Proceedings of 7th Transport Research Arena TRA 2018, April 16-19, 2018, Vienna, Austria

Towards a risk-based approach for the design of highly resilient future vehicles

Alastair R. Ruddle*

HORIBA MIRA Limited, Watling Street, Nuneaton, CV10 0TU, UK

Abstract

Current technological trends in transportation are towards increasing levels of automation, and ultimately to fully autonomous operation, as well as greater wireless connectivity. Although cars are among the best known examples, similar trends are also found in hazardous industrial environments, as well as in the marine and aerospace sectors. However, as the role of the driver/operator is progressively removed from vehicle control, the electronic systems that replace the human inputs will need to provide extremely high levels of dependability in order to ensure the public acceptability of these technologies. Thus, the electronic systems of future vehicles, as well as the intelligent transport systems that they interact with, will need to be designed to ensure a high degree of resilience to a wide range of threats. This paper outlines the elements of a unified risk-based approach to support the development of future vehicles that are highly resilient to environmental and criminal threats, thus ensuring acceptable levels of functional safety, safety of the intended functionality, cyber security and mission-critical functionality.

Keywords: Cyber security; electromagnetic field exposure; functional safety; risk analysis; system safety; system engineering; vehicle resilience.

* Corresponding author. Tel.: +44-247-635-5551; fax: +44-247-635-8551.
E-mail address: alastair.ruddle@horiba–mira.com

1. Introduction

One of the most significant of current trends in transportation is towards increasing levels of automation, and ultimately to fully autonomous operation, of vehicles. Although cars are among the best known examples (e.g. the Google car), similar trends are also to be found in hazardous industrial environments, as well as in the marine and aerospace sectors. However, as the role of the driver/operator is progressively removed from vehicle control, the electronic systems that replace the human inputs will need to provide extremely high levels of dependability in order to ensure the acceptability of these safety-related technologies to society. Furthermore, other major technological trends, such as increasing wireless connectivity and the rise of the internet-of-things, are making a much wider of range systems, including vehicles and transport infrastructure, potential targets for cyber security attacks.

In addition, the trend towards increasing electrification of vehicle powertrains has dependability implications for the electrical powertrain hardware and software, and safety implications in terms of high voltages and human exposure to low frequency magnetic fields associated with fluctuating traction currents and associated technologies such as wireless power transfer for traction battery charging. Interest in light-weight alternatives to traditional steel body structure has resulted in wider use of materials with limited or negligible electromagnetic shielding properties, with potential implications for the electromagnetic compatibility (EMC) of electronic systems, wireless communications performance, and human exposure to electromagnetic fields (EMF) up to mm-wave frequencies.

Thus, the electronic systems of future vehicles, as well as the intelligent transport systems that they may interact with, will need to be designed to ensure a high degree of resilience to a wide range of threats to their safety, security and mission-critical functionality. This paper outlines the elements of a unified risk-based approach to support the development of future vehicles that are highly resilient to these threats. Although the focus of this paper is primarily on automotive applications, the approach is equally applicable to other types of vehicle, and could also be adapted to other applications involving cyber-physical systems.

2. Vehicle resilience

The notion of resilience occurs in a disparate range of domains, including various branches of engineering as well as economics and the social sciences, amongst others. In essence, resilience is the ability to cope with change, but in terms of vehicle operation requires the ability to ensure the continued execution, or timely resumption, of its essential functions, safely and securely, accommodating/mitigating foreseeable safety hazards and other threats, and enable graceful degradation of performance otherwise. These threats may arise from criminal activity (e.g. hacking), but may also be due to technological issues (such as electromagnetic interference originating from on-board or off-board systems, or antenna performance limitations), or environmental effects such as the weather.

In Europe, the Whole Vehicle Type Approval (WVTA) legislation specifies the minimum requirements that vehicles must meet before they can be placed on the market (EU, 2007). Nonetheless, many vehicle manufacturers aim to exceed these minimum requirements, and instead employ their own in-house specifications. Their objectives in doing this include ensuring reliability and customer satisfaction, as well as providing a degree of "future-proofing" against potential changes in the operational environment over the lifetime of the vehicle.

In addition to this, a number of independent organizations in Europe carry out assessments of vehicles that also go beyond WVTA requirements, particularly in relation to vehicle safety and security, and make these results available to the public. These activities are motivated by government and consumer organisations, as well as by the insurance industry, who wish to promote enhanced safety for vehicle occupants and pedestrians during accidents, as well as improved levels of security against theft of vehicles and theft from vehicles. However, there are limitations in relying solely on standards, such as their focus on the intended use scenarios and the pace of development, which is becoming so rapid that it is increasingly difficult for standards to maintain their relevance.

Historically, development activities have largely been focused on the "intended use" of the vehicle, which includes its assumed behaviour and operating environment. However, this represents only a subset of all possible uses, and is complemented by the "unintended uses" (e.g. unintended behaviours such as EMC effects, or use in different environments), which can be considered in terms of those that are potentially "foreseeable" and those that are "unforeseeable" (see Fig. 1). Moreover, a subset of the unintended uses also includes "intentional misuses", such as hacking into vehicle systems or use of a car as a weapon, at least some of which will be reasonably foreseeable.

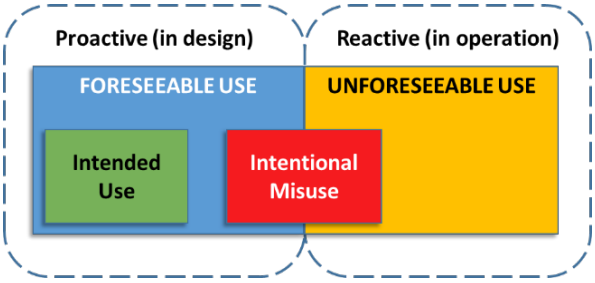

Fig. 1 Potential usage scenarios (shaded) and mitigation approaches (dashed)

However, the emergence of unforeseeable uses is inevitable, given the long operational lifetime of a car, the increasingly rapid pace of societal and technological change, possible climate change, and human ingenuity. Thus, consideration of the unintended usage scenarios will be essential for the development of resilient vehicles. Prior experience with computers and mobile phones, for example, makes it clear that cyber security attacks on intelligent and wirelessly connected vehicles are inevitable. In order to maximize resilience, a proactive approach is required at the design stage that takes account of the foreseeable hazards and threats, including foreseeable intentional misuse as well as foreseeable unintended usage scenarios, and takes steps to identify and mitigate those hazards/threats with the most severe implications. Inevitably some scenarios will be unforeseeable, and for these the response can only ever be reactive, responding to hazards and threats as they are identified during operation. Thus, threat intelligence gathering is an essential background activity in order to maximize knowledge of the foreseeable threats during future design activities and to ensure a timely response to emerging threats that are identified during the operational phase of the vehicle lifecycle.

Best practice design guidelines are also widely used by many engineering disciplines during development, but in many cases practical constraints and higher priorities from other disciplines may restrict the ability of the designer to comply with such recommendations. For example, in many applications the best location for an antenna is on the roof of the vehicle, but styling considerations and the proliferation of communications services are resulting in increasing pressure to avoid this location and exploit non-ideal mounting locations. This leaves the problem of how best to allocate priorities, by deciding where it is desirable to enforce (or acceptable to relax) compliance with best practice, and/or how to quantify and mitigate the anticipated performance shortfalls.

Thus, in order to maximize vehicle resilience it will be necessary to identify and mitigate those of the foreseeable threats/hazards that are associated with the most significant risks. The identification, analysis and mitigation of foreseeable safety hazards to achieve tolerable levels of risk is already widely undertaken in many industries, using a risk-based analysis approach in order to address the functional safety of electronic control systems.

3. Functional safety

The safety implications of programmable electronic control systems, which are often used to provide safety-related functions, have long been taken very seriously. However, it is recognized that completely eliminating safety risks is both impracticable and unaffordable. This has led to the development of a more pragmatic risk-based approach for assessing the functional safety of programmable electronic control systems, which is reflected in standards such as IEC 61508 (IEC, 2010) for process control applications, and ISO 26262 (ISO, 2011) for automotive applications. Risk analysis is a key element of IEC 61508, which reflects the following views on safety risks:

- zero risk is unachievable;
- safety must be considered from the outset;
- where risks are considered unacceptable, measures must be employed to reduce the risks to a level that is considered to be “broadly acceptable”.

In safety engineering a “safety hazard” is a source of possible “harm” to life, health, property or the environment. The “severity” of the outcome is a measure of the expected degree of harm that may result from that hazard in a specific situation. The associated “risk” is then a combination of the likelihood of occurrence of harm and the severity of that harm, such that the risk increases with greater probability and/or severity. In the functional safety approach, the safety hazards associated with potential failures of programmable electronic control systems are

identified and their associated severity and likelihood are evaluated, thus allowing their relative risk levels to be assessed. Measures can then identified that will reduce significant risks to tolerable levels.

In some sectors it is feasible to derive quantitative measures for the probability and severity parameters, with the result that the derived risk can also be quantified (e.g. IEC 61508, which was developed for process industries). In other applications, however, it is only possible to rank these measures in a qualitative manner. Such qualitative rankings often employ a classification based on order of magnitude differences, an approach that is adopted in ISO 26262. The severity classification of ISO 26262 (see Table 1) is linked to the Abbreviated Injury Scale (AIS) of the Association for the Advancement of Automotive Medicine (AAAM, 2005). In ISO 26262 the likelihood of harm occurring is rated in terms of likely "exposure" to the hazard (see Table 2) which is moderated by its "controllability" for an average driver (see Table 3). These three parameters are mapped (see Table 4) to the automotive safety integrity level (ASIL), which ranges from QM (i.e. requiring only conventional quality management approaches) where the risks are low, through to ASIL D (requiring the most rigorous development processes) where the risks are perceived to be at the highest tolerable level.

The purpose of risk analysis is to allow the analyst to identify and prioritize requirements for mitigating the risks, and thus ensure that the residual risks are acceptable. These activities can only be undertaken when the system characteristics and intended operating environment have been defined. Nonetheless, it is important to note that risk analysis activities can be initiated at the concept stage, and that this should be undertaken in order to ensure that risks are considered from the outset of the development lifecycle. The preliminary risk analysis can then be progressively refined as the design matures and the details become better defined, which may also lead to the identification of additional hazards that will need to be taken into account.

Table 1. ISO 26262 safety hazard severity categories.

Characteristics	Severity category			
	S0	*S1*	*S2*	*S3*
Description	No injuries	Light and moderate injuries	Severe and life-threatening injuries (survival probable)	Fatal and life-threatening injuries (survival uncertain).
Definition (normative)	<10% probability of AIS 1–6 injuries Damage not considered safety-related	>10% probability of AIS 1–6 injuries (and not S2 or S3)	>10% probability of AIS 3–6 injuries (and not S3)	>10% probability of AIS 5–6 injuries

Table 2. ISO 26262 safety hazard exposure categories.

Characteristics	Exposure category				
	E0	*E1*	*E2*	*E3*	*E4*
Description	Incredibly unlikely	Very low probability	Low probability	Medium probability	High probability
Duration related definition	Not specified	Not specified	< 1% of average operating time	1–10% of average operating time	> 10% of average operating time
Frequency related definition	Not specified	Situations that occur less often than once a year for the great majority of drivers	Situations that occur a few times a year for the great majority of drivers	Situations that occur once a month or more often for an average driver	All situations that occur during almost every drive on average

Table 3. ISO 26262 vehicle controllability categories.

Controllability category	Meaning
C0	Controllable in general
C1	Simply controllable
C2	Normally controllable
C3	Difficult to control or uncontrollable

Table 4. ISO 26262 safety risk mapping.

Severity category	Exposure category	Controllability category			
		C0	*C1*	*C2*	*C3*
S1	*E0*	QM	QM	QM	QM
	E1	QM	QM	QM	QM
	E2	QM	QM	QM	QM
	E3	QM	QM	QM	ASIL A
	E4	QM	QM	ASIL A	ASIL B
S2	*E0*	QM	QM	QM	QM
	E1	QM	QM	QM	QM
	E2	QM	QM	QM	ASIL A
	E3	QM	QM	ASIL A	ASIL B
	E4	QM	ASIL A	ASIL B	ASIL C
S3	*E0*	QM	QM	QM	QM
	E1	QM	QM	QM	ASIL A
	E2	QM	QM	ASIL A	ASIL B
	E3	QM	ASIL A	ASIL B	ASIL C
	E4	QM	ASIL B	ASIL C	ASIL D

4. Cyber security

Like safety, the elimination of cyber security risks is similarly impracticable and unaffordable, perhaps even more so as the security threat environment is constantly changing due to rapid technological development and the human ingenuity of attackers. Furthermore, a subset of security threats could potentially lead to safety hazards for cyber physical systems. Consequently, the EVITA project adapted the risk-based approach of functional safety for assessing automotive cyber security risks, providing the basis for a unified approach that allows the safety-related security analysis to be re-used in functional safety analysis (Ruddle et al., 2009). This was achieved by extending the ISO 26262 notion of severity from a single injury-based parameter to a multi-dimensional severity vector that includes not only possible impacts on safety, but also the potential for other types of "harm" that could result from information security breaches. The additional harm categories include financial losses, compromised privacy, and loss of system functionality that is not safety-related (see Table 5). Furthermore, the potential for these effects to be readily replicated in large numbers of vehicles, either of the same type or of different types but with the same or similar security vulnerabilities, was also taken into account. This results in a severity category (denoted *S4* in Table 5) that goes beyond the current range of ISO 26262, since the ISO 26262 severity scale does not consider the potential for readily duplicating deliberate attacks that may have very severe consequences for physical safety.

Table 5. Severity classification proposed in EVITA project for automotive cyber security threats.

Severity category	Categories of harm to stakeholders			
	Safety (S_S)	Privacy (S_P)	Financial (S_F)	Operational (S_O)
S0	No injuries.	No unauthorized access to data.	No financial loss.	No impact on operational performance.
S1	Light or moderate injuries.	Anonymous data only (no specific driver or vehicle data).	Low-level financial loss (~€10^1).	Operational impact not discernible to driver.
S2	Severe and life-threatening injuries (survival probable).	Identification of vehicle or driver.	Moderate financial loss (~€10^2).	Driver aware of performance degradation.
	Light/moderate injuries for multiple vehicles.	Anonymous data for multiple vehicles.	Low losses for multiple vehicles.	Indiscernible operational impacts for multiple vehicles.
S3	Life threatening (survival uncertain) or fatal injuries.	Driver or vehicle tracking.	Heavy financial loss (~€10^3).	Significant impact on operational performance.
	Severe injuries for multiple vehicles.	Identification of driver or vehicle, for multiple vehicles.	Moderate losses for multiple vehicles.	Noticeable operational impact for multiple vehicles.
S4	Life threatening or fatal injuries for multiple vehicles.	Driver or vehicle tracking for multiple vehicles.	Heavy financial losses for multiple vehicles.	Significant operational impact for multiple vehicles.

For the purposes of assessing the likelihood associated with cyber security threats, a probability ranking based on the inverse of the "attack potential" classification of ISO/IEC 18045 (ISO/IEC, 2008), moderated by the vehicle controllability (see Table 3) as appropriate for safety-related security threats, was adopted in EVITA in order to enable the identification of security-related risk levels (Ruddle et al., 2009). Attacks with low attack potential are those that are judged to be relatively easy to implement, therefore representing a high probability of such attacks being undertaken, whereas high attack potential reflects more difficult attacks with a correspondingly low probability of exposure to such threats.

The EVITA risk analysis was based on attack trees (Schneier, 2000), which were constructed in order to describe potential "attack methods" (i.e. sequences of steps) and to allow corresponding probabilities for successful attacks to be derived. Starting from high level attack goals, where the severity of the outcome can be assessed in terms of specific harm to particular stakeholders, the top-down attack tree analyses allowed a number of specific attacks on particular system assets to be identified. The attack potential was then assessed at the asset attack level, following which the attack tree logic can be used to derive the probability of achieving the desired attack goal. If an attack method can be implemented using any one of a number of possible asset attacks (i.e. an OR relationship), then the combined attack success probability is taken to be the highest of the attack success probabilities for the possible asset attack options (i.e. it is as easy as the easiest option). Where the attack method requires a conjunction of asset attacks (i.e. an AND relationship), then the combined attack success probability is taken to be the lowest of the attack success probabilities associated with the contributing asset attacks (i.e. it is as hard as the hardest of the essential steps).

A risk graph for cyber security threats was also proposed in the EVITA project (Ruddle et al., 2009), providing a mapping between the probability of successful attack, the security-related severity classifications of Table 5, and the controllability (see Table 3) for safety-related security threats. In addition, a mapping between the EVITA risk levels and the integrity levels of ISO 26262, IEC 61508, IEC 15408 (IEC, 2009) and the Motor Industry Software Reliability Association (MISRA) safety integrity levels (MISRA, 1994; MISRA 2007) has also been proposed (Ruddle and Ward, 2016).

5. Mission-critical functionality

The EVITA severity measures illustrated in Table 5 include an "operational" category, which represents loss of system functionality that is not safety-related, since one of the EVITA objectives was to separate out the safety-related aspects for treatment according to established ISO 26262 methods. Nonetheless, the non-safety operational impacts that were envisaged could range from the undetectable through to more significant effects of mission-critical importance, either because the vehicle is unable to perform essential functions, or exhibits behaviours of major irritation to vehicle users. Regarding the latter, unsatisfactory radio reception is among the most common sources of complaints from car owners. Customer satisfaction is certainly an aspect that is of critical economic importance to vehicle manufacturers. Satisfactory radio reception is therefore mission-critical in this sense, even though it has no impact on the primary vehicle function of providing transportation.

For threats to mission critical functions that are security related the "operational" component of the EVITA severity classification (see Table 5), together with the EVITA probability classification and risk mapping, provide methods for identifying relative risk levels. However, cyber security breaches are not the only possible origin of such non-safety operational impacts. For example, the corruption of a critical signal due to EMC effects that prevents the vehicle from starting, or loss/degradation of communications due to antenna performance limitations in some environments, or critical sensor data that is lost/unreliable under some climatic conditions, could be regarded as severe failures of mission-critical functions. It is equally important to address risks of this nature in order to achieve the goal of vehicle resilience.

In the aerospace industry, the Radio Technical Commission for Aeronautics (RTCA) has defined Development Assurance Levels (DALs) that are used in order to identify quantitative failure rate requirements for aircraft systems (RTCA, 2000; RTCA, 2011). Although the RTCA DALs are focused primarily on physical safety issues, they also take account of non-safety operational aspects, such as aircraft operation and crew workload. Thus, both safety and mission-critical functionality are compounded in the RTCA DALs.

Risks associated with vehicle functions that are neither safety nor security related but are nonetheless considered to mission-critical in some sense could be assessed in an analogous risk-based approach, using the exposure

classification (see Table 2) and risk graph (see Table 4) of ISO 26262 together with a severity classification for degradation of mission critical functions such as that proposed in Table 6 below. It should be noted that the "controllability" considerations used in functional safety assessments (see Table 3) are not relevant for the assessment of risks associated with the mission-critical functions considered here.

Table 6. Proposed severity categories for mission-critical threats (not safety or security related)

Characteristics	Severity category			
	S0	*S1*	*S2*	*S3*
Description	No impact on critical function	Critical function impairment barely discernible to driver	Driver aware of impaired critical function	Significant impact on critical function

The ISO 26262 exposure could be applied for this analysis, with the IEC 61508 or MISRA risk graphs since controllability in relevant here. However, it is first necessary to identify the functions and potential threats. An abstract functional model of the system can assist with many aspect of this process, including the analysis of functional safety (e.g. Ruddle et al., 2013), as well as threats to cyber security and mission-critical functionality.

6. Electromagnetic field exposure – safety of the intended functionality

Functional safety is concerned with the potential safety implications of failures in programmable electronic control systems. Some systems, however, also have the potential to present possible safety hazards even when operating correctly. For example, radio transmitters and wireless battery charging systems are potential electromagnetic compatibility (EMC) threats to other on-board electronic systems that could have implications for their availability and safe operation. However, electromagnetic fields are also known to produce undesirable physiological effects on human tissues (ICNIRP, 1998). Consequently, high frequency radio transmissions in and around vehicles (such as communications, radar etc.) may also present potential electromagnetic field exposure hazards for vehicle occupants (Ruddle, 2016), as well as other road users and bystanders. Furthermore, the stray low frequency magnetic fields associated with high voltage electrical powertrain systems may also present human field exposure hazards (Vassilev at al., 2015) as well as potential EMC threats to equipment such as active implanted medical devices (AIMD) or devices that are body-worn (Ruddle, Armstrong and Galarza, 2015). Analysis of such "safety of the intended functionality" (SOTIF) could also be addressed using a risk-based approach adapted from functional safety in a similar way to that used for cyber security. Controllability is not relevant in this application.

Potential health and safety hazards associated with electromagnetic fields are complex and frequency dependent, including both direct physiological effects and indirect effects on medical implants and body-worn devices. Thus, in order to identify appropriate severity ratings for electromagnetic effects on humans it is again useful to consider the severity of field exposure not as a single parameter, but instead as a vector with separate components as for cyber security. These components could relate to well-established acute physiological effects (including tissue heating and electro-stimulation of the nervous system), heating of metallic implants, and electromagnetic interference with active medical devices, as well as possible chronic effects. Where there is uncertainty about effects and threshold levels (such as chronic effects, metallic implant heating etc.) this could be accommodated by allocating more conservative severity ratings. The highest component rating could then provide an overall rating.

Various national and international bodies have recommended limits on human exposure to electromagnetic fields (e.g. ICNIRP, 1998; EU, 1999; EU, 2013), which vary with frequency and physiological effect, often using different exposure metrics, thus making assessment of the associated risks an even more complex process. Furthermore, the exposure limits are generally specified in terms of in-body quantities that are difficult or impossible to measure. Although proxy measures of the field environment as also permitted for exposures that are not highly localized, these also differ between physiological effects. For example, electrostimulation of the nervous system is assessed in terms of the instantaneous maximum field in the environment (denoted $|\mathbf{E}|$ and $|\mathbf{H}|$, for the electric and magnetic fields, respectively, in Tables 7–8 below), whereas tissue heating is assessed in terms of time-averaged field levels (denoted $\langle\mathbf{E}\rangle$, $\langle\mathbf{H}\rangle$ and $\langle\mathbf{S}\rangle$, for the electric and magnetic fields and power density, respectively, in Tables 7–10 below). Electrostimulation is not believed to result in long term physiological damage, but could potentially affect a driver's ability to control the vehicle due to twitches, illness (e.g. nausea), and associated distraction. Tissue heating, however, could potentially result in irreversible physiological damage.

Electrostimulation is considered to be the most significant acute physiological effect for frequencies from 1 Hz to 100 kHz (ICNIRP, 1998; EU, 1999; EU, 2013), which includes frequencies associated with time-varying traction

current and wireless charging of traction batteries. No limits relating to tissue heating are provided by 1999/519/EC below 100 kHz since heating is considered to be less significant at these frequencies. Nonetheless, heating of metallic implants is a potential hazard even at these frequencies, and low frequency magnetic fields could readily couple into the body to induce currents in the leads of active implanted medical devices (AIMD) such as pacemakers. Such effects on medical implants are considered to be beyond the scope of ICNIRP (ICNIRP, 1998) and related documents (EU, 1999; EU, 2013). However, the general public field reference levels recommended by ICNIRP (ICNIRP, 1998) have provided the basis for EMC test specifications for AIMD (e.g. CENELEC, 2004). The potential for heating of passive metallic implants at these field levels has also been considered in a few studies (Anderson and McIntosh, 2008), although not for frequencies below 100 kHz. Thus, AIMD and metallic implant responses at fields beyond ICNIRP 1998 general public levels are unknown.

At high frequencies it is not possible to compare the field reference levels directly with the immunity test specifications for AIMD. The AIMD immunity test levels are specified for devices to be tested outside the body, but the in-body fields are not readily related to the external field environment due to the complex interactions between the electromagnetic field and the body tissues. At low frequencies, however, the magnetic field in the body is essentially the same as the external magnetic field, since the magnetic permeability of body tissues is very close to that of free space and the conductivity is sufficiently low that the secondary magnetic fields associated with the currents induced in the body tissues are negligible. Results from numerical simulations of an inhomogeneous human simulant (with 35 different tissue types) exposed to uniform magnetic fields at frequencies from 10 Hz to 1 GHz indicate that the impact of the induced currents begins to become noticeable for frequencies above around 1 MHz (Leitgeb, Niedermayr and Loos, 2013). In the low frequency range, therefore, it is possible to relate the EMC immunity requirements for pacemakers to external magnetic field levels.

Electromagnetic field exposures in the automotive environment are also spatially non-uniform, with the result that exposure characteristics in different regions both within and outside the vehicle may well be different. In addition, therefore, it may also useful to consider the severity of the field exposure in relation to the field reference levels, or equivalent parameters, that are recommended in relevant documents (ICNIRP, 1998; EU, 1999; EU, 2013). Thus, a matrix of severity ratings corresponding to different field levels and effect categories could be assembled. However, as the importance of different effects changes with the frequency of the electromagnetic field the severity classifications must also be subdivided by frequency range, as outlined in Tables 7–10, which suggest illustrative examples based on the field reference levels recommended by the EU for general public (EU, 1999) and occupational (EU, 2013) exposures. In these tables, the highest severities for each field level are highlighted in a bold font. For frequencies below 100 kHz direct heating of human tissue is not considered to be significant, and is thus absent from Table 7. For frequencies from 100 kHz to 10 MHz, both electrostimulation and tissue heating are considered to be important, so both of these acute effects are represented in Table 8.

Table 7. Proposed severity classes for human electromagnetic field exposure threats: 1 Hz to 100 kHz.

Field exposure relative to EU field reference levels	Severity categories for direct and indirect effects			
	Electrostimulation effects	Metallic implant heating	AIMD EMC	Possible chronic effects
$\|\mathbf{E}\|, \|\mathbf{H}\| << 1999/519/EC$	***S0***	***S0***	***S0***	***S0***
$\|\mathbf{E}\|, \|\mathbf{H}\| \leq 1999/519/EC$	*S0*	***S1***	***S1***	***S1***
$1999/519/EC < \|\mathbf{E}\|, \|\mathbf{H}\| < 2013/35/EU$	*S2*	*S2*	***S3***	*S2*
$\|\mathbf{E}\|, \|\mathbf{H}\| > 2013/35/EU$	***S3***	***S3***	***S3***	***S3***

Table 8. Proposed severity classes for human electromagnetic field exposure threats: 100 kHz to 10 MHz.

Field exposure relative to EU field reference levels	Severity categories for direct and indirect effects				
	Electrostimulation effects	Tissue heating effects	Metallic implant heating	AIMD EMC	Possible chronic effects
$\langle\mathbf{E}\rangle, \langle\mathbf{H}\rangle, \|\mathbf{E}\|, \|\mathbf{H}\| << 1999/519/EC$	***S0***	***S0***	***S0***	***S0***	***S0***
$\|\mathbf{E}\|, \|\mathbf{H}\| \leq 1999/519/EC$	*S0*	*S0*	***S1***	***S1***	***S1***
$\langle\mathbf{E}\rangle, \langle\mathbf{H}\rangle \leq 1999/519/EC$	*S0*	*S0*	***S1***	***S1***	***S1***
$1999/519/EC < \|\mathbf{E}\|, \|\mathbf{H}\| < 2013/35/EU$	*S1*	*S1*	*S2*	***S3***	*S2*
$1999/519/EC < \langle\mathbf{E}\rangle, \langle\mathbf{H}\rangle < 2013/35/EU$	*S2*	*S2*	*S2*	***S3***	*S2*
$\langle\mathbf{E}\rangle, \langle\mathbf{H}\rangle, \|\mathbf{E}\|, \|\mathbf{H}\| > 2013/35/EU$	***S3***	***S3***	***S3***	***S3***	***S3***

Electrostimulation is not considered to be significant above 10 MHz, and field penetration into the body also decreases. Hence in Table 9, which encompasses vehicle communications frequencies, the electrostimulation and AIMD EMC columns are removed. Above 10 GHz, the heating effect is largely confined to the body surface, hence in Table 10, which covers automotive radar frequencies, the metallic heating of implants is also removed.

Table 9. Proposed severity classes for human electromagnetic field exposure threats: 10 MHz to 10 GHz.

Power density relative to EU field reference levels	Severity categories for direct and indirect effects		
	Tissue heating effects	Metallic implant heating	Possible chronic effects
<**E**>, <**H**>, <**S**> << 1999/519/EC	***S0***	***S0***	***S0***
<**E**>, <**H**>, <**S**> ≤ 1999/519/EC	*S0*	***S1***	***S1***
1999/519/EC < <**E**>, <**H**>, <**S**> < 2013/35/EU	***S2***	***S2***	***S2***
<**E**>, <**H**>, <**S**> > 2013/35/EU	***S3***	***S3***	***S3***

Table 10. Proposed severity classes for human electromagnetic field exposure threats: 10–300 GHz.

Power density relative to EU field reference levels	Severity categories for direct and indirect effects	
	Tissue heating effects	Possible chronic effects
<**S**> << 1999/519/EC	***S0***	***S0***
<**S**> ≤ 1999/519/EC	*S0*	***S1***
1999/519/EC < <**S**> < 2013/35/EU	***S2***	***S2***
<**S**> > 2013/35/EU	***S3***	***S3***

7. Conclusions

Completely eliminating all risks relating to the safety, security and mission-critical functionality of vehicle systems would be unaffordable, and is in any case unachievable in practice. Nonetheless, analysis of these risks in terms of not just the intended use, but also considering foreseeable use/misuse, provides an approach for managing the most significant risks in order to achieve resilient systems with acceptable levels of residual risk. The existing risk assessment measures and methods applied in functional safety can be adapted and augmented as needed to address threats other than those related to functional safety, as proposed in Table 11, although further work is required for some aspects (e.g. SOTIF), and to enable uncertain parameters to be handled more effectively in risk analyses. The severity of electromagnetic field exposure hazards is considered here as an example of a SOTIF approach.

Table 11. Proposed risk assessment approaches (and their scope) for vehicle resilience purposes.

Assessment aspect	System safety	Cyber security	Mission-critical functionality
Severity	ISO 26262 Severity (functional safety hazards) EVITA Severity (security related safety hazards) SOTIF – for specific issues (e.g. Tables 7–10 for human electromagnetic field hazards)	EVITA Severity (privacy and financial threats)	Table 6 (functional failures, environmental threats etc.) EVITA Operational Severity (security related operational threats)
Likelihood	ISO 26262 Exposure (functional safety and SOTIF, e.g. electromagnetic field hazards) EVITA Probability (security related safety hazards)	EVITA Probability (security related threats)	ISO 26262 Exposure (non-safety/security threats) EVITA Probability (security related threats)
Controllability	ISO 26262 Controllability (functional safety hazards)	ISO 26262 Controllability (safety related security threats)	*Not applicable*
Risk mapping	ISO 26262 Risk Graph (functional safety hazards) IEC 61508 or MISRA Risk Graph (SOTIF, e.g. electromagnetic hazards) EVITA Risk Graph (security related safety hazards)	EVITA Risk Graph (privacy and financial threats)	IEC 61508 or MISRA Risk Graph (non-safety/security threats) EVITA Risk Graph (security related operational threats)

It is considered that further development of such a risk-based approach to vehicle development will be essential in order to achieve sufficiently high levels of dependability and resilience against the wide ranging and evolving threats in the operating environment that will be needed to ensure the societal acceptability and commercial success of future connected and autonomous vehicle technologies.

Acknowledgements

Part of the research leading to these results was carried out in connection with the ICENITE project, which received funding from the UK Government's innovation agency Innovate UK (project reference 101665).

8. References

AAAM, 2005. Abbreviated Injury Scale. Association for the Advancement of Automotive Medicine, Barrington, IL, USA. [Online, 2018: https://www.aaam.org/abbreviated-injury-scale-ais/].

Anderson V., McIntosh, R., 2008. Guidelines for the RF exposure assessment of metallic implants. October 2008. [Online, 2018: https://www.researchgate.net/profile/Vitas_Anderson/publication/254340990_Guidelines_for_the_RF_exposure_assessment_of_metallic_implants/links/5446e22d0cf22b3c14e0b715.pdf].

CENELEC, 2004. EN 45502-2-1:2004, Active implantable medical devices – Part 2-1: Particular requirements for active implantable medical devices intended to treat bradyarrhythmia (cardiac pacemakers), September 2004.

EU, 2007. Directive 2007/46/EC of The European Parliament and of the Council of 5 September 2007 establishing a framework for the approval of motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles. Official Journal of the European Union, 9/10/2007, L 263, Vol. 50, pp. 1–160.

EU, 1999. 1999/519/EC: Council Recommendation of 12th July 1999 on the limitation of exposure of the general public to electromagnetic fields (0 Hz to 300 GHz). Official Journal of the European Communities, No. L 199, pp. 59–70, 30th July 1999.

EU, 2013. 2013/35/EU: Directive 2013/35/EU of the European Parliament and of the Council of 26th June 2013 on the minimum health and safety requirements regarding the exposure of workers to the risks arising from physical agents (electromagnetic fields) (20th individual Directive within the meaning of Article 16(1) of Directive 89/391/EEC) and repealing Directive 2004/40/EC. Official Journal of the European Union, No. L 179, pp. 1–21, 29th June 2013.

EVITA, 2008. E-safety vehicle intrusion protected applications. [Online, 2018: https://www.evita-project.org/index.html].

ICNIRP, 1998. Guidelines for limiting exposure to time-varying electric and magnetic fields (up to 300 GHz). Health Physics, Vol. 74, No. 4, pp. 494–522, April 1998.

ICNIRP, 2010. Guidelines for limiting exposure to time-varying electric and magnetic fields (1 Hz to 100 kHz). Health Physics, Vol. 99, No. 6, pp. 818–836, December 2010.

IEC, 2010. IEC 61508: Functional safety of electrical/electronic/programmable electronic safety-related systems. International Electrotechnical Committee, 2nd Edition, April 2010.

ISO, 2011. ISO 26262: Road vehicles – Functional safety. International Organization for Standardization, November 2011.

ISO/IEC, 2008. ISO/IEC 18045: Information technology – Security techniques – Methodology for IT security evaluation. ISO/IEC, August 2008.

ISO/IEC, 2009. ISO/IEC 15408: Information technology – Security techniques – Evaluation criteria for IT security. ISO/IEC, December 2009.

Leitgeb, N., Niedermayr F., Loos, G., 2013. Impact of EAS systems on implanted cardiac pacemakers and defibrillators. Journal of Electromagnetic Analysis and Applications, Vol. 5, pp. 67–73, February 2013.

MISRA, 1994. Development Guidelines for Vehicle Based Software. MIRA Limited, ISBN 0-9524156-0-7, November 1994.

MISRA, 2007. MISRA Guidelines for Safety Analysis of Vehicle Based Programmable Systems. MIRA Limited, ISBN 978-0-9524156-5-7, November 2007.

RTCA, 2000. DO-254: Design Assurance Guidance for Airborne Electronic Hardware. Radio Technical Commission for Aeronautics, Inc., Washington, DC, 19/04/2000.

RTCA, 2011. DO-178C: Software Considerations in Airborne Systems and Equipment Certification. Radio Technical Commission for Aeronautics, Inc., Washington, DC, 13/12/2011.

Ruddle, A.R., et al., 2009. Security requirements for automotive on-board networks based on dark-side scenarios, EVITA Deliverable D2.3, 30th November 2009.

Ruddle, A.R., Galarza, A., Sedano, B., Unanue, I., Ibarra, I., Low, L., 2013. Safety and failure analysis of electrical powertrain for fully electric vehicles and the development of a prognostic health monitoring system. Proceedings of 4th Hybrid and Electric Vehicles Conference (HEVC 2013), London, UK, November 2013.

Ruddle, A.R., Armstrong, R., Galarza, A., 2015. HEMIS Project (Electrical Powertrain HEalth Monitoring for Increased Safety of FEVs): Limitations of Electromagnetic Standards for Vehicles Equipped with Electrical Powertrain. In *Springer Lecture Notes in Mobility, Electric Vehicle System Architecture and Standardization Needs*, Muller B., Meyer, G. (Eds.), Springer International Publishing, Chapter 7, pp.105-115, April 2015.

Ruddle, A.R., Ward, D.D., 2016. Cyber security risk analysis for intelligent transport systems and in-vehicle networks. In "*Intelligent Transport Systems: Technologies and Applications*", Perallos, A., Hernandez-Jayo, U., Onieva, E., García-Zuazola, I.J., (Eds.). John Wiley & Sons, Chapter 5, pages 83–106, January 2016.

Ruddle, A.R., 2016. Preliminary estimates of electromagnetic field exposures due to advanced vehicle technologies. Proceedings of Loughborough Antennas and Propagation Conference, Loughborough, UK, November 2016.

Schneier, B., 2000. Secrets and Lies – Digital Security in a Networked World. New York. John Wiley & Sons, Inc., Chapter 21, 2000.

Vassilev, A., Ferber, A., Wherman, C.J., Pinaud, O., Schilling, M., Ruddle, A.R. Magnetic field exposure assessment in electric vehicles. IEEE Transactions on Electromagnetic Compatibility, Vol. 57, No. 1, pp. 35–43, February 2015.