# Cyber resilience in the digital roads ecosystem of the future

The criticality of the extended supply chain

Digital Intelligence

BAE SYSTEMS

# Executive Summary

Connected autonomy in vehicles is coming. In many senses it is already here. However, as we move forward, we expect to see increasing real-time interaction between vehicles, their environment, and wider services and systems. This interaction will include other vehicles, as well as environmental factors such as weather, roadside features, people and animals, alongside smart and/or connected roadside infrastructure, including charging and fuel stations.

As we shift from traditional fossil fuel based vehicles to a mixture of electrification and alternative fuels, the fuel and energy delivery systems themselves become smart, and may interact and exchange information with vehicles in ways previously unheard of. We already see this with Electric Vehicle (EV) chargers. This means that the security of roadside infrastructure, fuel and charging stations, back-end services and vehicles themselves will become increasingly important.

In the current world, a direct compromise or failure of one vehicle, asset or system in the transport ecosystem, rarely ripples to cause wider compromises or failures, albeit significant disruption can still arise from singular failures.

But as interconnectivity and connectivity increases, we are marching towards a future where a failure or compromise goes in a single or relatively low number of assets, vehicles or systems, to one where all vehicles, chargers, traffic guidance systems, automated collision avoidance systems could be compromised at once.

Whilst there is a societal acceptance that faults do occur, and society accepts one off and ad-hoc failures, and has even accepted systemic failures spread over a period of time, the thought of widespread simultaneous life and safety impacting failures of compromise is simply unpalatable to society.

## Connected autonomy in vehicles is coming.

The security of roadside infrastructure, fuel and charging stations, back-end services and vehicles themselves will become increasingly important.

# The burden of increasing complexity

There is an accelerating increase in complexity across the vehicle and transport ecosystem. This is both on an individual system or vehicle level, but also in-terms of the cross-coupling and dependence between systems and system components, and progressively between vehicles, infrastructure wider management and monitoring systems.

As can be seen from the rise in vulnerabilities and code flaws within even relatively simple software, an increasingly continuous stream of new vulnerabilities, flaws and bugs can expect to be identified across the transport ecosystem, within vehicles and supporting roadside and back-end infrastructure[1].

In addition, we should expect attackers to target transport and vehicle ecosystems, and we should anticipate some of these attacks to be successful. The difference, as we move forwards, is that due to the increasing connectivity between ever more mission critical systems, these attacks are expected to be of a more widespread nature, impacting more vehicles, systems, components at once.

Attackers' motives may also evolve, as they could be enabled and emboldened by increasing vehicle sophistication, connectivity, and ecosystem intra-dependence. For example, integrated payment systems introduce fraud opportunities. The integration and interdependency of control, information, safety, and wider operational systems widens the window for vehicles to be attacked and used both disruptively and or destructively.

Motivations could range from extortion threats to political or ideological activism, hostile nation-state based economic attacks to social destabilisation. Similarly, extraction and analysis of data from vehicles and or supporting infrastructure and services can give insight into people's behaviour, movements and wider "pattern of life" data[2] which may be used to attack both individual privacy levels, and also infer other activity or intelligence around specific locations or regions[3].

In addition, we are transitioning from systems that provide information or updates but the core operational functions are wholly contained with the vehicle itself, to one where elements of the core operational systems are either distributed across, or dependent upon many wider entities and systems. In this more connected and interdependent world, it is far easier for a compromise in one element of the ecosystem to impact a whole network of vehicles.

The simplest analogy would be to imagine a NotPetya style incident impacting safety or control systems across millions of vehicles whilst they were in operation. Within a connected and wholly autonomous world, this is exacerbated by the lack of human ability to intervene. But even without autonomy, this presents a real issue as humans react and respond to stimuli, and a compromise enables an attacker to interfere with information presented to the drivers, as well as their potential ability to respond.

Given that we know there will be vulnerabilities ripe for exploitation, and the history of cyber breaches indicates there will be cyber incidents in the connected transport world, this has potential to have widespread concerns and repercussions.[4]

Given what we know there will be vulnerabilities ripe for exploitation, and the history of cyber breaches indicates there will be cyber incidents in the connected transport world.

# So, why is it so hard to be secure, and remain secure?

We secure as best as we can, but we also know attackers will find a way in. We try to avoid vulnerabilities, and patch, update as best we can, but we know that there will still be exploitable vulnerabilities.

### The problem with the supply chain

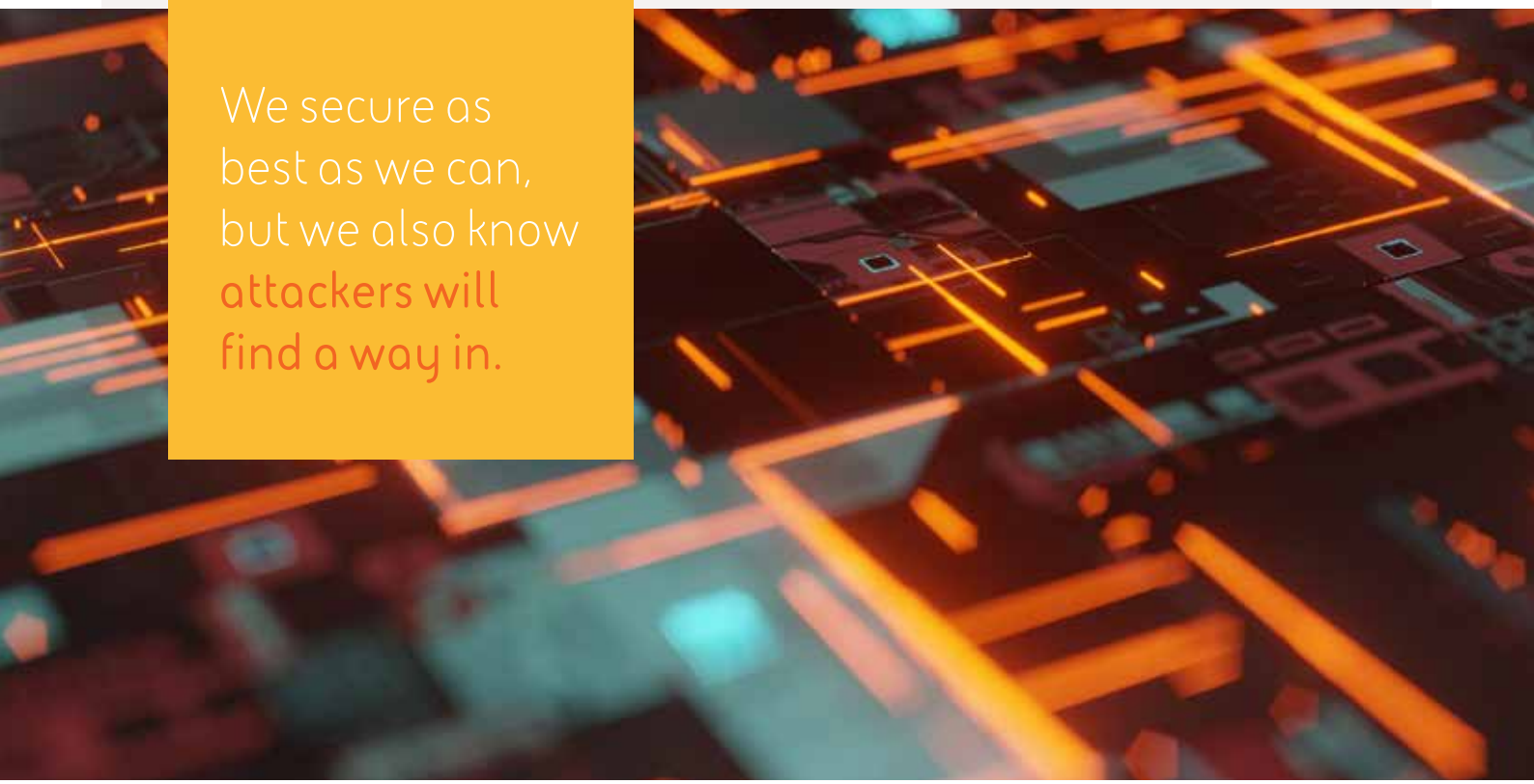
Who actually develops the software, the hardware, and the systems, ensure they are secure, and is then incentivised to patch, fix, and remedy these?

The vehicle or asset manufacturer: The vehicle manufacturer is up against strong commercial pressure to develop a product on time, with functionality and connectivity that appeals to the buyer, for the lowest cost. Diligence and assurance around security of systems and robustness of code is important, but hard to justify above a "minimum acceptable bar" of "just about good enough" which no-one can easily quantify, or measure, until things go wrong – by which time is too late.

A large proportion of the subsystems and information systems will be bought in from common suppliers across the vehicle industry. There may be an even smaller underlying supply base of key hardware components, and all of this will have an extended supply chain and its own supplier ecosystem. In addition, whilst the vehicle manufacturer in most cases will have the ability to push updates, they may be reliant on their supply chain to provide, test and assure these. In some cases, third party component suppliers or service providers may push their own updates directly.

In many cases the original equipment manufacturer (OEM) role acts as systems integrator, and may have little or no sight of the underlying code of the components packaged up into their final product.

We secure as best as we can, but we also know attackers will find a way in.



The suppliers to the OEM: Many suppliers will deliver software and system components to the OEM manufacturers. Many of these will have their own extended supply chains, and use third party software services, each with differing standards, diligence, rigour, and use of third party components, tools, libraries, some of which maybe supported or hide vulnerabilities[5].

In addition, standards may be immature, poorly understand, or the supplier may lack the skilled personnel to understand and apply these properly. There may be legacy components being reused or incorporated that do meet current standards. They will be under competitive cost and time pressure, and may vary in how strongly they are incentives to ensure their components are secure, robust, and to provide through life support, updates and patching for these.

In some cases, they may be able to push out updates to their products in components in use directly, in others they cannot, and need to provide these to their suppliers, subsystem integrators, and it trickles up the supply chain, eventually to the consumer's vehicle. And as organisations themselves they may be immature in cybersecurity and liable to attack.

The infrastructure provider: In many instances vehicles will interact digitally with roadside infrastructure, charging and fuel points, and other vehicles and traffic management systems. These wider systems will be owned, run, maintained by their own ecosystem of organisations, each with their own commercial interests, constraints and drivers. An exploitable vulnerability in any of these could impact the wider ecosystem.

For example, a compromised charger or fuel delivery point with a digital interface, could be provided by a charger supplier, delivers charge or fuel from a grid network provider, was procured by a car parking infrastructure company, but operated by a car park operator or the consumer.

A compromise might impact the charger or fuel point network, have knock on to fuel logistics, distribution or the energy grid, along with the vehicles that connect to them. Similarly, there will be underlying telecoms network, data service providers and organisations that manage, maintain and run vehicles and assets on behalf of businesses, transport infrastructure providers, consumers and other stakeholders. All of these will have their own vulnerabilities, and exposures.

Standards may be immature, poorly understand, or the supplier may lack the skilled personnel to understand and apply these properly.

# The schism between those impacted, and those able to mitigate the impact

In all these scenarios, there is often degrees of separation between:

- Those with the capability to create secure products, and product updates and ongoing support to the products; the system, subsystem, software, hardware providers and suppliers[6]
- Those with capability to deliver and apply updates to products and subsystems, usually the OEMs and some of the system/service providers
- Those carrying dealing with the impact at an individual level in the event of compromise, such as grid and fuel providers, consumers, passengers and drivers, bystanders to traffic chaos or those reliant on the logistic services provided
- The wider societal impact and risk from a widespread and systemic compromise, failure or other untoward behaviour. The government, along with wider citizens and businesses, all impacted by failure of the transport system, and subsequent loss of confidence

Those who feel the impact and carry the risk, are far separated from those in the supply chain empowered to minimise its likelihood, or mitigate its impact. This creates an incentivisation challenge.

So where does the liability lie? How will this work in practice so we are incentivised to ensure through life security and updates for transport systems and safe and performant operation?

The government can, and does apply regulatory measures on service providers and OEMs, which should be flowed down to service, component and software providers. However, we know that failures and compromises will still happen.

In the UK, the government has legislated that the liability for Connected and Autonomous Vehicles will sit with the insurance industry, on the basis that it is set-up, and best placed to determine where the actual liability of specific incidents lies[7]. However, this may result in an uninsurable risk that the industry is not prepared to tolerate, particularly in the case of widespread systemic impacts, failures or compromises.

In addition, leaving this for the insurance industry to pursue and assign may not, on its own, drive the correct behaviours out of the supply chain.

# So, how do we manage the risk?

We must accept that vehicles, infrastructure, fuel and energy distribution systems will be compromised in due course. And we must also accept that this will impact many assets, vehicles or entities at once. But it's not all bad news. In order to minimise this we should:

1. Ensure regulations and commercial incentives drive towards secure produce design, development and through-life accountability and responsibility for maintaining product security. This obligation should extend for the operational life of the systems infrastructure and vehicles, not just the suppliers desired operational and warranty period[8].

2. To reduce the impact of a compromise, and its ability to spread, we should aim for a heterogeneous ecosystem with diversity and minimise common points of failure to reduce the impact of systemic compromise and failures[9]. Whilst standards based approaches are essential to enable interoperability, diversity may be retained in the underlying implementation. This is likely to be truly challenging to achieve, as this diversity must originate and propagate right the way through the supply chain[10]. Existing trends in software and component reuse, however, act against implementation diversity.[11]

3. Design individual components, and systems to be able operate within a compromised system, such that the overall ecosystem is resilient to partial failure and compromise. Just like a generator in a power cut. The challenge here will be how the extended supply chain is incentivised to deliver this.

4. Consider the scenario where largescale compromises will happen. Design vehicles and systems that can sustain prolonged operation in secondary compromised or degraded states, and still safely fulfil their basic mission and operational functions, even if sub-optimally. Consider that in some cases practical recovery and restoration of these may be unfeasibly due to the large and distributed number of compromised components, vehicles or assets. In this case the secondary degraded mode should be such that it may be operational for extended periods, or even for the remainder of its lifetime.

# Conclusion

We live in a world of increasing complexity and ever increasing technology and service supply chains. As the digital roads and transport ecosystem becomes increasingly connected, and complex, software defects and security vulnerabilities will continue increase – it is the nature of commercial software development. Across the technology sector, software and system development processes do not consistently operate to high-levels of rigour and assurance that would catch and prevent this from happening.

Code and component reuse within the technology supply chain will result in many hidden common points of failure and vulnerability across our digital roads ecosystems. The length and opacity of technology supply chains, combined with component and code re-use endemic within the software industry will make us vulnerable to attack and compromise. These events will occur, and if unchecked, could impact large sections of the ecosystem at once.

There is, though, an opportunity to drive approaches to the development, design and operational of the connected vehicle ecosystem that provides both robustness to compromise, and limits the extent of the impact, by enabling the ecosystem to tolerate cyber events and operate safely despite widespread compromise. It may be as performant as it was, but it will operate, and safely.

However, a commercial culture of 'lowest bidder wins' in what is fiercely competitive market will not give us this. We need suppliers, manufacturers, and operators to take note, embed these approaches, and external support and influence to drive the desired behaviours:

- We need both regulatory and commercial incentives to drive through life security and updates throughout the product, vehicle and system lifecycle
- A recognition that 'lifecycle' extends to the whole life for a product or system, not just the manufacturers desired lifespan or their warrantee
- Maintain a diversified ecosystem where possible throughout the supply chain. Minimise common points of failure
- Expect vulnerabilities, failures and compromise
    - Design in resilience and robustness that expects failures and compromise within the ecosystem
    - Design and allow for degraded operational modes than enable mission and operational objectives to continue to be met, even compromised or under partial failure.

But critical to achieving the above is ensuring that we incentivise the extended supply chain, through a combination of both commercial and regulatory incentives. To be effective, this must also include a willingness to enforce obligations and commitments down the supply chain, whether contractual or regulatory.

# About the author

Alex Crompton is Head of Security Consulting at BAE Systems Digital Intelligence

alex.crompton@baesystems.com

[1] Trends of CVEs logged by NIST show year on year increase since 2016. Code "defects per million lines of code (MLoC)" typically varies between 600/MLoC to 6000/MLoC, of which typically 5% may also be security vulnerabilities. Taking an optimistic view point, for a typical modern vehicle with 100+MLoC, suggest there should be of the order of 3,000 security vulnerabilities in each vehicle. Predicting Software Assurance Using Quality and Reliability Measures (cmu.edu); Selecting Measurement Data for Software Assurance Practices (cmu.edu)

[2] Arguable this horse has already long bolted with the ubiquity of modern smartphones and their integration with social media and online platforms tracking movement and locations and transport is just catching up. E.g. within the Android ecosystem, Google Timeline, combined with smart assistants and search history and inspection of user g-mail gives significant insight into individuals movements, behaviour and interests– clearly it not just the google ecosystem that does this. Connected and integrated transport systems do however provide channel for a more physical and direct execution of activities however.

[3] An example from 2018, now fixed but illustrates the concept Fitness app Strava lights up staff at military bases - BBC News. from 2018, now fixed Individuals in military bases using the Strava app for fitness and sharing their activity publically ended up both "mapping" routes within bases, but also indicating where there bases where located.

[4] For more on the security challenges for CAVs: Security Challenges for Connected and Autonomous Vehicles | BAE Systems and common vulnerabilities connected vehicles: Common Connected Vehicle Vulnerabilities (techuk.org)

[5] Once again, Log4J is probably the most public recent example of vulnerable software component reuse, as well as Intel chip vulnerabilities from SPECTRE and MELTDOWN.

[6] There may be obligations on the OEM to support and patch equipment, but if this is not flowed down and enforced throughout the onward supply chain, this may become meaningless as the OEM may powerless to actually do this without supplier support.

[7] Driverless cars insurance laws receive Royal Assent (pinsentmasons.com)

[8] "Planned obsolescence" can very easily be built in through limitation of support and patching. This is notorious in the mobile phone industry. Vehicles prior to connectivity, this ongoing support and patching has been of limited impact. The introduction of large scale connectivity and data flow changes this.

[9] It could be argued that currently "diversity" & robustness is introduced into current systems through the behaviour and response comes from the human drivers. In a connected world however even human responses become vulnerable to systemic misinformation. And this is without considering autonomous scenarios that may or may not have a human fall-back.

[10] E.g. – lack of diversity into the CPU market resulted in widespread vulnerability due to SPECTRE & MELTDOWN vulnerabilities in many CPUs including Intel based, or derived processors.

[11] The widespread use of the Log4J software component when it was discovered to be vulnerable caught many by surprise in its ubiquity of use and general practice of code and component reuse in software. Similarly there is convergence in underlying CPU, memory and other semiconductor based hardware components.

## We are Digital Intelligence

The UK security and resilience sector is world renowned, and along with Defence exports, has long been recognised as an export opportunity for economic growth; however it is distinct from Defence exports, particularly in that it is a sector largely dominated by small to medium sized enterprises (SMEs).

The recently published Integrated Review places strengthening security and resilience at home and overseas at its heart. The sector is therefore well placed to help strengthen the security and resilience of our partners and allies, and as a valued capability it could help expand UK influence abroad in a post-pandemic and post-Brexit era.

The UK Government already uses security and resilience SMEs to delivery capacity development to partners and allies, but the scale of its interventions are limited by its ability to manage and integrate the work of multiple SMEs.


BAE Systems
Surrey Research Park
Guildford
Surrey GU2 7RQ
United Kingdom
T: +44 (0) 1483 816000

BAE Systems
8000 Towers Crescent Drive
13th Floor
Vienna, VA 22182
USA
T: +1 720 696 9830

BAE Systems
Level 1
14 Childers St
Canberra, ACT 2601
Australia
T: +61 1300 027 001

BAE Systems
Suite 905 Arjaan Office Tower,
Dubai Media City
Dubai
T: +971 (0) 4556 4700

BAE Systems
1 Raffles Place #42-01, Tower 1
Singapore 048616
Singapore
T: +65 6499 5000

BAE Systems, Surrey Research Park, Guildford, Surrey, GU2 7RQ, UK

E: learn@baesystems.com

W: baesystems.com/digital

linkedin.com/company/baesystemsdigital

twitter.com/BAES_digital




BAE SYSTEMS