FORUM AEROSPACE INNOVATION

➤ APRIL 25 AND 26, 2016

COLLABORATE GLOBALLY TO DEVELOP AEROSPACE INNOVATION

IN COLLABORATION WITH:

CRIAQ

ORGANIZED BY:

AÉRO MONTRÉAL 10 YEARS

Québec's Aerospace Cluster

Meeting the Challenges of Cyber security And Hacking To Insure Safety of Aircraft and Embedded Systems

Moderator: **Manon Gaudet**, ***GCED, CCISP, Cert. Cyber-Investigation***
National Research Council of Canada - Industrial Research Aid Program
Manon.gaudet@nrc-cnrc.gc.ca

Your moderator

Mrs. Manon Gaudet, CISSP, GCED, Cert. Cyber-Investigation.

Manon is an Industrial Technology Advisor (ITA) at the National Research Council of Canada's Industrial Research Assistance Program (NRC-IRAP). Specialised in ITC and Cyber Security.

Manon is a trusted advisor to long-term clients of NRC-IRAP. She combines extensive experience in research and development and information security, with experience in complex project management in various technological domains including embedded systems in SCADA, EDS, GPS systems and many others.

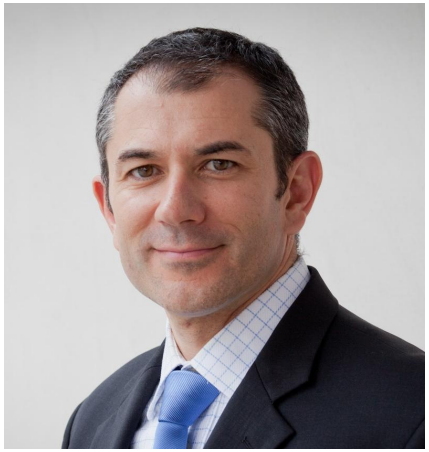
Prior to joining NRC-IRAP, Manon worked as a Chief Consulting Cybersecurity and Investigation for Ogham Technologies, and as an Information Security Advisor, Incident Response and Countermeasures lead at Desjardins, among others.

Manon holds a Bachelor Degree in Computer Science from Université de Montréal and a Cyber-Investigation Certificate from the Polytechnique Montréal. She holds a SANS-GCED, a CISSP from ISC2 and ITILv3 Foundation.

Who is NRC-IRAP ?

- **National Research Council of Canada - Industrial Research Aid Program**
- Program help SMEs build innovation via:
  - Financial support of R&D projects
  - Support advisory services
  - Partnerships and networking
  - 280 Industrial Technical Advisors across Canada
  - Cover all science domains

Panel Participants



Mr. Laurent Porracchia, Vice President, Industry and Government, Safran-Morpho Digital Security and Authentication Division

Laurent joined Morpho (Safran Group) in December 2010 as an IT security expert. Before joining Safran Group, he spent 17 years as an engineering officer in the French Air Force, first doing several operational missions with his fighter aircraft squadron and then, since 2005, implementing cybersecurity in classified networks for the French Department of Defense and also for the NATO networks.

Since February 2015, Laurent is heading the Business unit « Industry, Government and Defense » for the division Digital Security in Morpho.

Laurent holds an engineering diploma in aeronautics and a PhD in IT Security. He passed the following certifications : COBIT 5 Assessor, Lean IT Foundation and Certified Ethical Hacker.

He is also graduated from the NATO Communication and Information System School and has more than 10 years of best of breed experience in cybersecurity and aeronautics.

Panel Participants

Mr. Frédéric Audet, Project Manager, Thales Research and Technology, has over 22 years of system development experience as a practitioner for Thales, Intergraph, Futjisu (DMR) and Telus (Québec Téléphone).

During his career, Mr. Audet has conducted several research contracts for Defense Research and Development Canada at Valcartier as well as system integration contracts for major customers, whether in the segment of National Defence (DND), transportation, environment, land management or natural resources. Since 2013, he has the responsibility of managing Thales Research & Technology Cyber-Security portfolio.

Mr. Audet leads a team of experts in the fields of malicious code detection, forensics analysis, critical infrastructure protection, and cyber threat intelligence.

Mr. Frédéric Audet completed a Bachelor's degree in Computer Sciences (Engineering) at Laval University in 1994.

Panel Participants

Dr. Jeffrey Joyce is a principal of a Vancouver-based engineering consultancy, Critical Systems Labs (CSL), which provides clients with expertise in the specification, analysis and review of critical systems.

As a member of RTCA SC 205, he contributed to the development of RTCA DO 178C ("Software Considerations in Airborne Systems and Equipment Certification") and RTCA DO 333 ("DO-333 Formal Methods Supplement to DO-178C and DO-278A").

Dr. Joyce and his colleagues at CSL are using RTCA DO 326A ("Airworthiness Security Process Specification") and other resources to create solutions for clients that extend their approach to safety to take account of security threats.

Dr. Joyce earned a doctorate in Computer Science from Cambridge University, with earlier degrees from the University of Calgary and the University of Waterloo.

Panel Participants

Mr. Colin O'Flynn, CEO, *NewAE Technology*, hardware and embedded cybersecurity solutions

Colin O'Flynn is completing a PhD in embedded security research, and as part of this has released the first open-source toolchain for side-channel power analysis attacks, which also has turned into a small start-up in Halifax, NS. He previously worked at Atmel developing low-power wireless embedded systems.

Panel Participants

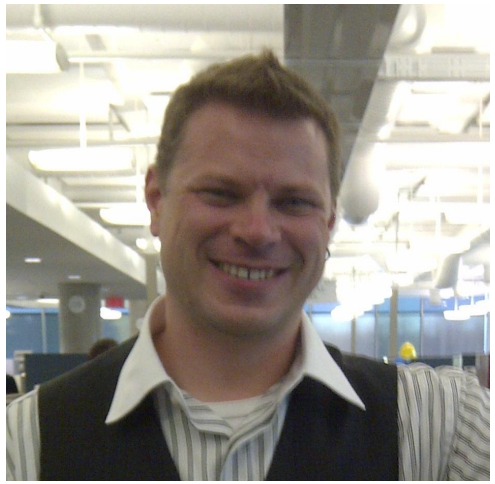
Mr. José M. Fernandez, Eng., Ph.D. Associate Professor, *École Polytechnique de Montréal*

M. José M. Fernandez is an associate professor in the Department of Computer & Software Engineering at the Ecole Polytechnique de Montreal, where he heads the Information Systems Security Lab. His research interests include the security of critical infrastructure control systems, Cyber Public Health, Cyber Crime and Cyber Warfare. In recent years, he has worked on aeronautical telecommunications systems security and on intrusion detection in Air Traffic Control systems. He has several years of professional experience in Computer Security in the private and public sector.

He holds two bachelor's degrees from MIT in Mathematics and Computer Engineering, a Master's from the University of Toronto in Cryptology, and a Ph.D. from the Université de Montréal in Quantum Computing. M. Fernandez is a private pilot with an instrument rating and an airplane owner.

Panel Participants

Mr. Jayson Agagnier, Sr. PKI Specialist, Carillon Information Security Inc.



Security professional with more than 25 years of experience in IT & Information Security working in various sectors such as Telecommunications, Oil, Gas & Energy, Semiconductors and Aerospace. He founded a start-up security consulting company during the dot-com era and most recently worked in the domain of aviation systems security and security certification. An active member of ARINC and RTCA working groups help to advance various security guidance material, acted as interim chairman of RTCA SC-216 Sub Group 4. I have participated in the development of DO-326A, DO-355 and DO-356.

FORUM AEROSPACE INNOVATION

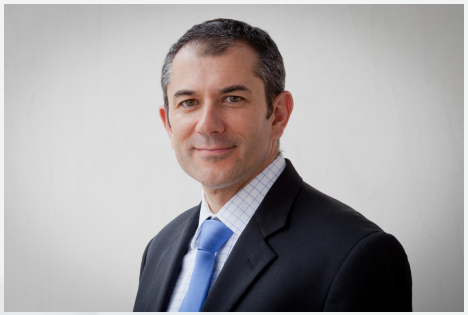
Meeting the Challenges of Cyber security And Hacking To Insure Safety of Aircraft and Embedded Systems

Mr. Laurent Porracchia, Vice President, Industry and Government, Safran-Morpho Digital Security and Authentication Division

AÉRO MONTRÉAL 10 YEARS

Who am I ?

- Laurent PORRACCHIA, PhD, CEH
- VP Digital Security , SAFRAN (Morpho)
- Spent more than 15 years in both Aerospace & Industry Cybersecurity
- Involved in various Cybersecurity Panels and Working Groups (EU, ATA…)



Some open challenges to address

- Mission critical data transfer
- Counterfeit or *non trusted* software
- Components Off The Shelf usage

Securing software supply chain

Field loadable software	Engine and other technical parameters	Simulation software	Computer numerical control files

Data origin must be verified

Software validation may be **online or offline**

Data integrity can be compromised on untrusted channels

Data can be transmitted on **physical medium or online**

Strong regulatory and corporate specific rules

The solution must be integrated in **existing business processes and tools**

Securing software supply chain

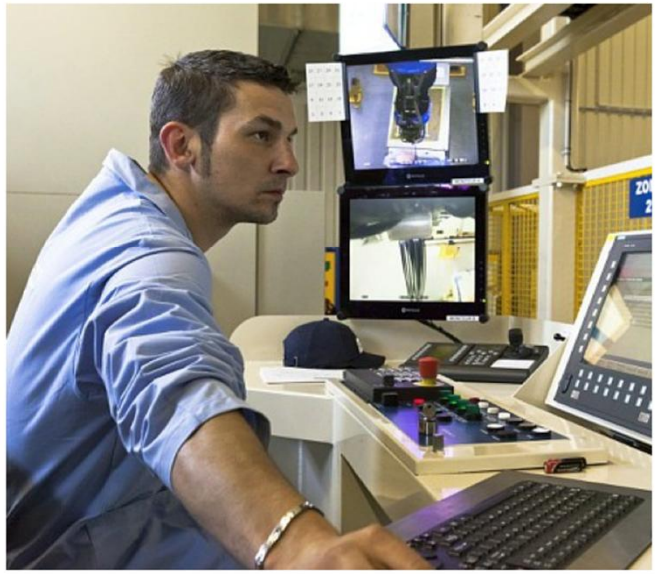
One versatile solution for Field Loadable Software, manufacturing (CNC) and simulation software, online and offline – for manufacturers, suppliers and MRO operators

The tools for online signature, timestamping and validation **run on entry level PCs**

Ready for **future authenticators**

Offline signature verification with a specific " Seal Box"

Compatible with Arinc loads



Meeting the Challenges of Cyber security And Hacking To Insure Safety of Aircraft and Embedded Systems

Mr. Frédéric Audet, Project Manager, Thales Research and Technology

Malware Detection and Analysis as a Service

Frédéric Audet

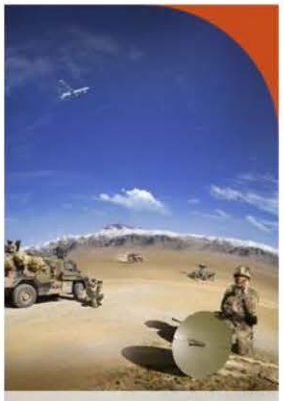
Cyber-security Research Portfolio Manager

Thales Research and Technology - Canada

What we do, who we serve

DUAL MARKETS
Military & Civil


AEROSPACE


DEFENCE


SECURITY


SPACE


GROUND TRANSPORTATION

Employees 62,000

Revenues in 2015 20.7 billion $CAD

Self Funded R&D in 2015 1.04+ billion $CAD

Global presence 56 countries

TRUSTED PARTNER FOR A SAFER WORLD

Critical Information Systems and Cybersecurity
A global reach, beyond local expertise

A global player

- 5,000 IT and security engineers, including 1,500 cybersecurity specialists

A major European leader in cybersecurity

Worldwide leader in data protection

- 3 Cybersecurity Operation Centres – CSOC (France, the Netherlands and the United Kingdom)
- 1 CERT-IST (Computer Emergency Response Team – Industry, Services and Tertiary sector)
- 5 high-security data-centres in France and in the United Kingdom

AERO MONTREAL 10 ANS

Avionics (Montreal)
Part of the Thales Aerospace Division

Established in Montreal since 1997 in close proximity to Bombardier Aerospace

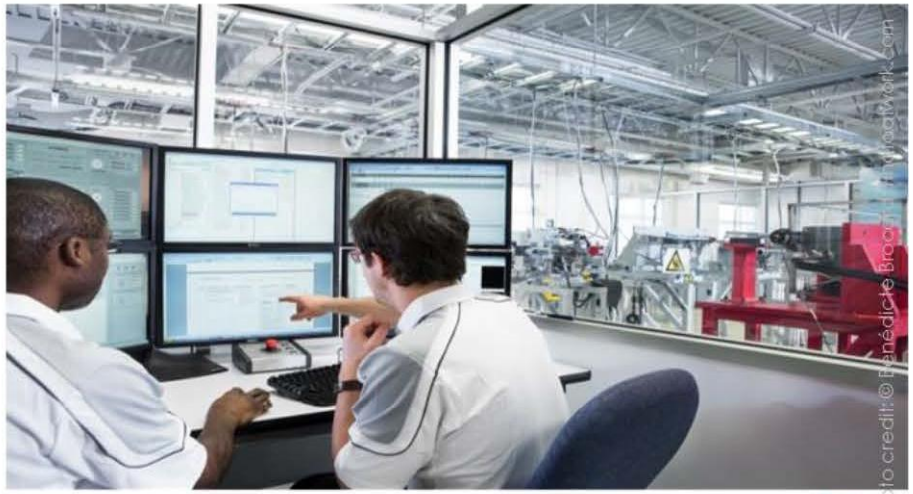
- 125+ employees
- 100 million+ in revenues
- Centre of competence for engineering of flight control systems

Mission: Serve business and regional aircraft markets (OEM & Airlines) in the Americas

- Bombardier Q400

Key areas of expertise:

- Fly-by-wire and avionics
- System engineering for complex systems
- Software for highly critical systems
- Supply chain management and On-Time Delivery



Aerospace: InFlyt Experience

Deployed in 70 airlines worldwide with 2000 aircraft flying, 500+ of which are already connected

- IFE and Connectivity systems have merged in our offer
- We are strong #2 globally in connected IFE systems market with ambition to be the leader
- Low double digit growth rate anticipated over next 5 years
- 2000 employees in 30 facilities
- OS transitioned to Android with external applications development portal

FORUM INNOVATION AÉROSPATIALE

In Canada, we have our products on over 200 aircrafts

- Air Canada, Jazz, Westjet

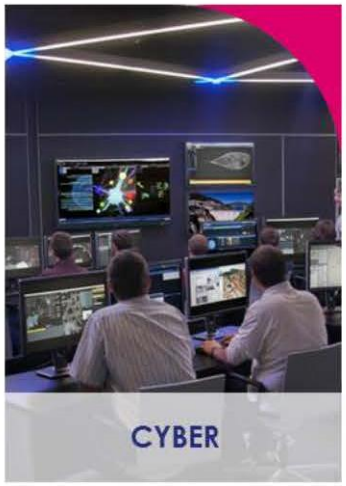
Partnered with TRT Canada on several innovation projects

Our commitment to Technology & Innovation

FORUM INNOVATION AÉROSPATIALE

Thales Research & Technology - Canada

5th worldwide – Located in Quebec City



Employees
40

R&D Thales Canada
30 million $CAD investment

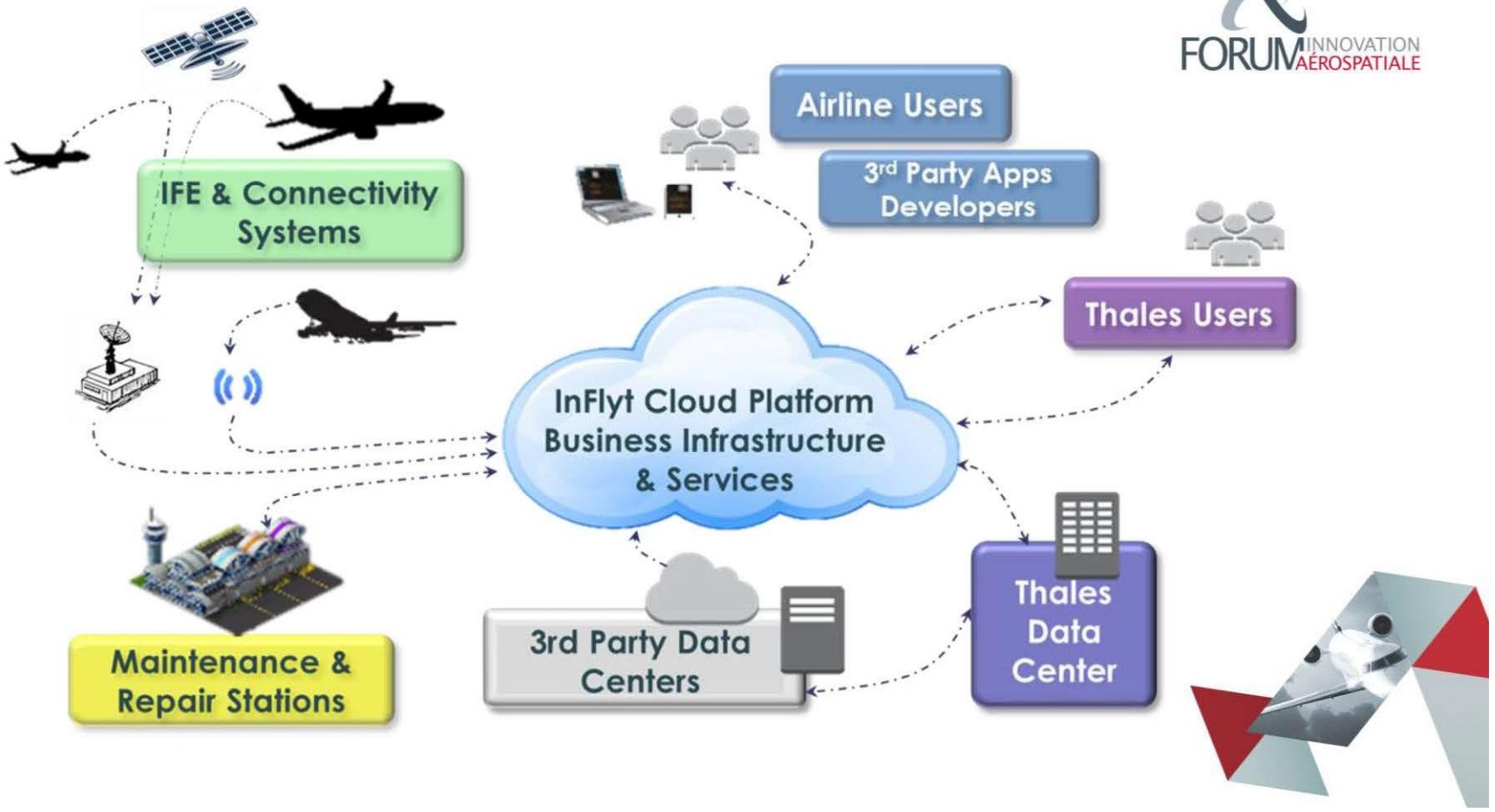
Patents since 2003
37+

Academic presence
6 Canadian universities

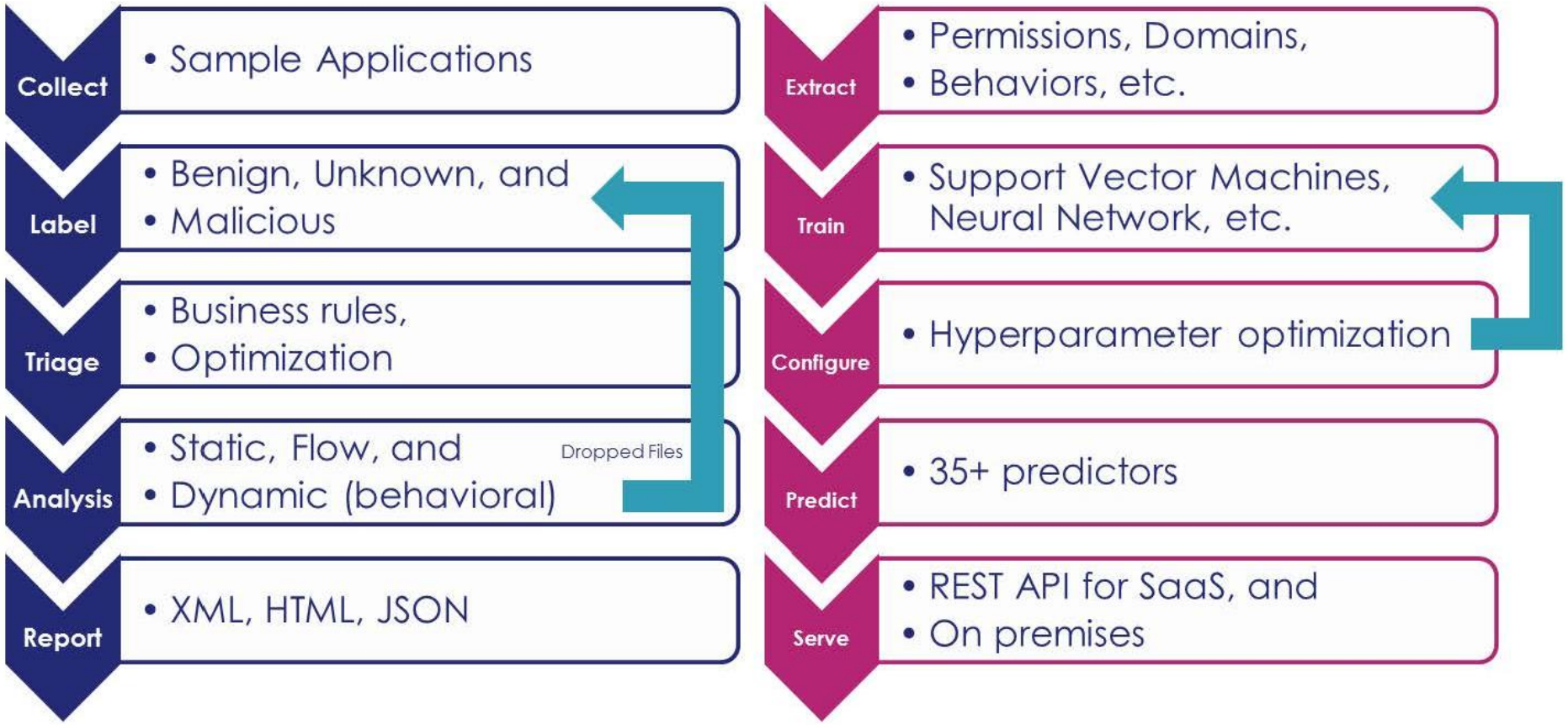
INAUGURATION 13 Nov. 2012

AERO MONTREAL 10 ANS

Inflight Entertainment & Connectivity Ecosystem



Malware Detection and Analysis as a Service



On-line Watch & Learn | Differentiator

Malware detection as a Service

- App vetting for private (enterprise) store
- Network sandbox (BYOD)
- Multi-Analysis (Static, Dynamic, Flow)

Resilient Predictor

- Sustained 94%+ accuracy over 2015
- False positive rate 3.8%

Custom System

- OS version, Platform (SVDU, TPMU)
- Virtual and Physical

Meeting the Challenges of Cyber security And Hacking To Insure Safety of Aircraft and Embedded Systems

Mr. Jeff Joyce, Principal, Critical Systems Labs Inc.

Aircraft Systems, Safety and Cybersecurity: RTCA DO-326A guidance

FORUM INNOVATION AÉROSPATIALE

Critical Systems Labs

Strategic Insight for Safety

AERO MONTRÉAL 10 ANS

Flight Safety - Historically

Flight Safety Today

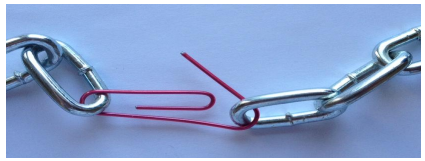
Could a cyber-attack lead to a aircraft failure condition?

- Aircraft connectivity increasing
- New aircraft architecture
- New aircraft systems
- Reliance on COTS HW & SW
- Cybersecurity attacks increasing
- Lack of aviation security framework

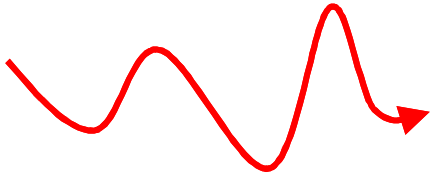
Vulnerability to such attacks has been publicly demonstrated

Not Just an IT Security Problem

- Mitigating safety risk due to security threat is NOT just an IT security problem
- Must identify what failure conditions could be caused or enabled by attacks
- Cause-effect connection between security vulnerability and failure condition can be complex

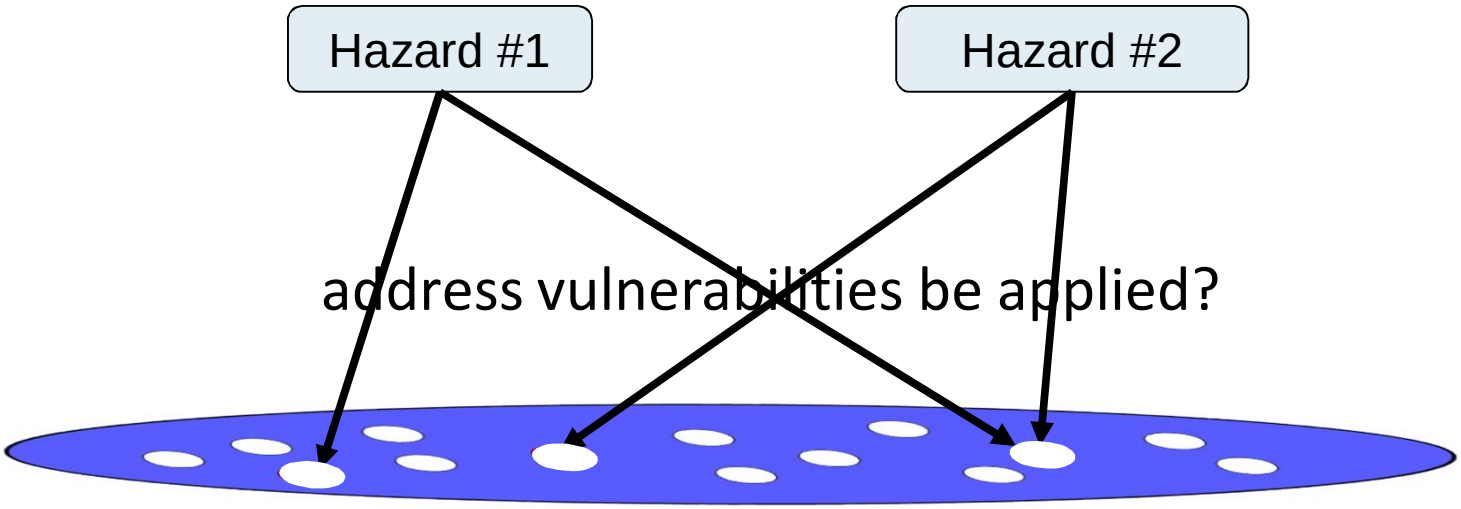


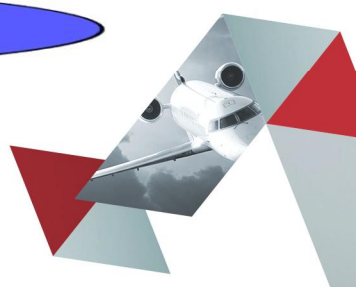
security vulnerability



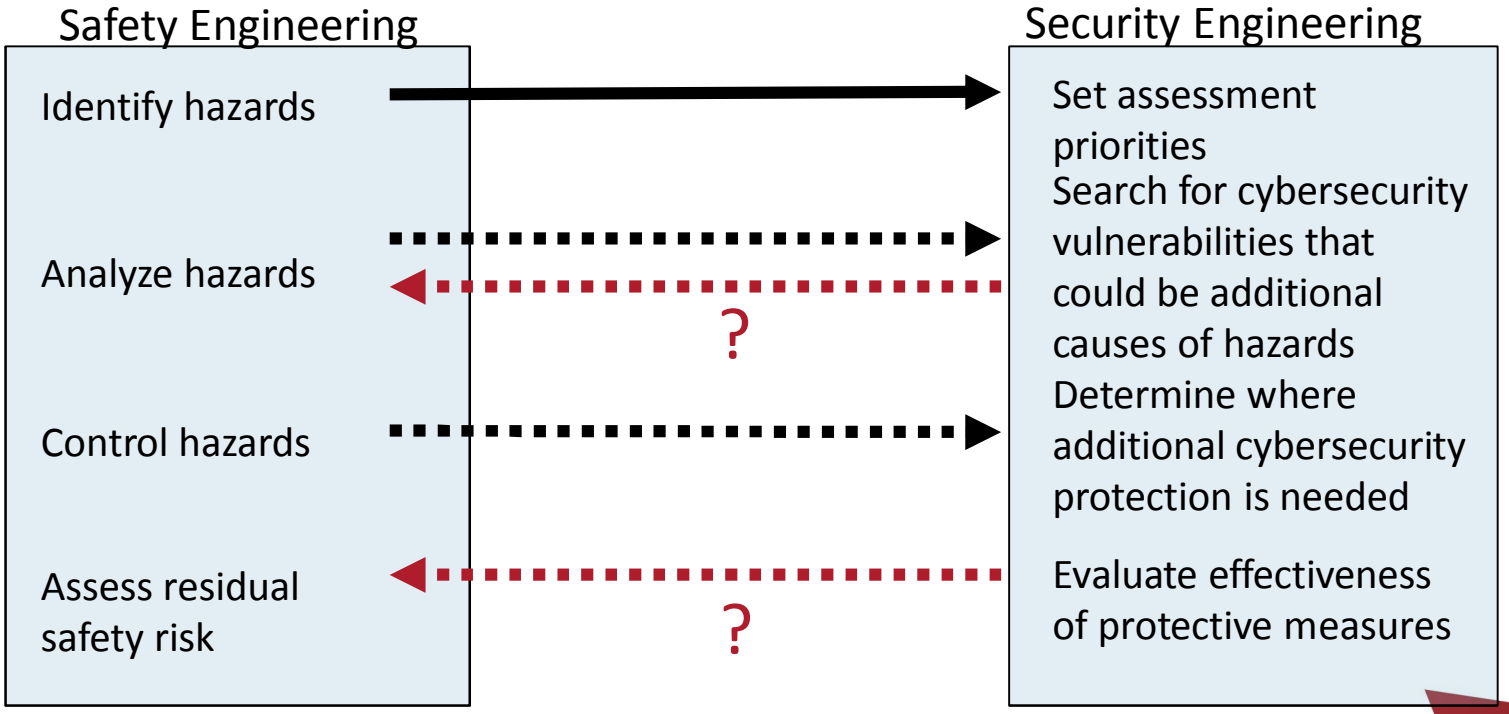
failure condition

Use Safety to Focus Security Assessment on Hazard Causes





Parallel Engineering Processes



Civil Aviation Regulation Context

2006 — Lack of overall airworthiness rules or regulations addressing cybersecurity

Until now — Short term: Issue ad-hoc special conditions

Going forward — Long term: Establish an airworthiness security regulation framework

Not yet — New airworthiness rules; New airworthiness standards to comply with rules

Airworthiness authorities would like to see:

- a cybersecurity risk assessment at the aircraft level
- top-down analysis similar to safety assessment
- synergies between safety assessment and security assessment analysis

Done, i.e., 326A, 355

RTCA DO-326A and DO-355

DO-326A / (ED-202A)	**Airworthiness Security Process Specification**	During development: • Top down risk assessment process with a generic set of activities • A set of security development activities • Interfaces with the safety assessment process
DO-355 / (ED-204)	**Information Security Guidance for Continuing Airworthiness**	During aircraft operation and maintenance: • Airborne Software • Aircraft Components • Aircraft Network Access Points • Ground Support Equipment • Ground Support Information Systems • Digital Certificates • Aircraft Information Security Incident Management

Legislation

SECURITY WEEK
INTERNET AND ENTERPRISE SECURITY NEWS, INSIGHTS & ANALYSIS

Malware & Threats | Cybercrime | Mobile & Wireless | Risk & Compliance | Security Architecture

Home › Vulnerabilities

Proposed Cyber AIR Act Would Force Cybersecurity Standards for Aircraft

By Kevin Townsend on April 08, 2016

"Cyber AIR" Act Would Direct FAA to Establish Cybersecurity Standards for Aircraft

Senator Edward Markey (D-Mass.), Thursday, introduced a proposed new Cyber AIR Act as amendments to the FAA Reauthorization Bill currently being debated by the Senate. His bill follows his own investigation into the security practices of airlines and aircraft manufacturers.

CSL works with clients to …

- adapt processes to comply with standards, e.g., RTCA DO-326A, RTCA DO-355, SAE ARP 4761, RTCA DO-178C
- identify causes of safety risk that result from unrecognized security vulnerabilities
- identify conflicts between safety mitigations and security mitigations which could result in costly changes and delays if not discovered until late in development
- avoid wasteful duplication of effort, e.g., safety engineers searching for security vulnerabilities that are already known to the security specialists
- more effectively allocate resources to mitigate security risks through linkage with the safety process
- gain a competitive business advantage in a world marketplace that is increasingly concerned about security threats

CSL Seeks Innovation Partners to …

- Implement engineering processes in compliance with RTCA DO-326A including details of …
  - Security effectiveness objectives
  - Security effectiveness requirements
  - Security assurance actions
- Improve methods and tools for developing Assurances Cases that combine safety and security evidence
- Develop new tools for Security Logfile Analysis based on formal (mathematical) logic

Questions?

Laurent.Fabre@cslabs.com

Jeff.Joyce@cslabs.com

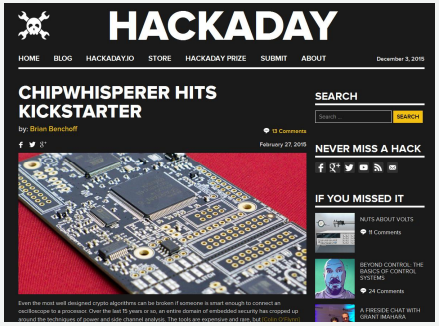
FORUM AEROSPACE INNOVATION

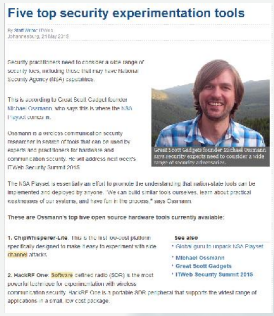
Meeting the Challenges of Cyber security And Hacking To Insure Safety of Aircraft and Embedded Systems

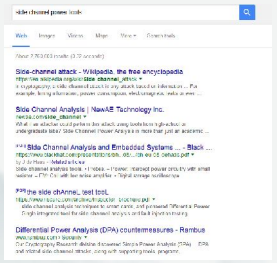
Mr. Colin O'Flynn, CEO, NewAE Technologies

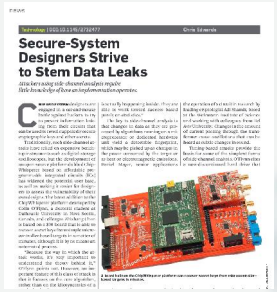
AÉRO MONTRÉAL 10 YEARS

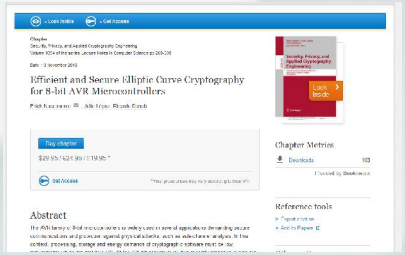
NewAE Technology Inc.







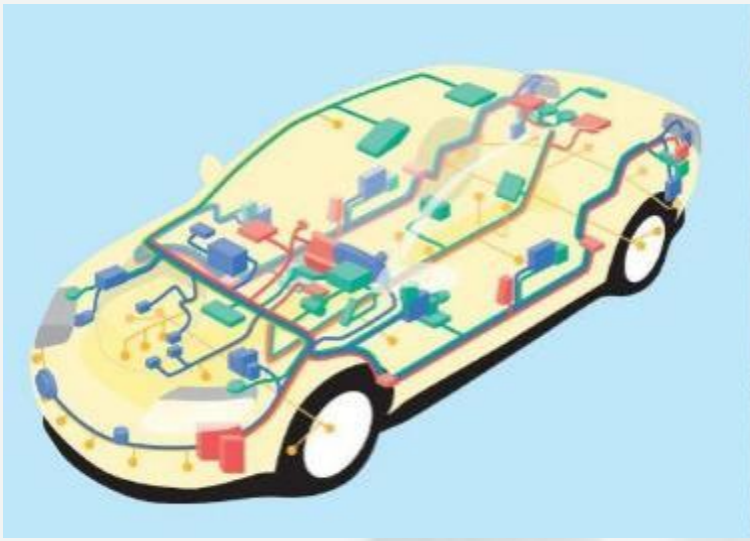




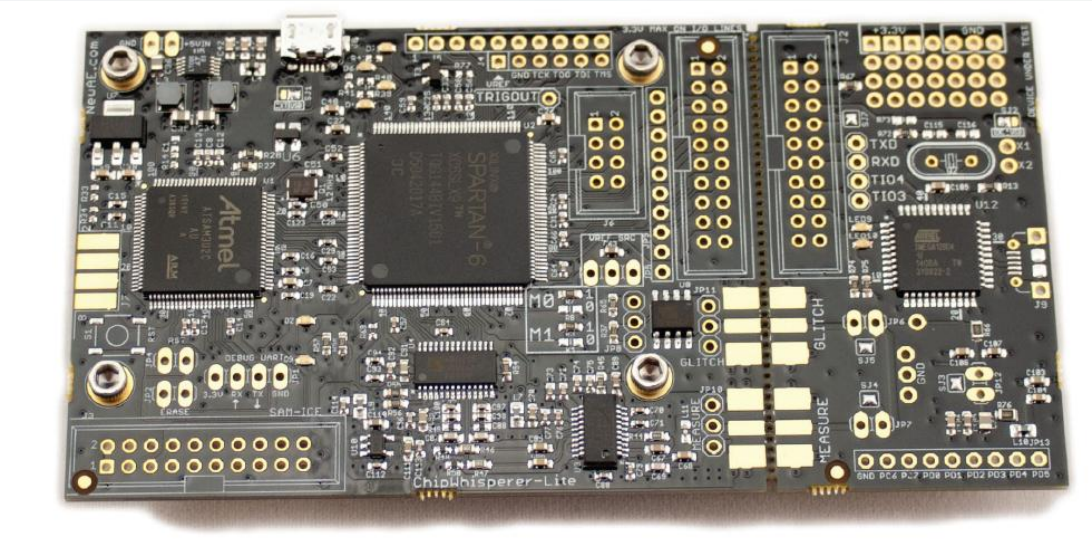
AERO MONTRÉAL 10 ANS

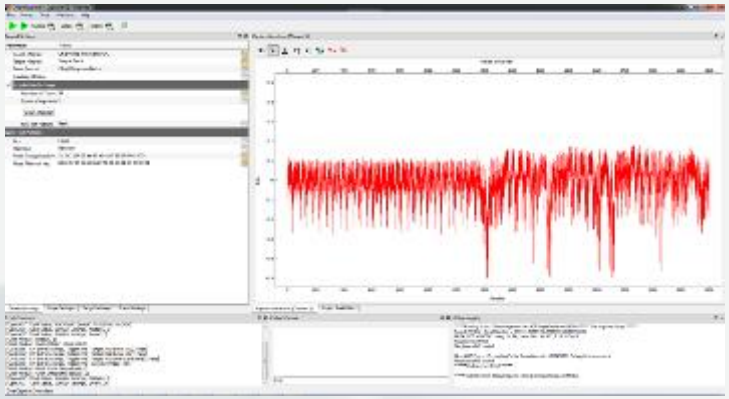
FORUM INNOVATION AÉROSPATIALE

New Threat Models

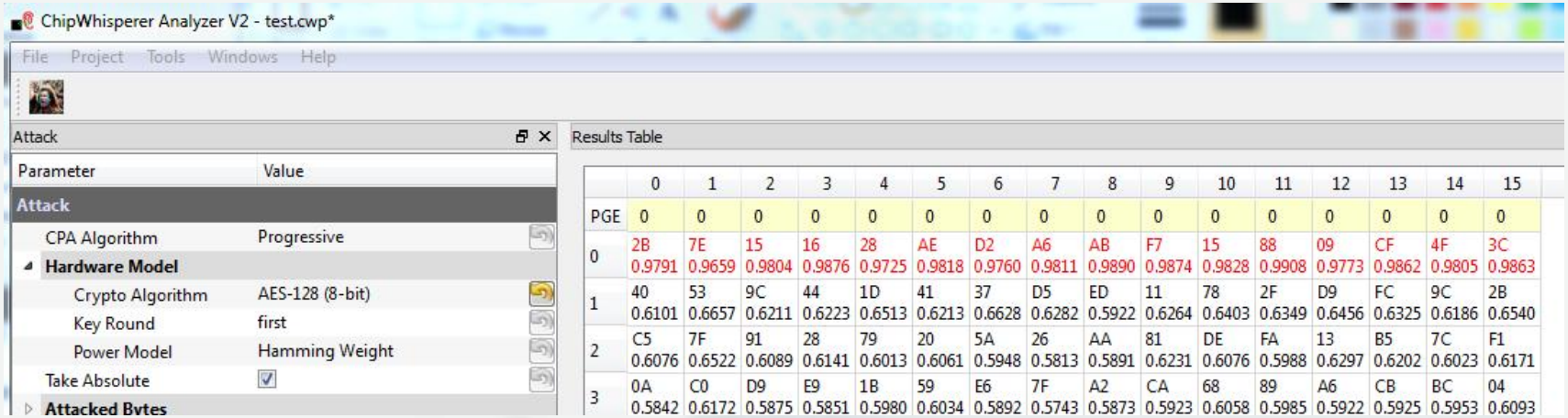


Testing Embedded Systems





Example: Breaking AES-128



	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
PGE	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	2B 0.9791	7E 0.9659	15 0.9804	16 0.9876	28 0.9725	AE 0.9818	D2 0.9760	A6 0.9811	AB 0.9890	F7 0.9874	15 0.9828	88 0.9908	09 0.9773	CF 0.9862	4F 0.9805	3C 0.9863
1	40 0.6101	53 0.6657	9C 0.6211	44 0.6223	1D 0.6513	41 0.6213	37 0.6628	D5 0.6282	ED 0.5922	11 0.6264	78 0.6403	2F 0.6349	D9 0.6456	FC 0.6325	9C 0.6186	2B 0.6540
2	C5 0.6076	7F 0.6522	91 0.6089	28 0.6141	79 0.6013	20 0.6061	5A 0.5948	26 0.5813	AA 0.5891	81 0.6231	DE 0.6076	FA 0.5988	13 0.6297	B5 0.6202	7C 0.6023	F1 0.6171
3	0A 0.5842	C0 0.6172	D9 0.5875	E9 0.5851	1B 0.5980	59 0.6034	E6 0.5892	7F 0.5743	A2 0.5873	CA 0.5923	68 0.6058	89 0.5985	A6 0.5922	CB 0.5925	BC 0.5953	04 0.6093

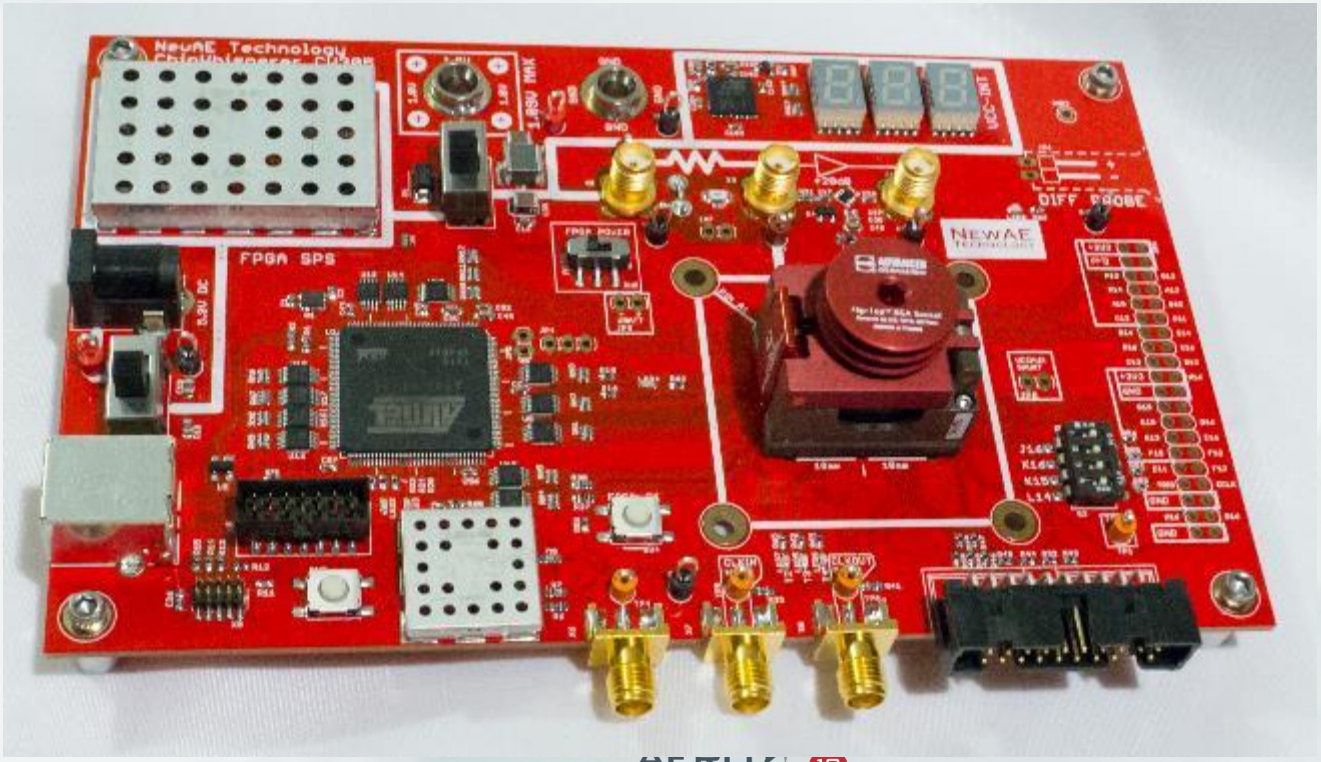
Current Customers

FORUM INNOVATION AÉROSPATIALE

Commercial	Academic	Military/Government
Tesla, Intel, Google, Underwriters Laboratories, Sony	Georgia Tech, FUNCAMP – Fundação de Desenvolvimento da Unicamp, University of Windsor, Université Paris Sorbonne Paris IV, Stanford	Lockheed Martin, Los Alamos National Laboratory Est. 1943, Defence R&D Canada / Défense, SwRI
15% - Company 11% - Individual	30%	44%

AÉRO MONTRÉAL 10 ANS

Future Developments



Meeting the Challenges of Cyber security And Hacking To Insure Safety of Aircraft and Embedded Systems

Mr. José M. Fernandez, Associate professor,
Department of Computer & Software Engineering,
École Polytechnique de Montréal

Meeting the Challenges of Cyber security And Hacking To Insure Safety of Aircraft and Embedded Systems

Mr. Jayson Agagnier, Sr. PKI Specialist, Carillon Information Security Inc.

Aircraft Systems – Safety vs. Security.

- Aircraft are designed to be “safe”
- “Safety” does not equal “security” and “security does not equal “safety”
- The terminology IS NOT interchangeable.
- Guidance material exist for the design of airborne systems.
  - DO-178(B/C) & DO-254
- Guidance material exists for safety.
  - SAE ARP 4754A & ARP 4761
- Guidance material recently published for security.
  - DO-326A, DO-355 & DO-356

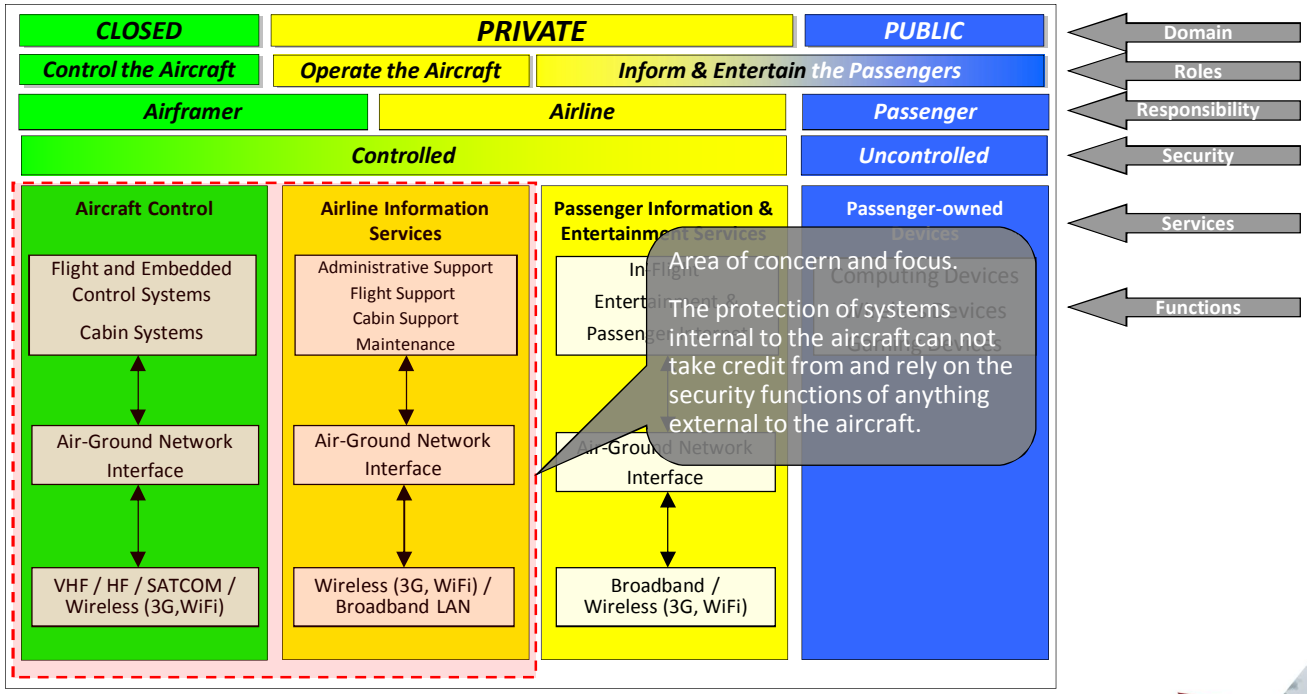
Aircraft Systems – Security Requirements.

- Special conditions related to electronic delivery of software to aircraft becoming increasingly common place.
- Current security methods are complex and impose unnecessary burden on aircraft operators.
- The press is reporting on the perceived risk with little to no understanding of the actual risks.
  - The general public and therefore law makers are becoming increasingly concerned about these risks.

Secure Electronic Delivery of FLS/LSAP to Aircraft Systems – Areas of concern.

ARINC Report 811

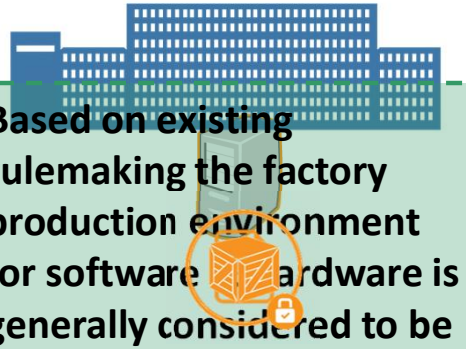
Guidance to describe aircraft operations & maintenance considering security aspects. ARINC 811 depicts aircraft network security domains, major aircraft system, & access properties (closed, private, & public) and users of each domain.



Secure Electronic Delivery of FLS/LSAP to Aircraft Systems.

FORUM INNOVATION AÉROSPATIALE

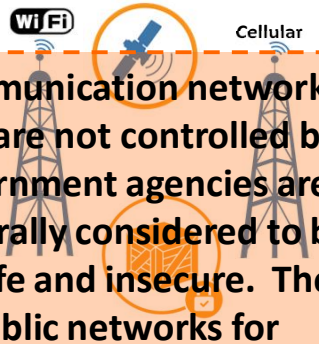
FLS/ LSAP FACTORY ENVIRONMENT



Based on existing rulemaking the factory production environment for software hardware is generally considered to be safe.

The software is placed into a secure IDS environment in the factory prior to delivery to the aircraft using established standards and regulations accepted by the certification authorities.

COMMUNICATION NETWORKS



Communication networks that are not controlled by government agencies are generally considered to be unsafe and insecure. The use of public networks for software delivery to aircraft systems is of great concern by various regulatory authorities around the world.

Software is transmitted via aircraft communication either to the operator network or to the aircraft. Integrity is usually checked against tampering during transmission via insecure networks.

AIRCRAFT ENVIRONMENT

The aircraft is generally considered safe & established rulemaking exists for certain types of software delivery to aircraft systems. Electronic delivery of software to aircraft systems is currently subject to ad-hoc rulemaking via special conditions.

The part is uncrated and installed on aircraft, the security validation is performed by the aircraft system.

The part is uncrated and installed on aircraft system based on established and approved processes and procedures.

AERO MONTREAL 10 ANS

FORUM AEROSPACE INNOVATION

Meeting the Challenges of Cyber security And Hacking To Insure Safety of Aircraft and Embedded Systems

Questions from the host!

AÉRO MONTRÉAL 10 YEARS

FORUM AEROSPACE INNOVATION

Meeting the Challenges of Cyber security And Hacking To Insure Safety of Aircraft and Embedded Systems

Questions from YOU!

AÉRO MONTRÉAL 10 YEARS

Challenges of Cyber security in Safety of Aircraft and Embedded Systems

FORUM AEROSPACE INNOVATION

Thank you!

Manon Gaudet, ***GCED, CCISP, Cert. Cyber-Investigation***

National Research Council of Canada - Industrial Research Aid Program

Manon.gaudet@nrc-cnrc.gc.ca

AERO MONTREAL 10 YEARS