EP90group

MERLIN

Vehicle security assessments that empower end to end fleet management

Individual (operational and bespoke) or fleet solutions

An adversary mindset across all domains (social engineering, hardware, software, communications, physical, supply chain and process / policy)

Prepared for: WEBSITE
Prepared by:
Email: info@ep90group.co.uk
5 November 2019
Output reference number:

EP90group

VEHICLE SECURITY ASSESSMENT

Deter, Detect and Delay

(Time to **detect** + Time to **understand** + Time to **react**) **<** Time for **Compromise**

ABOUT EP90GROUP

EP90group Ltd is a specialist UK company operating across **law enforcement**, **national security**, **military**, **commercial cyber security** and **automotive**.

We are an **equipment** and **property interference tool manufacturer** and **developer**. With our deep understanding of automotive high integrity systems (fail operational, fail safe and fail secure), we excel at **protective** and **operational security assessments**.

We undertake **government** and **commercial consultancy projects.** We have extensive **testing facilities, including RF and 4G / 5G,** and regularly contribute to international standards in automotive cyber security. These include BSi PAS1885, ISO TC22-SC21, WG11 and SAE 21434.

We are part of Cyber Security Centre, WMG, University of Warwick - a **GCHQ academic centre** of excellence for research and teaching programmes.

A CHANGING WORLD

Since reaching mass adoption in the 1980s, ground vehicle electronic systems have evolved. They are now a complex tangle of distributed devices operating on open networks using both public and more obscure protocols.

These electronic systems control a vast array of features and functions to ensure a safe vehicle (Figure 1), all of which are considered in a robust safety strategy and are exhaustively tested for 'fail safe' and 'fail operational' under FMEA (Failure mode and effects analysis).

Currently, ground vehicles, maritime and aviation are shifting from a collection of electronic control units connected by networks to a distributed computer network programmed as a car, boat or plane.

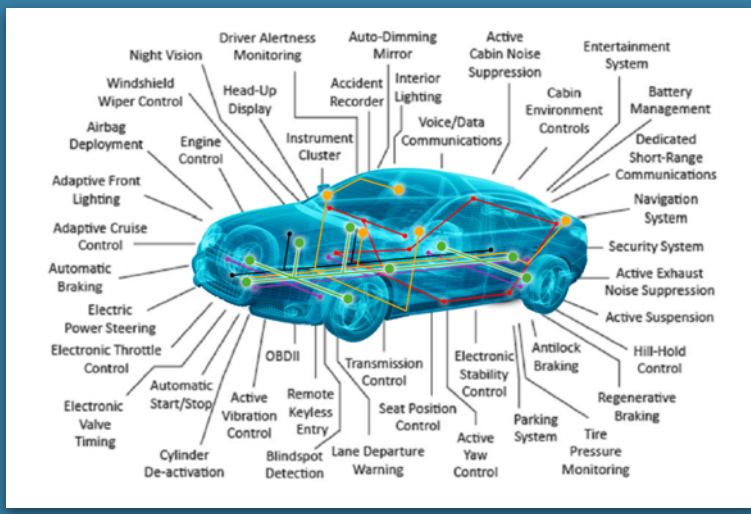


Figure 1

WHAT'S CHANGED?

Automotive safety and security has evolved since vehicles became common consumer items.

From occupant and pedestrian crash safety to theft protection, systems and electronic processes are constantly evolving to meet the changing needs of their environment.

Have you ever hired a car, connected your phone and seen the previous user's contact directory?

Since the late 1990s, information derived from automotive sensors have enabled comprehensive diagnostics and aviation style prognostics as well as remote access for global monitoring, servicing and repair.

Vehicle telematic systems have become increasingly sophisticated so fleet managers have in-life service information and driver behaviour assessment data to improve fuel economy and mechanical assessments.

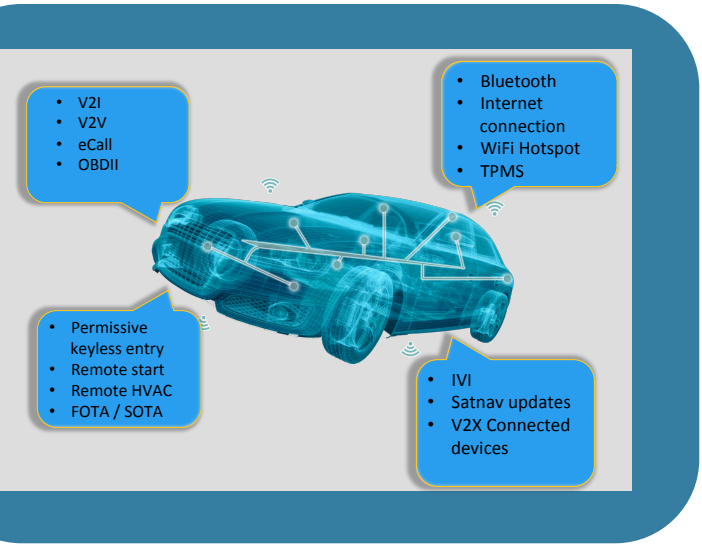
The agriculture sector too has adopted complex telematics systems with remote control and semi-autonomous farming capabilities to raise efficiency. This has led to a proliferation of aftermarket devices: e.g. insurance telematics and black box recorders.

Would you know if an extra module was fitted to your vehicle when it was out of your control?

From the perspective of protective security and Technical Surveillance Counter Measures / EMSEC[1], this data rich landscape has quickly become a new frontier in operational security, one that requires an assured response to deliver secure operational outcomes, stringent privacy, and the confident prevention of cyber physical attacks.

ASSESSMENT METHODOLOGY: SECURITY DOMAINS

Our extensive security knowledge feeds into our comprehensive approach to security and includes the following domains as default and builds upon attack pattern mechanisms identified by US mitre.org.

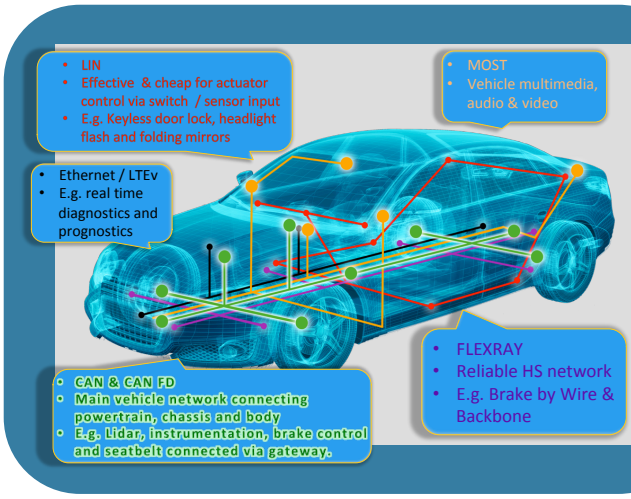


Social Engineering: the manipulation and exploitation of people. Techniques convince a target to perform actions or divulge confidential information. The term typically applies to trickery or deception for the purpose of information gathering.

Hardware: the exploitation of physical hardware used in computing systems. Techniques include the replacement, destruction, modification and exploitation of hardware components to attempt a negative technical impact.

Attacks fall into several categories depending on the attacker's sophistication and the systems targeted. These differ from software attacks as hardware-based attacks target the chips, circuit boards, device ports, and other components that comprise a computer system or embedded system. Sophisticated attacks may involve adding or removing jumpers to an exposed system or applying sensors to portions of the motherboard to read data as it traverses the system bus.

[1] EMSEC - Electromagnetic Security a subset of COMSEC - communications security.



Software: the exploitation of software applications. Techniques exploit weaknesses in application design or implementation to achieve a desired negative technical impact.

Physical: this category focuses on physical security and techniques exploiting weaknesses in the physical security of an asset or system.

Communications: the exploitation of communications and related protocols by an adversary to intercept, interrupt, modify or fabricate communications.

Supply chain: disruption of the supply chain lifecycle by manipulating computer system hardware, software, or services for the purpose of espionage, critical data or technology theft, or the disruption of mission-critical operations or infrastructure.

Supply chain operations are typically multi-national with parts, components, assembly, and delivery occurring across multiple countries, thereby offering attackers multiple points for disruption.

Process and Policy: weaponising a system's policies and processes against a target. Often, reversing a sequence within a process chain can have consequential results: e.g. such as locking the doors then alarming the door, which if swapped, may not have a direct detrimental effect but could allow a new defeat tactic to operate.

A safety strategy may also trigger certain systems to de-rate in order to preserve safety, but weaponising that same strategy can bring about an intentionally less-desired effect.

EP90GROUP RESPONSE

The first step is to ***Deter*** through extensive baseline assessments, informed selection and, where necessary, target hardening. This mitigates insecurity and is risk balanced with operational usability and guidance.

A combination of physical and cyber security assessments provide an informed knowledge platform with which to *Deter* with 'defence in depth' or a mobius defence.

The second step is to ***Detect*** - a combination of security hygiene, operational maintenance and operational security, and guidance adherence. Coupled with sound investigation methods, this will *Detect* adversary action.

Lastly we ***Delay*** adversary activity.

We instigate tactics that maximise cyber resilience and strengthen the ability to rebound and recover after adversary activity.

The *Delay* builds time, which when aggregated with 'time to *Detect'* and 'time to understand', ensures that the total time is less that the 'time for compromise'.

"What if a whole vehicle security assessment existed, spanning physical and cyber attack surfaces, to enable better operational security against peer adversaries?"

END TO END SOLUTIONS

We are experienced operating through an asset's entire lifecycle and our services feed into full end to end fleet management.

Specify: We can work with you to set high level and detailed asset requirements (bespoke and fleet solutions), including cost benefit analysis, service design and service value (availability, adaptability, necessity, operational relevance, usability and affordability) across a range of financial models.

Design: We can design systems, policies, guidance and components to meet requirements or evolving requirements, and have a long history of specialist asset manufacture and project management.

Procure (Build, Adapt and Convert): We can procure assets, project manage the entire process and bespoke build, adapt or convert in line with your requirements and maintenance plans, (excise and insurance as well, if required).

Manage: We can provide full in-life service schedule and delivery. Not only the implementation of factory service schedule, updates, settings and consumables, but recalls, bespoke service schedules, diagnostics and prognostics to ensure that any asset is operational for the maximum utility. Within *Manage* we can undertake regular TSCM and cyber hygiene assessments and undertake the pre- and post-security assessment if or when an asset is out of the controller's control. We refer to this as the *cyber valet* and is described below in *Pricing Structure*.

End of Life disposal. When end of life is agreed, we securely ensure that all sensitive data and information is removed from an asset, such that an Operational Security Advisor (OpSy) is satisfied and an organisation's environmental commitments are upheld.

THE VALUE PROPOSITION

With the current state of security outlined, this poses two key questions:

1. **What if a capability was developed so individual asset and fleet controllers have a reliable, repeatable, robust, holistic, end to end security assessment that services a fleet through its entire life?**

2. **Additionally, how would this evolve to become the ultimate fleet management service combining traditional fleet services, with TSCM and TEMPEST assessments and Cyber Security / Resilience?**

The outcomes of these would be a significant improvement to operational security, substantial savings through a central shared service or via a variety of fleet services, and additional assurances in an ever-privacy-conscious and security-aware society.

SCENARIO 1: a high net worth individual forgets to, or does not realise they have to, or, does not know how to, wipe their digital footprint from a holiday hire vehicle. Digital artefacts include home address, significant addresses, contacts directory and SMS messages.

SCENARIO 2: an asset controlled by a local *cleared* chauffeur is damaged in a minor road traffic collision. It is repairable, but the chauffeur is concerned about how this affects their employment and takes their car to a local independent body shop for a discreet repair. It transpires that the airbag module is defective and needs replacing.

The module contains vehicle systems data from the vehicle that reveals information about seat occupancy and journeys made over the past three months. The module is disposed of on the grey market having been exchanged for an aftermarket counterfeit with defective firmware causing the airbag to deploy during an operation.

SCENARIO 3: unbeknown to the same chauffeur, the minor accident was staged and whilst an official module is replaced, the data is exfiltrated by a national state and an additional module is covertly fitted to facilitate additional surveillance activity - ultimately compromising a series of operational deployments.

Our response to these scenarios, and countless others, is **Merlin**.

WHAT IS MERLIN?

Merlin takes traditional end to end fleet management, adds comprehensive bespoke maintenance schedules, and combines everything with a full suite of Technical Surveillance Counter Measures (TSCM) technicals and behaviours, and *TEMPEST* EMSEC.

Merlin fuses these with a comprehensive cyber security and cyber resilience practice.

This covers from the point of acquisition, through design and build, during operation (including cyber hygiene) and ends with secure disposal.

Any Operational Security Advisor has a total picture of an asset's security hazards, as well as steps taken to Deter, Detect and Delay or React to a hazard.

In some instances, inherited assets need assessing and baselining even after operational deployment.

Merlin is flexible and configurable to adapt to your requirements.

REPRESENTATIVE USE CASES

1. A government department is considering whether to change its vehicle fleet for environmentally friendly alternatives. The pool fleet is for routine and essential travel from buildings around central London while the same vehicles will enable senior staff and drivers to perform their duties. Some equipment is sensitive and requires additional protective security. Some locations are designated sensitive.

   A full security assessment is required for three candidate vehicles prior to a 100 vehicle order. The assessment should include standard physical security, communications bearers and digital identities, and maintenance security through to disposal. In addition to the relative assessment, recommendations are required for mitigation and operation guidance in operation.

2. A multinational hire company is successfully sued by a global company because commercially sensitive information is publicly recovered from a hire car rented by a senior executive. The hire company is sued for damages as well as breach of terms, leading to significant financial damages and significant reputation damage. The hire company requires an effective method of wiping personal and identifying data from its fleet at handover. It tenders for equipment to satisfy this task and requires an assessment of each of the responders.

PRICING STRUCTURE

Fixed prices are difficult to maintain within such a rapid technologically evolving sector so we regularly configure and tailor our services to meet your needs. The two tables below provide an indicative structure which we use to provide guidance to clients with broad categories of assets reflecting their relative complexity and variation. Basic, Intermediate and Advanced are broad categories reflecting asset complexity. Prices are exclusive of VAT.

The Cyber Valet is a combination of three different services. **TSCM** can be a bespoke service, as too can a **cyber security** assessment. **Cyber Resilience** assesses how effective an asset would be in recovering from adversary activity.

The Cyber Valet can be purchased as a package.