SECURE CAV

Advanced cybersecurity for connected and autonomous vehicles

The Applicability of Automotive Cybersecurity Standards

Prepared by Copper Horse

Authors James Tyrrell, David Rogers

Version Updated • January 2023

Version Control

Version	Date	Comment
1.00	23/07/2021	First draft prepared for initial group review
1.10	10/08/2021	Threat analysis and risk assessment section added
Final	Nov 2021	Final version for project end
1.20	17/01/2022	Updated to match information added in January 2022
1.30	30/01/2023	Updated information and standards for January 2023

Table of Contents

Scope 5
Abbreviations 5
Introduction 6
Automotive security standards and recommendations 6
Visual summary 7
Considerations 7
Timeline 8
Information relevancy and standards evolution 9
Threat analysis and risk assessment 9
Security auditing 10
Purchasing costs including referenced material 10
Membership discounts 10
Differences in pricing between platforms 10
Modelling different sized organisations 11
How to try before you buy? 11
Rental model 11
Subscription model 11
Standards composition 12
Cost of standards development 12
Pay to play 12
FRAND and Royalty Free models 13
Discussion 13
The good 13
The bad 13
Closing remarks 14
Reference material and further reading 15
Appendix 1 – List of automotive security standards and recommendations 16
Recommendations directly addressing automotive security 16
ISO 21434 16
ISO/PAS 5112:2022 16
SAE J3101 16
SAE J3061 16
UK Government's Key Principles of Cyber Security for Connected and Automated Vehicles 16
BSI PAS 1885 18
UNECE WP.29 18
ITU-T X.1373 19
ENISA 19
TR 68 - 3 (Singapore) 20
US DoT NHTSA 21

US H.R.701 21
Extensions to safety considerations 21
ISO 26262 series and related 20
SAE J2980_201804 24
ISO/PAS 21448 24
UK Code of Practice: Automated vehicle trialling 24
PAS 11281:2018 (Connected automotive ecosystems. Impact of security on safety. Code of practice) 24
General foundations AEC-Q100 series 25
Coding and software guidelines 25
ISO/TR 15497 25
MISRA 25
ASPICE 26
IATF 16949 26
NTIA software component transparency and SBOMs 26
General foundations 27
BS 10754-1 27
BS EN IEC 60812 27
BS EN IEC 61025. 27
BS EN 61508 series 27
IEC TR 62443 series 28

Scope

This work examines the applicability of automotive cybersecurity standards around the world, firstly by capturing a longlist of recommendations and guidance and then organising these details into related themes to better consider the following -

- How relevant is the information? Which standards can be safely dropped and ignored?
- What documents are being referenced and how are the recommendations being regulated?
- Do the standards make an impact on real-world cyber security of vehicles or is the process too slow / the guidance too vague or abstract to enable the required changes in industry?
- What is the additional engineering burden on the automotive industry and the surrounding ecosystem?

Finally, we consider the purchasing costs that OEMs and their suppliers would need to budget for to access the necessary information and discuss the implications of this, reflecting of the original aims of standards and their benefit to society.

Abbreviations

AEC - Automotive Electronics Council (US body establishing electronic components standards for use in harsh automotive environments).

ASPICE - Automotive Software Performance Improvement and Capability dEtermination.

BSI - British Standards Institution (UK national standards body).

GSMA - Industry organisation represents the interests of mobile network operators worldwide.

ETSI – European Telecommunications Standards Institute.

IATF - International Automotive Task Force (alternative to ASPICE).

IEC - International Electrotechnical Commission (standards organisation).

ISO – International organisation for standardisation.

ITF - International Transport Forum (intergovernmental organisation with 63 member countries).

ITU - International Telecommunication Union (United Nations agency for information and communication technologies).

MISRA - Motor Industry Reliability Association (consortium focused on safe and secure application of embedded control systems and standalone software).

NTIA - US National Telecommunications and Information Administration.

PAS – Publicly available specification (a fast-track standardisation document).

SAE - Association of engineers and technical experts in aerospace, automotive and commercial vehicle industries.

SEI - (Carnegie Mellon) Software Engineering Institute, US.

UNECE WP.29 - United Nations Economic Commission for Europe World Forum for Harmonization of Vehicle Regulations.

US DoT NHTSA - United States Department of Transportation National Highway Traffic Safety Administration.

Introduction

To be effective, standards must combine ‘capability’ and ‘functionality’ – in other words, offer ‘the power to do something’ and ‘the ability to do that task well’.

Leaning on academic work in this area (see ‘reference material and further reading’) the contribution of standards is, ideally, fourfold – they can i) protect the safety of the community; ii) facilitate international trade; iii) enhance the interoperability of technologies and processes; and iv) facilitate technological change and economic development by reducing information asymmetry.

Putting some of this in the context of automotive cybersecurity, recommendations should limit the freedom of bad actors to cause harm to drivers, passengers and other road users. In the widest of terms, the beneficiary of capable and functional standards is – or should be – society.

Keeping this statement in mind, we will now compile a comprehensive list of automotive standards and recommendations, together with the reference material that supports them. Our goal is to gain a better view of the landscape and determine how well standards in the automotive security domain are doing their job based on the metrics introduced above.

Automotive security standards and recommendations

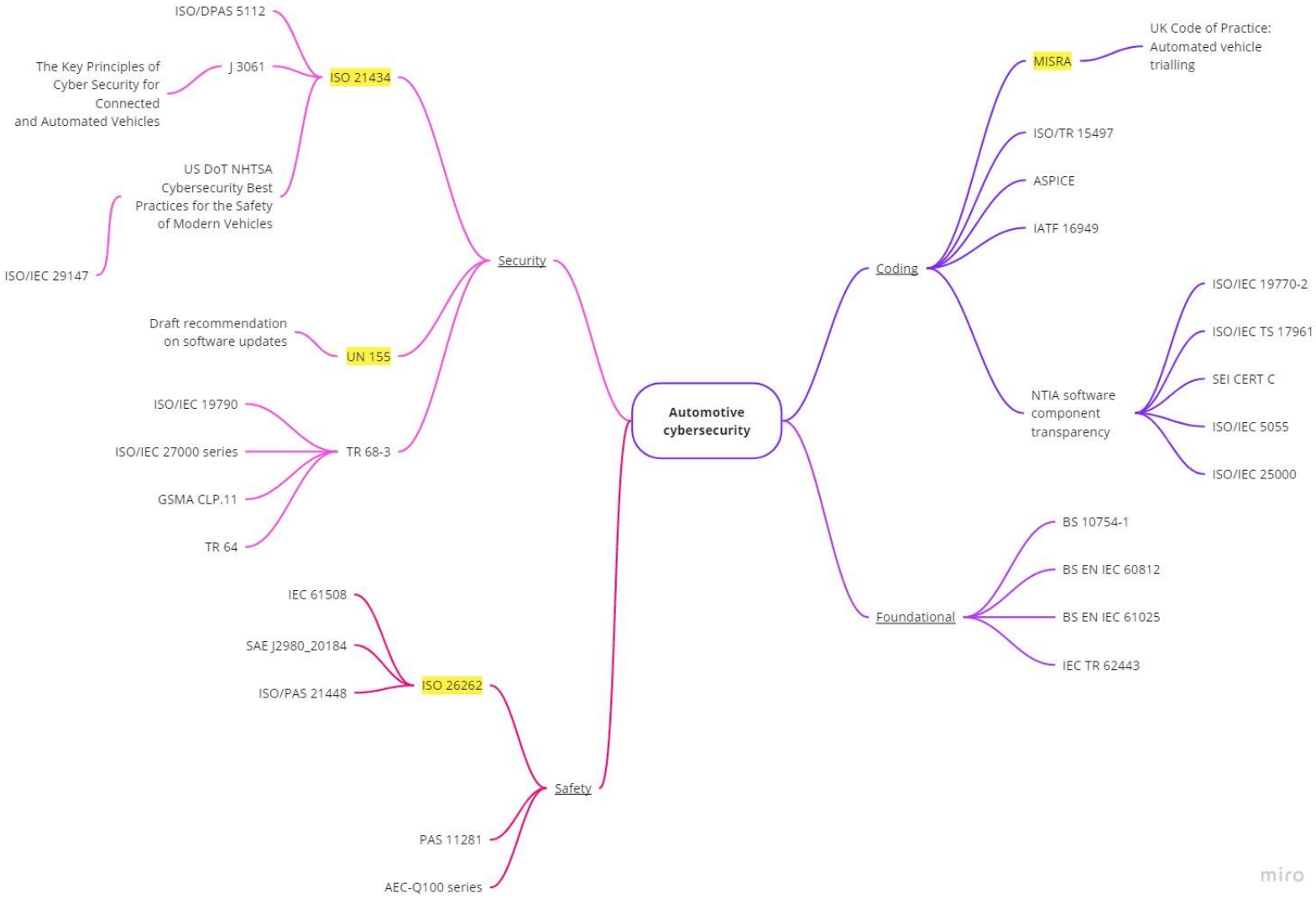
The available guidance on automotive cybersecurity can be classified into the following groups –

- Recommendations directly addressing automotive security
- Extensions to safety considerations
- Coding and software standards
- General foundations

Full details can be found in Appendix 1 – Automotive security standards and recommendations.

Visual summary

The following diagram summarises the relationships between various automotive standards and groups them into four categories.



Considerations

Although the guidance has been divided into four groups to help visualise the standards landscape, clearly no group should be considered in isolation. The cybersecurity measures that are applied must still comply with safety guidelines. National standards must be adhered to if OEMs wish to sell products into those markets, even if the guidance doesn't apply at home.

There are potential workflow issues too, particularly as the number of software elements on modern vehicles increases. It's reported that car makers have a superset of 120 ECUs to select from to create a system architecture. The full suite comprises around 100 million lines of source code, which includes 10 million conditional statements and 3 million functions.

To define, test and integrate components, automotive engineering has adopted a V-shaped model, whereas application development tends to favour continuous integration – a process that can be pictured as a circle or figure of eight. Given these organisational differences, there may have to be some reconciliation between the two development approaches to make sure that firms are able to apply recommendations in a timely fashion.

Another issue, particularly with increased use of open source software, is the need to track which versions are in use and licensing implications for developers. It's apparent from work such as the NTIA's guidance on software transparency that there is a growing focus on compiling and maintaining a software bill of materials, encouraging firms to request this information from their suppliers. Failure to do so will weaken the impact of mandating software updates for vehicles as OEMs will have less visibility on where the vulnerabilities lie within their products.

Timeline

While there are many established international standards for IT security and industrial control systems, these recommendations don't address directly the needs of vehicle makers. Over time, the automotive sector has taken a number of steps to address this.

1994

MISRA publishes development guidelines for vehicle-based software.

2015

SAE formed Vehicle Cybersecurity Systems Engineering Committee to address automotive-specific threats and vulnerabilities in the US market.

2016

SAE published J3061, Cybersecurity Guidebook for Cyber-Physical Vehicle Systems. Recommendations cover the complete vehicle lifecycle from concept phase through production, operation, service and decommissioning. The standard is a precursor to ISO 21434 and calls for lifecycle approach to cybersecurity engineering.

2018

ISO 26262 (second edition) is published. The final version includes comments on the interaction between safety and security (Annex E), but participants agreed that safety and cybersecurity will be treated in separate standards.

2019

MISRA and AUTOSAR announced that their industry standard for best practice in C++ will be integrated into one publication.

2021

Final version of ISO 21434 published. The standard supersedes J3061 and provides a framework for implementing a CSMS (in line with WP.29 UNECE recommendations) and managing road vehicle cybersecurity risk.

The re-work of SAE J3061 was published. The publication states that "This recommended practice establishes a set of high-level guiding principles for Cybersecurity as it relates to cyber-physical vehicle systems.". The document set should provide a more technical companion to ISO 21434.

2022

ISO/PAS 5112:2022 was published. The document is based on ISO 21434 and provides guidelines for auditing the cybersecurity engineering of road vehicles, a function that is mandated through the WP.29 UNECE regulations.

July - WP.29 UNECE regulations (UN155) came into force for ‘new vehicle types’ (vehicles in development) due to be sold in the EU.

The US DoT NHTSA 'Cybersecurity Best Practices for the Safety of Modern Vehicles' was published, updating the Agency’s non-binding and voluntary guidance to the automotive industry for improving motor vehicle cybersecurity.

A number of referenced cyber / information security specifications in ISO were updated.

2024

July - WP.29 UNECE regulations come into force for all new vehicles being sold in the EU.

Information relevancy and standards evolution

As the timeline highlights, standards are being introduced to specifically address the topic of automotive cybersecurity and these frameworks represent key focal points for developers. Collectively, this guidance brings together practices from safety engineering, secure coding and build on more established activities in the IT sector.

There are signs of standards evolution. J3061 was introduced as a stop-gap, filling a void while decisions were made on the next steps, and has now been superseded by ISO 21434.

However, while ISO 21434 sets the scene, the standard has benefited from the re-working of J3061, to provide guidance on topics such as security testing methods and security tools that developers can apply to mitigate identified threats.

ISO 26262 started the discussion on the interaction between safety and cybersecurity and it’s logical to expect that future editions of this standard will provide more details on security-aware safety topics.

In 2023, at SAE, there are three work-in-progress standards:

- ISO/SAE PAS8475: Road Vehicles – Cybersecurity Assurance Levels and Targeted Attack Feasibility
- J3254: Automotive Cybersecurity Maturity Model Best Practice
- J3061-2: Security Testing Methods

Threat analysis and risk assessment

Threat Analysis, Risk Assessment, & Vulnerability Analysis Methods listed in the previous publication of J3061 include -

- EVITA Method (E-safety Vehicle InTrusion protected Applications)
- EVITA Applied at the Feature Level using THROP (Threat and Operability Analysis)
- TVRA (Threats, Vulnerabilities and Risks (TVR) of a system to be Analyzed)
- OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation)
- HEAVENS (HEAling Vulnerabilities to ENhance Software Security and Safety)
- Attack Trees • Software Vulnerability Analysis

ISO/SAE 21434 followed in the footsteps of J3061, leaving the choice of method for attack path analysis open to the user. However, notes are provided that highlight the usefulness of attack trees, attack graphs and taxonomy mnemonic-based approaches such as STRIDE. The security objectives listed (Safety, Financial, Privacy, Financial) were suggested by EVITA[1] – a European project (2008-2011) designed to capture security requirements and explore threat scenarios for automotive networks – and re-used in HEAVENS[2] – a Volvo-coordinated Swedish project (2013-2016) identifying security vulnerabilities in automotive systems. The information is available in the public domain as well as being included in Annex H of the ISO spec.

[1] https://www.researchgate.net/publication/46307752_Security_requirements_for_automotive_on-board_networks_based_on_dark-side_scenarios_Deliverable_D23_EVITA_E-safety_vehicle_intrusion_protected_applications

[2] https://autosec.se/wp-content/uploads/2018/03/HEAVENS_D2_v2.0.pdf

Security auditing

ISO/SAE 21434 sets a requirement for component testing to search for unidentified vulnerabilities. Methods can include penetration testing, vulnerability scanning and/or fuzz testing.

Work (ISO/PAS 5112:2022) provides guidelines for auditing the cybersecurity engineering of road vehicles. There are some higher level assessment details provided in UN155 regarding the requirements for issuing a certificate of compliance for a cyber security management system (CSMS).

Purchasing costs including referenced material

Ideally, to maximise their application and to reap the full benefits of their development, standards should be readily available to all. But, as this study shows, in many cases the guidance must be purchased, which presents a barrier – particularly for developers seeking to apply a comprehensive set of recommendations to their products or services.

Based on a truncated list of 49 standards either directly or closely related to automotive security (gathered from the literature and available to purchase online), developers would require more than GBP **6.6k** to access this critical information. This has also increased by just under 16.7% (from GBP 5.5k when prices were originally checked in 2021/2022). Note that whilst prices have increased in most standards bodies, exchange rates have changed too – the same methodology and exchange rate service was used to calculate this information. Some of the standards appear to have increased in price where there have been updates to them recently. Three standards were reduced in price with one: 'BSI PAS 1885 – The fundamental principles of automotive cyber security – specification', being offered for free. Our analysis reveals that each of these standards costs an average of GBP 137.73 to purchase (up from GBP 114.12 in 2022) – although the prices vary considerably from GBP 15 to GBP 388.

Membership discounts

BSI members receive a 50% discount on BSI standards, with annual membership ranging from GBP 207 to GBP 1471 (in 2023) depending on the type of organisation. Taking this into account and bundled rates, the cost of the 49 identified standards falls from GBP 6.6k to **5.5k** in 2023.

Differences in pricing between platforms

Comparing the cost of ISO standards available through ISO's own web store versus BSI's online shop highlights some differences in pricing across the two platforms. Taking, ISO 26262 as an example – BSI offers sections 1 to 10 as a bundle for GBP 1810 to non-members (or GBP 905 to members – badged as a 50% discount – who are required to pay an annual membership upwards from GBP 207) – note that this price has not changed since 2022. Buying the same standards from the ISO store would cost GBP 1251.82. (GBP 1122 in 2022). The strangest scenario is for non-members looking to purchase standards individually from the BSI website. Again, using ISO 26262 as an example, customers would pay more than GBP 2000 over the original ISO price if they bought the sections one by one from the BSI store. In 2022, applying a member discount would broadly return the cost to the original ISO price. However, in 2023, there has been an inflation in the prices charged by BSI related to this set of specifications. To purchase the set individually in 2023 with the BSI member discount the price would be an additional GBP 434 compared with 2022. At the current 2023 prices, in comparison with buying direct from ISO it would cost GBP 400.18 more (even with the member discount). With no discount, it would cost a total of GBP 3304 to buy the set of standards individually from BSI.

ISO 9001 is another curious example. In 2022 this standard could be purchased for EURO 18.48 (GBP 15.94) from the Estonian Centre for Standardisation and Accreditation, CHF 135 (GBP 110) directly from the ISO shop or for GBP 150 (75 member) from BSI.

Finally, for the standards investigated, comparing 2022 pricing with 2023, the general price increases were as follows:

- AIAG: No change
- ANSI: No change
- BSI: 6.03%
- IEC: 6.06%-10.53%
- ISO: 4.81%-4.9%
- MISRA: No change
- SAE: 40.56%-47.2%
- SSC: 0.1%-20%

Some outliers in terms of price reductions or large price increases were observed too.

Modelling different sized organisations

So far in this section, we have simply considered the price that an individual would need pay to purchase a target list of standards. But within an organization there could be multiple people who would need access to such documents and to factor that in we consider two additional scenarios: i) a small firm with three employees who need access and ii) a larger company with five employees engaged in standards related activities.

From our research, it appears that standards are typically licensed for individual use, but a cost reduction factor is offered when multiple copies are required – although the specific formulae are not always listed on the various websites. Instead, customers are requested to contact the standards body for details. In our calculations, we have applied the most generous factors that were publicly available although we cannot guarantee that all standards bodies would use identical formulae. However, our method does acknowledge that discounting is available for multiple copies.

Applying these factors (see table below) to our three people (small firm) and five people (larger firm) scenarios, together with the estimated BSI membership costs, gives pricings of just over GBP **8.1k** and **12k**, respectively. In 2022 it would have been just over 7.2k and 10.7k, respectively.

Scenario	Number of copies required	Multiplier applied to single user price	Estimated BSI membership fee / GBP
3 people (small firm)	3	x 1.5	207
5 people (larger company)	5	x 2.0	1471

Table 1 – Pricing factors considered when modelling different sized organisations.

How to try before you buy?

Aside from the cost itself, there are other shortcomings to a model where users are required to pay for standards. For customers, purchasing decisions must largely be made based on previewing the table of contents as the bulk of the document is only accessible once bought, which makes evaluating the relevancy of requirements problematic. And when multiple copies are required, the consequences grow. If users cautiously buy a single standard first, then they lose out on the full multiple copy discount. But by going all in, buyers risk that their multiple copy purchase could turn out to be wasteful many times over if the information is mismatched to their application.

If you were buying a book you might be able to browse through a copy, read a sample chapter or consult reviews either in the press or added by other readers. But what mechanisms can standards developing organisations deploy so that the user knows in advance whether the standard will be useful or implementable?

ISO has made available some content ahead of purchase on its online browsing platform, but much of the material is greyed out and clicking on these sections brings up the following message - '*Only informative sections of standards are publicly available. To view the full content, you will need to purchase the standard by clicking the "Buy" button.*'

Rental model

Interestingly, some national standards bodies appeared to have provided a range of standards through a rental model where for a few Euros you could access the material for 24 hours to make a decision on whether you'd like to purchase the information on a permanent basis. Sadly, this model appears to have been phased out.

Subscription model

BSI offers a service dubbed BSOL which is an online standards management tool hosting more than 100,000 standards from a range of organisations (BSI, ISO, EN, BS, PAS, ASTM and IEC) that can be accessed remotely and by multiple users. For a fee (which is undisclosed) customers gain access to modules covering different industry areas. Standards are updated automatically when newer versions become available.

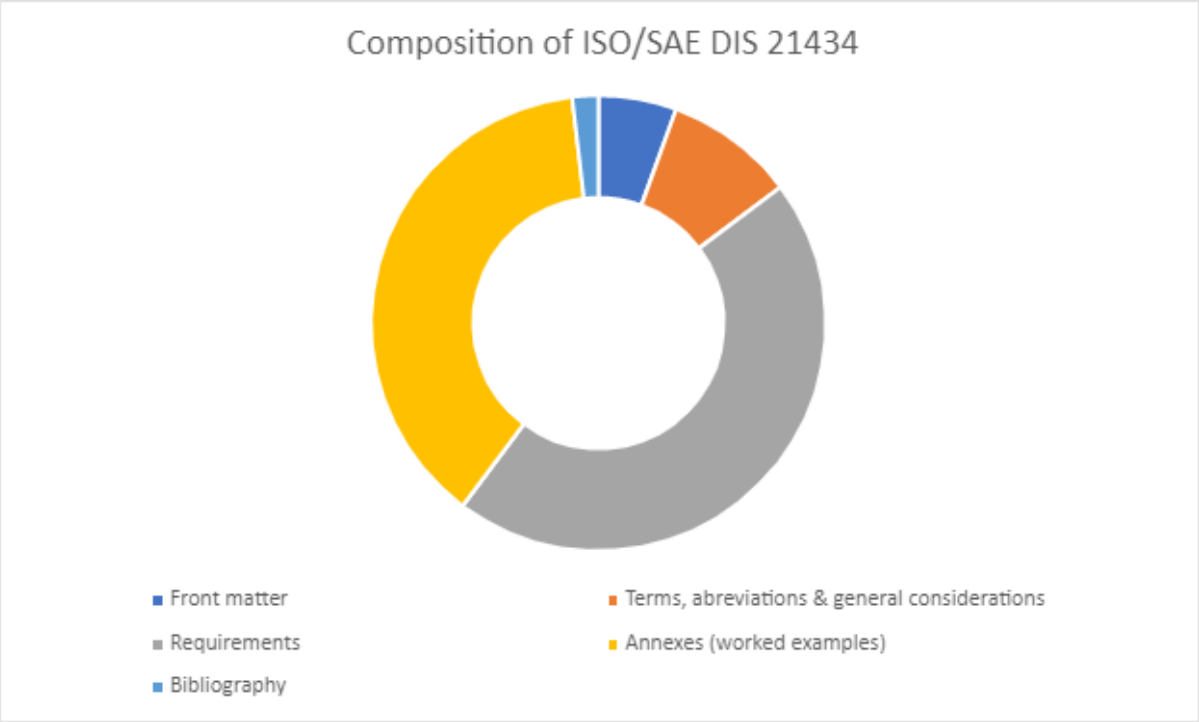
To benefit smaller organizations, who may not need access to a full module, customers can subscribe to a user-selected list of 10 standards.

Subscription models lend themselves well to digital content, at least on the basis of games, movies, music, financial analysis and news. Although, in terms of 'try before you buy' many of these offer a free or heavily discounted trial period so that customers can evaluate the service before making a full financial commitment.

The transition from print to digital media is definitely a bump in the road that standards setting organisations must contend with as users will expect business models to change.

Standards composition

Taking ISO/SAE DIS 21434 as an example, the document is primarily a mix of requirements and worked examples.



Cost of standards development

Having discussed the purchase price of standards, it is worth looking at the costs involved in standards development and where different organisations choose to apply these charges.

First a standard must be drafted to meet a market need, shared, discussed, commented upon and then voted for. Once finalised, the text must be formatted and the document published to allow distribution. Also, standards must be reviewed and updated accordingly.

Today, it is common to find standards available in digital formats, although many standards setting organisations continue to provide a second distribution channel offering paper copies. In its 2030 strategy document, ISO has pledged to '*Invest in training and technology to improve and streamline the standards development and production processes,*' which suggests that there could be savings to be found in those areas.

Standards setting organisations also engage in training and contribute to auditing activities through their members – although this can be a source of revenue rather than a cost. It is also important to note that standards bodies benefit greatly from the work of volunteers.

Pay to play

Members pay an annual fee to participate in standards activities, gaining access to working documents under development. However, the final edited versions are free (electronic download) at the point of use once published. Membership fees vary for different bodies. ETSI's membership dues range from EUR 2000 (GBP 1757) for universities, public research bodies and not-for-profit user associations, EUR 3000 (GBP 2635) for micro-enterprises (<10 head count), to EUR 154720 (GBP 135908) depending on the participant's 'Electronic Communications Related Turnover' with reductions for universities, micro-enterprises and SMEs.

Based on the numbers of participants, the rewards of membership appear to be worth the annual fees. Participants have gone on record to say that they value taking part in standards development as it allows them to influence the content and gives an early view of upcoming recommendations, providing the opportunity to stay ahead of those who don't have a seat at the table.

Organisations such as the W3C have a pay-to-play approach, but are extremely transparent, with many of their discussions taking place on public mailing lists and with their drafts and outputs being publicly available. This drives engagement and scrutiny, which in turn leads to memberships by organisations that want to contribute to that activity. The outputs of other organisations are also public and freely useable – ETSI is another example.

These organisations are successfully able to maintain themselves through the member fees, with different levels for different sizes of business or academia etc. The net result is a very positive contribution back to society in general and clearly stimulates economic growth.

FRAND and Royalty Free models

Where a standard adopts technology that is covered by a patent, the standard setting organisation will typically require that any rights holder for a patent declared within a particular standard makes the technology available under fair, reasonable, and non-discriminatory (FRAND) terms. For example, during the proposal or development of a standard, ETSI[3] asks that its members '*inform the Director General in a timely fashion if they are aware that they hold any patent that might be essential*'. Standard Essential Patents holders are then '*requested to provide an irrevocable undertaking in writing that they are prepared to grant irrevocable licenses on Fair, Reasonable and Non-Discriminatory ("FRAND") terms and conditions.*'

FRAND doesn't necessarily prevent Standard Essential Patent holders from passing a charge onto users implementing the standard, although some organisations discourage this.

To enable continued innovation and widespread adoption of web standards, '*W3C operates under a royalty-free patent policy[4] by which participants in standards development make commitments to license their standards-essential patents royalty-free to implementers and users of the W3C specifications.*'

FRAND is a big topic and a full discussion is beyond the scope of this paper, but it's worth noting that standard essential patents (SEPs) affect markets – both positively and negatively – in more ways than you would imagine.

The extraordinary growth in container shipping only occurred when one of the container firms put a royalty free option on the table by giving up its corner fitting patents[5]. Up until that point there had been a stalemate, with rival companies holding out for their design to become the standard and looking forward to the licensing revenue that would ensue. The firm that released its patents gave up the prospect of licensing revenue, but benefited from the boom in the sector that followed as shipping companies and ports ramped up their investment in equipment now that a universal design had been agreed.

When these models work well, stakeholders gain from the collaborative innovation and proliferation of the underlying technologies. However, disputes over SEPs can lead to market failure.

Discussion

The good

Today, there are a growing number of cybersecurity recommendations available that are tailored to the needs of the automotive industry. And these sit upon a wealth of more general advice that together offer OEMs and their suppliers an increasingly capable framework for developing and maintaining secure vehicles and related systems. Also, it is encouraging to see collaboration within this space such as the joint work by SAE and ISO on the development of the 21434 standard and by MISRA and AUTOSAR on harmonising C++ coding guidelines.

The prevailing wisdom, expressed through a number of reports, is that standards are good for supply chains. When questioned, more than 70% of UK businesses stated that *'standards had contributed to improving their supply chain by improving the quality of supplier products and services.*' Their positive effect extends further on this theme by strengthening client-supplier relationships through greater confidence, again according to survey results.

The bad

Developing vehicle cybersecurity takes time. It cannot be assumed that security solutions and processes that have proven to be effective elsewhere will translate seamlessly across into the automotive sector. Vehicles are different to conventional IT assets – they are exposed to all weathers, vibrations and easily found in public places. There are other demands too. Auto-makers are well-versed in designing for safety, but cybersecurity requirements are a relatively new addition to the workflow and must (see WP.29 UNECE regulations) be considered from design through to decommissioning, as must the protection of driver data.

---

[3] https://www.etsi.org/intellectual-property-rights
[4] https://www.w3.org/Consortium/Patent/
[5] https://www.economist.com/podcasts/2021/09/13/thinking-inside-the-box-the-story-of-the-shipping-container

To arrive at this destination, OEMs and their suppliers need to gather standards, recommendations and guidelines so that they are in a position to specify and verify components with respect to their cybersecurity capabilities. And the big question is – while the available documentation may be capable, how functional is this body of knowledge when it requires more than GBP 6.6k to access?

If this cost is passed on to customers then stakeholders will be under pressure to apply the minimum recommendations given the fierce competition on price within the automotive sector. Also, it is not just OEMs that need to be familiar with the standards. Suppliers further down the chain must also be in the loop so that their solutions pass verification – and they too will need to budget for access to the necessary information.

For society to benefit fully from standards, a goal that we made reference to in the introduction, their cost should be reconsidered. There are parallels with the tension that can be seen in academic publishing where knowledge behind a paywall limits its application. In this case, researchers have responded by pushing for an open-access model and making their submitted work freely available. It has put journal publishers under scrutiny to explain their costs and standards bodies may have to do the same, if not simply to explain the wide range of pricing that exists.

In order to sell their vehicles into certain territories, OEMs will have to comply with the cybersecurity regulations that apply and purchase the standards and recommendations that are referenced – no vehicle approval, no revenue. On this basis, it appears that standards bodies have the upper hand, but society is in a position to demand more.

Closing remarks

Keeping standards' prices high – even when the bulk of the technical input and oversight required to create a standard in the first place is provided at no cost to the standards body itself, via the various committee members and contributors – puts market growth at risk as the participation of SME's who cannot absorb the costs will be hampered, stifling the innovation that such firms may otherwise be in a position to bring. It's also worth noting, as others have done, that access to knowledge or information on standards is an important factor in exporters' ability to comply with regulations. An additional point of friction is between companies and suppliers working together, again hitting SMEs hard and potentially excluding them. The cumulative effect could substantially constrain innovation and collaboration.

Obviously, someone has to pay for standards to be produced. Whatever cost model is used, if the net effect is restricting the readability of standards – it is a negative outcome for humanity. Transparency of standards is crucial in ensuring the quality of what is being produced and ensuring that they can be widely scrutinised. Standards bodies that do not make their documentation outputs freely available suffer from the fact that no-one can evaluate whether a standard is well-written, useful or even applicable. This can create a situation where regulators and industry all endorse a standard 'in name', without ever having read it. The ultimate outcome of this is poor for everyone. It wastes economic activity around the world and potentially ruins burgeoning startups through to mature businesses. In the cyber security world it has greater implications – it could make the world less secure, but we'll save that topic for another day.

In its 2030 strategy document, ISO has pledged to 'Invest in training and technology to improve and streamline the standards development and production processes,' which suggests that there could be savings to be found. We look forward to them.

Reference material and further reading

‘The role of standards in motivation the ITS world’ - Scott W. Cadzow

https://youtu.be/IL3_-8Y92ug

‘Automotive Cybersecurity Standards - Relation and Overview’ (published in the book ‘Computer Safety, Reliability, and Security, pp.153-165) – Christoph Schmittner

https://www.researchgate.net/publication/335557258_Automotive_Cybersecurity_Standards_-_Relation_and_Overview

‘Cybersecurity in the driver’s seat’ – Clare Naden, ISO

https://www.iso.org/news/ref2584.html

UN Regulations on Cybersecurity and Software Updates to pave the way for mass roll out of connected vehicles

https://unece.org/sustainable-development/press/un-regulations-cybersecurity-and-software-updates-pave-way-mass-roll

‘Building Secure Cars’ (chapters 1 and 2) – Dennis Kengo Oka

https://www.wiley.com/en-gb/Building+Secure+Cars:+Assuring+the+Automotive+Software+Development+Lifecycle-p-9781119710745

‘Securing the modern vehicle’ – An independent study carried out by the Ponemon Institute

https://www.sae.org/binaries/content/assets/cm/content/topics/cybersecurity/securing_the_modern_vehicle.pdf

‘Benefits, costs and consequences of standards setting: a literature review’ - Aikaterini Poustourli and Maria E Georgakalou

https://www.researchgate.net/publication/304777503_Benefits_Costs_and_Consequences_of_Standards'_setting_A_literature_review

‘How software is eating the car’ -

https://spectrum.ieee.org/cars-that-think/transportation/advanced-cars/software-eating-car

‘Economic contribution of standards to the UK economy’ -

https://www.bsigroup.com/LocalFiles/en-GB/standards/BSI-standards-research-report-The-Economic-Contribution-of-Standards-to-the-UK-Economy-UK-EN.pdf

‘ISO strategy 2030’

https://www.iso.org/files/live/sites/isoorg/files/store/en/PUB100364.pdf

Appendix 1 – List of automotive security standards and recommendations

Recommendations directly addressing automotive security

ISO 21434

1. ISO/SAE 21434:2021, Road Vehicles – Cybersecurity Engineering
   Lists engineering requirements for cybersecurity risk management, including threat modelling, so that organisations operating in the automotive sector are better placed to tackle evolving attack methods. Note that the document does not prescribe specific technologies or solutions.
   2023: CHF 208, 2022: CHF 198

   External references within the recommendation:
   ISO 31000, Risk management – Guidelines
   2023: CHF 92, 2022: CHF 88

   ISO 26262-3:2018, Road vehicles – Functional Safety – Part 3: Concept phase
   2023: CHF 145, 2022: CHF 138

ISO/PAS 5112:2022

2. ISO/PAS 5112:2022 – Road vehicles — Guidelines for auditing cybersecurity engineering
   The guidelines are based on ISO 21434 (see 1) and intended to be used to audit a cybersecurity management system as defined by UNECE WP.29 regulations (see 7).
   2023: CHF 124

SAE J3101

3. SAE J3101 – Hardware Protected Security for Ground Vehicles J3101_202002 (2020)
   The standard provides a perspective on security mechanisms supported in hardware for automotive use cases, along with best practices for using such mechanisms. Such hardware-based approaches are necessary to ensure that systems are able to resist attacks that would otherwise defeat software-only based implementations.
   2023: USD 153, 2022: USD 85

SAE J3061

4. SAE J3061 – Cybersecurity Guidebook for Cyber-Physical Vehicle Systems J3061_201601 (2021)
   Recommendations cover the complete vehicle lifecycle from concept phase through production, operation, service and decommissioning. The standard is a precursor to ISO 21434 and calls for a lifecycle approach to cybersecurity engineering. As mentioned in the timeline section above, this 2021 is an update to the 2016 version, stabilizing the work. This re-work of SAE J3061 was originally reported to be in three parts. Part 1 to describe a threat and risk analysis method for classifying threats within an Automotive cybersecurity Integrity Level (AcSIL) framework. Part 2 giving an overview of security testing methods for software and hardware. Part 3 to discuss security tools. The publication states that “This recommended practice establishes a set of high-level guiding principles for Cybersecurity as it relates to cyber-physical vehicle systems.“ The document set should provide a more technical companion to ISO 21434.
   2023: USD 161, 2022: USD 85

UK Government’s Key Principles of Cyber Security for Connected and Automated Vehicles

5. HM Government: The Key Principles of Cyber Security for Connected and Automated Vehicles (2017)
   Published in August 2017 and created by the UK’s Department for Transport, in conjunction with Centre for the Protection of National Infrastructure (CPNI), the guidance is split into eight key principles — each with sub-details — to support all parties in the manufacturing supply chain in tightening automotive cybersecurity. Topics include taking ownership of organisational security, the importance of using a defence-in-depth design approach as well as performing appropriate management and

assessment of risk, securing and controlling the storage and transmission of data, and the need for product aftercare and incident response to ensure that systems are secure over their lifetime.
Freely available

External references within the recommendation:
SAE
J3061 – Cybersecurity guidebook for cyber-physical vehicle systems
J3101 – Requirements for hardware protected security for ground vehicle applications
ISO
9797-1 – Security techniques: message authentication codes – specifies a model for secure message authentication codes using block cyphers and asymmetric keys
2023: CHF 166, 2022: CHF 158
12207 – Systems and software engineering – software lifecycle processes
2023: CHF 166, 2022: CHF 158
15408 – Evaluation of IT security – specifies a model for evaluating security aspects within IT
Note that this was revised in 2022.
2023: CHF 208, 2022: CHF 178
27001 – Information security management system
Note that this was revised in 2022.
2023: CHF 124, 2022: CHF 118
27002 – Code of practice – security – provides recommendations for information management (contains guidance on access control, cryptography and supplier relationship)
Note that this was revised in 2022.
2023: CHF 208, 2022: CHF 178
27010 – Information security management for inter-sector and inter-organizational communications
2023: CHF 145, 2022: CHF 138
27018 – Code of practice – handling PII / SPI (privacy) – protection of personally identifiable information (PII) in public clouds
2023: CHF 124, 2022: CHF 118
27034 – Application security techniques – guidance to ensure software delivers necessary level of security in support of an organisations security management system
2023: CHF 187, 2022: CHF 178
27035 – Information security incident management
2023: CHF 124, 2022: CHF 118
29101 – Privacy architecture framework
2023: CHF 166, 2022: CHF 158
29119 – Software testing standard
Note that this was revised in 2022.
2023: CHF 166, 2022: CHF 178
DEFSTAN
05-138 – Cyber security for defence suppliers
Freely available
NIST
800-30 – Guide for conducting risk assessments
Freely available
800-88 – Guidelines for media sanitization
Freely available
SP 800-50 – Building an information technology security awareness and training program
Freely available
SP 800-61 – Computer security incident handling guide
Freely available
Other
Microsoft security development lifecycle (SDL)
Freely available
SAFE Code best practices
Freely available
OWASP Comprehensive, lightweight application security process (CLASP)
Freely available
HMG Security policy framework
Freely available
PAS 1192-5 – BSI publication on security-minded building information modelling, digital built

environments and smart asset management (Withdrawn and replaced with BS EN ISO 19650-5)
BS EN ISO 19650-5:2020 – Organization and digitization of information about buildings and civil engineering works, including building information modelling (BIM). Information management using building information modelling. Security-minded approach to information management
2023: GBP 232, 2022: GBP 120
PAS 754 – BSI publication on software trustworthiness, governance and management (Withdrawn following the publication of BS 10754-1:2018)
BS 10754-1:2018 – Information technology. Systems trustworthiness. Governance and management specification
2023: GBP 232, 2022: GBP 218
BS ISO/IEC 11179-5, BS ISO/IEC/IEEE 15288:2015, BS EN ISO/IEC 27002, BS ISO/IEC/IEEE 42010, BS EN ISO/IEC 27001

BSI PAS 1885

6. BSI PAS 1885 (The fundamental principles of automotive cyber security – specification)
   Intended for vehicle manufacturers, tier-1 and tier-2 suppliers, authorised service centres, aftermarket suppliers, road/highway authorities and service providers to both the vehicle and its occupants and/or cargo, the recommendations are aimed at helping all parties involved in the vehicle lifecycle and ecosystem improve their understanding of how to maintain vehicle security and the security of associated intelligent transport systems (ITS).
   2023: GBP 0, 2022: GBP 124
   Informative references - BS ISO 55002, IEC 62443, PAS 555, BS 7858, BS ISO 55000, BS ISO/IEC 29100, ETSI TR 102 893, BS ISO 26262, BS ISO/IEC 27001, PAS 1192-5:2015, BS EN ISO/IEC 27001:2017, BS 10010:2017, PAS 183:2017, BS ISO/IEC 38505-1:2017, PAS 185:2017, PAS 754:2014, PAS 555:2013, BS EN ISO 15118-1:2015, BS ISO/IEC 15408-1:2009, BS ISO 55001:2014, PAS 11281:2018, BS ISO/IEC 38500:2015, BS ISO/IEC 27032:2012

UNECE WP.29

7. UNECE WP.29: UN Regulation No. 155 – 2021, Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system
   The regulations require that automotive providers have a cybersecurity management system (CSMS) in place for the lifetime of the vehicle. Vehicle categories include passenger cars, vans, trucks and buses, and light four-wheeler vehicles if equipped with automated driving functionalities from level 3 onwards (this is to cover new automated pods and shuttles as well as trailers, if fitted with at least one electronic control unit).

   From a threat analysis and risk assessment perspective, it is noteworthy that the guidance specifies a baseline for threats, vulnerabilities and attack methods (available in Annex 5 of the document) that should be considered and defended against.

   To sell into the markets where UNECE WP.29 regulations apply, manufacturers will have to demonstrate to national technical services or homologation authorities (who will likely base their audits on ISO/PAS 5112:2022) that they fulfil the following requirements:

   – Cyber Security Management System is in place and its application to vehicles on the road is available;
   – Provide risk assessment analysis, identify what is critical;
   – Mitigation measures to reduce risks are identified;
   – Evidence, through testing, that mitigation measures work as intended;
   – Measures to detect and prevent cyber-attacks are in place;
   – Measures to support data forensics are in place;
   – Monitor activities specific for the vehicle type;
   – Reports of monitoring activities will be transmitted to the relevant homologation authority.

   Freely available

   Refers to: ISO 26262-2018, ISO/PAS 21448, ISO/SAE 21434

8. UNECE WP.29: Recommendation on Software Updates of the Task Force on Cyber Security and Over-the-air issues (2020)
   The document provides information on managing software updates so that they can be performed safely and securely over-the-air; noting the increased importance (given the rising number of software elements in a vehicle) of being able to implement software corrections and add new features without the hassle and expense of recalling models to dealerships.

   Vehicle manufacturers will need to obtain a certificate of compliance for their software update management system (SUMS) – much like they will need to for their cybersecurity management system (CSMS).

   Freely available
   No references.

ITU-T X.1373

9. ITU-T X.1373: Secure software update capability for intelligent transportation system communication devices
   Offers practical advice that can be used by car manufacturers and ITS-related industries regarding secure software update procedures between a software update server and vehicles with appropriate security controls.
   Freely available
   External references within the recommendation:
   ITU-T X.509, ITU-T X.1521, ISO/IEC 15408-1, ISO/IEC 27000:2014

ENISA

10. Good practices for security of Smart Cars (2019)
    Created to help promote cybersecurity for connected and automated cars across Europe, the report raises awareness on relevant threats and risks with a focus on “cybersecurity for safety”.
    Freely available

    Refers to:
    ETSI TS 102 940 v1.3.1, “Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management
    Freely available
    ETSI TS 102 941 V1.2.1 “Intelligent Transport Systems (ITS); Security; Trust and Privacy Management
    Freely available
    ETSI TS 102 942 V1.1.1 “Intelligent Transport Systems (ITS); Security; Access Control”
    Freely available
    ETSI TS 102 943 V1.1.1 “Intelligent Transport Systems (ITS); Security; Confidentiality services”
    Freely available
    SAE J3061 “Cybersecurity Guidebook for Cyber-Physical Vehicle Systems
    SAE J3016 “Taxonomy and Definitions for Terms Related to Driving Automations Systems for On-Road Motor Vehicles”
    Freely available (USD 0)
    ISO/SAE CD 21434 “Road Vehicles – Cybersecurity engineering
    Auto-ISAC “Automotive Cybersecurity Best Practices – Executive summary”
    Freely available (USD 0)
    ITF/OECD “Safer Roads with Automated Vehicles”
    Freely available
    BSI PAS 1885:2018 The fundamental principles of automotive cyber security specification
    2023: GBP 232, 2022: GBP 218
    IEC - IEC 62443-3-3:2013 System security requirements and security levels
    2023: CHF 330, 2022: CHF 310
    ISO - ISO/IEC 27001:2013 Information technology -- Security techniques – Information security management systems – Requirements
    2023: CHF 124, 2022: CHF 118
    ISO - ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls

2023: CHF 208, 2022: CHF 178
NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations
Freely available
NIST - NISTIR 8183: Cybersecurity Framework Manufacturing Profile
Freely available
SANS Institute - Vulnerability Management: Tools, Challenges and Best Practices
Freely available
NIST - Draft NISTIR 8228: Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks
Freely available
NIST - NIST SP 800 30r1 - Guide for Conducting Risk Assessments
Freely available
NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security
Freely available
ETSI - ETSI TR 102 893 V1.2.1 -- Intelligent Transport Systems: Security, Threat, Vulnerability and Risk Analysis
Freely available
International Telecommunications Union - Security capabilities supporting safety of the Internet of things
Freely available
I Am The Cavalry: Five Star Automotive Cyber Safety Program
Freely available
IEC - IEC 62443-2-1:2010 Establishing an industrial automation and control system security program
Freely available
PRESERVE - Security Requirements of Vehicle Security Architecture v1.1
Freely available
NIST - NIST SP 800-146 Cloud Computing Synopsis and Recommendations
Freely available
oneM2M - Standards for M2M and the Internet of Things - TR 0008 Security V2.0.0 - Security. Technical Report
Freely available

TR 68 - 3 (Singapore)

11. TR 68 – 3: 2019, Technical Reference for Autonomous vehicles – Part 3 : Cybersecurity principles and assessment (Singapore)
    Describes a framework for assessing the cybersecurity of Autonomous Vehicles deployed on public roads.
    2023: SGD 32.50, 2022: SGD 26

    Normative references:
    GSMA CLP.11 - IoT security guidelines and CLP.17 IoT Security Assessment.
    Freely available
    ISO/IEC 19790:2012 - Information technology – Security techniques – Security requirements for cryptographic modules.
    ISO/IEC 26262 series - Road vehicles – Functional safety
    ISO/IEC 27000 series - Information technology – Security techniques – Information security management systems – Overview and vocabulary
    ISO/SAE 21434 - Road vehicles – Cybersecurity Engineering (under development)
    NIST SP 800-115 - Technical Guide to Information Security Testing and Assessment, 2008
    OWASP Open Web Application Security Project
    SAE J3016 - Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles
    SAE J3061 - Cybersecurity Guidebook for Cyber-Physical Vehicle Systems
    WP.29 - UNECE ITS/AD CS/OTA
    TR 64: 2018 Guidelines for IoT Security for Smart Nation
    SGD: 51.40, 2022: SGD 51

US DoT NHTSA

12. US DoT NHTSA Cybersecurity Best Practices for the Safety of Modern Vehicles (2022)
    Updates the Agency's non-binding and voluntary guidance to the automotive industry for improving motor vehicle cybersecurity.
    Freely available
    Refers to:
    ISO 21434
    ISO/IEC 29147:2018, Information Technology Security Techniques Vulnerability Disclosure
    2023: CHF 145, 2022: CHF 138

US H.R.701

13. US H.R.701 – SPY Car Study Act

    The 'Security and Privacy in Your Car' (SPY) Act was proposed in the US (originally in 2015 and then reintroduced in 2017 and 2019) to determine appropriate cybersecurity standards for motor vehicles, and for other purposes. The bill in its earlier forms requires the National Highway Traffic Safety Administration to report on standards for the regulation of the cybersecurity of motor vehicles manufactured or imported for sale in the United States. And, more recently, has cast its attention on consumer needs and driving data (see below).

    2017 (S.680 – 115th Congress - SPY Car Act of 2017)

    2019 (S.2182 – 116th Congress - SPY Car Act of 2019)

    In this version, the bill directs the NHTSA to 'require the fuel economy labelling that manufacturers attach to motor vehicles to display a cyber dashboard with a standardized graphic to inform consumers about the extent to which the vehicle protects individuals' cybersecurity and privacy beyond the minimum requirements'.

    There is also an additional focus on so-called driving data – defined as 'any electronic information collected about the status of the vehicle, including the location and speed of the vehicle; and any owner, lessee, driver or passenger of a vehicle'. The 2019 version directs the Federal Trade Commission to 'require manufacturers to notify owners or lessees about the collection, retention and use of driving data and provide an option to terminate such data collection and retention, and to prohibit manufacturers from using such data for advertising or marketing without the owner's or lessee's consent'. The Bill was read twice referred to the Senate Committee on Commerce, Science and Transportation on the 18th of July 2019.

Extensions to safety considerations

ISO 26262 series and related

The series, derived from IEC 61508, comprise a functional safety standard targeting the lifecycle of automotive equipment and systems. The approach features the use of an 'Automotive Safety Integrity Level' ASIL, which ranges from A (least strict) to D (most strict). Annex E of ISO 26262 gives guidance on the interaction between safety and cybersecurity. Edition 3 (in discussion) could contain more details on security-aware safety topics.

14. ISO 26262-1:2018 Road vehicles — Functional safety — Part 1: Vocabulary
    2023: CHF 40, 2022: CHF 38
    Normative references:
    ISO 26262 (all parts), Road vehicles — Functional safety
15. ISO 26262-2:2018 Road vehicles — Functional safety — Part 2: Management of functional safety
    2023: CHF 166, 2022: CHF 158
    Normative references:
    ISO 26262-1, Road vehicles — Functional safety — Part 1: Vocabulary
    ISO 26262-3:2018, Road vehicles — Functional safety — Part 3: Concept phase
    ISO 26262-4:2018, Road vehicles — Functional safety — Part 4: Product development at the system level

ISO 26262-5:2018, Road vehicles — Functional safety — Part 5: Product development at the hardware level
ISO 26262-6:2018, Road vehicles — Functional safety — Part 6: Product development at the software level
ISO 26262-7:2018, Road vehicles — Functional safety — Part 7: Production, operation, service and decommissioning
ISO 26262-8:2018, Road vehicles — Functional safety — Part 8: Supporting processes
ISO 26262-9:2018, Road vehicles — Functional safety — Part 9: Automotive Safety Integrity Level (ASIL)-oriented and safety-oriented analyses

16. ISO 26262-3:2018 Road vehicles — Functional safety — Part 3: Concept phase
2023: CHF 145, 2022: CHF 138
Normative references:
ISO 26262-1, Road Vehicles — Functional Safety — Part 1: Vocabulary
ISO 26262-2:2018, Road Vehicles — Functional Safety — Part 2: Management of functional safety
ISO 26262-4:2018, Road vehicles — Functional safety — Part 4: Product development at the system level
ISO 26262-8:2018, Road vehicles — Functional safety — Part 8: Supporting processes
ISO 26262-9:2018, Road vehicles — Functional safety — Part 9: Automotive Safety Integrity Level (ASIL)-oriented and safety-oriented analyses
17. ISO 26262-4:2018 Road vehicles — Functional safety — Part 4: Product development at the system level
2023: CHF 145, 2022: CHF 138
Normative references:
ISO 26262-1:2018, Road vehicles — Functional safety — Part 1: Vocabulary
ISO 26262-2:2018, Road vehicles — Functional safety — Part 2: Management of functional safety
ISO 26262-3:2018, Road vehicles — Functional safety — Part 3: Concept phase
ISO 26262-5:2018, Road vehicles — Functional safety — Part 5: Product development at the hardware level
ISO 26262-6:2018, Road vehicles — Functional safety — Part 6: Product development at the software level
ISO 26262-7:2018, Road vehicles — Functional safety — Part 7: Production, operation, service and decommissioning
ISO 26262-8:2018, Road vehicles — Functional safety — Part 8: Supporting processes
ISO 26262-9:2018, Road vehicles — Functional safety — Part 9: Automotive Safety Integrity Level (ASIL)-oriented and safety-oriented analyses
18. ISO 26262-5:2018 Road vehicles — Functional safety — Part 5: Product development at the hardware level
2023: CHF 208, 2022: CHF 198
Normative references:
ISO 26262-1, Road vehicles — Functional safety — Part 1: Vocabulary
ISO 26262-2:2018, Road vehicles — Functional safety — Part 2: Management of functional safety
ISO 26262-4:2018, Road vehicles — Functional safety — Part 4: Product development at the system level
ISO 26262-6:2018, Road vehicles — Functional safety — Part 6: Product development at the software level
ISO 26262-7:2018, Road vehicles — Functional safety — Part 7: Production and operation
ISO 26262-8:2018, Road vehicles — Functional safety — Part 8: Supporting processes
ISO 26262-9:2018, Road vehicles — Functional safety — Part 9: Automotive Safety Integrity Level (ASIL)-oriented and safety-oriented analyses
19. ISO 26262-6:2018 Road vehicles — Functional safety — Part 6: Product development at the software level
2023: CHF 187, 2022: CHF 178
Normative references:
ISO 26262-1, Road Vehicles — Functional Safety — Part 1: Vocabulary
ISO 26262-2:2018, Road Vehicles — Functional Safety — Part 2: Management of functional safety
ISO 26262-3:2018, Road vehicles — Functional safety — Part 3: Concept phase
ISO 26262-4:2018, Road vehicles — Functional safety — Part 4: Product development at the system level
ISO 26262-5:2018, Road vehicles — Functional safety — Part 5: Product development at the hardware level
ISO 26262-7:2018, Road vehicles — Functional safety — Part 7: Production, operation, service and

decommissioning
ISO 26262-8:2018, Road vehicles — Functional safety — Part 8: Supporting processes
ISO 26262-9:2018, Road vehicles — Functional safety — Part 9: Automotive Safety Integrity Level (ASIL)-oriented and safety-oriented analyses

20. ISO 26262-7:2018 Road vehicles — Functional safety — Part 7: Production, operation, service and decommissioning
2023: CHF 92, 2022: CHF 88
Normative references:
ISO 26262-1, Road vehicles — Functional safety — Part 1: Vocabulary
ISO 26262-2:2018, Road vehicles — Functional safety — Part 2: Management of functional safety
ISO 26262-3:2018, Road vehicles — Functional safety — Part 3: Concept phase
ISO 26262-4:2018, Road vehicles — Functional safety — Part 4: Product development at the system level
ISO 26262-5:2018, Road vehicles — Functional safety — Part 5: Product development at the hardware level
ISO 26262-8:2018, Road vehicles — Functional safety — Part 8: Supporting processes
ISO 26262-9:2018, Road vehicles — Functional safety — Part 9: Automotive Safety Integrity Level (ASIL)-oriented and safety-oriented analyses
21. ISO 26262-8:2018 Road vehicles — Functional safety — Part 8: Supporting processes
2023: CHF 187, 2022: CHF 178
Normative references:
ISO 26262-1, Road vehicles — Functional safety — Part 1: Vocabulary
ISO 26262-2:2018, Road vehicles — Functional safety — Part 2: Management of functional safety
ISO 26262-3:2018, Road vehicles — Functional safety — Part 3: Concept phase
ISO 26262-4:2018, Road vehicles — Functional safety — Part 4: Product development at the system level
ISO 26262-5:2018, Road vehicles — Functional safety — Part 5: Product development at the hardware level
ISO 26262-6:2018, Road vehicles — Functional safety — Part 6: Product development at the software level
ISO 26262-7:2018, Road vehicles — Functional safety — Part 7: Production, operation, service and decommissioning
ISO 26262-9:2018, Road vehicles — Functional safety — Part 9: Automotive Safety Integrity Level (ASIL)-oriented and safety-oriented analyses
22. ISO 26262-9:2018 Road vehicles — Functional safety — Part 9: Automotive safety integrity level (ASIL)-oriented and safety-oriented analyses
2023: CHF 145, 2022: CHF 138
Normative references:
ISO 26262-1:2018, Road vehicles — Functional safety — Part 1: Vocabulary
ISO 26262-2:2018, Road vehicles — Functional safety — Part 2: Management of Functional Safety
ISO 26262-3:2018, Road vehicles — Functional safety — Part 3: Concept phase
ISO 26262-4:2018, Road vehicles — Functional safety — Part 4: Product development at the system level
ISO 26262-5:2018, Road vehicles — Functional safety — Part 5: Product development at the hardware level
ISO 26262-6:2018, Road vehicles — Functional safety — Part 6: Product development at the software level
ISO 26262-7:2018, Road vehicles — Functional safety — Part 7: Production, operation, service and decommissioning
ISO 26262-8:2018, Road vehicles — Functional safety — Part 8: Supporting processes
23. ISO 26262-10:2018 Road vehicles — Functional safety — Part 10: Guidelines on ISO 26262
2023: CHF 187, 2022: CHF 178
Normative references:
ISO 26262-1, Road vehicles — Functional safety — Part 1: Vocabulary
24. ISO 26262-11:2018 Road vehicles — Functional safety — Part 11: Guidelines on application of ISO 26262 to semiconductors
2023: CHF 208, 2022: CHF 198
Normative references:
ISO 26262-1, Road vehicles — Functional safety — Part 1: Vocabulary
25. ISO 26262-12:2018 Road vehicles — Functional safety — Part 12: Adaptation of ISO 26262 for motorcycles

2023: CHF 166, 2022: CHF 158
Normative references:
ISO 26262-1, Road vehicles — Functional safety — Part 1: Vocabulary
ISO 26262-2:2018, Road vehicles — Functional safety — Part 2: Management of functional safety
ISO 26262-3:2018, Road vehicles — Functional safety — Part 3: Concept phase
ISO 26262-4:2018, Road vehicles — Functional safety — Part 4: Product development at the system level
ISO 26262-5:2018, Road vehicles — Functional safety — Part 5: Product development at the hardware level
ISO 26262-6:2018, Road vehicles — Functional safety — Part 6: Product development at the software level
ISO 26262-7:2018, Road vehicles — Functional safety — Part 7: Production, operation, service and decommissioning
ISO 26262-8:2018, Road vehicles — Functional safety — Part 8: Supporting processes
ISO 26262-9:2018, Road vehicles — Functional safety — Part 9: Automotive Safety Integrity Level (ASIL)-oriented and safety-oriented analyses

SAE J2980_201804

26. SAE J2980_201804: Considerations for ISO 26262 ASIL Hazard Classification
A companion to ISO 26262, J2980 gives a method together with examples of determining the Automotive Safety Integrity Level (ASIL) for automotive motion control electrical and electronic (E/E) systems – limited to passenger cars weighing up to 3.5 metric tons. Note that the document prioritises collision-related hazards associated with motion control systems as these scenarios tend to generate higher ratings.
2023: USD 143, 2022: USD 85
Normative references:
ISO 26262 series

ISO/PAS 21448

27. ISO/PAS 21448:2019 Road vehicles — Safety of the intended functionality
The guidance — which was originally going to be a section of ISO 26262, but has since been published as its own standard — considers intended use and reasonably foreseeable misuse together with potentially hazardous system behaviour as inputs to design, verification and validation measures that together provide 'safety of the intended functionality' (SOTIF). This was further updated in 2022.
2023: CHF 208, 2022: CHF 178
Normative references:
ISO 26262-1:2018, Road vehicles — Functional Safety Part 1: Vocabulary

UK Code of Practice: Automated vehicle trialling

28. UK Code of Practice: Automated vehicle trialling
Published in 2019, the code requires that software is tested and appropriate measures are in place to manage data security and the risk of unauthorised data access – among a long list of other requirements. Vehicle manufacturers and organisations providing systems for trial in the UK are recommended to follow the UK Government's Key Principles of Cyber Security for Connected and Automated Vehicles (see 5).
Freely available

PAS 11281:2018 (Connected automotive ecosystems. Impact of security on safety. Code of practice)

29. PAS 11281:2018 (Connected automotive ecosystems. Impact of security on safety. Code of practice)
Not directly referenced by the UK code of practice (see 28), but can be considered as related guidance as the recommendations concern the management of security risks that might compromise safety in a connected automotive ecosystem.
2023: GBP 98, 2022: GBP 92
Informative references - BS ISO/IEC 29147, BS ISO 26262, ISO 10393, BS 10754, PAS 1885, BS EN

IEC 62443, BS ISO/IEC 27035, BS ISO 20077-1, IEC 61508:2011, BS ISO 55000, BS EN ISO/IEC 27042, BS EN ISO/IEC 27037, PAS 1085, BS ISO/IEC/IEEE 15288, IEC 61511-1, BS ISO 28000, PD ISO/IEC TS 17961:2013, BS EN ISO/IEC 27002:2017, BS EN ISO 22300:2018, BS ISO/IEC 15026-2:2011, PD ISO/IEC GUIDE 51:2014, PAS 1192-5:2015, PD ISO/IEC TR 24772:2013, BS ISO 26021-2:2008, BS ISO/IEC 27032:2012, BS ISO 14229-1:2013

General foundations AEC-Q100 series

30. General foundations AEC-Q100 series
    The series establishes electrical qualification requirements for components deployed in the harsh conditions of an automotive environment.
    Freely available
    Referenced docs include:
    SAE J1752/3 Integrated Circuits Radiated Emissions Measurement Procedure
    MIL-STD-883 Test Methods and Procedures for Microelectronics
    MIL-STD-750 Test Methods for Semiconductor Devices
    JEDEC JESD-22 Reliability Test Methods for Packaged Devices
    UL-STD-94 Tests for Flammability of Plastic materials for parts in Devices and Appliances
    IPC/JEDEC J-STD-020 Moisture/Reflow Sensitivity Classification for Plastic Integrated Circuit Surface Mount Devices
    JESD89 Measurement and Reporting of Alpha Particle and Terrestrial Cosmic Ray-Induced Soft Errors in Semiconductor Devices
    JESD89-1 System Soft Error Rate (SSER) Test Method
    JESD89-2 Test Method For Alpha Source Accelerated Soft Error Rate
    JESD89-3 Test Method for Beam Accelerated Soft Error Rate

Coding and software guidelines

Automobiles have been accumulating lines of code for some time, primarily in the electronic control units that reside within the vehicle. But greater connectivity, an increase in driver assistance, more data-enabled services and a switch from fossil fuels to electric power will see software play an even wider role in the sector.

Given this trend in new vehicles – sometimes dubbed CASE by analysts, referring to ‘Connected’, ‘Autonomous’, ‘Shared & Services’ and ‘Electric’ aspects of the future vehicle landscape – it will be more important than ever for OEMs and their suppliers to adopt secure coding practices. At the same time, developers will need to track not just their own code, but all software versions that are deployed in their products so that security patches can be applied when vulnerabilities come to light.

The following recommendations apply.

ISO/TR 15497

31. ISO/TR 15497:2000, Road vehicles — Development guidelines for vehicle-based software
    Aimed at automotive software engineers, managers and other stakeholders relating to embedded vehicle software – the recommendations consider a range of issues, including diagnostics and integrated vehicle systems; integrity; noise; EMC; real-time performance; control systems software; metrics; verification and validation; and subcontracting of software development.
    2023: CHF 187, 2022: CHF 178

MISRA

Originally formed to develop guidelines for creating automotive software, the MISRA consortium (a Motor Industry Reliability Association) offers best practice applicable to both embedded control systems and standalone software.

Guidelines -

32. MISRA C: 1998
    Written for C90, has 127 coding rules.
33. MISRA C: 2004
    Written for C90, has 142 coding rules.
34. MISRA C++: 2008

Guidelines produced for C++ in recognition of its growing use in the field
2023: GBP 15, 2022: GBP 15

35. MISRA C: 2012
    Extends support to C99, while maintaining guidelines for C90, has 143 coding rules.
    2023: GBP 15, 2022: GBP 15
36. MISRA C: 2012 Amendment 1 (released 2016)
    Includes 156 rules and 17 directives, giving a total of 173 guidelines.
37. MISRA C: 2012 Amendment 2 (released 2020)
    Two additional rules, taking the total number of guidelines up to 175.
38. MISRA C:2012 — Addendum 2
    Mapping of MISRA rules to the C Secure rules in ISO/IEC TS 17961:2013.
39. MISRA C:2012 — Addendum 3
    Mapping of MISRA rules to the CERT C rules.

Further events - MISRA to merge C++ guidelines with AUTOSAR

ASPICE

40. Automotive SPICE Process Reference Model Process Assessment Model Version 3.1 (2017)
    A framework for quality management in the automotive sector (ASPICE = Automotive Software Performance Improvement and Capability dEtermination)
    Freely available
    Refers to - ISO/IEC 33001:2015, ISO/IEC 33002:2015, ISO/IEC 33003:2015, ISO/IEC 33004:2015, ISO/IEC 33020:2015, ISO/IEC 15504-5:2006, ISO/IEC 12207:2008, ISO/IEC/IEEE 29119-1:2013, ISO/IEC/IEEE 29119-3:2013 So, ISO/IEC/IEEE 24765:2010 S, ISO/IEC 25010:2011, ISO/IEC 12207, ISO/IEC 15288

IATF 16949

41. IATF 16949:2016
    An alternative to ASPICE (see above), the recommendations provide a standard for quality management to be used in conjunction with ISO 9001:2015. IATF = International Automotive Task Force
    2023: USD 150, 2022: USD 150

    Requires ISO 9001:2015
    2023: CHF 145, 2022: CHF 138

NTIA software component transparency and SBOMs

42. NTIA software component transparency
    In 2021, the US National Telecommunications and Information Administration (NTIA) stated that it was working with the automotive sector to report on ‘Supplier recommendations for industry standards to automakers’ over the next 12 months. NTIA provides guidance on how to produce, deliver, update and consume Software Bills of Materials (SBOMs). The National Highway Traffic Safety Administration’s (NHTSA) ‘Cybersecurity Best Practices for the Safety of Modern Vehicles’ guidance recommendation which was published in 2022 (referenced above) has specific requirements related to tracking and maintaining software and hardware components.
    Freely available

    Refers to:
    ISO/IEC 19770-2:2015: Information Technology - Software Asset Management - Part 2: Software Identification Tag
    2023: USD 225, 2022: USD 225
    ISO/IEC TS 17961:2013 Information technology — Programming languages, their environments and system software interfaces — C secure coding rules
    2023: CHF 187, 2022: CHF 178
    SEI CERT C Coding Standard
    Freely available
    ISO/IEC 5055:2021 Information technology — Software measurement — Software quality

measurement — Automated source code quality measures
2023: CHF 208, 2022: CHF 198
ISO/IEC 25000:2014 Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — Guide to SQuaRE
2023: CHF 145, 2022: CHF 178

General foundations

BS 10754-1

43. BS 10754-1:2018 (Information technology – Systems trustworthiness. Governance and management specification)
    A widely applicable approach to improving the trustworthiness of systems, software and services.
    2023: GBP 232, 2022: GBP 218
    Normative references - BS ISO/IEC 11179-5, BS ISO/IEC/IEEE 15288:2015, BS EN ISO/IEC 27002, BS ISO/IEC/IEEE 42010, BS EN ISO/IEC 27001
    Informative references - ITU-T Recommendation X.1520, BS ISO 31000, BS ISO/IEC 19770-1, BS EN ISO/IEC 27000, BS EN ISO/IEC 17024, ITU-T Recommendation X.1521, ITU-T Recommendation X.1525, BIP 0008-1, BS EN 61508 (all parts), BS ISO/IEC 20000-1, BS EN ISO/IEC 17043, BS EN ISO 9001, BS ISO/IEC 15408-1, BS ISO/IEC 19770-2, BS ISO/IEC 27034-1, BS ISO/IEC 15504 (all parts), ITU-T Recommendation X.1544, BS EN ISO/IEC 17025, ITU-T Recommendation X.1524, BS ISO/IEC 33001:2015, BS EN ISO 22301:2014, BS EN ISO 9000:2015, BS EN ISO/IEC 27043:2016

BS EN IEC 60812

44. BS EN IEC 60812:2018 Failure modes and effects analysis (FMEA and FMECA)
    Considers the planning, performance, documentation and maintenance of FMEA to raise awareness of how an item or process might fail to perform its function and the treatments that could be applied.
    2023: GBP 388, 2022: GBP 280
    External references within the recommendation:
    IEC 60050-192 – International electrotechnical vocabulary – Part 192: Dependability

BS EN IEC 61025.

45. BS EN IEC 61025. Fault tree analysis (FTA)
    Public comments are being invited for the upcoming version with the comment period open between 5th April 2023 and 6th June 2023. As with the current document, it will support the identification and analysis of combinations of conditions and factors that risk the occurrence of undesirable outcomes, or ‘top events’.
    2023: CHF 36, 2022: GBP 36

BS EN 61508 series

Methods concerning the application, design, deployment and maintenance of safety-related systems, applicable to a wide range of industries. Note that IEC 61508 formed the basis for ISO 26262.

46. BS EN 61508-1:2010. Functional safety of electrical/electronic/ programmable electronic safety-related systems. General requirements
    2023: GBP 276, 2022: GBP 260
47. BS EN 61508-2:2010. Functional safety of electrical/electronic/ programmable electronic safety-related systems. Requirements for electrical/electronic/ programmable electronic safety-related systems
    2023: GBP 298, 2022: GBP 280
48. BS EN 61508-3:2010. Functional safety of electrical/electronic/ programmable electronic safety-related systems. Software requirements
    2023: GBP 120, 2022: GBP 298
49. BS EN 61508-4:2010. Functional safety of electrical/electronic/ programmable electronic safety related systems. Definitions and abbreviations
    2023: GBP 232, 2022: GBP 218

50. BS EN 61508-5:2010. Functional safety of electrical/electronic/ programmable electronic safety related systems. Examples of methods for the determination of safety integrity levels
2023: GBP 262, 2022: GBP 246
51. BS EN 61508-6:2010. Functional safety of electrical/electronic/ programmable electronic safety related systems. Guidelines on the application of IEC 61508-2 and IEC 61508-3
2023: GBP 316, 2022: GBP 298
52. BS EN 61508-7:2010. Functional safety of electrical/electronic/ programmable electronic safety related systems. Overview of techniques and measures
2023: GBP 356, 2022: GBP 336

IEC TR 62443 series

Devised to support the secure operation of industrial automation and control systems, the guidance notes that cyberattacks on critical infrastructure can put public health at risk and threaten the environment. Recommendations focus not just on the technology, but also on the work processes, countermeasures and employee roles.

53. IEC 62443-2-1:2010. Industrial communication networks - Network and system security - Part 2-1: Establishing an industrial automation and control system security program
2023: CHF 380, 2022: CHF 340
54. IEC TR 62443-2-3:2015. Security for industrial automation and control systems - Part 2-3: Patch management in the IACS environment
2023: CHF 330, 2022: CHF 310
55. IEC 62443-2-4:2015+AMD1:2017 CSV. Consolidated version. Security for industrial automation and control systems - Part 2-4: Security program requirements for IACS service providers
2023: CHF 580, 2022: CHF 550
56. IEC TR 62443-3-1:2009. Industrial communication networks - Network and system security - Part 3-1: Security technologies for industrial automation and control systems
2023: CHF 360, 2022: CHF 330

[END OF DOCUMENT]