

Challenges in Vehicle Systems Resilience

車両システムの安定性における課題

David WARD

Since the introduction of the first microprocessor-based systems into mass-produced vehicles in the 1980s, the electronics content of automobiles has continued to grow. Future trends including moves towards autonomous vehicles and connected cars will continue this growth. Historically disciplines such as reliability analysis and systems engineering have been used to develop robust electronic systems and more recently functional safety builds on these foundations. However the future growth means that it is important to consider the holistic issue of resilience of electronic systems with a cross-disciplinary approach incorporating wider issues including cybersecurity and fail operational properties.

1980年代にマイクロプロセッサシステムが量産車に初めて導入されて以降、自動車に搭載される電子機器は増加の一途である。自動運転車やコネクテッドカーへの移行が予想される今後の傾向としても、この増加は続くと思込まれる。歴史的には、信頼性解析やシステムエンジニアリングなどの分野が、耐久性のある電子システムの開発に応用されてきた。最近でも、機能安全はこれらの基礎の上に構築されている。しかし、今後も電子機器導入がさらに増加することから、サイバーセキュリティや故障時動作継続特性などより幅広い視点を取り入れた横断的アプローチにより、電子システム故障からの復帰という全体的な課題を検討することが重要である。

Introduction

While the history of electrical and electronic systems in vehicles is nearly as old the car itself, it was in the 1980s that significant growth in the electronics content of mass-produced vehicles first started. The 1980s saw the introduction of tailpipe emissions regulations, initially in the USA, that required the engine to be electronically managed in order to meet the required targets.

The growth in electronic systems has continued unabated; the trend is typically that advanced systems are first introduced into luxury vehicles and then become standard fitment in mass-market vehicles once the technology becomes accepted and commoditized. The following table shows for each recent decade a key electronic system that has started to be fitted to mass-market vehicles as standard and the motivation for this.(Table 1)

はじめに

車両用の電気・電子システムの歴史は、自動車自体の歴史とほぼ同じくらい古いですが、量産車の電子機器搭載量の大幅な増加が最初に始まったのは、1980年代であった。1980年代には、まず米国で排ガス規制が導入され、その要求目標を達成するために、エンジンを電子的に制御することが求められた。

その後、電子システムの技術は継続的に進歩してきた。典型的な動向として、先進的なシステムは、まず高級車に導入され、その技術が受け入れられて商品化されてから量産車の標準装備になる。

以下の表は、量産車に標準装備され始めた主要電子システムとその誘因を、最近の各年代ごとに示す(Table 1)。

車両の電子機器搭載量については様々な統計が引用されているが、典型的な見積りによれば、車両の部品代のうち、20~40%が電気・電子システムであり(車両の市場とブランドにより異なる)、約100個のコンピュータシステムが含まれている。いくつかの資料によると、今や自動車は、Boeing社787 Dreamlinerよりも多くのソフトウェアを搭載(Figure 1)しているとされるが、著者の考えでは同列に比較することはできないと思われる。

Table 1 Each recent decade a key electronic system

Decade	System	Motivation
1980s	Engine management	Emissions legislation
1990s	Restraints e.g. airbags	Market forces
2000s	Electronic stability control	Legislation
2010s	Driver assist e.g. AEB	Market forces e.g. EuroNCAP

Various statistics are quoted for the electronics content of vehicles but typical estimates are that between 20% and 40% of the value of the bill of materials in a vehicle is in its electrical and electronic systems (depending on the market and brand of the vehicle) with around 100 computer systems. Some sources cite that vehicles now contain more software than a Boeing 787 Dreamliner although in the author’s opinion this may not be comparing like-for-like. (Figure 1)

In the future the major trends will be the “connected car” and greater use of driver assist systems leading to deployment of systems with higher degrees of automation and eventually fully autonomous vehicles.

Development of the “connected car” is proceeding in three directions. Firstly, vehicle-to-vehicle and vehicle-to-infrastructure communications continue to be developed and deployed in some markets (notably the long-standing use in Japan, and a recent legislative mandate in the USA). Secondly, some vehicle manufacturers already embed a cellular modem for remote diagnostics and service, and the European e-call requirements will mandate fitting of such technology.

However the third significant growth area is the use of consumer devices in the vehicle that effectively make the car an “always on” internet node due to 3G/4G wireless connectivity. Many manufacturers are providing seamless integration and “hand off” between consumer devices and Apps in the car; and also the facility for a wireless hotspot in the car.

The safety and reliability of these electronic systems has always been a consideration for the industry but these parallel developments of connected cars and greater use



Figure 1 Which has the most software?

of autonomy means that ensuring the resilience of these systems is now a top priority for the industry.

What is Vehicle Systems Resilience?

HORIBA MIRA is using the term “vehicle systems resilience” to refer to the properties or attributes of the mission-critical electronic systems used on vehicles. As shown in Figure 2, traditionally development of all vehicle systems (not only the electronic systems) has considered their reliability using failure mode avoidance techniques such as failure mode and effect analysis (FMEA) and fault tree analysis (FTA). Many vehicle engineering lifecycles use a “V” model or waterfall model derived from systems engineering where high level requirements derived from product attributes are cascaded down through successive levels of architectural design until a suitable level of detail for implementation is reached. The implemented elements are then integrated and verified in a stepwise fashion to demonstrate confidence in the completed product.

More recently functional safety has become an integral part of the development lifecycle. In its widest sense, functional safety is the part of overall system safety concerned with demonstrating that technology-based systems operate correctly in response to their inputs (and therefore do not generate a potentially unsafe condition by incorrect operation). Specifically in the automotive industry, the international standard ISO 26262^[1] is concerned with avoiding hazards that could result from malfunctioning behaviour of electrical or electronic systems.

The scope of ISO 26262 is therefore narrower in comparison to some other practices in functional safety, since it is only concerned with the requirements for design of

今後は、「コネクテッドカー」と運転支援システムの利用増大が大きな流れになる。これが、自動化の度合いを高めたシステムの展開につながり、最終的には完全自動運転車両に至るであろう。

業界にとって、これらの電子システムの安全性と信頼性は、常に検討事項であり続けてきたが、コネクテッドカーの並行開発と自動運転機能の利用拡大は、これらのシステムの安定性が今や業界の最優先事項であることを意味している。

車両システムの安定性とは何か？

HORIBA MIRAは、「車両システムの安定性(回復力)」という言葉を用いて、車両で使われる不可欠な電子システムの特徴または属性を指すために用いている。Figure 2に示すように、伝統的にあらゆる車両システム(電子システムに限らない)の開発では、故障モード影響解析(Failure Mode and Effect Analysis: FMEA)や故障の木解析(Fault Tree Analysis: FTA)などの故障モード回避技術を用いてシステムの信頼性を考慮してきた。

最近では、機能安全が開発ライフサイクルに不可欠な部分となって

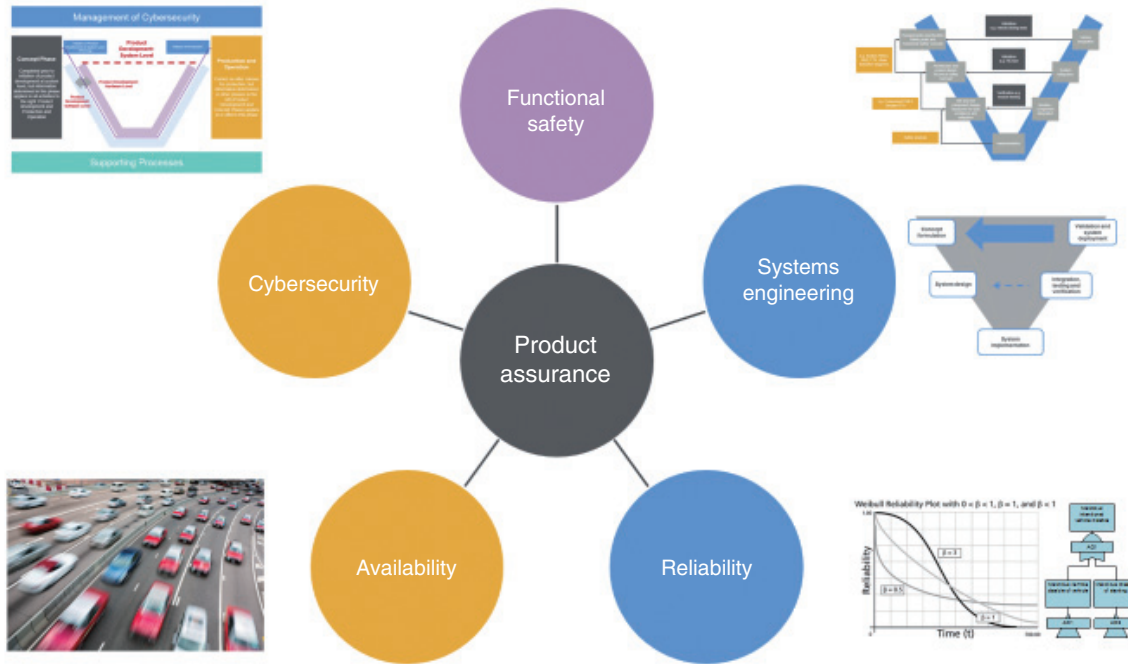


Figure 2 Product integrity and assurance in road vehicles

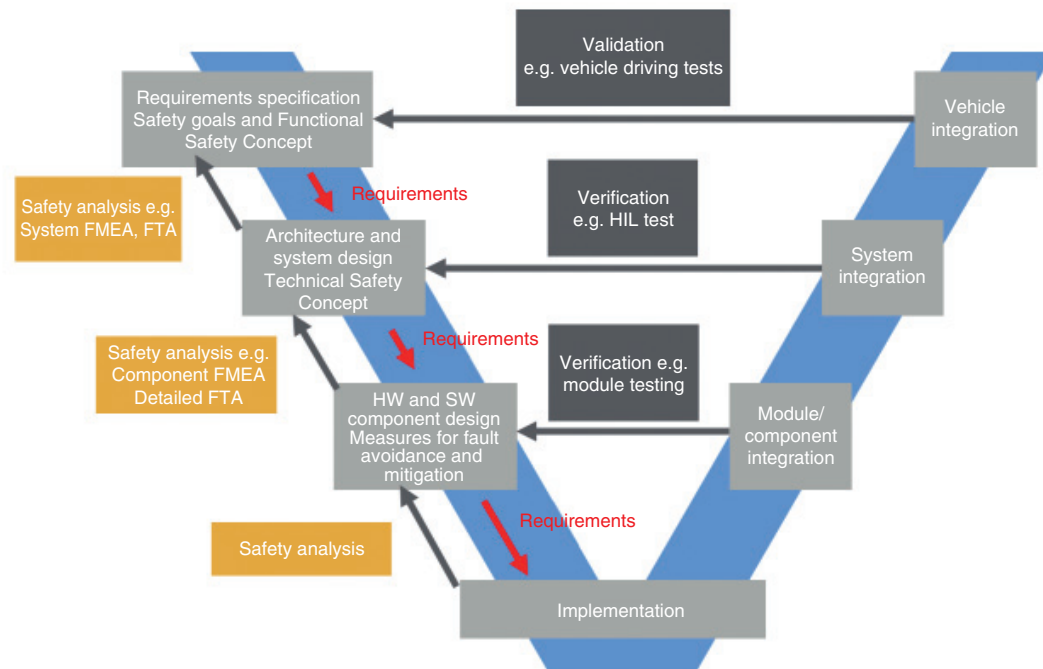


Figure 3 Concept of systems "V" model in ISO 26262

いる。最も広い意味では、機能安全は、関係するシステムの安全性全体の一部であり、技術ベースのシステムが入力に対して正確に作動する(すなわち、誤操作により潜在的に危険な状況を生み出さない)ことを示している。特に自動車産業においては、国際標準 ISO 26262^[1]が、電気・電子システムの誤作動に起因する危険の回避に関して定めている。

ISO 26262は、品質管理システムで規制されるような基礎的要件よりも厳密な要件をエンジニアリングプロセスに導入する。その主な理由のひとつとして、電子システムの複雑さゆえに、製品開発ライフサイクルの最後に試験を行い、見つかった問題に「事後的」

アプローチを適用するだけでは、製品が「正しい」ことを証明できないことが挙げられる。代わりに、システムの不具合の影響と不具合の原因を理解し、不具合の適切な防止策をシステムの設計に取り入れるために、システムエンジニアリングと信頼性解析の原理を適用することで、システムの信頼性を育むプロセスが求められる。ISO 26262は、他の機能安全基準と同様に、電子システムの設計に求められる厳密さを指すために「安全度」という言葉を用いている。また、ISO 26262は、Figure 3に示すようにシステムエンジニアリングにおける古典的な「V」モデルに基づいている。

2011年にISO 26262の初版が発行されて以来、業界はこの課題に

Table 2 A summary of the SAE Levels and example features; this is necessarily simplified and interpreted so the reader is referred to SAE J3016^[2] for full details.

SAE Level	Degree of automation	Driver in loop?	Example feature
0 – no automation	Warning only	Yes – full time	Lane Departure Warning (LDW)
1 – driver assistance	Speed only or steering only	Yes – full time	Lane Keep Assist (LKA)
2 – partial automation	Speed and steering	Yes – full time	Traffic Jam Assist (TJA)
3 – conditional automation	Full automation of specific driving tasks	Yes – part time, expected to respond to request to intervene within a defined period of time	Highway chauffeur
4 – high automation	Full automation of specific driving tasks	No – under defined constraints	Automated valet parking
5 – full automation	Full automation under all environmental and traffic conditions	No	Self-driving car that can execute a complete arbitrary journey

systems based upon electrical and electronic technology. It is not concerned with how to design safely other elements such as hydraulic components even though, by definition, these also come into the scope of a wider “functional safety” activity.

ISO 26262 introduces requirements for rigour in the engineering process that go beyond the base level of requirements such as those regulated by a Quality Management System. One of the key reasons for this is that, due to the complexity of the electronic systems, it is not possible to demonstrate that a product is “correct” simply by testing it at the end of the product development lifecycle and applying a “fly-fix-fly” approach to any issues found. Instead a process of building confidence into the system is required through applying the principles of systems engineering and reliability analysis to understand the consequences of malfunction of the system, the causes of malfunction and to ensure adequate defences against them are designed in to the system. ISO 26262, in common with other functional safety standards, uses the term “safety integrity” to refer to the rigour required in design of an electronic system. ISO 26262 is also based on the classical “V” model in systems engineering as shown in Figure 3.

However in reality many practitioners focus on malfunctions – avoiding random faults in hardware or systematic faults in the system, hardware or software design – rather than on malfunctioning behaviour. We will return later in this paper to consider some important additional factors

that are part of this wider term.

Since the initial publication of ISO 26262 in 2011, the industry has taken up the challenge and functional safety is now a core discipline in the design of vehicles and their components. However the two key growth aspects of autonomous functions and connected vehicles means that the required robustness of vehicles is a wider issue than safety integrity alone. We consider two of the key implications of these technologies to demonstrate the need to consider resilience, not only safety integrity.

Fail Operational Behaviour

In ISO 26262, there are a number of unwritten assumptions including

- The driver is part of the control loop of electronic systems and whether the driver can react to mitigate the outcome of hazards is considered during the hazard analysis activity.
- Fail-silent behaviour (i.e. to remove electronically-controlled functions) is generally considered as a suitable final reaction to system malfunction.
- “Drive by wire” functions in steering and braking retain a mechanical fall-back in case of total failure of the electronically controlled functions.

These assumptions are reasonable for a vehicle and systems where the driver is expected to be monitoring and controlling functionality on a full-time basis. These assumptions extend to some of the automated functions

取り組み、今や機能安全は、車両とその部品の設計において中心的な分野となっている。しかし、自動運転機能とコネクテッドビークルという二大成長分野においては、車両に求められる強靱性が、単なる安全度よりも幅広い問題であることを意味する。私たちは、これらの技術に含まれる二つの重要な意味を考え、安全度だけでなく回復力を考慮する必要がある。

故障時動作継続挙動

ISO 26262には、以下を含めて明示されていない多くの仮定がある。

- ・ドライバーは、電子システムの制御ループの一部であり、危害要因がもたらす結果を緩和するためにドライバーが対応できるかどうか、危害要因分析作業時に考慮される。
- ・フェイルサイレント挙動(すなわち、電子制御機能を取り除くこと)は、一般的にシステム不具合に対する適切な最終反応とみなされる。
- ・ステアリングとブレーキングにおける「ドライブ・バイ・ワイヤ」機能は、電子制御機能が完全に故障した場合に備えて機械的代替手段を保持する。

already being introduced, at least in systems defined as Level 1 or Level 2 functions in accordance with the SAE taxonomy of autonomous functions^[2], where the systems support some aspects of driving but the driver is expected to be in full-time control. Examples of this are seen in functions where the driver is still expected to keep hold of the steering wheel such as Lane Keep Assist (LKA), a Level 1 function, and Traffic Jam Assist (TJA), a Level 2 function.

As more advanced autonomous systems are introduced, the need for “fail operational” behaviour is emerging. “Fail operational” behaviour means that there are circumstances where it is not appropriate to remove the electronic function in case of malfunction and instead continued operation or “availability” over a defined period of time is required.

Example requirements for such behaviour include

- An electrical power steering system (EPAS) used as an actuator for a Level 3 lane-change function must have defined availability over the typical time required to complete such a manoeuvre;
- A Level 3 system might require to hand-over to the driver, and if the driver does not respond in a timely manner initiate a safe stop (“automatic emergency landing”);
- An arbitrary journey conducted “end to end” under full autonomy requires availability to complete the mission.

It is therefore acknowledged that future features associated with SAE Level 3 and above driver assist functions (leading up to full autonomy) have requirements for availability and to “fail operational”.

There are two principal solutions emerging to fail operational requirements. One solution is to use existing systems as a back-up, for example since electronic stability control (ESC) permits individual wheel braking this could be used for a short-term backup if EPAS fails although such a solution is likely to only be feasible to bring the vehicle to a safe stop in a relatively short time window,

これらの仮定は、ドライバーが機能性を常時監視して制御することを期待される場合には、車両とシステムにとって合理的である。これらの仮定は、少なくともLevel 1またはLevel 2のシステム(自動化機能のSAE分類^[2]による)に導入済みの自動化機能に適用される。こうしたシステムは特定の運転を支援するが、ドライバーはいつでも操作可能な状態にあることを期待されている。その例として、Level 1の車線維持支援機能(Lane Keep Assist : LKA)やLevel 2の渋滞支援機能(Traffic Jam Assist : TJA)などでは、ドライバーはステアリングホイールを保持し続けることを依然として期待されている。SAEのレベル区分と代表的な装備について概要をTable 2に示す。この表はやむを得ず内容を簡略化してある

The alternative solution is to provide some form of redundancy within the systems themselves so that they can continue operating in a defined manner in the presence of one or more failures. In ISO 26262 Edition 2 it is proposed to give some consideration to these types of fail operational requirements but these are currently at the level of hardware and software solutions to achieve a defined availability. Further guidance is needed to identify how this availability is identified and defined particularly in the areas of:

- Performing hazard analysis and risk assessment; we consider that a “layered” approach is required incorporating safety of the intended functionality (i.e. non-faulted behaviour), malfunctioning behaviour, and performance of a backup system (e.g. an “automatic land” function). Such an analysis may therefore result in different sets of safety requirements and attributes (integrity, availability) for the different layers.
- Methods that can be used to specify and evaluate architectures required for fail operational requirements. The present proposals in the draft of Part 5 (hardware) of ISO 26262 Edition 2 are focussed on hardware-level solutions e.g. microcontroller architectures. This guidance needs translating to the system architecture level. For example, for an EPAS that needs availability for the duration of an autonomous mission, should a classical “2 out of 3” redundant architecture be used?
- Specifying hardware targets (metrics) against random hardware failures. The current approach in ISO 26262 is based on a classical approach to hardware reliability but the methods and targets may need revisiting for availability requirements.

Cybersecurity

Another increasingly important aspect of resilience is cybersecurity. The electronic systems in modern vehicles are considered to be cyber-physical systems – that is, systems of collaborating computational elements controlling

ため、詳細についてはSAE J3016^[2]を参照のこと。

より先進的な自動運転システムの導入に伴い、「故障時動作継続」挙動の必要性が高くなっている。「故障時動作継続」挙動は、不具合発生時に電子機能を除去することが適切ではなく、代わりに継続的な動作または所定の時間での「可用性」が必要になることを意味する。

故障時動作継続の要件に対して、二つの主要なソリューションがある。ひとつは、既存のシステムをバックアップとして用いることである。もうひとつのソリューションは、ひとつまたは複数の

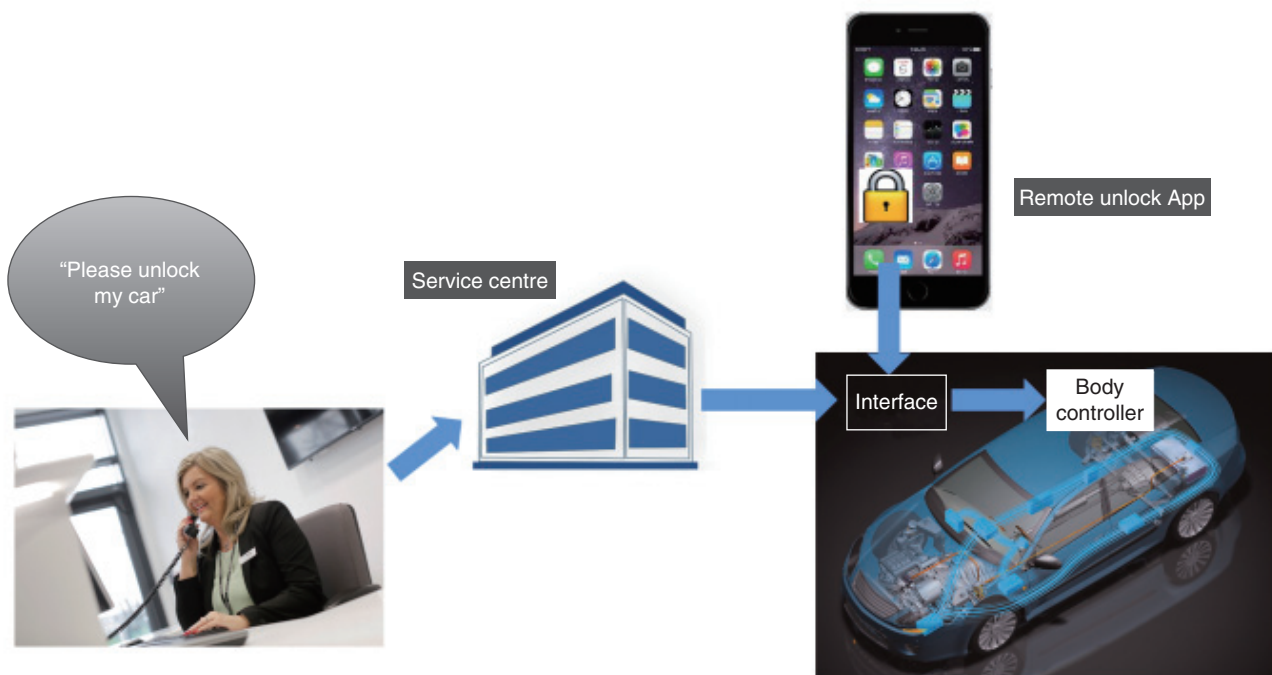


Figure 4 A typical connected car application – remote unlocking

physical entities. Due to the fact that vehicles and their systems have increasing levels of external connectivity, risk to cyber-physical systems may arise due to an attack exploiting a vulnerability in these connections. Cybersecurity refers to avoiding risk to cyber-physical systems due to an attack. Note that while cybersecurity often assumes malicious activity, accidental activity should also be considered (e.g. an enthusiastic vehicle owner who tries to make their own wireless connection to a vehicle system which has an unforeseen consequence).

Security of IT-based systems is a well-established discipline and is an important part of securing “connected car” applications. Figure 4 shows a typical application where remote unlocking of a vehicle is possible either by the vehicle owner using a smartphone App, or by making contact with a service centre that can issue a remote unlocking command. In this concept, all of the assets shown are potential attack points for an attacker for example by:

- Impersonating the owner calling the centre;
- Social engineering of the service centre personnel to gain access to credentials;
- Conducting a “man in the middle” attack on the communications between the service centre and the vehicle, or between the smartphone and the vehicle;
- Introducing a compromised App into the smartphone.

When evaluating cybersecurity risk, the severity of consequences and the likelihood of mounting a successful attack need to be considered. Consequences of a cybersecurity attack may include loss of privacy, financial loss to owners, operators or manufacturers of vehicles, loss of reputation, operational limitations and safety concerns. The likelihood of mounting a successful attack depends on a number of factors including whether a potential attacker needs access to specific information about the

故障が存在してもシステムが所定の方法で動作を続けられるように、システム自体の中になんらかの形の冗長性を持たせることである。

サイバーセキュリティ

回復力に関して重要性を増しているもうひとつの側面が、サイバーセキュリティである。注意すべき点として、多くの場合、サイバーセキュリティは悪意ある行為を想定しているが、偶発的行為も考慮すべきである。

IT ベースのシステムのセキュリティは、確立された専門分野であり、「コネクテッドカー」アプリケーションの保護における重要な部分である。Figure 4に示す典型的なアプリケーションでは、車両の所有者がスマートフォンアプリを用いて、またはリモートロック解除コマンドを発行可能なサービスセンターに連絡することにより、車両のリモートロックを解除することができる。このコンセプトでは、示されているすべての資産が、以下の例のような攻撃を受ける可能性がある。

- ・所有者になりすましてセンターへ電話をかける。
- ・サービスセンターのスタッフがソーシャルエンジニアリングに

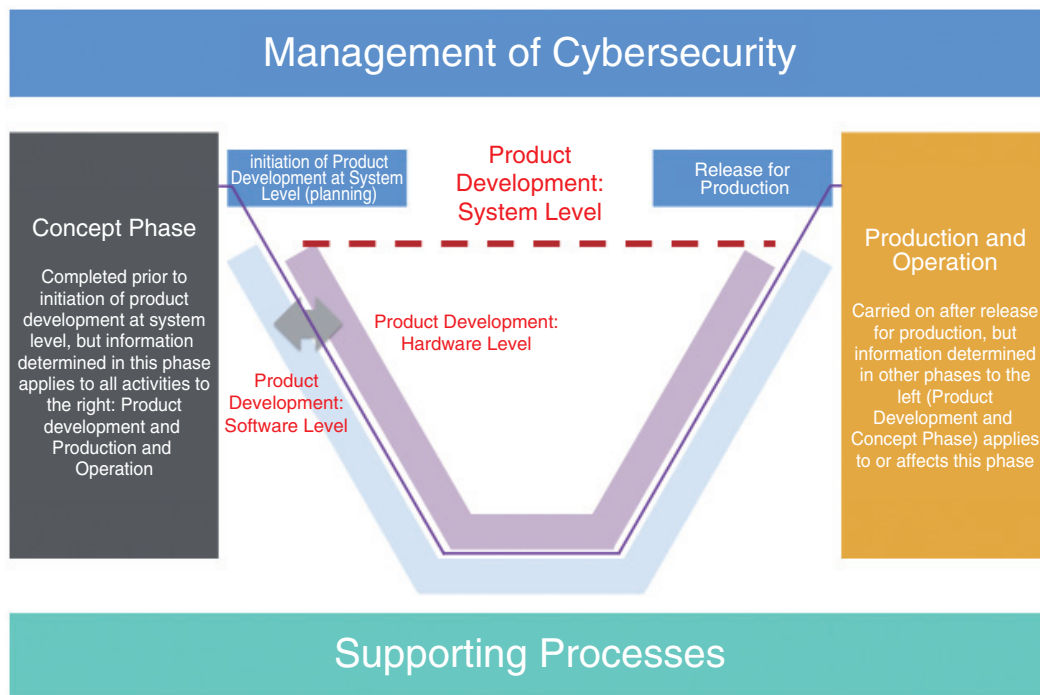


Figure 5 SAE J3061™ lifecycle. © SAE International

system and specialist tools or resources, and the time needed to develop the exploit^[3].

In terms of approaches for protecting cyber-physical systems, established IT security principles need to continue to be applied to assets such as back office systems and App development. However specialized techniques are needed for in-vehicle aspects where the security countermeasures need to be scaled to align with the requirements of real-time embedded control systems. It should also be noted that many aspects of research into vehicle cybersecurity are focussing on the external interfaces and how to secure this against attack; however this must be seen as the first line of defence. Given the continually developing nature of cybersecurity threats, a “defence in depth” strategy that also covers aspects such as internal communications buses in the vehicle is also needed to help defend the system against “zero day” exploits – once a vulnerability in an interface is discovered, it is immediately exploitable until an update is applied to resolve it.

The automotive industry has recognized the need for standards to address cybersecurity development of embedded systems and has recently published an SAE Recommended Practice J3061™, Cybersecurity Guidebook for Cyber-Physical Vehicle Systems^[4]. A key aspect of this document is that it recommends a lifecycle for cybersecurity engineering that is derived from the ISO 26262 safety lifecycle and can also be aligned with it. This recognizes that functional safety and cybersecurity share many common aspects and that certain activities need to be harmonized, for example a cybersecurity attack may be the cause of a functional safety hazard. The J3061™ lifecycle is shown in Figure 5.

A further important aspect of cybersecurity concerns testing and evaluation. The industry needs to work with trusted partners who can evaluate and demonstrate cybersecurity concerns and solutions in safe and secure environments, rather than using public infrastructure for studies and demonstrations. This will require the development of appropriate capabilities for conducting research

より機密情報へのアクセスを得る。

- ・ サービスセンターと車両の間、またはスマートフォンと車両の間の通信への「中間者」攻撃の実施。
- ・ スマートフォンへの不正アプリの導入。

自動車産業は、組み込みシステムのサイバーセキュリティ開発に取り組むには基準が必要であることを認識しており、最近、SAE推奨基準 J3061™「サイバーフィジカル車両システムのためのサイバーセキュリティガイドブック (Cybersecurity Guidebook for Cyber-Physical Vehicle Systems)^[4]」を発行した。この文書の重要な側面は、ISO 26262の安全ライフサイクルに由来し、同基準と

整合可能なサイバーセキュリティエンジニアリングのライフサイクルを推奨していることである。このガイドブックは、機能安全とサイバーセキュリティが多くの共通の側面を共有し、いくつかの活動を調和させる必要があることを認識している。たとえば、あるサイバーセキュリティ攻撃は、機能安全危機の原因となる可能性がある。J3061™ライフサイクルをFigure 5に示す。

回復性のその他の側面

上記の明らかになりつつある側面の他にも、以下を含め、システムの回復性に寄与する多くの要素がある。

into potential vehicle vulnerabilities in a confidential manner, and enabling evaluation of real vehicles and systems in a secured environment. Typical requirements for such evaluations could include:

- A quarantined environment where resilience evaluation can be conducted using realistic infrastructure (e.g. cellular communications) without disrupting public services;
- The ability to exercise vehicles and their systems in realistic operating conditions (e.g. driving at speed, concerning with a stability control intervention) without the use of public roads;
- The ability to combine multiple aspects of resilience during an evaluation e.g. combining electromagnetic interference with exploitation of a security vulnerability;
- Conducting evaluations according to a well-defined code of ethics e.g. in terms of confidentiality.

Other Aspects of Resilience

Besides the emerging aspects noted above, there are a number of other factors that contribute to resilience of systems. These include:

- Human interactions: for example ensuring that clear and understandable information on the operation of a system is given to the driver, that such information is not distracting, and that the interfaces are defined in such a way that the possibility of mis-operation by the driver is avoided.
- The behaviour of mechanical systems as a cause of the behaviour of electronic systems: some practitioners take a very narrow view when applying ISO 26262 but it is important to consider all external interfaces and the influence that these may have on correct operation of the system.

Conclusions

Systems engineering and reliability analysis techniques have provided a strong foundation for many of the

challenges faced in the current generation of vehicles, as reflected in practices such as ISO 26262. To face the challenges of future vehicles, including connected cars and greater use of autonomy, a cross-disciplinary approach based on the concept of resilience is required. This encompasses many of the attributes required including safety integrity, availability, reliability and cybersecurity.

References

- [1] ISO 26262:2011, "Road vehicles - Functional safety"
- [2] SAE J3016, "Surface Vehicle Information Report, Taxonomy and Definitions for Terms Related to On-Road Motor Vehicle Automated Driving Systems", January 2014.
- [3] ISO/IEC 18045:2008, "Information technology - Security techniques - Methodology for IT security evaluation".
- [4] SAE J3061™, "Surface Vehicle Recommended Practice, Cybersecurity Guidebook for Cyber-Physical Vehicle Systems", January 2016.



David WARD

General Manager
Functional Safety
HORIBA MIRA Ltd.
Ph. D.

- ・人間との相互作用：たとえば、システムの動作に関する明確で理解可能な情報をドライバーに与えること、その情報がドライバーの注意をそらせることないこと、そしてドライバーの誤操作が避けられるようにインターフェイスが定められていること。
- ・電子システムの挙動の原因となる機械システムの挙動：専門家がISO 26262を適用する際には視野が狭くなりがちであるが、あらゆる外部インターフェイスと、それらがシステムの正確な動作に及ぼす影響を考慮することが重要である。

まとめ

システムエンジニアリングと信頼性解析技術は、ISO 26262などの基準に反映されているように、現世代の自動車が直面する課題の多くに強力な基盤を提供してきた。コネクテッドカーや自動運転の利用拡大を含む今後の自動車の課題に対応するためには、回復力のコンセプトに基づく分野横断的なアプローチが求められる。これには、安全度、可用性、信頼性、サイバーセキュリティなどの必要な属性の多くが含まれる。