Faculdade de Design, Tecnologia e Comunicação
Universidade Europeia

Relatório do Trabalho de Pesquisa

Cibersegurança em Veículos Modernos

Pedro Cunha (20200908)

Índice

1 Introdução

O tema que irá ser abordado neste documento é a cibersegurança nos veículos modernos, no entanto, antes de abordar este tema é necessário introduzir outro conceito importante que está diretamente relacionado com o tema principal, nomeadamente, Internet of Things, desta maneira poderá ser feita uma melhor análise daquilo que são os veículos modernos, isto porque os novos paradigmas tecnológicos vieram redefinir o conceito tradicional daquilo que é efetivamente um veículo, além disso serão ainda avaliadas quais são os seus principais benefícios e vantagens, assim como as suas principais desvantagens, riscos e fragilidades ao nível de cibersegurança.

1.1 Internet of Things (IoT)

A Internet of things [1] surgiu pela primeira vez na década de 90, quando alguns supermercados do Reino Unido experimentaram utilizar cartões de fidelidade com um pequeno chip incorporado que, por sua vez, funcionava via rádio. Este chip recebeu o nome de RFID (Radio Frequency Identification) [2], e permitia que pequenos fragmentos de informações pudessem ser transmitidos de maneira independente, isto é, sem a necessidade de recorrer a uma rede com fio ou a um leitor.

Certo dia, um fabricante desses cartões apresentou a tecnologia a Kevin Ashton, um pioneiro tecnológico britânico, na altura era um jovem funcionário da marca de cosméticos P&G e enfrentava um desafio: descobrir uma forma de controlar o stock de mercadorias nas lojas que vendiam os produtos da marca. Ao conhecer a tecnologia RFID, teve uma ideia: incorporar microchips nos produtos, recebendo, assim, dados que indicariam se os itens haviam sido vendidos ou se estavam em falta nas prateleiras. Foi dessa forma que, em 1999, acabou por idealizar um sistema de sensores que poderiam conectar o mundo físico à Internet.

Podemos então dizer que esta tecnologia se trata da rede de objetos físicos (“coisas”) – que possuam qualquer tipo de sensores, software ou outras tecnologias com o objetivo de conectar e trocar dados com outros dispositivos e sistemas através da Internet sem a necessidade de interação entre humanos ou interação do humano com o computador. Estes dispositivos variam desde objetos domésticos comuns a ferramentas industriais sofisticadas. Atualmente existem mais de 7 bilhões de dispositivos deste tipo conectados, e os especialistas esperam que este número cresça para cerca de 22 bilhões até 2025, segundo a multinacional de tecnologia e informática norte-americana, Oracle [3].

Mas qual é a importância da Internet of Things? A verdade é que nos últimos anos, tem se tornado numa das tecnologias deste seculo que mais tem tido progressos, visto que temos a possibilidade de conectar objetos do dia a dia como eletrodomésticos e veículos à internet por meio de dispositivos incorporados, e deste modo é possível estabelecer uma comunicação perfeita entre pessoas, processos e objetos.

Por meio de computação de baixo custo, Cloud, Big Data, Analytics, tecnologias móveis e entre outras tecnologias, estes objetos podem partilhar e recolher dados com o mínimo de intervenção homem-máquina e no fundo é como se mundo físico e o mundo digital cooperassem entre si.

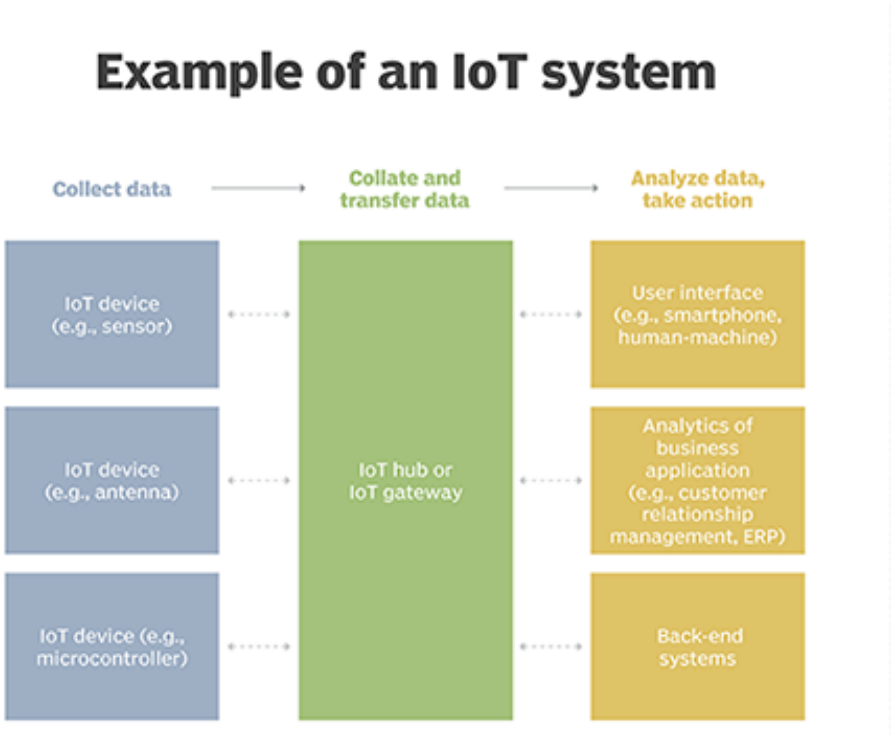

Fig.1 – Funcionamento de um sistema de IoT

2 IoT na Indústria automóvel

Tendo isto em conta, cada vez mais, as organizações de diversas indústrias recorrem à Internet of Things para atuar com mais eficiência, entender melhor os clientes de modo a oferecer um melhor atendimento, melhorar a tomada de decisões e sobretudo aumentar os lucros, uma das indústrias onde isto se tem vindo a verificar cada vez mais é na indústria automóvel, mas de que maneira isto acontece e quais são os benefícios?

A verdade é que nos dias de hoje as pessoas estão cada vez mais preocupadas em arranjar maneiras de simplificar as suas vidas, bem como as atividades que realizam no seu dia-a-dia, nomeadamente a condução que por vezes pode tornar-se numa atividade desgastante e stressante, devido ao facto das longas filas que se formam, especialmente em hora de ponta, visto que cerca de 4 milhões de portugueses utilizam o carro para ir trabalhar, estes números são de um estudo realizado pela Marktest [4] em 2019, e o valor representa 59% dos indivíduos com carta de condução de ligeiros em território nacional. Devido a estes fatores, os potenciais compradores de um carro novo procuram um veículo futurista com o qual possam estar conectados e interagir, tornando a condução numa atividade mais simples e segura e sobretudo menos stressante.

Tendo isto em conta, a Internet of Things aplicada à indústria automóvel consiste na integração de componentes como sensores, gadgets e apps em veículos de modo a criar sistemas complexos, como sistemas de previsão de futuras manutenções e sistemas de gestão de frotas por exemplo, transformando de certa forma os veículos numa espécie de inteligência quase artificial na medida de possuírem a capacidade de tomar certas decisões por si mesmos.

Para além disto, a Internet of things permite ainda a implementação de muitas inovações na indústria, como foi o caso dos carros conectados e dos carros autónomos.

2.1 Categorias

A Internet of Things define 3 categorias distintas de veículos:

I. Um **carro conectado** é um veículo com acesso à internet e que está conectado a dispositivos internos e externos. Estes veículos estão conectados por uma rede chamada CV2X (cellular vehicle to everything) que conecta veículos e sistemas de transporte inteligentes entre si. Com base na conexão do veículo com diferentes objetos, a CV2X é subdividida em quatro categorias: Vehicle to Vehicle (V2V), Vehicle to Infrastructure (V2I), Vehicle to Pedestrians (V2P) e Vehicle to Network (V2N).

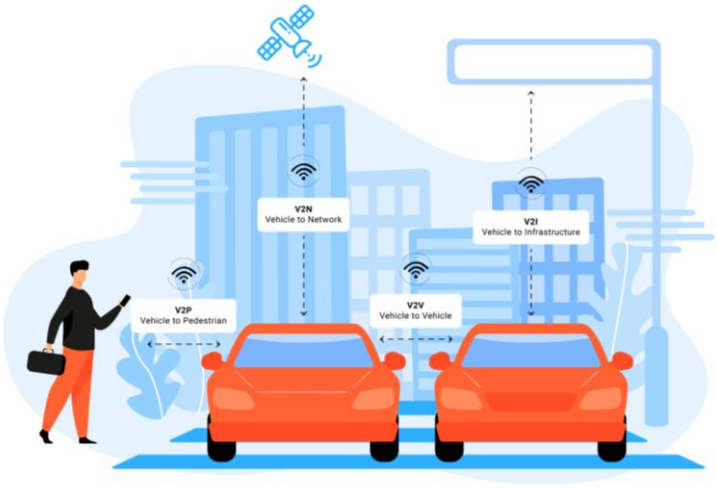

Fig.2 – Categorias de CV2X

II. Os **Smart cars** possuem uma eletrónica avançada incorporando Inteligência Artificial orientada pelo sistema. Uma das características de destaque é a possibilidade de se conduzir parcialmente sozinho, no entanto necessita da intervenção de um humano.

III. Por fim, os **Carros autónomos** são capazes de detetar o ambiente ao seu redor e operar sem intervenção humana, possui a capacidade de poder ir a qualquer lugar e fazer aquilo que um motorista humano faz. Atualmente, a Society of Automotive Engineers (SAE) define 6 níveis distintos de automação de condução que vão desde o Nível 0 (totalmente manual) até ao Nível 5 (totalmente autónomo):

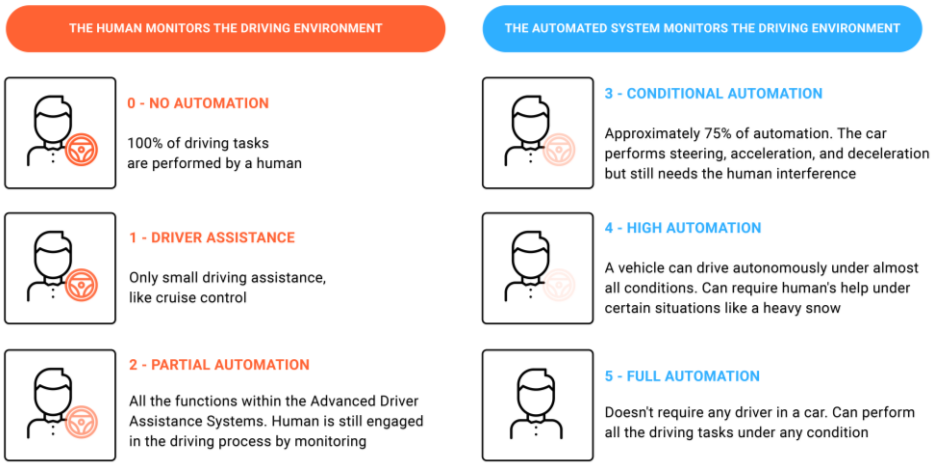

Fig.3 – Níveis de automação definidos pela SAE

2.2 Benefícios e Vantagens

A implementação da Internet of things nesta Indústria proporcionou benefícios e vantagens sobretudo para duas das partes interessadas na mesma, ou seja, tanto para os fabricantes:

- Melhoria na recolha e análise de dados de modo a melhorar e agilizar todo o processo de fabricação;
- Evitar riscos e perdas financeiras;
- Elevar os padrões de segurança industrial;
- Monitoramento de roubo de equipamentos.

Como também para os proprietários dos automóveis, nomeadamente:

- A possibilidade de consultar facilmente toda a informação relativa ao seu veículo através de uma app móvel que em modelos mais recentes, que são, naturalmente, mais tecnológicos permite executar diversas funcionalidades como ligar o motor, verificar o nível de combustível e até pré-aquecer o carro ligando o ar condicionado. Exemplo disto são apps como: Mercedes Me, Tesla App, Fordpass, entre muitas outras;
- Obter uma análise preventiva sobre a condição do carro e, portanto, a oportunidade de reduzir os custos de manutenções, além de tornar a condução mais segura.

2.3 Desvantagens e Riscos

Apesar de existirem muitas vantagens, existem também muitas desvantagens associadas, isto porque na maior parte dos casos, a componente de segurança é normalmente adiada ou mesmo esquecida no ciclo de desenvolvimento dos produtos, não só na indústria automóvel, mas em todas as indústrias no seu geral, com exceção daquelas em que a segurança é crucial e/ou o seu foco principal, como a indústria dos smartphones e dos computadores, por exemplo.

Desta maneira, passemos a enumerar quais são os maiores riscos associados a este tipo de veículos ao nível da cibersegurança, isto porque regra geral, estes veículos conectam-se à Internet via WLAN - Wireless Local Area Network [5], que se trata de uma rede local que usa ondas de rádio para transmitir dados e para se conectar à Internet, não havendo a necessidade de usar os cabos tradicionais para conectar os diversos dispositivos.

Inicialmente os equipamentos necessários para a criação de uma WLAN eram muito caros, por isso, eram usados somente em grandes organizações, no entanto, com a evolução da tecnologia e com a natural diminuição dos custos com equipamento, passou a ser incorporada em todos os tipos de equipamentos que usamos no nosso dia-a-dia, especialmente o padrão de transmissão Wi-Fi (Wireless Fidelity) [6], que é uma das tecnologias usadas pela WLAN e que permite a ligação de computadores portáteis, smartphones, etc., que não estejam muito distantes do ponto de acesso. A segurança de uma WLAN é feita através da autenticação do utilizador, evitando acessos não autorizados e também com a criptografia de dados, para proteção dos dados transmitidos pela rede.

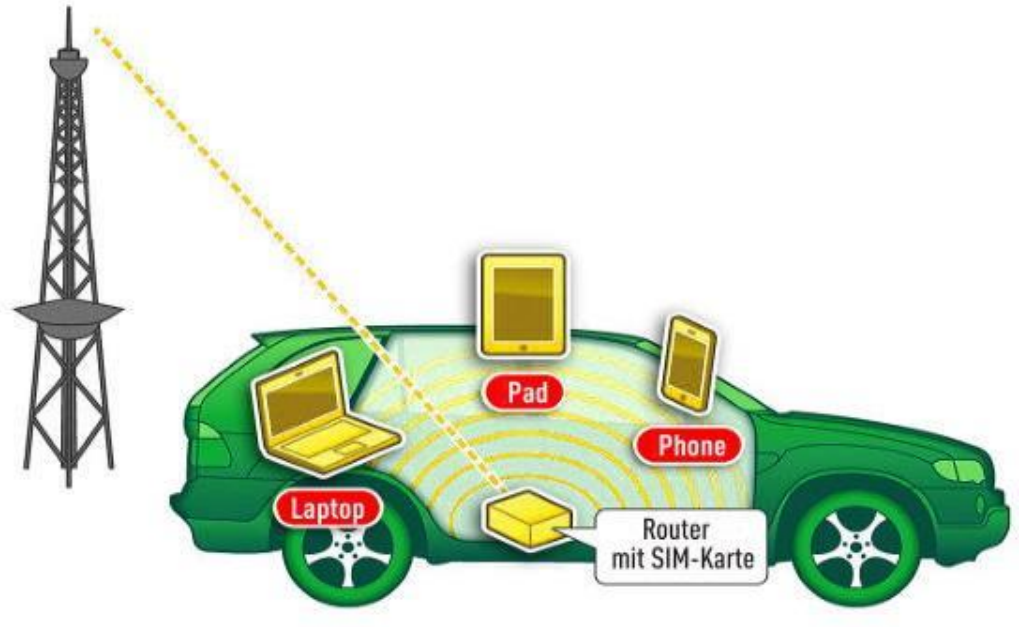

Fig.4 – Esquema de WLAN aplicado em veículos

Deste modo, estes veículos podem então partilhar a internet com dispositivos internos e externos, o que leva à criação de vulnerabilidades, tais como:

I. **Roubo de dados pessoais**: Cada vez existe um maior número de sensores integrados nos veículos, o que aumenta também a possibilidade dos hackers roubarem informações de identificação pessoal através dos sistemas do veículo, nomeadamente, dados da viagem, localização, preferências de entretenimento ou até mesmo informações financeiras.

II. **Manipular sistemas críticos de segurança**: Existe a possibilidade de hackers assumirem o controlo de aspetos críticos de segurança de um veículo, nomeadamente, a sabotagem do sistema de cruise control para que consigam manipular os sistemas de direção e/ou travagem.

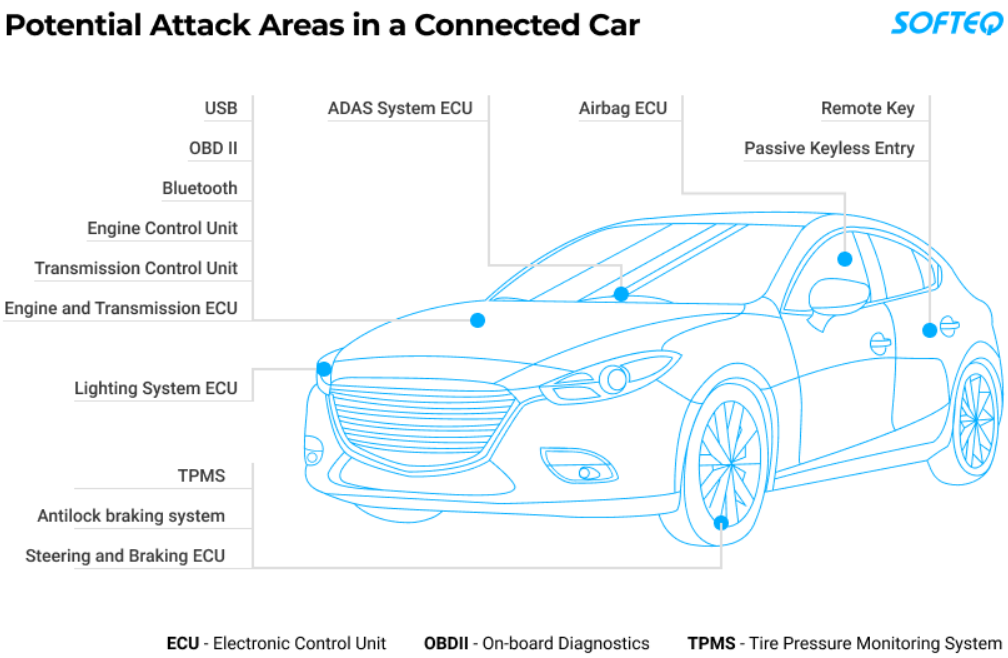

Fig.5 – Potenciais áreas de ataque em veículos conectados

III. **Vulnerabilidades de segurança de apps móveis**: À medida que mais apps móveis são lançadas pelos fabricantes, mais estas se tornam alvos dos hackers, e mais grave que isto é o exemplo do Nissan Leaf, em que os testadores de segurança demonstraram o quão simples era obter acesso não autorizado para conseguir controlar remotamente funções como: volante aquecido, assentos e ar condicionado. Num veículo elétrico, isto pode facilmente drenar a bateria e tornar o veículo imóvel. De acordo com a Gartner, 75% das apps móveis falham nos testes básicos de segurança [7]. O número de vulnerabilidades de segurança existentes nos sistemas Android e iOS são também uma fonte de preocupação.

IV. **Roubo de veículos**: Como as chaves presenciais e as apps móveis vieram substituir as chaves tradicionais, os ladrões podem obter acesso não autorizado ao veículo de uma maneira relativamente fácil, intercetando a comunicação entre um smartphone ou a chave e o veículo, usando dispositivos que estendem o alcance do sinal wireless e que emulam a chave para aceder ao veículo usando a própria chave do proprietário.

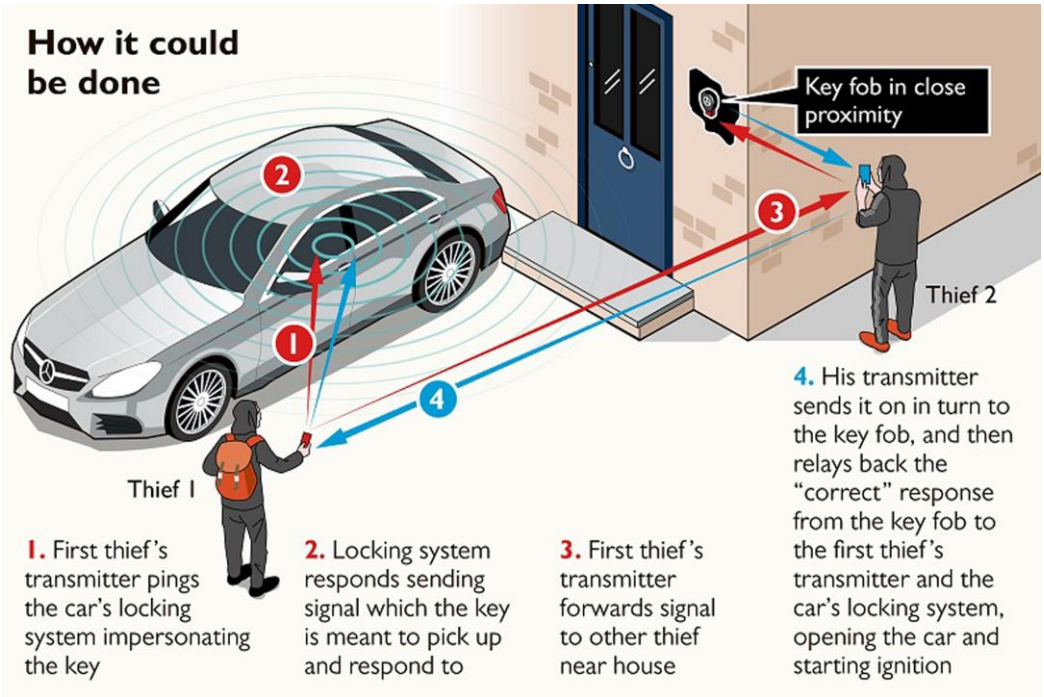

Fig.6 – Esquema de como os ladrões efetuam roubos de veículos conectados

V. **Falta de segurança "projetada"**: A indústria automóvel possui pouca experiência histórica em lidar com riscos de cibersegurança, o que ficou evidente pela falta de segurança incorporada em muitos dos componentes de software e hardware nas primeiras gerações de carros conectados que foram lançados no mercado e além disso, há também uma profunda falta de testes de segurança rigorosos, e grande parte destes testes ocorrem numa fase muito tardia do ciclo de desenvolvimento do produto.

VI. **Vulnerabilidades de segurança na cadeia de fornecimento**: Os fabricantes dependem de fornecedores para que estes lhes forneçam sistemas, software e componentes de hardware para os seus veículos. No entanto, a menos que os fabricantes imponham requisitos rigorosos de cibersegurança aos seus fornecedores, o risco de introduzir vulnerabilidades de segurança por meio destes componentes é bastante elevado.

3 Conclusão

Para concluir, é correto afirmar que a integração da Internet of Things na indústria automóvel teve um grande impacto no seu geral, trazendo inúmeros benefícios e vantagens, mas que, naturalmente, são também acompanhados de algumas desvantagens e riscos que deverão ser combatidas pelos fabricantes que por sua vez devem preocupar-se em dar mais importância à componente da segurança no ciclo de desenvolvimento dos seus produtos, investindo em especialistas e em pesquisa e investigação nesta área, visto que, como vimos, a tendência é o numero de equipamentos conectados aumentar ainda mais nos próximos anos e portanto, os ataques irão ser uma realidade ainda mais frequente, e é portanto importante prevê-los e saber como agir caso aconteçam, para isto é necessário encontrar uma estratégia ideal de cibersegurança tendo em conta as cinco etapas principais listadas abaixo:

I. Estabelecer uma abordagem de security-by-design de modo a assegurar uma boa segurança desde o início, em vez de corrigir as falhas à medida que elas surgem;
II. Avaliar possíveis ameaças cibernéticas e elaborar um perfil de risco, considerando áreas e componentes vulneráveis do ponto de vista do cliente e da empresa;
III. Elaborar um plano de ação e um guião estratégico de implementação de cibersegurança;
IV. Planear e implementar uma abordagem de segurança end-to-end para impedir que terceiros acedam a dados enquanto são transferidos para a cloud e vice-versa;
V. Identificar as tecnologias e o conjunto de soluções para evitar ou responder rapidamente a ataques.

Além de definir uma estratégia, os fabricantes devem ainda adotar standarts e regulamentos de cibersegurança para proteger os seus veículos, e de certa maneira, proteger também o seu meio envolvente, isto abrange peões, animais e outros veículos, alguns exemplos de standarts relevantes encontram-se listados abaixo:

- WP.29 da Comissão Económica das Nações Unidas para a Europa (UNECE) [8]
- ISO 24089 – Software Update Engineering standards [9]
- ISO 21434 Road Vehicles—Cybersecurity Engineering standards [10]
- ISO/TC 204 – Intelligent transport systems [11]
- ISO 22737 – Intelligent transport systems [12]

Estes standarts e regulamentos, podem beneficiar as diversas partes interessadas na indústria automóvel incorporando uma forte cultura de cibersegurança, quantificação de riscos cibernéticos, gestão de riscos, administração e controlo e processos tecnológicos, e acima de tudo ajudam a manter os veículos, motoristas e peões seguros.

Referências Bibliográficas

[1] S. Kumar, P. Tiwari, and M. Zymbler, "Internet of things is a revolutionary approach for future technology enhancement: A Review - Journal of Big Data," SpringerOpen, 09-Dec-2019. [Online]. Available: https://journalofbigdata.springeropen.com/articles/10.1186/s40537-019-0268-2. [Accessed: 18-May-2022].

[2] F. Chetouane, "An overview on RFID technology instruction and application," IFAC-PapersOnLine, 31-Aug-2015. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S240589631500350X. [Accessed: 18-May-2022].

[3] "What is the internet of things (IOT)?," What Is the Internet of Things (IoT)? | Oracle Portugal. [Online]. Available: https://www.oracle.com/pt/internet-of-things/what-is-iot/. [Accessed: 18-May-2022].

[4] "Quatro Milhões de Portugueses Vão de Carro para o trabalho," idealista.pt/news, 02-Mar-2020. [Online]. Available: https://www.idealista.pt/news/financas/economia/2020/02/28/42577-quatro-milhoes-de-portugueses-vao-de-carro-para-o-trabalho-lisboa-e-porto-fogem-a-regra. [Accessed: 24-May-2022].

[5] A. Mourad, S. Muhammad, M. O. A. Kalaa, H. H. Refai, and P. A. Hoeher, "On the performance of WLAN and bluetooth for in-car infotainment systems," Vehicular Communications, 04-Sep-2017. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2214209617300669. [Accessed: 18-May-2022].

[6] "What is wi-fi? - definition and types," Cisco, 22-Dec-2021. [Online]. Available: https://www.cisco.com/c/en/us/products/wireless/what-is-wifi.html#~q-a. [Accessed: 24-May-2022].

[7] "Gartner says more than 75 percent of mobile applications will fail basic security tests through 2015," Gartner. [Online]. Available: https://www.gartner.com/en/newsroom/press-releases/2014-09-14-gartner-says-more-than-75-percent-of-mobile-applications-will-fail-basic-security-tests-through-2015. [Accessed: 24-May-2022].

[8] "WP.29 - introduction," UNECE. [Online]. Available: https://unece.org/wp29-introduction. [Accessed: 18-May-2022].

[9] "ISO/DIS 24089," ISO, 15-Apr-2022. [Online]. Available: https://www.iso.org/standard/77796.html. [Accessed: 18-May-2022].

[10] "ISO/SAE 21434:2021," ISO, 31-Aug-2021. [Online]. Available: https://www.iso.org/standard/70918.html. [Accessed: 18-May-2022].

[11] "Standards by ISO/TC 204," ISO, 23-May-2022. [Online]. Available: https://www.iso.org/committee/54706/x/catalogue/. [Accessed: 24-May-2022].

[12] "ISO 22737:2021," ISO, 06-Jul-2021. [Online]. Available: https://www.iso.org/standard/73767.html. [Accessed: 24-May-2022].