THALES

Building a future we can all trust

Verification and Legal Consequence

VeTSS Annual Event 21.05.2024

Peter Davies – Directory Security Concepts

OPEN

Who am I, Where do I Come from, Why should you listen …

Peter Davies

Thales

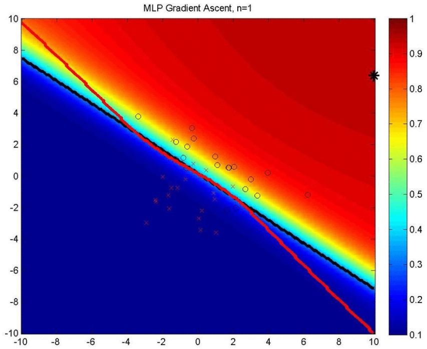
I am

- A Security Expert
  - 2000+ exploits in the automotive domain.
- Specialized in the convergence of Safety and Security
- Leading Expert on
  - Countering Cyber Attacks targeted Supply Chain Infiltration
  - Cyber Physical Attacks
  - Leader of:
    - 5 Cyber Security aspects of CAV research activities
    - 2 Hardware Security
- 39+ years of verifying security systems
- I do security where it can't afford to fail

Open

What I Will Talk About

- Challenges of verification in large scale, composed systems … particularly in the face of cyber-attacks
- Progress with methods used to provide legally sustainable arguments
- Reimagining where tools are used

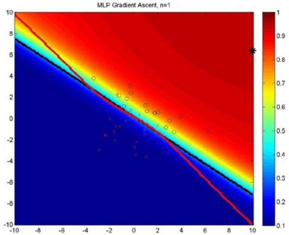


Open

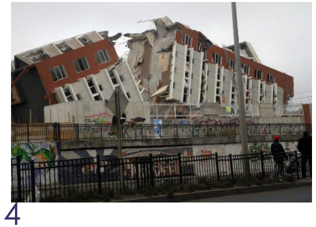
Some Observations …

“A System is Resilient if, and only if, there is justifiable and enduring confidence that it will function as expected, when expected”

- ➢ **Security professionals are particularly bad at describing the quality of mechanisms without ever concerning itself with their effectiveness ;**



- ➢ **Security involves understanding what you have and how it will fail. Poisoning and evasion attacks are not new but essential to understanding Machine learning and AI ;**



- ➢ **How making a system strong against one type of event will make it brittle against others;**

Open

THALES

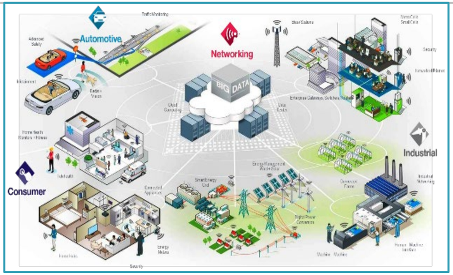
Framing Remarks – The Problem …

We have never before attempted to achieve anything that mattered in a system of the scale and complexity of the one we are now relying on.

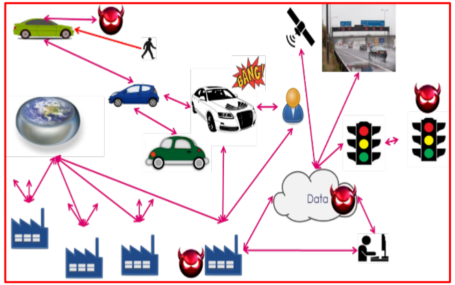
- A complex, hyper-connected, bottom-up system with emergent properties for which there is no guiding mind.

- A system yielding its benefits at scale.
- Price sensitive, worldwide and mobile system with vast amounts of data.
- Owned by no one but in it both strict and contract liability apply and must coexist.
- Multi vendor with legal obligations not to exclude suppliers from the supply chain.
- Increasingly integrated with global information and management networks.

- Intertwined and interconnected components which interact.
- Adaptive behaviour according to history or feedback
- Self organization
- Emergence which is not always predictable, centrally controlled or engineered
- Constantly changes appearing dispositional and lacking causality
- Extreme 'cascading' behaviour, power laws can be observed – minor input changes can result in major output changes.



Who's the defendant, liable, the plaintiff and what court and where?



Framing Remarks – The Problem …

We have never before attempted to achieve anything that mattered in a system of the scale and complexity of the one we are now relying on.

CHAOS

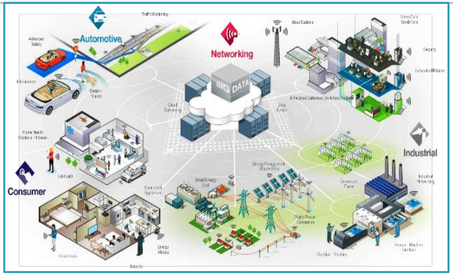
Branch of mathematics that deals with complex systems whose behavior is highly sensitive to slight changes in conditions, so that small alterations can give rise to strikingly great consequences.

- Owned by no one but in it both strict and contract liability apply and must coexist.
- Multi vendor with legal obligations not to exclude suppliers from the supply chain.

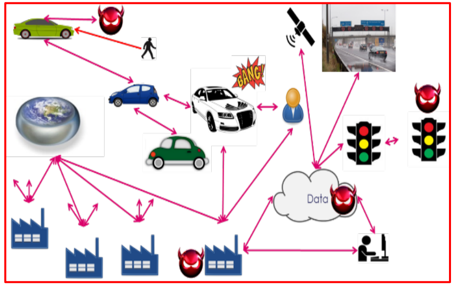
EMERGENCE

Properties that arise from the interactions of the parts of a complex system, but do not belong to any individual part. They are unexpected and unpredictable based on the knowledge of the individual parts alone.

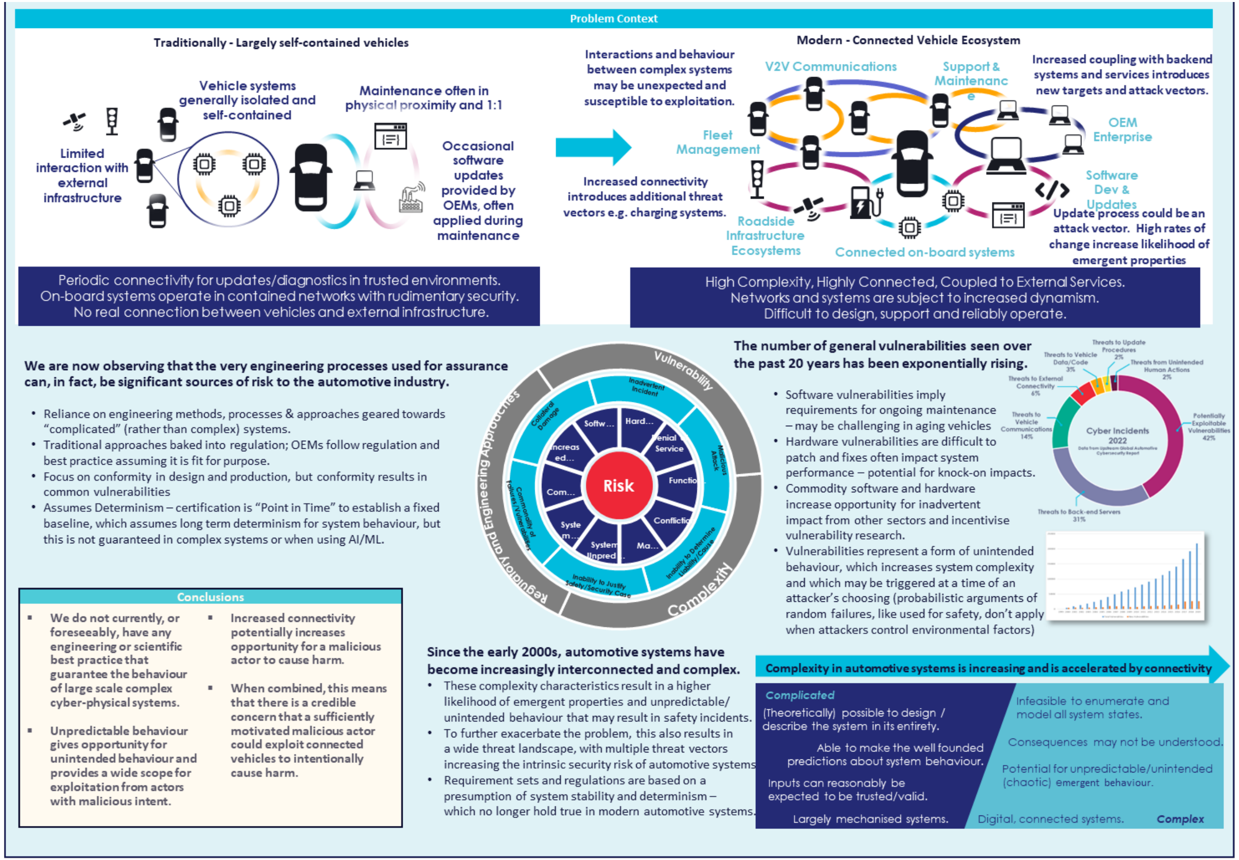
- Emergence which is not always predictable, centrally controlled or engineered
- Constantly changes appearing dispositional and lacking causality
- Extreme 'cascading' behaviour, power laws can be observed – minor input changes can result in major output changes.



Who's the defendant, liable, the plaintiff and what court and where?



What an attack looks like …



Problem Context

Traditionally - Largely self-contained vehicles

Vehicle systems generally isolated and self-contained
Maintenance often in physical proximity and 1:1
Limited interaction with external infrastructure
Occasional software updates provided by OEMs, often applied during maintenance

Periodic connectivity for updates/diagnostics in trusted environments.
On-board systems operate in contained networks with rudimentary security.
No real connection between vehicles and external infrastructure.

Modern - Connected Vehicle Ecosystem

Interactions and behaviour between complex systems may be unexpected and susceptible to exploitation.
V2V Communications
Support & Maintenance
Increased coupling with backend systems and services introduces new targets and attack vectors.
OEM Enterprise
Fleet Management
Increased connectivity introduces additional threat vectors e.g. charging systems.
Software Dev & Updates
Update process could be an attack vector. High rates of change increase likelihood of emergent properties
Roadside Infrastructure Ecosystems
Connected on-board systems

High Complexity, Highly Connected, Coupled to External Services.
Networks and systems are subject to increased dynamism.
Difficult to design, support and reliably operate.

We are now observing that the very engineering processes used for assurance can, in fact, be significant sources of risk to the automotive industry.

- Reliance on engineering methods, processes & approaches geared towards "complicated" (rather than complex) systems.
- Traditional approaches baked into regulation; OEMs follow regulation and best practice assuming it is fit for purpose.
- Focus on conformity in design and production, but conformity results in common vulnerabilities
- Assumes Determinism – certification is "Point in Time" to establish a fixed baseline, which assumes long term determinism for system behaviour, but this is not guaranteed in complex systems or when using AI/ML.

The number of general vulnerabilities seen over the past 20 years has been exponentially rising.

- Software vulnerabilities imply requirements for ongoing maintenance – may be challenging in aging vehicles
- Hardware vulnerabilities are difficult to patch and fixes often impact system performance – potential for knock-on impacts.
- Commodity software and hardware increase opportunity for inadvertent impact from other sectors and incentivise vulnerability research.
- Vulnerabilities represent a form of unintended behaviour, which increases system complexity and which may be triggered at a time of an attacker's choosing (probabilistic arguments of random failures, like used for safety, don't apply when attackers control environmental factors)

Cyber Incidents 2022
Data from Upstream Global Automotive Cybersecurity Report
Potentially Exploitable Vulnerabilities 42%
Threats to Back-end Servers 31%
Threats to Vehicle Communications 14%
Threats to External Connectivity 6%
Threats to Vehicle Data/Code 3%
Threats to Update Procedures 2%
Threats from Unintended Human Actions 2%

Conclusions

- We do not currently, or foreseeably, have any engineering or scientific best practice that guarantee the behaviour of large scale complex cyber-physical systems.
- Unpredictable behaviour gives opportunity for unintended behaviour and provides a wide scope for exploitation from actors with malicious intent.
- Increased connectivity potentially increases opportunity for a malicious actor to cause harm.
- When combined, this means that there is a credible concern that a sufficiently motivated malicious actor could exploit connected vehicles to intentionally cause harm.

Since the early 2000s, automotive systems have become increasingly interconnected and complex.

- These complexity characteristics result in a higher likelihood of emergent properties and unpredictable/ unintended behaviour that may result in safety incidents.
- To further exacerbate the problem, this also results in a wide threat landscape, with multiple threat vectors increasing the intrinsic security risk of automotive systems
- Requirement sets and regulations are based on a presumption of system stability and determinism – which no longer hold true in modern automotive systems.

Complexity in automotive systems is increasing and is accelerated by connectivity

Complicated

(Theoretically) possible to design / describe the system in its entirety.

Able to make the well founded predictions about system behaviour.

Inputs can reasonably be expected to be trusted/valid.

Largely mechanised systems.

Infeasible to enumerate and model all system states.

Consequences may not be understood.

Potential for unpredictable/unintended (chaotic) emergent behaviour.

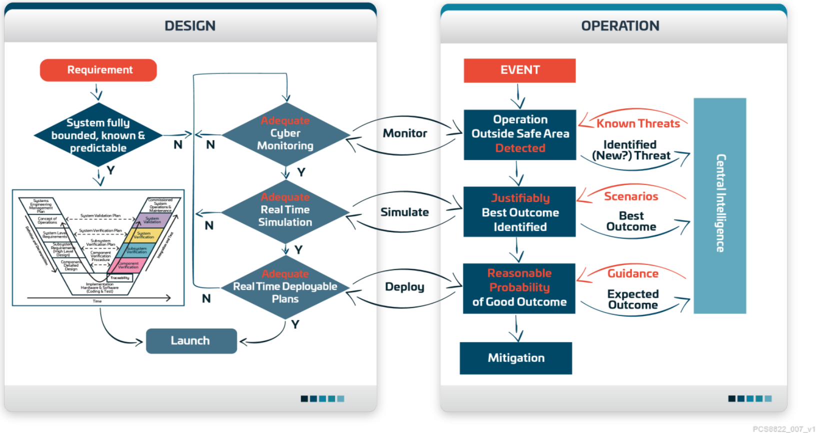
Digital, connected systems.

Complex

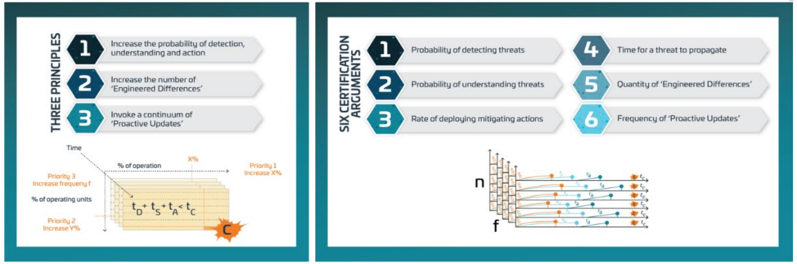
A Methodology for Resilience …

CyRes is an operational methodology, suitable for standardisation, for which:

- **The methodology itself** is capable of being tested in court or by publicly appointed regulators.
- **Operators** understand what evidence should be produced by it and are able to measure the quality of that evidence.
- **The evidence produced** is capable of being tested in court or by publicly appointed regulators.



DESIGN
Requirement
System fully bounded, known & predictable
N
Y
Systems Engineering Management Plan
Concept of Operations
System Level Requirements
Subsystem Requirements (High Level Design)
Component Detailed Design
Implementation Hardware & Software (Coding & Test)
Traceability
Component Verification
Subsystem Verification
System Verification
System Validation
Commissioned System Operations & Maintenance
System Validation Plan
System Verification Plan
Subsystem Verification Plan
Component Verification Procedure
Definition and Decomposition
Integration and Test
Time
Launch
Adequate Cyber Monitoring
Adequate Real Time Simulation
Adequate Real Time Deployable Plans
N
Y
OPERATION
EVENT
Monitor
Simulate
Deploy
Operation Outside Safe Area Detected
Justifiably Best Outcome Identified
Reasonable Probability of Good Outcome
Mitigation
Known Threats
Identified (New?) Threat
Scenarios
Best Outcome
Guidance
Expected Outcome
Central Intelligence
PCS8822_007_v1



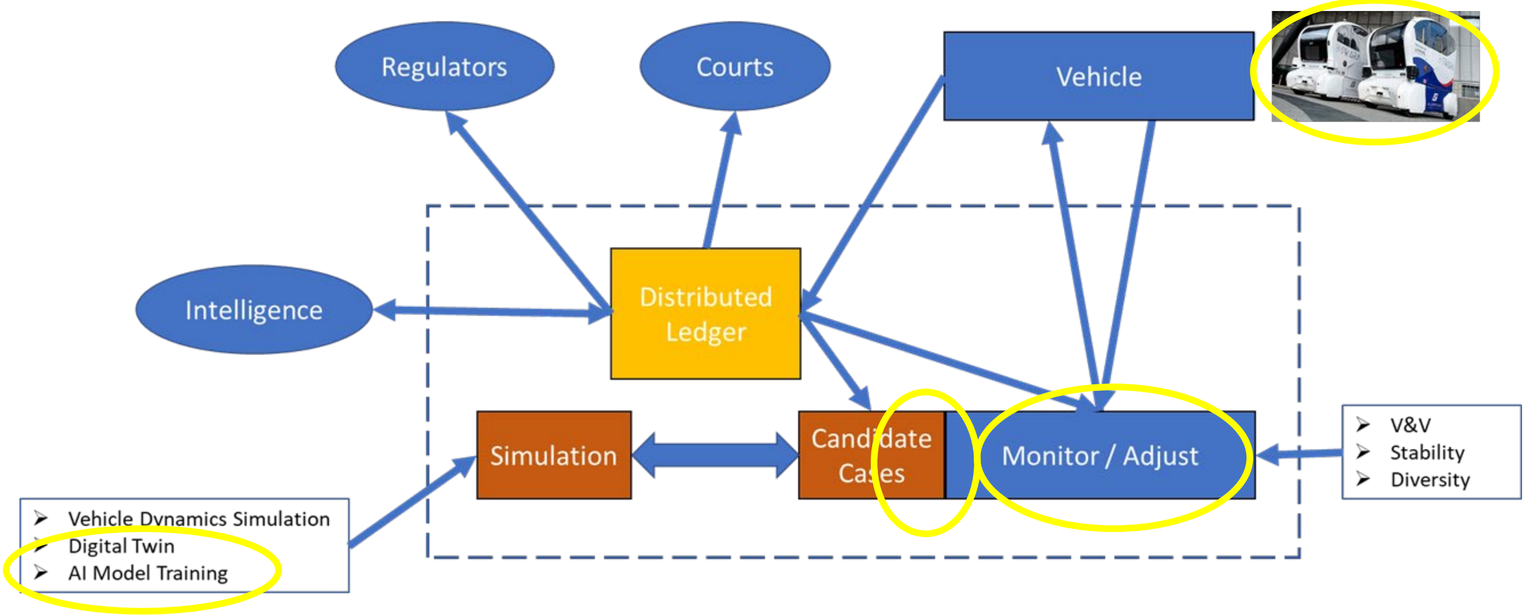
THREE PRINCIPLES
1 Increase the probability of detection, understanding and action
2 Increase the number of 'Engineered Differences'
3 Invoke a continuum of 'Proactive Updates'
Time
% of operation
X%
Priority 1 Increase X%
Priority 3 Increase frequeny f
% of operating units
Priority 2 Increase Y%
$t_D + t_S + t_A < t_C$
C
SIX CERTIFICATION ARGUMENTS
1 Probability of detecting threats
2 Probability of understanding threats
3 Rate of deploying mitigating actions
4 Time for a threat to propagate
5 Quantity of 'Engineered Differences'
6 Frequency of 'Proactive Updates'
n
f
r_a
t_c

CYBER RESILIENCE = FUNCTION (P_D, P_U, r_a, t_c, n, f)

PCS8822_032_v1

Open

…. And Its Use In Practice …



There are two main elements of admissibility: the physical element (the artefact) and the process (technical) by which the artefact has been handled.

'Digital forensics is meant to be based on science, not supposition'

One of the key tenets of any operational Cyber Resilient methodology must be that it should generate evidence in a style and of form that can be taken to court.

What an attack looks like …

Successful Cyber Attacks Against 5G Systems :

- Contradictions that may arise in the data stream
- Denial of Service – Cycles, processing out of bounds, timing
- Non-Determinism – Arbitration between Complex Algorithms with no ground truth
- Transition Analog / Digital
- Technology Interaction e.g. error correction as input to ML
- Attack Detection & Attack Management (Function and Control)

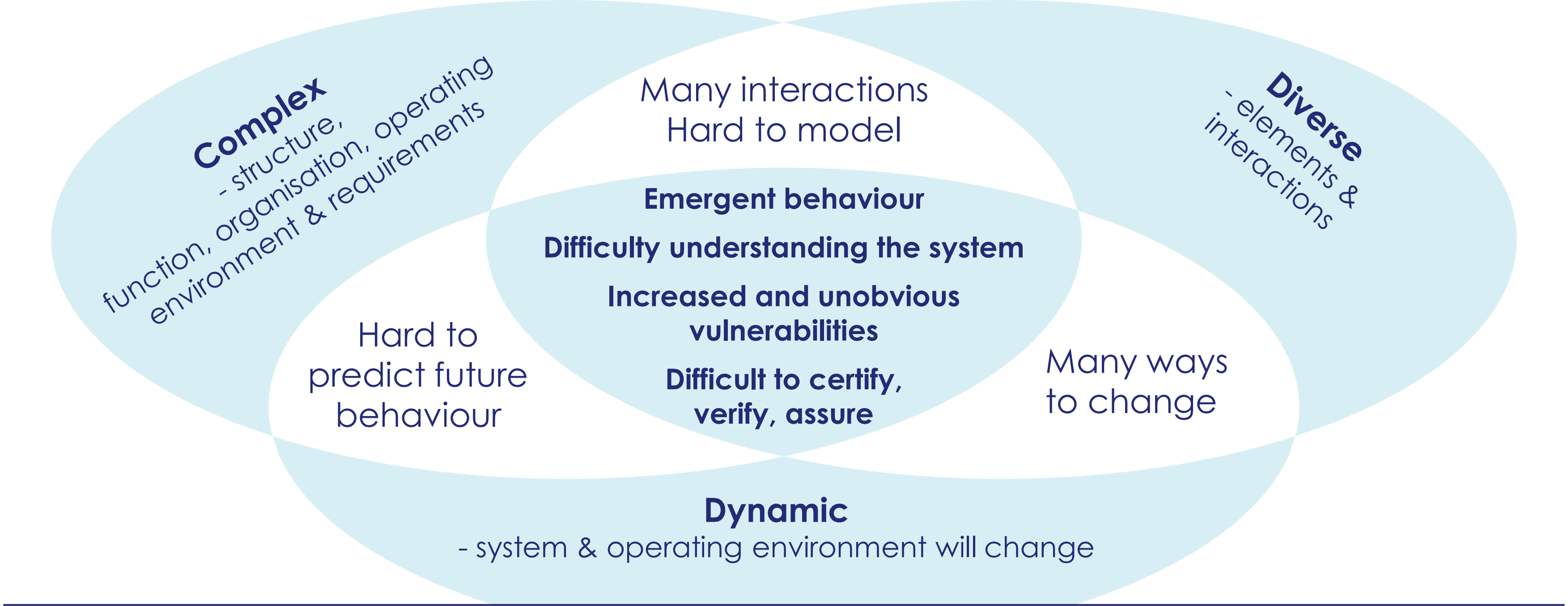
Method: Attack under controlled conditions

Attack Vectors Against 5G O-RAN Systems :

- Failure Modes - Components interact by ICDs and / or SLAs these specify positive requirements but behaviour under failure cannot be exhaustively specified.
- It is practically impossible to deliver a contractually binding commitment to an absolute level of quality under a network slice.
- Encryption makes systems vulnerable to DoS by eg. key exhaustion.

- **Method: Attack under controlled conditions**

Complex dynamic system (CDS) properties and consequences



Complex
- structure, function, organisation, operating environment & requirements

Diverse
- elements & interactions

Dynamic
- system & operating environment will change

Many interactions
Hard to model

Hard to predict future behaviour

Many ways to change

Emergent behaviour

Difficulty understanding the system

Increased and unobvious vulnerabilities

Difficult to certify, verify, assure

Impossible or financially impossible to address everything at design time. Operational performance, safety, security & resilience is required.

Resilience, Methods and Evidence …

One of the key tenets of any operational Cyber Resilient methodology must be that it should generate evidence in a style and of form that can be taken to court.

There are two main elements of admissibility: the physical element (the artefact) and the process (technical) by which the artefact has been handled.

'Digital forensics is meant to be based on science, not supposition'

Cyber is Not Academic - And The Law Is …

Criminal Law

- **Purpose: <u>punitive</u> + deterrent (**for breaching a specified requirement to protect others/society)
- State vs legal person (organisation) or natural person (individual): 'vertical' + adversarial
- Key stages:
  - ➢ Investigation
  - ➢ Prosecution
  - ➢ Punishment/sanction
- Who?
  - ➢ Legislators
  - ➢ Police
  - ➢ Regulators
  - ➢ Criminal Courts – Judges (sometimes juries)
- Probability and '*how safe?*' (inc HSWA issues)

Civil Law

- **Purpose: restorative** and (where necessary) **compensatory**
- Govern legal relations between persons (legal and/or natural): 'horizontal' + adversarial
- Examples:
  - ➢ Commercial or personal contracts
  - ➢ Obligations of road users to each other
  - ➢ Civil obligations arising under statute or regulations
  - ➢ Insurance contracts (*n.b. can't insure against criminal penalties)*
- Civil Courts and Tribunals
- Arbitration/Adjudication etc
- *[Civil 'penalties' – a hybrid]*

Potential for parallel criminal and civil risks arising from same factual event
Your Cyber Resilience Strategy Must Be Robust In The Face Of Both Of These and Internationally

Resiliency based approach to performance, safety & security

- **Maximise performance**
- **Minimise harm and damage resulting from faults, failures, attacks**
- **Evidence to achieve regulatory compliance**
- **Evidential standard for use in a Court of Law**

- **Generalised approach to safety rather than specific issue safety**
  - Impossible to remove all faults and failures from a Complex Dynamic System
  - Impossible to prevent all cyber attacks

- **What the system does when failure occurs becomes a priority**
  - Focus on resilience and the control of harm
  - Reduce, control and recover from harm, rather than eliminate completely
  - Get the system back to required levels of performance, safety and security

Industry and business consequences

- Future services will be fast paced & tech focused
- Highly scrutinised
- Regulated
- Crimiinal responsibilities
- Huge financial losses
- Reputational damage
- Legal prosecutions
- Increased insurance premiums

Open

THALES