THALES

RESAuto - CHERITech 2024

Peter Davies
Director – Security Concepts

23rd April 2024

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 and elsewhere.
- 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 Telecoms Security
    - 2 Hardware Security
- 39+ years of verifying security systems in hardware
- I do security where it can't afford to fail

TRUSTED & GLOBAL & INSIGHT

THALES

The RESAuto Project …

RESAuto will

- **Demonstrate Digitally Secure by Design in**
  - **complex interconnected systems which are subject to international regulatory and legal controls, with**
  - **conflicting through-life objectives of safety, privacy and access to data (competition law).**

RESAuto has

- **Access to data-points that will allow numeric corroboration of potential impacts of a CHERI-based solution.**
  - **The costs of achieving the objectives are understood and controlled across the industry with examples such as the introduction of UNECE Cyber management (2021-2022) providing key data points.**
  - **RESAuto has access to global insurance industry actuarial tables relating to the automotive sector.**
- **Access to key UK and international players to achieve impact.**
  - **UK, German, French, US, Asian automakers, their Tier suppliers AND their engineering toolchain suppliers**
  - **Silicon, SiC designers and fabs for CPUs, AI processors, Sensors, Compound, Powertrain and Energy Electronics**
  - **Auto, transport, power, healthcare, defence**

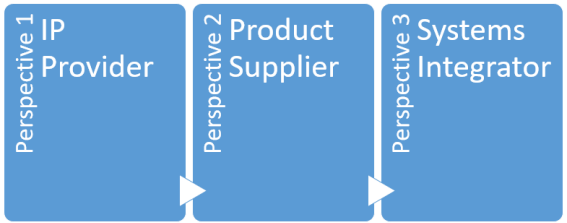
The RESAuto project team is led by Thales-UK, a world leading UK company in CNI and IoT with global reach and track record of working with academic partners to commercialise UK research.

TRUSTED GLOBAL INSIGHT

THALES

What I will talk about [RESAuto] …

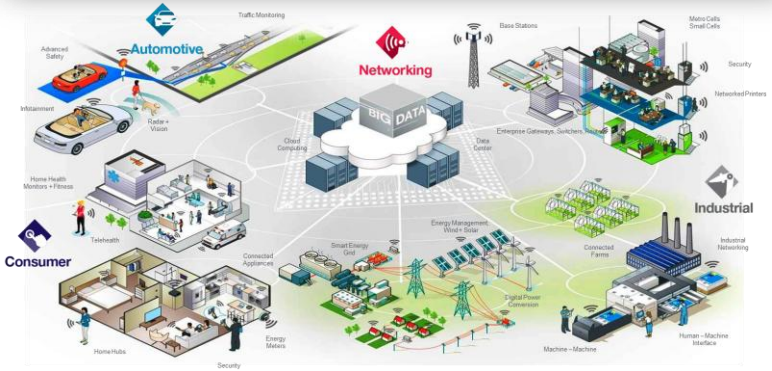
- Looking at the economic benefits and disbenefits of the CHERI approach in engineering based and often regulated industries.
- Implications for skills, power consumption, safety criticality.
- Complex supply chains considering how benefits and disbenefits manifest:
  - IP suppliers (eg chip vendor)
  - Product suppliers (eg T1)
  - and Systems integrators (eg OEM)



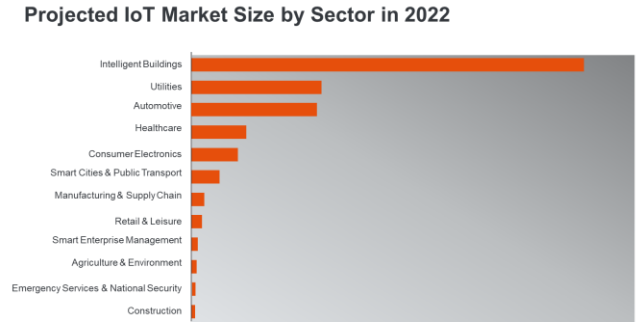
- Why Auto?
  - Costed and monitored through life on and off vehicle cyber management plan
  - Unaffordability of cyber major factor in withdrawing, delaying vehicles during 2023

Some Framing Remarks …

Software eats the world what's left is data



"103 exabytes of data is generated by vehicles every day" – IBM 2015



Data rules and what's left is hyperconnected complex systems with Safety of Life considerations

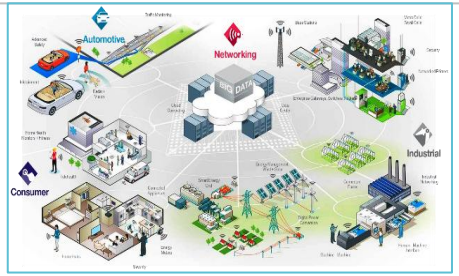
Framing Remarks – The Problem …

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.

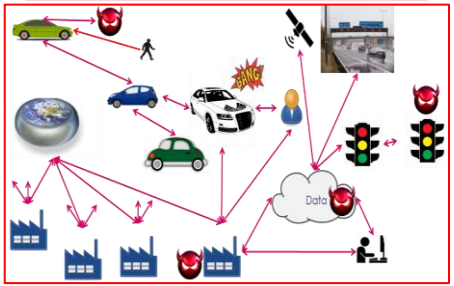
- A complex, hyper-connected, bottom-up system with emergent properties for which there is no guiding mind.

- A system yielding its benefits at scale.
- Price sensitive, worldwide and mobile system with vast amounts of data.
- Owned by no-one but in which 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?



THALES

Framing Remarks – The Problem …

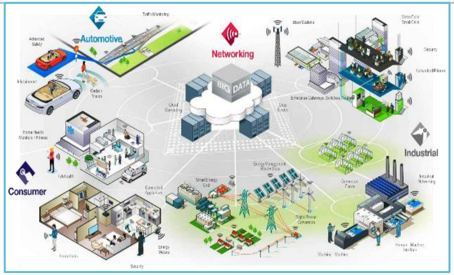
We have never before attempted to achieve anything that mattered in a system of the scale and complexity of the one we are now relying on.

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.

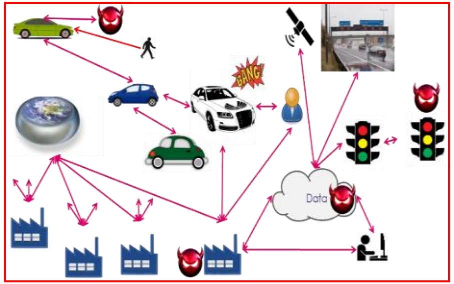
- ➢ Owned by no one but in it both strict and contract liability apply and must coexist.
- ➢ Multi vendor with legal obligations not to exclude suppliers from the supply chain.

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?



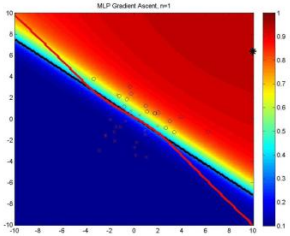
TRUSTED GLOBAL INSIGHT

THALES

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;**

Cyber 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'

Is Memory Safety Valued?

In 2016, IEEE Spectrum magazine released a chart showing the top languages. Ada ranked 40th by the level of importance. By 2019, Ada had gone down to 43rd. These rankings seem to show that this language is not performing well.

Cyber is Not Academic - And The Law Is …

Criminal Law

- **Purpose: punitive + 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

TRUSTED GLOBAL INSIGHT

Datapoints …

- We have used datapoints from significant actual industrial code bases
  - 500+ person years, 2.5m+ lines of code,
  - Refined and efficient engineering processes
    - MISRA C / C++and CERT C
  - Regulated industries including telecoms, finance, transport, aerospace, space and defence
- Develop an initial set of economic hypotheses for discussion with the automotive and other industries rather than simply asking them what they think.

Metrication …

- Access metrication of
  - Currently anticipated costs of achieving cyber safety together with
  - Costs of insuring business outcome
- Actually
  - Measure how the costs of achieving cyber resilience might be affected were a CHERI like solution to be available
  - Where and how would hardware security need to be integrated into the engineering and business activities to realise these cost benefits.

Supply Chain …

- Based on datapoints from eg. the Spectre and Meltdown cyber-attacks we have also been looking at how benefits at one point in the supply chain might not necessarily manifest for other points ie. we have been looking at some of the dysfunctionalities of markets containing this type of solution.

Hardware Cyber Security and Cross layer Exploits …

Meltdown
Cache side channel attack, Rogue Data Cache Load, reading kernel memory from user space

Spectre
Cache side channel attack, Speculation Attacks, Bounds Check Bypass, Branch Target Injection, Read-only Protection Bypass

RIDL
Rogue in-flight data load

Side channel loading / bypassing

Fallout
Leaking Data on Meltdown-resistant CPUs

ZombieLoad
Cross-Privilege-Boundary Data Sampling

Foreshadow
Key extraction via Transient Out-of-order Execution, L1 Terminal Fault

CLKScrew
Sophisticated power-management APIs induce (**under voltage**) faults in the processor entirely remotely (ARM based devices)

V0LTpwn
HW-oriented SW-controlled attack (**under volt a core**) affecting integrity of computation in virtually any execution mode on x86 processors

Precursor:
Dark Silicon Tech Issue (**reliability, leading edge**) – more SW-controlled PM

Rowhammer
Bit flips in DRAM modules, generate HW faults from SW software, fixing bugs ultimately requires deploying new HW,
Affected: memory modules on off-the-shelve computing HW
Not affected: memory inside the processor, such as cached memory and register values.

Spoiler
Speculative Load Hazards Boost Rowhammer and Cache Attacks

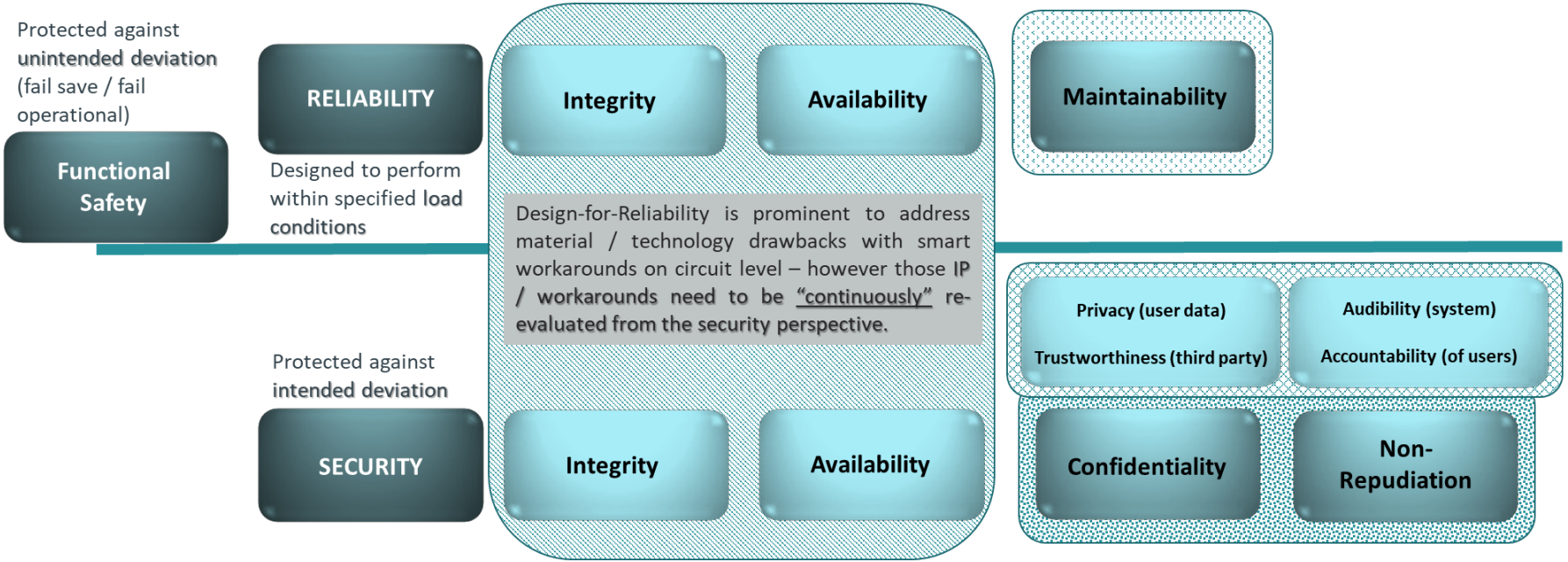
Precursor:
Sensitivity of memory technologies (**reliability, leading edge**)

CacheBleed
Timing Attack on OpenSSL Constant-time RSA.

CacheBleed
a cryptographic side-channel attack that uses ML to exploit a timing side-channel via the translation look-aside buffer (TLB) on modern microprocessors that use simultaneous multithreading

Some recent HW based attacks exploiting 'bugs' in the HW / microarchitecture

Hardware Cyber Security – Contradictory Objectives …



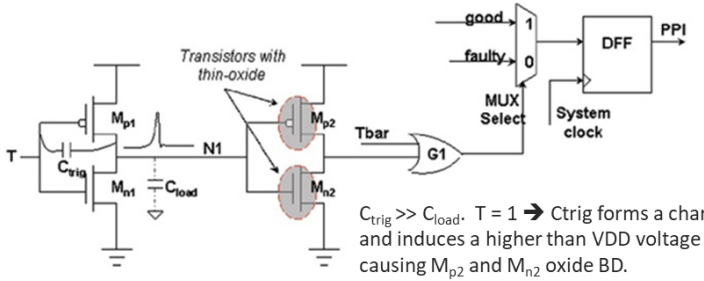
Many of today's automotive systems do not consider security concerns at system level (distributed & security concept separated ECUs) – w/o the awareness of "unsecurity", **the system safety will be undermined !**

TRUSTED & GLOBAL & INSIGHT

THALES

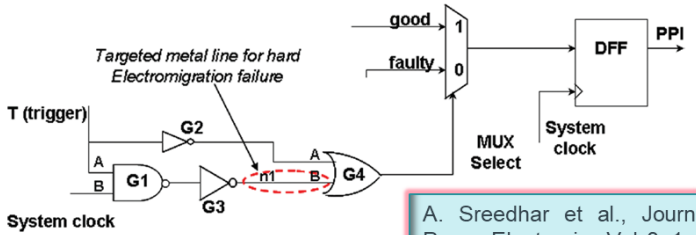
Hardware Cyber Security and Reliability …

TDDB Reliability Trojan – Pulse Degradation



$C_{trig} >> C_{load}$. T = 1 ➔ Ctrig forms a charge pump and induces a higher than VDD voltage on node N1 causing M_{p2} and M_{n2} oxide BD.

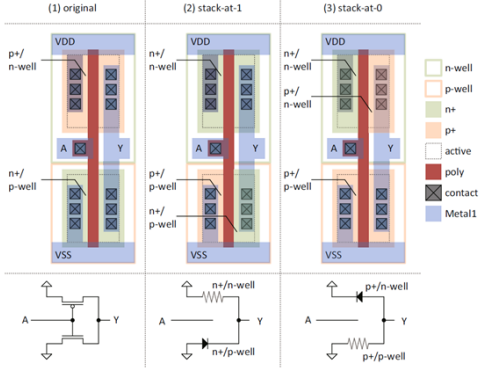
EM Reliability Trojan – positive edge CLK current pumping



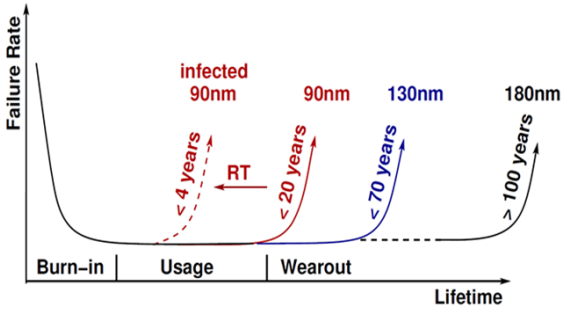
A. Sreedhar et al., Journal of Low Power Electronics Vol. 8, 1–10, 2012

Diffusion Programmable Devices (**Dopant Trojans**)

T.Sugawara, CHES 2014



Effect of NBTI / HCI Reliability Trojans on lifetime



Y. Shiyanovskii et al., 2010 NASA / ESA Conference on Adaptive Hardware & Systems

Reliability Trojans – playing against the reliability community

TRUSTED GLOBAL INSIGHT

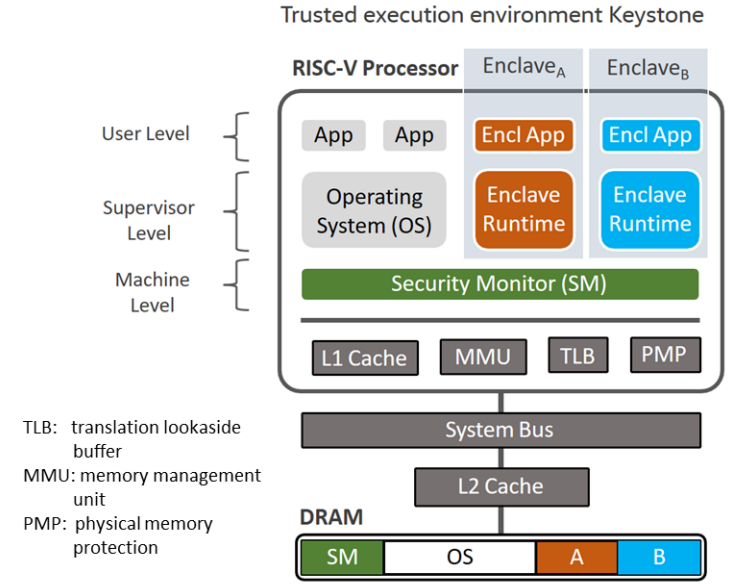
THALES

Hardware Cyber Security and Trusted Execution Environments …

	Hardware-based trusted execution environments (TEEs)	C3. Software Adversary	C4. Physical Adversary	C5. Side-Channel Adversary	C6. Ctrl-Channel Adversary	C7. Low Software TCB	C8. No Hardware Modification	C9. Resource Management	C10. All Applications	C11. High Expressiveness	C12. Low Porting Efforts
Intel	SGX	●	●	○	○	●	○	○	○	○	○
	Haven	●	●	○	○	○	●	◑	◑	●	●
	Graphene-SGX	●	●	○	○	○	●	◑	◑	●	●
	Scone	●	●	○	○	◑	●	○	◑	●	◑
ARM	TrustZone	●	○	○	○	○	○	●	●	●	○
	Komodo	●	●	○	●	◑	●	◑	●	◑	●
	OP-TEE	●	●	○	○	○	●	●	●	●	●
	Sanctuary	●	○	◑	○	○	●	◑	●	●	●
AMD	SEV	◑	◑	○	○	●	○	●	●	●	●
	SEV-ES	●	●	○	○	●	○	●	●	●	●
RISC-V	Sanctum	●	○	●	●	◑	○	◑	◑	◑	●
	TIMBER-V	●	●	○	○	●	○	●	◑	●	◑
	MultiZone	●	●	●	●	◑	●	○	○	○	◑
	Keystone	●	●	●	●	◑	●	●	●	◑	●

D. Lee et al., EuroSys 2020

1st Intl. WS on Secure RISC-V Architecture Design Exploration (SECRISC-V'20)



None of the TEEs consider the reliability concerns of the system that they are part of level and without this awarenes, **system security will be undermined !**

TRUSTED & GLOBAL & INSIGHT

THALES

Some Questions We Have Asked …

- Can the CHERI solution reduce the software engineering skillset or are we moving the problem from a skill set/software issue to a design issue?
- Does CHERI provide a more efficient way to diagnose memory errors prior to going to market, in essence, can it be used as a diagnostic tool in addition to other static analysis tools?
- How can we examine if CHERI can be directly deployed?
- How will the solution affect future products or services?
- What are the social and economic benefits realised by the solution?
- How to assess potential productivity increase through the use of the solution?
- How is it possible to provide a level of assurance that adopting the CHERI framework will enhance the systems Cyber Resilience?
- What are the use cases for CHERI and how may they benefit from it?
- CHERI lengthens/ pads pointer addresses in memory, could padding create future emergent problems?

More Questions We Have Asked …

- What performance overhead does CHERI generate and will these performance overheads ultimately increase energy consumption for example in cloud data centres?
- Is the CHERI solution compatible with other chips in the same system? What if one of the chips failed and needed to be replaced? Would CHERI still work?
- What are the benefits of CHERI in a standalone system versus a complex (interconnected) system?
- Can CHERI be used as an addition to existing diagnostic tools to highlight weaknesses in existing static analysis tools?
- CHERI claims it can separate CPU compartments, would this method allow a third party to write code without having access to other areas?
- Does CHERI provide an effective digital twin of a legacy system that is capable of generating memory errors in run time/operation?

FLiNT

Calls for global 'data extradition treaties' after Brighton road tragedy

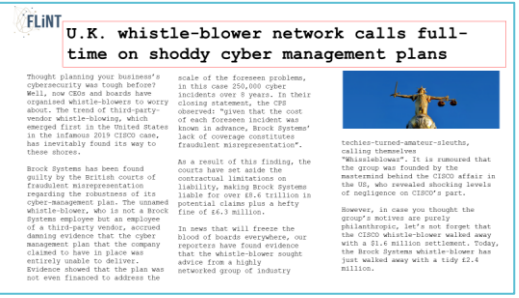
The United Road Transport Union is calling for new international data extradition treaties to be signed to help authorities get to the ground truth in road traffic incident investigations. The call comes after a young family was killed on the M23 just outside Brighton last month, in the latest road tragedy to be blamed on a cyber-security breakdown. Their hatchback was involved in a fatal collision when the Automated Lane Keeping Assist of a Dutch-owned SUV allegedly failed and the Ukrainian driver lost control of the vehicle. The SUV driver, who escaped the collision unhurt, was initially suspected of falling asleep at the wheel. But in a statement released through his union yesterday he insists that the Lane Assist feature "froze-up" in the minutes before the accident.

He claims that the feature was remotely "hacked" and that he had struggled desperately for a minute or more to recover control of the steering system, trying to take corrective action to avoid the fatal collision. With the support of his union, he is now calling for the vehicle software manufacturer XG to share user data that he believes would help prove the automated Lane Assist was compromised. He hopes these data will also provide evidence to show that he took prompt and appropriate action in his attempts to regain control of the vehicle.

XG have refused to allow access to such data, citing European privacy and security regulations. They deny any liability in the cluster of recent cases involving their automated driver assist products.

URTU spokesman William Johnson read a statement earlier today by the memorial flowers laid out at the scene of the accident

"This tragedy highlights the importance of sharing data across jurisdictions" he said. "If this accident had been caused by faulty brakes or tyres, then police could check the physical evidence. They need access to the systems data to investigate properly. This isn't about cyber security, it's about cyber safety." The URTU will ballot their members on strike action to support this case on Monday.



FLiNT

U.K. whistle-blower network calls full-time on shoddy cyber management plans

Thought planning your business's cybersecurity was tough before? Well, now CEOs and boards have organised whistle-blowers to worry about. The trend of third-party-vendor whistle-blowing, which emerged first in the United States in the infamous 2019 CISCO case, has inevitably found its way to these shores.

Brock Systems has been found guilty by the British courts of fraudulent misrepresentation regarding the robustness of its cyber-management plan. The unnamed whistle-blower, who is not a Brock Systems employee but an employee of a third-party vendor, accrued damning evidence that the cyber management plan that the company claimed to have in place was entirely unable to deliver. Evidence showed that the plan was not even financed to address the scale of the foreseen problems, in this case 250,000 cyber incidents over 8 years. In their closing statement, the CPS observed: "given that the cost of each foreseen incident was known in advance, Brock Systems' lack of coverage constitutes fraudulent misrepresentation".

As a result of this finding, the courts have set aside the contractual limitations on liability, making Brock Systems liable for over £6.6 trillion in potential claims plus a hefty fine of £4.3 million.

In news that will freeze the blood of boards everywhere, our reporters have found evidence that the whistle-blower sought advice from a highly networked group of industry

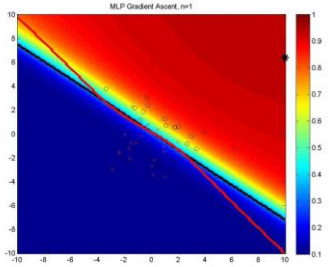
techies-turned-amateur-sleuths, calling themselves "Whistleblowers". It is rumoured that the group was founded by the mastermind behind the CISCO affair in the US, who revealed shocking levels of negligence on CISCO's part.

However, in case you thought the group's motives are purely philanthropic, let's not forget that the CISCO whistle-blower walked away with a $1.6 million settlement. Today, the Brock Systems whistle-blower has just walked away with a tidy £2.4 million.

Thank you

Peter Davies
Director Security Concepts

peter.davies@uk.thalesgroup.com



THALES