Cybersecurity – A vendors perspective

Architecture, Threat, and Mission

Binny Sarien
Security Design Authority Thales Australia

THALES
Building a future we can all trust

Agenda

Cyber security from a vendors perspective

- Emphasis on deliberate planning (in line with organisational strategy)
- Accurate requirements specification (practical)
- Regional mandates and customer requirements

Key situational awareness aspects

- Architecture and design (peer review is very important)
- Threat modelling (it assists with risk based decision making)
- Critical Vs Non Critical aspects based on mission objectives

A robust cyber security solution

- Balance technical solution and robust procedures (cost benefit analysis)
- Cybersecure-by-design - security aspects present from the beginning
- Ongoing cyber services

THALES
Building a future we can all trust

Cybersecurity is in Thales DNA

As a **leader in cyber security** and the **worldwide leader in data protection,**
Thales addresses the entire information security lifecycle, the cornerstone of **digital trust.**

5 000
CYBERSECURITY SPECIALISTS

5 CYBERSECURITY OPERATIONS CENTRES
+
5 DATA CENTRES

Security for
19 of the 20
LARGEST BANKS

High grade
DATA SECURITY
solutions for
50
COUNTRIES
INCL. NATO COUNTRIES

Operation and cybersecurity of critical information systems for over
130
CUSTOMERS

Cybersecurity for
9 of the top 10
INTERNET GIANTS

80%
protection of the world
PAYMENT TRANSACTIONS

Security for
4 of the biggest 5
OIL COMPANIES

THALES
Building a future we can all trust

Unique expertise in both ATM & Cybersecurity

The strength of a global vision combining

ATM Operational Technology (OT) and Information Technology (IT) cybersecurity

Expertise & consulting services

- Education & Training
- Risk Assessment
- Roadmapping

Operational Services

- Detection & monitoring
- Security Operations Center
- Rapid Reaction Team

Products & Systems

- Probes & multilevel Gateways
- Analytics platform
- Identity Management System
- Cybersecure architecture

THALES
Building a future we can all trust

Cyber Security Implementation – Vendor Perspective

- Vital that cyber security aspects are included in overall strategic objectives of the project
  - Security objectives should be clearely defined and agreed
  - Changing security requirements half-way leads to of complications (cost/engineering)
- No Gold standard cyber security template that can be tagged on at the end of the strategic planning
  - Cyber security solutions must be specific to strategy, operating environnent and resources available
  - Expectation management from security tools perspective
- Cyber security requirements need to be realistic
  - What are the constraints? budget/skillset/performance
  - Risk based approach (security vs safety)
- ATM infastructure should comply with the national security authority
  - To be taken into account during requirements gathering
  - Good to establish liaison early and bring them along on the journey

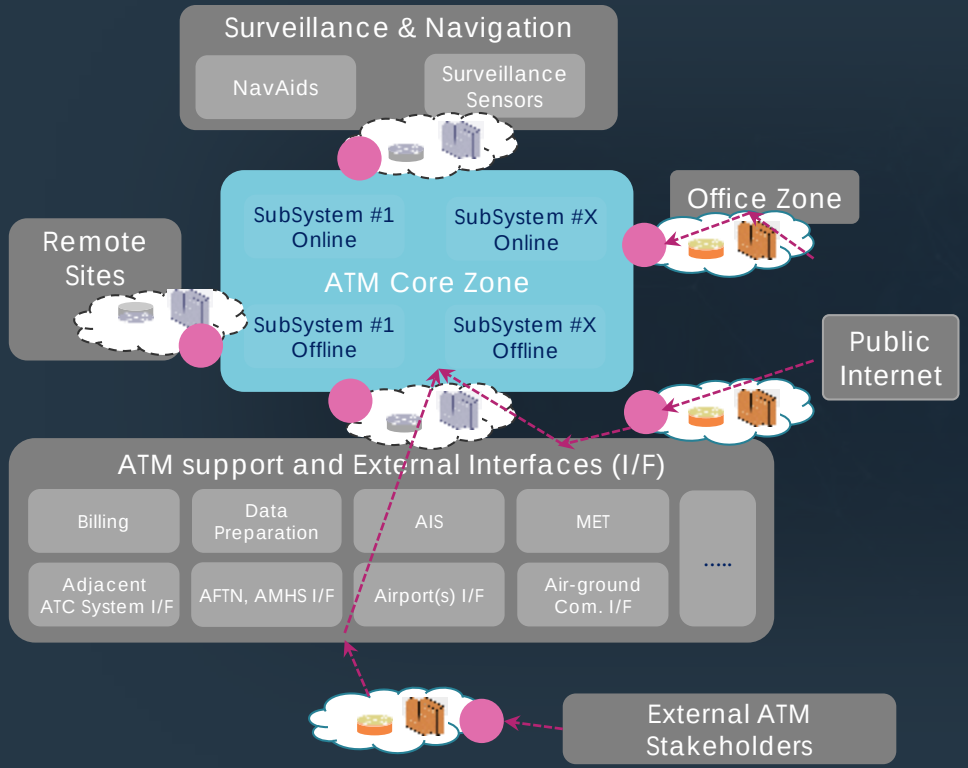
THALES
Building a future we can all trust

Cyber Security Situational Awareness

Architecture – Network Awareness

- Design discipline and Asset management
- Operational Technology Vs Information Technology
- Routine Vulnerability auditing & management
- System Development Life Cycle
- Applicable security control
- Control testing
- Network Zoning

Zone concept applied to ATM



Assessment points

Refined with the ANSP considering

- Trusted/Untrusted zones
- Security policies including isolations between zones
- Safety objective

Cyber Security Situational Awareness

Threat Awareness

- Threat modelling (internal / external – various techniques attack trees / STRIDE etc)
- Developing indicators of warning
- Liaising with cross-industry and cross-government communities (information sharing)
- Purple Teaming
- Very important for making risk-based decisions.

Asset to Threat mapping - STRIDE model

Firmware	Certificates & keys	Credentials	Network Communication	Configuration	Voice Records	Event logs	Device Resources
Code injection (T)	Replace certificate (TE)	Admin impersonation (SRIE)	Impersonation (SRIE)	Tamper config (T)	Tamper records (T)	Tamper system time (TR)	Debug port abuse (TI)
Reverse engineering (I)	Side channel analysis (I)	Replace credentials (T)	Tamper Package (T)	Impersonation (SI)	Impersonation (SI)	Impersonation (SI)	Eavesdropping busses (I)
Break secure state (TIE)	Corrupt certificate (TD)	Side channel analysis (I)	MITM (RI)	Device Disconnected (TD)	Unauthorised access (IE)	Supress / Erase events (TR)	Abuse resources (DE)
FW corruption (TD)		Corrupt certificate (TIE)		Unauthorised Access (IE)		Unauthorised access (IE)	
Escalation of privilege (IE)							

- S Spoofing of user identity
- T Tampering
- R Repudiation
- I Information Disclosure
- D Denial of Service
- E Elevation of Privilege

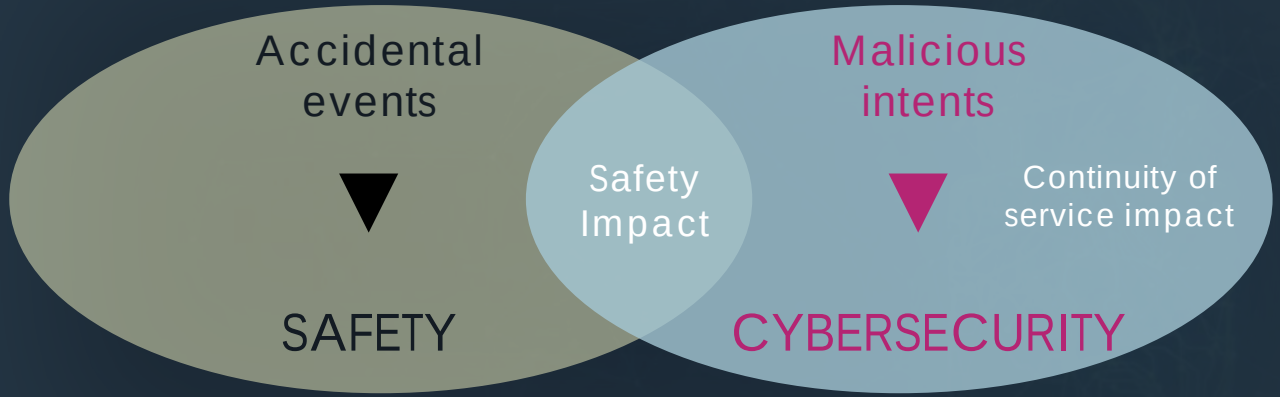
THALES
Building a future we can all trust

Cyber Security Situational Awareness

Mission Awareness

- Create a common and comprehensive picture of the critical dependencies
- Test security tools with critical functions (safety/performance)
- If cannot block, then ensure that you can record and monitor (appropriate incident response)
- Communication flow in case of an incident

What makes a good solution? Cybersecurity objective



THALES
Building a future we can all trust

Summary

Cyber objectives aligned with organisation, national requirements, and risk appetite.

System of Systems approach

Maintain cyber security situational awareness

- Architecture
- Threat intelligence & management
- Mission critical objectives
- Training and congingency planning

Thank you

Binny Sarien Binny.Sarien@thalesgroup.com.au