THALES

ISO 26262 Practitioners Workshop

Automotive Security and Cross Sector Learning

Peter Davies - Thales

26TH JANUARY 2017

What I will talk about?

- What is a Vehicle
- Cyber Threats
- The Attack Surface
- Security and Safety
- Legal and Liability Approaches
- So what does this Mean?

- Syntax v Semantics in Cyber Security
- Federated Liability
- The Inability to reverse out once benefits have been taken
- Speed of Remediation

THALES

Characteristics of an Automotive What am I going to Conclude?

1. **Distributed:** An Automotive System must be seen as inherently and increasingly a Federated Safety Critical System which is not owned by a single entity.

2. **Bottom Up:** Particularly with respect to Safety, data, system and component owners must be in a position to make statements about their own part of the system.

3. **Defensive:** It will not simply be good enough in the face of a cyber attack to say that the 3rd party originator was authorised to make that request it will also be necessary to understand that request to have been reasonable.

4. **Reactive:** Once value has been taken, failure to understand the 'clean up' process will open the system to cyber blackmail.

THALES

How do we do Security / Safety

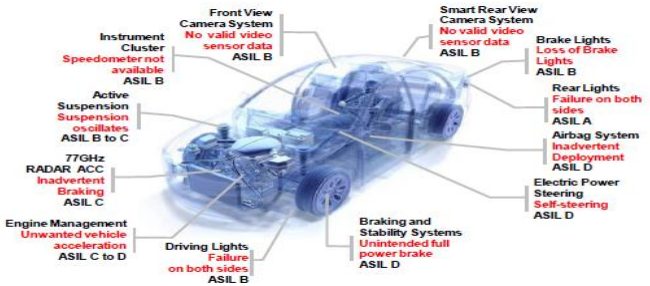
- Basic Strategy
  - Defend the trusted core
  - Restrict Access
  - Analyse in Depth
  - Strength to withstand a prolonged siege by a determined attacker.

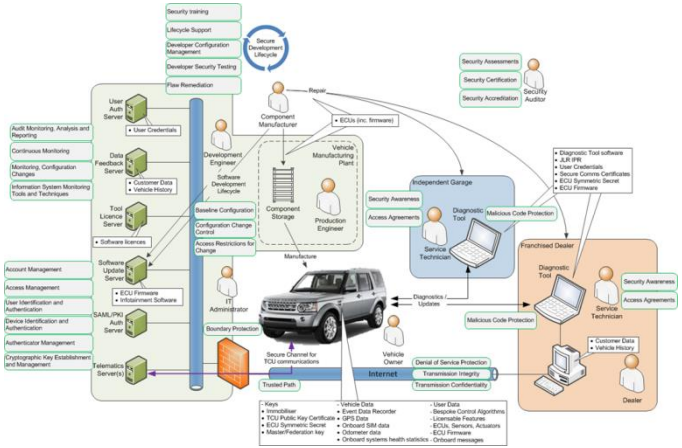
- Strongpoints
- Protected inter strongpoint supply routes
- Proactive attack against threats

THALES

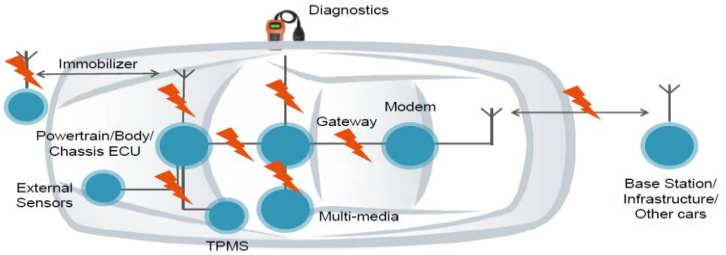
How do we do Security / Safety

- Basic Strategy
  - Defend the trusted core
  - Restrict Access
  - Analyse in Depth
  - Strength to withstand a prolonged siege by a determined attacker.





- Strongpoints
- Protected inter strongpoint supply routes
- Proactive attack against threats



THALES

Security Techniques and what they are used for?

The field of computer security lacks the rigorous experimental methods and data analytic processes which would enable it to understand such issues as fundamental principles and causalities, to predict where and when innovations will work, and to determine how successful tools and policies can be generalized[1]

- Signatures.
- Encryption.
- Roots of Trust
- Hashes
- Code Signing
- Code Authenticity.
- Supply Chain Control.
- Message and Information Integrity.
- Bandwidth Protection
- Data Privacy

What happens when one of your clients Roots of trust is hacked?

Security is not a useful concept it is more normal to speak of the certainty with which a desired characteristic is achieved.

The inability to make numerically significant claims in the face of cyber attacks is the major impediment to sustainably realising the benefits of digitisation.

1. Security is about Control: Insights from Cybernetics MIT Lincoln Labs

THALES

Threats?

- Resource Exhaustion.
- Breaching of Boundaries.
- Denial of Service

- Programming Techniques
  - Data Driven
  - Program Driven

- Gaps in Analysis

- Rejection at the Boundary vs rejection in the core.

- Supply Chain Control.

- Message and Information Integrity.
- Bandwidth Protection

- Data Privacy

Who is Responsible for Having a Cyber Safe System

Data Protection / Privacy

- Responsible Authority External:
  - eg. Information Commissioner
- Legally Recognised Authority Internal:
  - Data Controller
- Typical Standards that might apply:
  - ISO27001,
  - FIPS 140,
  - Common Criteria,
  - Cyber Essentials

Cyber Requirements are in conflict with each other

Confidentiality
Integrity
Authenticity

Safety

- Responsible Authority External:
  - Criminal Courts
  - Civil Courts
- Legally Recognised Authority Internal:
  - Safety Engineer
- Typical Standards that might apply:
  - ISO26262

Confidentiality
Integrity

Business Advantage

- Responsible Authority External:
  - Criminal Courts
  - Civil Courts
- Responsible Authority Internal:
  - None
- Typical Standards that might apply:
  - None as yet

So What Is a Cyber Threat?

A Cyber Threat is not Statistically Neutral

- Traditional Safety cases (10^{-9} etc.) are based on statistically neutral assumptions
- A cyber attack will identify a case that arises 0.0001% of the time and exploit it 100% of the time.

A Cyber Threat will Not Align With Your Defences

- Automated tools will / may assist with the analysis of your code and hardware.
- A cyber attack will use those elements that you were forced to consider out of scope.

THALES

So What Is a Cyber Threat?

- **Statistically Neutral Failures** – typically this will include correct specification and coding implemented controlled hardware.
- The analysis techniques for this are relatively established including standards such as MISRA-C, CERT and others and have established tools to allow and facilitate their inclusion into a numerically significant safety case.
- Where safety is a consideration then the numerical calculations (or their rough equivalent) look at the likelihood of failures occurring naturally; for the automotive sector typically this will be embodied in a 26262 analysis ie. the data security analysis must form part of not be separate from the safety case .
- Where the consideration is not specifically deemed relevant to safety, as might be the case with personal information or low level ADAS for instance numeric calculations (or their rough equivalent) are unlikely to be required though international directives and other industry requirements may mandate adherence to security standards such as PCI, FIPS-140, and Common Criteria depending on the use to be made of the data.

So What Is a Cyber Threat?

- **Non-Statistically Neutral Attacks** – typically this includes what are known as Cyber Attacks which focus on known or as yet unknown failures that can be created or exploited to have an effect.
- Where safety is a consideration then the calculations would in this case need to focus on the effect of directed exploits rather than the likelihood of failures occurring naturally. This may well undermine a case that has been made with a probability of 10^{-9} to one that may only be sustainable at or less 10^{-4} … in the worst case 0.
- In addition data security threats falling into this category have the potential to redefine all parts of the connected system (On-Board and Off-Board) to be safety critical (ASIL3).
- **There is currently no commonly agreed methodology for addressing this aspect of data security and particularly its consequence for the safety case of critical functions that can be directly applied to a sector having the characteristics of the Automotive Sector (scale, pace, cost etc.).**
- **Furthermore it is unlikely that such a methodology (mooted ISO, SAE etc.) would emerge and be legally sustainable in the timeframe that they are needed.**

THALES

So What Is a Cyber Threat?

- In particular we note that many of the techniques that we have been told are important in achieving higher SAE levels (data driven, data fusion, AI and cybernetics) will inherently bring larger proportions of the connected code base into scope for analysis with respect to its safety implications.

- Being able to correctly analyse and successfully and subsequently bring forward the projected benefits will involve a careful understanding of how systems may viably and properly be segmented and safely operated. In particular this involves understanding how critical parts of the system may protect themselves in such a way that, at the level of information and data, they may continue to operate safely and with no 'common mode failure' in the face of other parts of the system that are fatally compromised; ie. in the case of a POD it simply cannot be a requirement for safe operation that the Off-Board system for ordering and delivering services is written and maintained to safety critical

So What Does This Mean?

1. **Distributed:** An Automotive System must be seen as inherently and increasingly a Federated Safety Critical System which is not owned by a single.

2. **Bottom Up:** Particularly with respect to Safety, data, system and component owners must be in a position to make statements about their own part of the system.

3. **Defensive:** It will not simply be good enough in the face of a cyber attack to say that the 3rd party originator was authorised to make that request it will also be necessary to understand that request to have been reasonable.

4. **Reactive:** Once value has been taken, failure to understand the 'clean up' process will open the system to cyber blackmail.

THALES

THALES