerability Analysis** (Scanning, Basic Robustness Testing, Advanced Robustness Testing, Non-Intrusive Pentesting)

Active Certificate Monitoring/Vulnerability Surveillance



Smart Integration into the Life-Cycle



KEY TAKEAWAYS

Key Takeaways

01 AUTOMATISATION & AGILE METHODOLOGY

Allow to automate Security Reqs/Questionnaire acts as guidelines, not much overhead evidence docs, and reduced testing time

02 RECOGNIZE EXISTING EVALUATION METHODOLOGY

Requirements could be simply mapped to other certification schemes allowing recognition of existing methodologies by composition such as SOGIS CC evaluations for underlying platforms. In any case all types and formats of evidence could be reused as is under this Scheme.

03 REDUCE COSTS

The evaluation must address priorities and is time-constrained, thus limiting its delays and cost, but still offering a guarantee that experts have spent time analyzing the product most valuable security functionalities

04 COMPARE IOT DEVICES

The accurate evaluation scope coupled with the security functionalities and the defined set of security requirements are a result of accurate security analysis/threat modelling, The Evaluation metrics and ratings are simple and expressive

05 REQUIREMENTS TAILORED TO THE INTENDED USE

The scope of evaluation focuses on the HW & SW forming the IoT Device but the threat model covers the operational environment including the final application, interfaces and other components connected to the product if any.

Key Takeaways

06 COST-EFFICENT CERTIFICATION MAINTENANCE

Provide a smart framework to define, attest and maintain the certificates delivered for IoT devices after issuance. Patching & Temporary Mitigation are allowed.

07 CREATE INCENTIVE FOR VENDORS

Minimum Effort required on providing evidence, simple metrics, clear requirements, security valued by customer

08 INVOLVE IOT SERVICE PROVIDERS

Expressing security L Level Rating + Community creating awareness. IoT Service Providers and Customers trust the vendors

09 SIMPLE METRICS

Requirements and Test Procedures must be expressed in simple wording allowing the vendors and CABs to implement and test efficiently.

10 REGULATIONS COMPLIANT

Incorporate Cybersecurity, Safety and Resilience in Regulations (by design).

Thank you!

Questions?

Roland Atoui
Managing Director
@Roritto
linkedin.com/in/rolandatoui

RED ALERT LABS
IoT Security

ICAO

North American Central American and Caribbean (NACC) Office
Mexico City

South American (SAM) Office
Lima

ICAO Headquarters
Montréal

Western and Central African (WACAF) Office
Dakar

European and North Atlantic (EUR/NAT) Office
Paris

Middle East (MID) Office
Cairo

Eastern and Southern African (ESAF) Office
Nairobi

Asia and Pacific (APAC) Sub-office
Beijing

Asia and Pacific (APAC) Office
Bangkok

THANK YOU