ASSOCIAÇÃO BRASILEIRA DE ENGENHARIA AUTOMOTIVA

WHITE PAPER

CYBERSECURITY

2025

aea

SUMÁRIO

1 INTRODUÇÃO

A necessidade de criar sistemáticas de proteção a sistemas digitais nasce junto com os próprios sistemas. Desde os primórdios da programação, teoricamente já se podia prever questões de segurança relacionadas a eles. Em 1966, o cientista húngaro John von Neumann levanta hipóteses de sistemas que conseguiriam autorreplicar-se e já em 1971, o CREEPER (um Worm, criado por Bob Thomas e aperfeiçoado por Ray Tomlinson) aparecia e ganhava o título de primeiro vírus de computador. Ele era capaz de infectar outras máquinas conectadas localmente e deixar uma cópia de si onde passava. Na mesma época Ray desenvolve o REAPER que tinha como objetivo encontrar máquinas que haviam sido "infectadas" pelo Creeper para apagar o vírus – nesse contexto nascia o primeiro antivírus. Outros vírus surgem e inicialmente eram criados como brincadeiras apenas.

Na época que a conectividade ainda não tinha os padrões que conhecemos hoje (internet, por exemplo), as "infecções" se davam pela utilização de disquetes "contaminados". O primeiro vírus relatado como sendo de distribuição foi o "Elk Cloner", e tinha como alvo os computadores Apple II.

O termo vírus de computador é atribuído a Fred Cohen, que em seu artigo "Computer Viruses - Theory and Experiments" o define como um programa capaz de infectar outras máquinas, espalhando-se por um sistema de computador ou rede.

Ao lado da necessidade de se criar mecanismos de proteção para ataques por vírus, outras disciplinas evoluíram ao longo da história para proteger além das máquinas, os dados que os sistemas trocam. A Criptografia e a Criptoanálise figuram como tópicos fundamentais no contexto da cibersegurança.

Ainda na década de 60, sistemas embarcados (Embedded System – combinação de hardware e software desenvolvidos para uma função específica) passam a ser utilizados a fim de reduzir o tamanho e peso do "Apollo Guidance Computer", um sistema digital instalado no módulo de comando Apollo e também no módulo Lunar. Esses dispositivos ganham relevância e passam a ser utilizados em maior escala em sistemas de controle para mísseis (Autonetics, D-17B, 1965).

Já em 1968, sistemas embarcados passam a ser encontrados também no setor automotivo, empregados no controle do sistema de injeção elétrica (Volkswagen, Volkswagen 1600, 1968).

Desde então, o uso de sistemas embarcados nos veículos só mostra uma evolução. Espalhou-se pelos sistemas de Chassis (ABS, TCS, ESC), de segurança (Air Bags), de carroceria, de entretenimento, de estacionamento. O veículo se tornou um sistema complexo com milhões de linhas de código (SW), diversos computadores interconectados tanto dentro do espaço do veículo como no ambiente externo através de interfaces de conectividade. Não é possível imaginar o futuro da mobilidade que não seja eletrificada, automatizada e conectada.

A evolução dos veículos implica em cada vez mais elevar-se a importância do SW. Espera-se que o veículo seja definido em verdade pelo SW que contém (SDV -> Software-defined vehicle). Em uma alusão cotidiana, o sistema veicular poderia ser comparado a um aparelho celular, composto por um HW, um sistema operacional, e os APP´s que realmente o definem.

Considerando a importância que o SW já tem nos sistemas veiculares, e levando-se em conta a sua crescente utilização é fundamental atentar-se aos riscos associados à invasão dos sistemas e à alteração desse SW que, em última análise, podem alterar a própria definição do veículo.

Nesse contexto a cibersegurança veicular se apresenta com intuito de proteger os sistemas contra ataques ou alterações seja durante a fase de desenvolvimento de um projeto, seja durante a utilização do produto, considerando que as estratégias de manipulação e ataques evoluem. Ela busca a proteção em diferentes níveis: dentro de cada sistema embarcado em si (protegendo o SW gravado nos microcontroladores), definindo autenticação de informações dentro das redes veiculares e cuidando das interfaces de conectividade com o meio externo.

Ao longo da última década muitos esforços foram alocados para aumentar o nível de proteção dos sistemas embarcados tanto para os dispositivos de HW como nas tecnologias de SW. Considerando que a sofisticação dos ataques também evolui, é esperado que os investimentos em cibersegurança sejam constantes a fim de garantir a proteção dos sistemas mesmo depois de seu lançamento.

O intuito deste white paper é fomentar a discussão de cibersegurança para o setor automotivo no Brasil, apresentar as ações que estão sendo tomadas no Brasil e em outras regiões em termos de regulamentação e normatização, analisar os impactos dessas implementações em outros mercados e entender quais outros desafios teremos em nossa realidade.

2 VOCABULÁRIO

Attack – *Ataque*

Ação ou interação deliberada com um item ou componente do sistema ou seu ambiente de operação que tem potencial de resultar em uma consequência adversa.

Threat *– Ameaça*

Attack Feasibility *– Viabilidade de um ataque*

Propriedade que mede quão fácil/provável que um ataque em específico seja bem sucedido.

Attack Path *– Caminho de ataque*

Sequência de ações de um atacante que culminam em um ataque bem sucedido. Um caminho de ataque viável resulta em um cenário de ameaça (Threat Scenario).

Attack Surface *– Superfície de ataque*

Conjunto de caminhos pelos quais um atacante pode entrar em um sistema e potencialmente comprometê-lo. Quanto menos isolado um sistema, maior sua superfície de ataque. Sistemas acessíveis apenas fisicamente tem uma superfície de ataque menor do que sistemas conectados à redes locais (ex: Bluetooth) que por sua vez tem superfície menor que sistemas conectados à Internet ou outras redes de longo alcance e troca remota de informações.

Cybersecurity *– Cibersegurança*

No contexto dos sistemas eletrônicos de um veículo, trata-se da condição na qual todos os recursos (assets) identificados como críticos estão protegidos de forma satisfatória contra quaisquer ameaças.

Cybersecurity Goal *– Meta de Cibersegurança*

Requisito de alto nível (não detalhado tecnicamente) a ser implementado no sistema de modo a mitigar uma ou mais ameaças identificadas.

Cybersecurity / Security Concept *– Plano de Segurança*

Coleção de requisitos e especificações de um sistema definidos de modo a atender as metas de cibersegurança (cybersecurity goals) propostas. Acaba sendo a especificação sistêmica detalhada e técnica de quais tecnologias, protocolos, soluções, etc devem ser adotadas de modo que todas as metas/objetivos de cibersegurança sejam cumpridos.

Damage Scenario *– Cenário de Dano*

Potencial consequência adversa após o comprometimento de uma propriedade de cibersegurança ou recurso do sistema por um ataque.

Threat Scenario *– Cenário de Ameaça*

Conjunto de ações potencialmente negativas que culminam em um cenário de danos.

Penetration Testing *– Teste de Intrusão*

Tipo de teste de cibersegurança no qual são mimetizados ataques, os mais parecidos possíveis com situações de mundo real, de modo a identificar possíveis caminhos de ataque e meios de comprometer o sistema. (NIST SP 800-115)

Risk *– Risco*

No contexto da cibersegurança automotiva (ISO/SAE 21434) trata-se de uma estimativa das incertezas em se garantir a cibersegurança do sistema, expressa em termos da viabilidade de um ataque e seus potênciais impactos, consequências e desdobramentos.

Availability *– Disponibilidade*

Propriedade de um dado ou informação de ser acessível e usável quando demandado.

Integrity *– Integridade*

Authenticity *– Autenticidade*

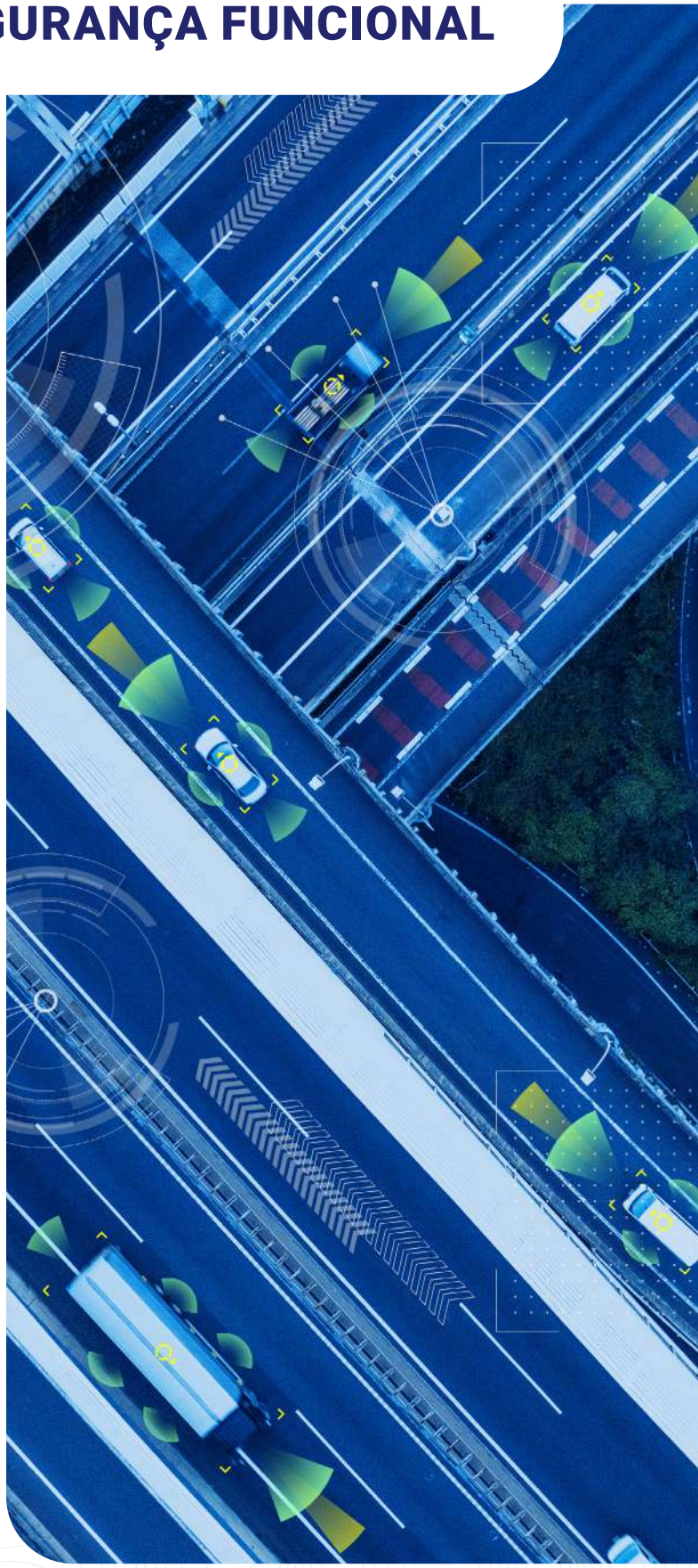
Propriedade obtida por meio do emprego de métodos criptográficos que conferem à uma transmissão, informação, ou mensageiro a capacidade de serem verificados e sua validade atestada.

Confidentiality *– Confidencialidade*

Asset *– Recurso*

Safety *– Segurança (funcional)*

3 CIBERSEGURANÇA X SEGURANÇA FUNCIONAL
(FUNCTIONAL SAFETY)



Segurança, de modo geral, pode ser definida como um conjunto de medidas que visam proteger pessoas ou objetos de riscos, danos ou perdas. Com a expansão de sistemas e dispositivos eletroeletrônicos inteligentes, novos riscos vêm sendo inseridos no cotidiano das pessoas, exigindo novos e complexos requisitos de segurança. (https://www.iec.ch/functional-safety)

A Segurança Funcional busca a ausência de riscos provenientes do mal funcionamento técnico de sistemas. Sob a perspectiva de um sistema, significa que um controle atuante deve detectar situações de falha e impedir que este estado ou condição perigosa permaneça e afete seus usuários.

Com o objetivo de evitar essas situações perigosas, a IEC 61508 fornece padrões de segurança funcional para o ciclo de vida de sistemas e produtos elétricos, eletrônicos ou eletrônicos programáveis. Essa norma permite o desenvolvimento de uma abordagem técnica uniforme e genérica que pode ser aplicada a todos os sistemas de segurança de hardwares e softwares relacionados.

A ISO 26262, "Road vehicles – Functional safety", é a adaptação da IEC 61508, a qual visa atender às necessidades específicas da aplicação de sistemas elétricos e/ou eletrônicos em veículos rodoviários. Essa adaptação contempla todas as atividades do ciclo de vida de segurança de sistemas compostos por componentes elétricos, eletrônicos e software. Esse ciclo abrange as principais atividades de segurança durante a fase conceitual, desenvolvimento do produto, produção, operação, serviço e desativação de uma maneira sistêmica e metodológica.

Como definida no capítulo 2, a Cibersegurança é a prática de proteger ativos de informação tais como sistemas, computadores, servidores, entre outros contra ameaças cibernéticas ou ataques maliciosos. É comum encontrarmos o conceito de Segurança Funcional sendo confundido com o conceito de Cibersegurança. Porém, verifica-se que a Segurança Funcional busca evitar riscos provenientes de falhas internas dos dispositivos (podem ser gerados por fatores internos e externos, mas não intencionais), as quais podem vir a gerar danos para seus usuários. Já a Cibersegurança visa proteger os sistemas de ataques externos (intencionais). Portanto, são conceitos complementares, porém diferentes.

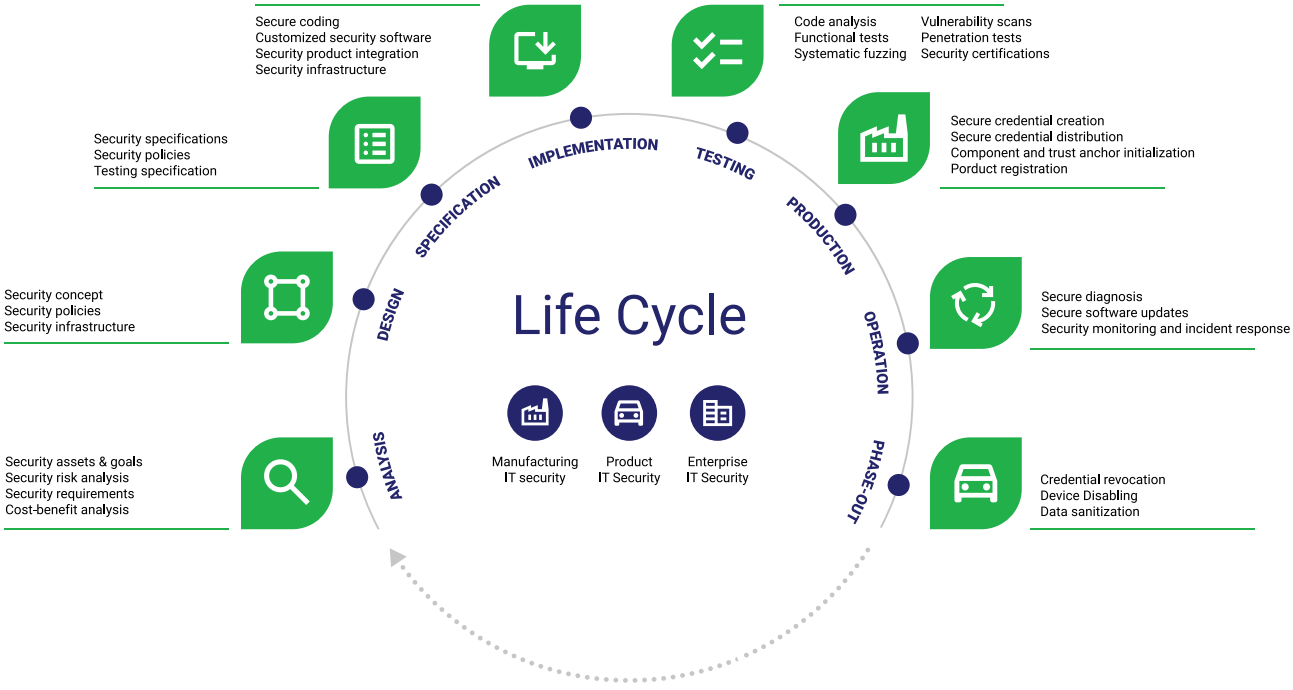
4 DIMENSÃO HOLÍSTICA DA CIBERSEGURANÇA
(CICLO DE VIDA DO PRODUTO)

O desenvovimento de sistemas eletro-eletrônicos automotivos que sejam suficientemente cibersegu-ros apresenta desafios notáveis. Podemos citar a natureza "evolutiva" das ameaças, a longa vida útil dos veículos, a complexa interação entre diversos fornecedores e integradores e, finalmente, as novas arquiteturas eletro-eletrônicas desenvolvidas para suportar as novas tendências da mobilidade (ADAS, Conectividade, Eletrificação, FOTA, etc..)

Diferentemente de outras propriedades funcionais ou de segurança do sistema, a cibersegurança pode ser comprometida com apenas uma vulnerabilidade ou ponto do ataque bem explorado por um atacante. Desse modo, é importante ter em mente como cada um dos elos da cadeia de desenvolvimento, produção e operação do sistema que pode ser afetado e quais medidas devem ser tomadas em cada fase. Esse tipo de ideia não se resume ao contexto de desen-volvimento de produto/sistema, mas também deve ser replicado a nivel organizacional. Todas as orga-nizações envolvidas no processo devem estar pron-tas para lidar com esse tema, por meio da criação de estruturas de governança e o estabelecimento de políticas internas de documentação, concientização, análise e gestão de riscos, auditorias, gerenciamento de ferramentas e compartilhamento de informação.

O diagrama abaixo ilustra uma proposta de divisão dessas fases e suas atividades mais importantes:

A HOLISTIC APPROACH TOWADS CYBERSECURITY



Análise

O sistema a ser protegido e seu contexto de operação devem ser inicialmente estudados em profundidade. Os elementos chaves a serem defendidos devem ser identificados, caminhos de ataque previstos e um modelo de atacante gerado. O primeiro passo é a execução de uma análise de ameaças e determinação de riscos (TARA – "Threat Analysis and Risk Assesment"). Esse processo avalia de forma metodológica e completa quais são as ameaças às quais o sistema em estudo está submetido, quais os possíveis impactos caso essas ameaças se concretizem (dano à vida e propriedade, financeiros, dano à imagem, privacidade, operacional, etc..) e, finalmente, quantifica qual o nível de risco presente. São então propostas medidas de alto nível para o gerenciamento e mitigação desses riscos, as metas de cibersegurança.

Design e Conceito

O próximo passo é o desdobramento dos conceitos e medidas de mitigação de risco de alto nível definidos na fase anterior em requisitos técnicos detalhados, capazes de serem implementados. Aqui são definidas quais tecnologias, sistemas, protocolos de criptografia e estratégias serão utilizadas de modo a mitigar os riscos encontrados na fase de análise até um nível aceitável. É também definida a arquitetura geral do sistema e da infraestrutura de suporte que será utilizada durante seu desenvolvimento, teste, produção, operação e descomissionamento.

Especificação Técnica

A fase de especificação técnica é uma extensão do design e conceito. Aqui todos os detalhes a nível de implementação são definidos. Quais as rotinas detalhadas a serem empregadas na produção do sistema ou equipamento? Como será gerado e armazenado o material criptográfico inicial? Como ele será injetado no sistema de forma segura? Quais algoritmos serão utilizados para garantir os requisitos de autenticação, disponibilidade, confidencialidade e integridade do sistema? Quais técnicas de criptografia simétrica, assimétrica, assinatura segura, comunicação segura (TLS por exemplo) estarão presentes no sistema e como eles serão implementadas? Todos esses detalhes são definidos nessa fase. Nesse contexto, é importante que o hardware escolhido e a infraestrutura de apoio e amparo ao sistema sejam também especificadas de forma a atender os requisitos do conceito de segurança.

Implementação

Uma vez que todos os requisitos em alto, médio e baixo nível foram bem definidos e validados, é iniciada a implementação de fato do sistema. Aqui o ponto chave é que sejam seguidas boas práticas de cibersegurança na criação e integração de código e também na adoção de componentes de software que tenham procedência atestada e estejam alinhados com os requisitos do sistema. (HW e ambiente de produção)

Fase de Testes

Dada a natureza dinâmica das ameaças de cibersegurança e a complexidade dos sistemas à serem protegidos, os testes e a fase de validação como um todo são peças fundamentais das estratégias de cibersegurança. Devem ser avaliados os componentes individualmente, a qualidade de sua implementação e então sua integração no sistema como um todo. Aqui estão presentes aspectos de implementação de forma bastante clara, mas também do ambiente de produção, operação e descomissionamento do sistema, que também precisam ser testados.

Os testes e processos de validação variam bastante também em termos de sua natureza: existem testes automatizados (Fuzz Testing e Vulnerability Scanning por exemplo) e testes manuais conduzidos por especialistas (Pentesting em geral). Existem testes nos quais nada ou muito pouco é conhecido sobre o sistema pelo time de teste (black-boxing) passando por casos mistos (grey-boxing) até avaliações onde todas as informações estão disponíveis (white-boxing). Finalmente, existem testes específicos para a infraestrutura de produção, monitoramento em campo e operação do sistema. A adoção de forma integrada de todas essas metodologias garante que o que foi avaliado e prescrito na fase de conceito e implementado posteriormente não apresenta pontos falhos ou vulnerabilidades ocultas e tem sua cibersegurança garantida.

Produção

A fase de produção é crítica quando se busca garantir a cibersegurança de um sistema. Todos os elos na cadeia devem ser pensados e estarem integrados na estratégia geral para que se atinja uma proteção holística conforme previsto incialmente. Os alvos presentes na cadeia produtiva vão desde os computadores responsáveis pela geração de código de produção até a linha em si, com destaque para as estações de

"flash", que lidam com material criptograficamente relevante (exemplo: chaves criptográficas). Se destacam a adoção de tecnologias como a "assinatura" de software e o uso de sistemas centralizados de gerenciamento e injeção de chaves criptográficas e código.

Operação

A evolução tecnológica e a progressiva descoberta de vulnerabilidades nos sistemas eletrônicos confere à cibersegurança um caráter temporal. Elementos que hoje estão protegidos podem ser comprometidos ao longo de sua vida útil, tornando imprescindível a necessidade de mecanismos de monitoramento continuo e resposta à incidentes.

Phase-Out

Por fim, a cibersegurança também deve ser considerada nos processos de descomissionamento e phase-out de sistemas automotivos. Um exemplo clássico são os certificados que permitem o estabelecimento de comunicação segura entre a nuvem e os componentes do veículo, que devem ser periodicamente atualizados e então revogados em casos de furto ou fim de vida. De maneira geral, todos os dados que sejam criptograficamente relevantes ou então sejam considerados como pessoais (LGPD) devem ser completamente sanitizados antes que o veículo seja descomissionado para que não sejam utilizados de forma indevida.

5 ESTADO DA ARTE
- NORMATIZAÇÕES E REGULAMENTAÇÕES

A cibersegurança, embora relativamente recente na indústria automotiva, beneficia-se da disponibilidade de tecnologias e ferramentas consolidadas, bem como de lições aprendidas e processos já estabelecidos em outros setores. Contudo, é crucial reconhecer as peculiaridades inerentes aos produtos automotivos.

Um exemplo notável é o ciclo de vida prolongado dos veículos, que exerce um impacto significativo nos processos de segurança, especialmente nas estratégias de atualização de software e firmware. Diante desse cenário, torna-se imperativo que a indústria estabeleça um conjunto robusto de boas práticas, visando garantir um design seguro a longo prazo. Essas diretrizes fortalecerão a segurança global e assegurarão a proteção do produto final.

Historicamente, a indústria tem abordado a cibersegurança de forma fragmentada, definindo diretrizes individualizadas para os diversos participantes da cadeia de suprimentos e operando com escopo limitado em cada país. Esses esforços incluem o estabelecimento de uma base de referência para ameaças, vulnerabilidades e métodos de ataque, bem como recomendações para montadoras e seus fornecedores avaliarem seus impactos.

No entanto, organismos internacionais têm agido prontamente para preencher essa lacuna. Atualmente, há um esforço contínuo para assegurar que a cibersegurança se torne uma prioridade para os fabricantes em todos os níveis da cadeia de suprimentos automotiva.

5.1 NORMATIVA VS. REGULAÇÃO

Normas e diretrizes contêm especificações técnicas detalhadas, refletem o estado da arte e promovem a colaboração industrial em escala global, sendo formuladas por consenso. Embora não sejam de cumprimento obrigatório ou juridicamente vinculativas, idealmente, consolidam-se como prática comum, representando a forma acordada de executar processos.

As regulamentações estabelecem objetivos e metas de política de longo prazo, definindo os requisitos mandatórios a serem atendidos. Possuem força jurídica vinculante em todos os países signatários (também denominados “partes contratantes”).

A adesão a uma norma não garante, por si só, a conformidade com as leis aplicáveis.

5.2 O CAMINHO ATÉ UMA NORMATIVA DE CIBERSEGURANÇA DEDICADA PARA A INDÚSTRIA AUTOMOTIVA

5.2.1 Linha do tempo

1994

MISRA publica diretrizes para o desenvolvimento de software para aplicações automotivas.

2015

SAE cria o Comitê de Engenharia de Sistemas de Cibersegurança de Veículos como resposta a ameaças e vulnerabilidades específicas da indústria automotiva nos Estados Unidos.

2016

SAE publica a normativa J3061 Cybersecurity Guidebook for Cyber-Physical Vehicle Systems. As recomendações abrangem todo o ciclo de vida do veículo, desde a fase de conceito até a produção, operação, serviço e desativação. O padrão é um precursor da ISO 21434 e exige uma abordagem de ciclo de vida para a engenharia de segurança cibernética.

2018

ISO publica a segunda versão da norma 26262. Esta versão inclui comentários sobre a interação entre segurança cibernética e segurança funcional, mas o consenso é que os assuntos devem ser tratados em normativas diferentes.

2019

MISRA e AUTOSAR anunciam que as normativas da indústria sobre melhores práticas na programação de C++ serão integradas numa única publicação.

2021

A versão final ISO 21434 é publicada. Esta norma substitui a J3061 e fornece uma estrutura para implementar um sistema de gerenciamento de segurança cibernética (CSMS) e gerenciar o risco de segurança cibernética de veículos.

2022

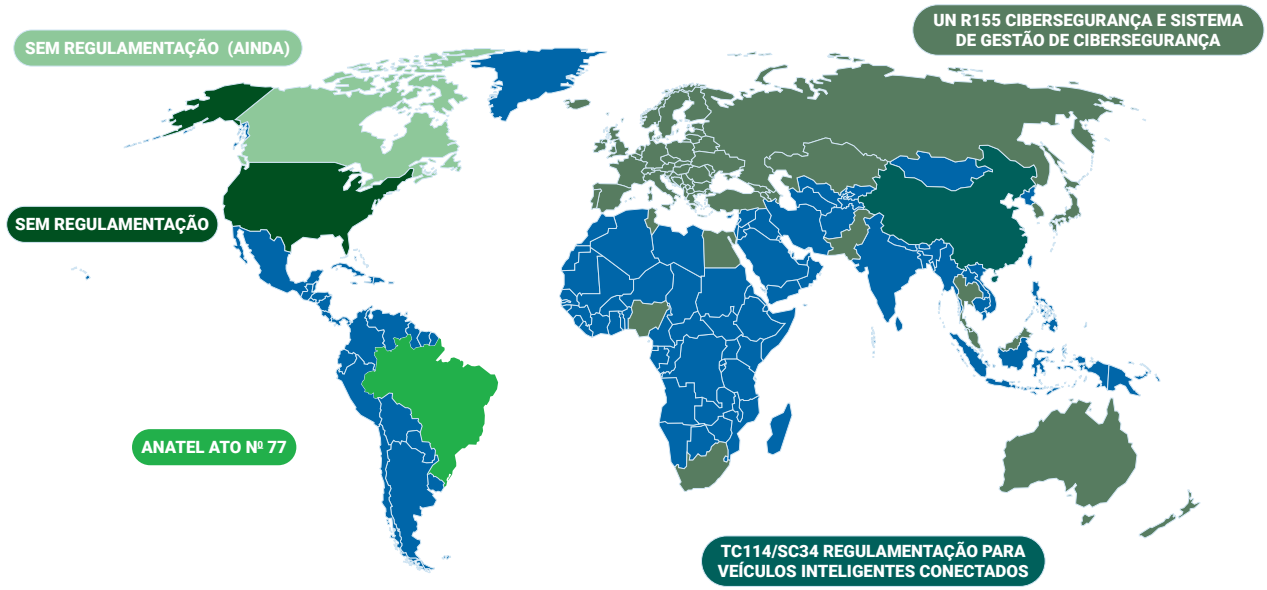
Em julho a regulação da WP29 UNECE (R155) começa a ser aplicável para novos modelos de veículos a serem vendidos nos 58 países que assinaram o acordo de 1958 das nações unidas.

2024

Em julho a regulação da WP29 UNECE (R155) começa aplicar para todos os novos veículos vendidos nos 58 países que assinaram o acordo de 1958 das nações unidas.

5.3 VISÃO MUNDIAL DA REGULAÇÃO DE CIBERSEGURANÇA

VISÃO GLOBAL SOBRE AS REGULAMENTAÇÕES DE CIBERSEGURANÇA



5.3.1 Acordo de 1958 das Nações Unidas

O Acordo de 1958 estabelece o quadro jurídico para a adoção de regulamentos técnicos harmonizados das Nações Unidas, aplicáveis a veículos de rodas, equipamentos e peças, visando a segurança e a proteção ambiental. Adicionalmente, este acordo promove o reconhecimento recíproco das homologações emitidas sob estes regulamentos.

WP.29: Fórum Regulatório Global:

O Fórum Mundial da Comissão Econômica das Nações Unidas para a Europa (UNECE) para Harmonização das Regulamentações de Veículos (WP.29) é um fórum regulatório global único, inserido na estrutura institucional do Comitê de Transporte Terrestre da UNECE. Este fórum desempenha um papel crucial na elaboração e harmonização de regulamentações automotivas em escala mundial.

A UNECE WP29 define os requisitos para aprovação de tipo. Os membros são:

• Autoridades de aprovação de tipo

• Organismos de certificação

• OEM e Fornecedores de nivel Tier 1

A UNECE anunciou em junho de 2020 os regulamentos WP.29 R155 e R156.

O regulamento R155 exige a implementação de um Sistema de Gestão de Cibersegurança (CSMS) abrangente, que cobre todas as fases do ciclo de vida do veículo, desde o desenvolvimento até a produção e pós-produção. Este regulamento responsabiliza os OEMs por assegurar que seus fornecedores estejam em conformidade com as medidas de segurança especificadas.

O regulamento R156 foca na segurança do software de pós-produção, incluindo o software em si e os procedimentos de atualização over-the-air (OTA). Software aprovado durante a produção, sob o regulamento WP.29 R155, deve passar por nova aprovação se qualquer modificação no veículo afetar seu desempenho técnico ou a documentação original da aplicação.

Abrangência Geográfica:

Atualmente, o WP.29 abrange 54 países participantes dos Acordos e Convenções de Transporte da UNECE de 1958, incluindo a União Europeia, Reino Unido, Japão e Coreia do Sul.

Na União Europeia, o novo regulamento de cibersegurança é obrigatório para todos os novos tipos de veículos fabricados a partir de julho de 2022, e para todos os veículos novos produzidos a partir de julho de 2024.

O Brasil não é signatário do Acordo de 1958 da UNECE. No entanto, o setor automotivo brasileiro aplica regulamentações e normas desenvolvidas por organizações internacionais. O país tem desenvolvido seu próprio regime regulatório, que, embora baseado em iniciativas internacionais, não adota integralmente as normativas da UNECE ou as FMVSS, permitindo adaptações às particularidades do mercado local.

5.3.1.1 Japão

O governo japonês estabeleceu regulamentos nacionais para cibersegurança e atualização de software, com implementação inicial em abril de 2020, aplicável a novos veículos equipados com nível 3 ou superior de condução autônoma. Esta iniciativa precedeu as regulamentações europeias.

A regulamentação foi oficialmente publicada em julho de 2020 e entrou em vigor em novembro do mesmo ano.

A partir de julho de 2022, os regulamentos nacionais de Cibersegurança/Atualização de Software (CS/SU) foram harmonizados com os regulamentos da ONU, estendendo-se a todos os veículos novos, independentemente do nível de automação.

O processo de harmonização continua em ritmo acelerado, impulsionado pela obrigatoriedade dos requisitos do regulamento R155 da União Europeia, que exige a certificação de todos os novos veículos, independentemente do tipo, a partir de julho de 2024.

5.3.1.2 Coreia do Sul

A regulamentação sul-coreana adota um modelo de auto certificação, onde os fabricantes atestam a conformidade com os requisitos dos Padrões de Desempenho e Segurança de Veículos Automotores e Peças de Veículos da Coreia (KMVSS) após conduzirem testes internos. Os relatórios de testes devem ser disponibilizados ao governo mediante solicitação, e o governo realiza testes aleatórios em veículos selecionados anualmente.

O país planeja adotar a maior parte do padrão de cibersegurança da UNECE. No entanto, algumas disposições da legislação local necessitam de revisão para harmonizar o sistema legal nacional com o padrão internacional. Consequentemente, a implementação integral da norma internacional adotada em 2022 é inviável, exigindo o desenvolvimento paralelo de normas nacionais.

Apesar do sistema de auto certificação e da estrutura dos KMVSS, o padrão de cibersegurança da ONU está alinhado com o sistema de aprovação de tipo. Portanto, para estabelecer uma regulamentação de cibersegurança eficaz na Coreia do Sul, são necessárias revisões adicionais para conciliar o sistema jurídico doméstico com o padrão internacional.

Assim como no Japão, o processo de harmonização está em andamento, acelerado pela obrigatoriedade dos requisitos do regulamento R155 da União Europeia, que exige a certificação de todos os novos veículos, independentemente do tipo, a partir de julho de 2024.

5.3.2 ESTADOS UNIDOS

O modelo regulatório dos Estados Unidos adota um esquema de autocertificação. Atualmente, não existe uma regulamentação federal obrigatória específica para cibersegurança automotiva.

A National Highway Traffic Safety Administration (NHTSA) desenvolveu um conjunto de diretrizes de melhores práticas, inicialmente publicado em 2016: "NHTSA Cybersecurity Best Practices for the Safety of Modern Vehicles"

A NHTSA publicou uma atualização deste documento em setembro de 2022. Embora não possua caráter obrigatório, espera-se que estas diretrizes sejam adotadas como padrão pela indústria.

Apesar da não obrigatoriedade, a publicação destas diretrizes evidencia uma crescente preocupação com a cibersegurança na indústria automotiva dos EUA. As diretrizes de melhores práticas de cibersegurança automotiva incluem:

• Referências à norma ISO/SAE 21434, que abrange gerenciamento de segurança, gerenciamento de cibersegurança dependente de projeto, técnicas de avaliação de risco, atividades contínuas de cibersegurança e cibersegurança nas fases de desenvolvimento de conceito e pós-desenvolvimento de veículos rodoviários.

• Referências aos sete guias de melhores práticas do Auto-ISAC, que cobrem diversos tópicos de cibersegurança, incluindo treinamento, desenvolvimento de produtos e resposta a incidentes.

• Diretrizes técnicas detalhadas aplicáveis a dispositivos da Internet das Coisas (IoT). Muitas destas diretrizes são baseadas em quatorze vulnerabilidades exploradas, que são detalhadas nos documentos.

5.3.3 CANADA

O Canadá adota um modelo regulatório similar ao dos Estados Unidos, baseado em autocertificação.

A agência governamental Transport Canada, em colaboração com departamentos federais, a indústria e especialistas em cibersegurança, desenvolveu um conjunto de orientações e ferramentas para a cibersegurança de veículos. Estes recursos auxiliam as partes interessadas do setor no desenvolvimento de estratégias organizacionais de cibersegurança veicular. Em conjunto, eles fornecem informações relevantes sobre ameaças à cibersegurança veicular e práticas recomendadas para manter uma postura de segurança robusta. E incluem as seguintes publicações:

• "Canada's Vehicle Cyber Security Guidance" - Publicado em maio de 2020

• "Canada's Vehicle Cyber Security Assessment Tool (VCAT)" - Publicado em agosto de 2021

• "Transport Canada's Vehicle Cyber Security Strategy" - Publicado em agosto de 2021

• "Security Credential Management Systems – Model Canadian Certificate Policy" - Publicado em 30 de novembro de 2021

O Canadá participa ativamente de regulamentações e normativas internacionais, como a UNECE R155 e a ISO/SAE 21434, e colabora com a NHTSA nos EUA em tópicos relacionados. Portanto, é provável que os OEMs já estejam em grande parte em conformidade com as diretrizes canadenses, caso sigam os requisitos internacionais.

As diretrizes do Canadá, apesar de não possuírem aplicabilidade regulatória imediata, estabelecem uma base legal potencial para futuras ações das autoridades contra OEMs em casos de falhas de cibersegurança. A ausência de obrigatoriedade regulamentar atual não impede que estas diretrizes sejam utiliza-

das como referencial em processos judiciais futuros.

5.3.4 CHINA

A China tem estabelecido diretrizes para regulamentar a Internet dos Veículos (IoV), com o objetivo de intensificar a padronização de dados e a segurança cibernética no setor.

Em 7 de março de 2022, o Ministério da Indústria e Tecnologia da Informação da China (MIIT) publicou as "Diretrizes para a Construção do Sistema Padrão de Segurança Cibernética e Segurança de Dados da Internet dos Veículos", delineando um roteiro para o desenvolvimento de padrões industriais de dados e segurança cibernética em diversas áreas.

As normas abrangem requisitos técnicos para segurança de hardware, incluindo equipamentos de bordo, terminais e equipamentos de infraestrutura rodoviária; software, como plataformas de serviço e aplicativos; e padrões para o tratamento de dados e outros requisitos de segurança cibernética. O Ministério definiu objetivos claros para a regulamentação do setor:

2023:

Em julho de 2023, o MIIT, em colaboração com a Administração Nacional de Padronização, emitiu as "Diretrizes para a Construção do Sistema Padrão da Indústria Nacional da Internet de Veículos" revisadas, visando fornecer à indústria um guia para a construção de sistemas com conteúdo mais abrangente e lógica mais clara.

Até 2025:

• Alcançar um sistema de padrões de segurança cibernética e segurança de dados para IoV relativamente completo

• Formular mais de 100 conjuntos de padrões.

• Melhorar a cobertura de padrões em subcampos.

• Melhorar a aplicação das normas.

• Apoiar o desenvolvimento seguro e saudável da indústria IoV.

5.3.5 BRASIL

A cibersegurança de sistemas automotivos com conexão à internet é regulamentada pela ANATEL através do Ato nº 77/2021, que estabelece os Requisitos de Segurança Cibernética para Equipamentos de Telecomunicações. Este documento fornece recomendações aos fabricantes e fornecedores, e institui um Programa de Supervisão de Mercado. O ato também define os critérios para certificação e homologação de equipamentos em relação aos requisitos de segurança.

Inicialmente, a conformidade com os requisitos do Ato nº 77/2021 não era obrigatória. A definição dos requisitos obrigatórios para os diversos tipos de equipamentos homologados pela ANATEL depende de propostas de regulamentação adicional, a serem elaboradas e submetidas ao Conselho Diretor da agência pelo recém-criado Grupo Técnico de Segurança Cibernética e Gestão de Riscos de Infraestrutura Crítica (GT-Ciber).

Devido à aplicação restrita a equipamentos com conexão à internet, no setor automotivo, a regulamentação afeta especificamente os veículos que integram algum tipo de conectividade. A declaração de conformidade é realizada pelo fornecedor do componente que se enquadra na descrição de aplicabilidade, no momento da homologação do equipamento para uso no país.

Recentemente, a ANATEL tornou obrigatória a aplicação dos requisitos do Ato nº 77/2021 para a homologação de equipamentos CPE (Consumer Premises Equipment) através do Ato nº 2436/2023. Esta medida indica uma tendência de expansão da obrigatoriedade para outros grupos de dispositivos no futuro.

6 UNECE WP29
– R155 & R156

UNECE WP.29

Com o aumento da complexidade de sistemas automotivos e da quantidade de concorrentes no mercado, é natural que ocorra uma descentralização na produção dos diversos componentes – físicos ou não – que compõe um veículo. Por outro lado, isso leva também ao surgimento de incompatibilidades entre subsistemas e arquiteturas, seja por diferenças culturais, legislações locais ou mesmo métodos de projeto de cada fabricante, montadora ou fornecedor. Consequentemente, emerge a necessidade de criação de padrões a fim de garantir compatibilidade entre diferentes montadoras, fabricantes e/ou fornecedores.

Nesse contexto, a Comissão Econômica das Nações Unidas para a Europa (UNECE - United Nations Economic Commission for Europe) criou o grupo de trabalho (Work Party) UNECE World Forum for Harmonization of Vehicle Regulations – também conhecida como WP.29. O forum mundial se reúne três vezes por ano para discutir e definir uma infraestrutura global comum de desenvolvimento de sistemas automotivos a partir de regulamentações relacionados à segurança e ao desenvolvimento sustentável. Mais de 120 representantes do setor automotivo participam ativamente das discussões no fórum e apontam grupos informais para atuar em problemas específicos que requerem solução urgente ou conhecimento específico.

Cibersegurança no contexto automotivo

A recente eletrificação e digitalização dos automóveis modernos é uma realidade que acelera a cada ano. A adição de módulos eletrônicos, funções de conectividade e assistências ao condutor, ao mesmo tempo em que aumentam a segurança funcional, aumentam também as superfícies de ataques cibernéticos. Além de poderem corromper funcionalidades do veículo, atacantes podem roubar diversos dados coletados pelo veículo para fins variados.

Diante desse cenário de aumento de riscos, fica evidente a necessidade do desenvolvimento de medidas de segurança cibernética que protejam tanto os componentes eletrônicos físicos quanto dados armazenados, redes e canais de comunicação, tais como Wifi, LTE, rádio, Bluetooth, barramentos CAN, Ethernet, etc.. Outro agravante para esse cenário é a evolução dos métodos de ataques, que evoluem junto com novas tecnologias. Por fim, o fato de veículos serem bens de consumo de vida longa (>= 10 anos) faz com que algumas medidas de segurança presentes no veículo se tornem obsoletas ao longo de sua vida útil, revelando novas vulnerabilidades que podem ser exploradas por atacantes.

Assim, faz-se necessária a existência de sistemas de gerenciamento de vulnerabilidades e atualizações de software que, no mínimo, sejam capazes de acompanhar o surgimento de novas vulnerabilidades e técnicas de ataque que se desenvolvem ao longo do tempo. Nesse contexto, a WP.29 criou duas regulamentações voltadas aos processos relacionados à cibersegurança automotiva e empresarial do setor: R155 e R156, visando impor requisitos mínimos para sistemas de gerenciamento de cibersegurança e de atualização de softwares automotivos, respectivamente. Tais regulamentações estão em vigor nos países da União Europeia, Reino Unido, Japão e Coreia do Sul para aprovação de novos modelos de veículos desde julho de 2022 e passaram a valer, a partir de julho de 2024, para todos os veículos em comercialização, incluindo modelos anteriores a essa data que seguem sendo produzidos e vendidos. Dessa forma, veículos anteriores a julho de 2024 podem e devem passar por atualizações visando a aprovação nas regulamentações R155 e R156 para serem comercializados.

Regulamentação R155

A regulamentação R155 é chamada originalmente de “Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system” ou Provisões uniformes acerca da aprovação de veículos com relação à cibersegurança e ao sistema de gerenciamento de cibersegurança, em tradução livre. Ela referencia a norma ISO/SAE 21434 (“Road vehicles – Cybersecurity Engineering”), que define requisitos de engenharia e uma metodologia de análise e avaliação de riscos de cibersegurança para a arquitetura E/E (elétrica e eletrônica) de automóveis rodoviários em relação à sua concepção, desenvolvimento, fabricação, operação, manutenção e descomissionamento, incluindo sistemas, componentes, interfaces e comunicações.

A R155 visa criar requisitos mínimos para a aprovação de veículos (type approval) no que diz respeito ao sistema de gerenciamento da cibersegurança (CSMS – Cyber Security Management System) sem impor métodos ou requisitos de implementação técnica dos sistemas. O CSMS é um sistema de gerenciamento voltado para a indústria automotiva e deve definir responsáveis pela cibersegurança tanto de governança quanto de seus produtos, bem como mapear e monitorar vulnerabilidades e riscos, mitigando-os quando for possível ou justificando aqueles que se decidir assumir. Deve ainda ser auditável e ter seus processos bem documentados a fim de obter a aprovação segundo a regulamentação R155. A existência de tal sistema é obrigatória e regulamentada em território europeu e em outros países que optarem por adotar a R155 como norma.

Para obter a aprovação para um veículo, a montadora deve comprovar à autoridade responsável que o CSMS implementado inclui todo o ciclo de vida do produto, desde sua concepção até seu descomissionamento. O CSMS deve definir processos diversos no contexto da cibersegurança, incluindo processos de governança internos da montadora, métodos de testes realizados no projeto do veículo, procedimentos de identificação de ataques e aquisição de dados, gerenciamento de riscos identificados, respostas a tentativas de ataque com ou sem sucesso, dentre outros. Em seu anexo 5, a R155 apresenta diversos exemplos de referência para vulnerabilidades e ataques para diferentes cenários de dano, além de métodos de mitigação dos riscos para tais ataques e vulnerabilidades. A regulamentação também define requisitos que a autoridade aprovadora deve cumprir ao longo do processo de avaliação do CSMS.

Em caso de não conformidade com as definições da regulamentação, a R155 determina que a aprovação do veículo quanto ao sistema de gerenciamento de cibersegurança pode ser negada ou revogada. A aprovação pode ser revogada também em reavaliações, que podem ocorrer de forma espontânea, de acordo com a autoridade aprovadora, ou com uma frequência esperada de 3 anos.

Regulamentação R156

A regulamentação R156 dispõe sobre o sistema de gerenciamento de atualizações de software (SUMS – Software Update Management System). A fim de obter a aprovação de um SUMS, uma montadora deve manter e apresentar documentações diversas acerca do sistema e métodos de atualização de software, indicando, por exemplo, o nível de segurança contra ataques cibernéticos dos canais pelos quais o software é enviado aos veículos – seja ele over-the-air¬¬ ou não. Um SUMS deve definir de maneira sistemática processos e procedimentos para a entrega de atualizações de software para veículos. Note que não há exigência explícita para existência de conectividade nos veículos a serem aprovados segundo a R156. Assim, pode-se obter a aprovação mesmo que não se use atualizações over-the-air, contanto que os requisitos da regulamentação sejam cumpridos. Isso é importante para garantir que veículos projetados antes da vigência da R156 sejam elegíveis para aprovação, sem a necessidade de grandes mudanças em sua arquitetura.

A R156 define diversos processos que devem estar devidamente documentados e implementados no contexto da montadora que busca aprovação para seu SUMS. Processos como documentação e armazenamento de informações relevantes à regulamentação, versionamento e históricos de versões anteriores de softwares, verificação de impacto de uma atualização em outros sistemas do veículo aprovados segundo outras regulamentações, dentre outros. Esses processos devem estar de acordo com as determinações da regulamentação R156 para que o SUMS seja aprovado. A implementação e aspectos técnicos do SUMS são de responsabilidade da montadora que busca aprovação e não são especificados pela regulamentação.

São definidos também requisitos relacionados especificamente a SUMS que possuam funcionalidade de atualização over-the-air (OTA). Nesse caso, são impostos requisitos como a capacidade do veículo de retornar à versão anterior e/ou a um estado seguro de funcionamento após uma tentativa falha de atualização.

Apenas obter a primeira aprovação segundo os requisitos da R156 ainda não é suficiente para a manutenção da aprovação do sistema como um todo. A regulamentação define ainda que novas avaliações podem ser feitas de forma periódica a cada 3 anos, com a possibilidade de se refazer uma avaliação de forma espontânea pela autoridade aprovadora – da mesma maneira como é definido para a regulamentação R155.

Implicações no setor automotivo europeu e brasileiro

As regulamentações R155 e R156 da UNECE buscam uniformizar os requisitos mínimos necessários para que tanto o CSMS quanto o SUMS de um tipo

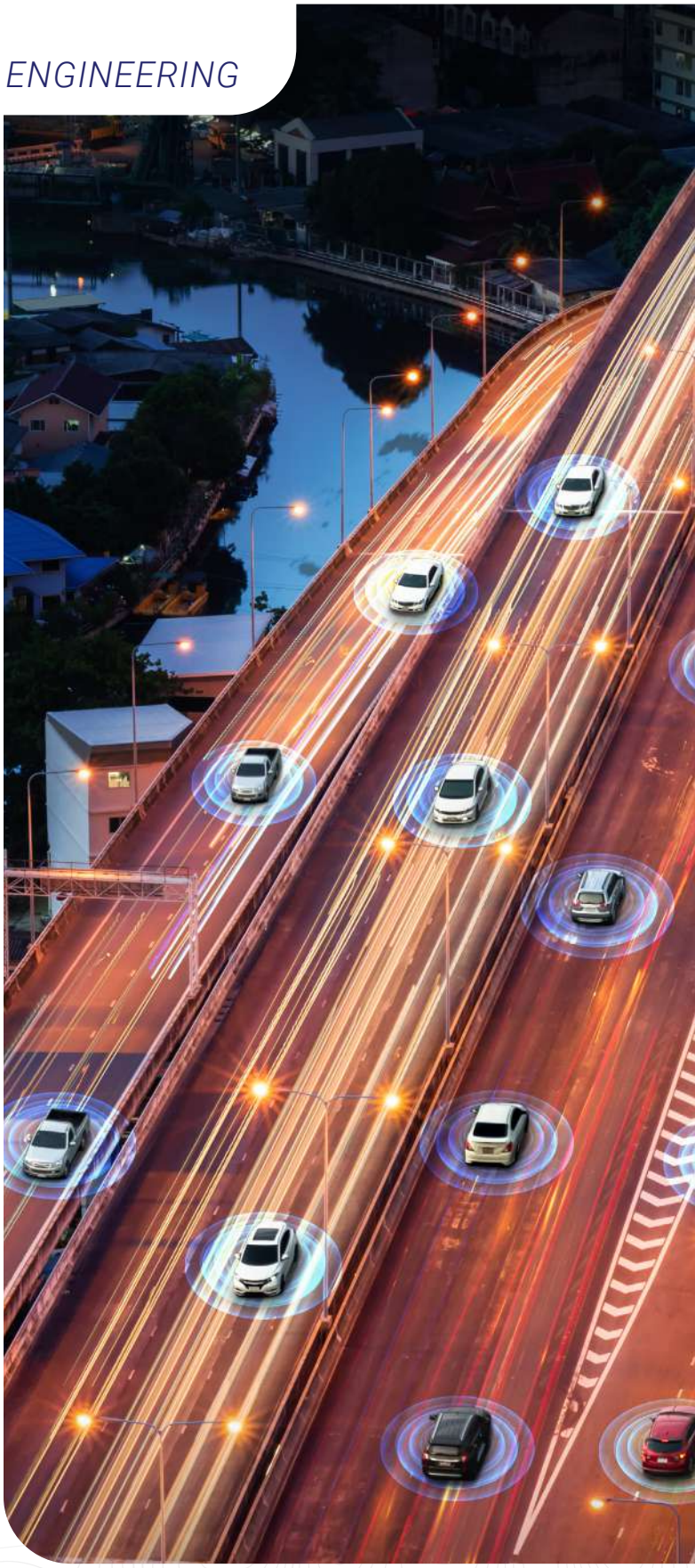
ou modelo de veículo sejam aprovados e certificados, criando um padrão de qualidade que deve ser alcançado pelas montadoras e fornecedores. Dessa maneira, busca-se garantir que todo veículo tenha um nível mínimo de segurança cibernética em seus componentes, desestimulando a ação de atacantes mal-intencionados e evitando que o mau uso pelo condutor ou passageiro possa causar vazamento de dados, perda de funcionalidade do veículo, ou outros cenários de dano.

No mercado brasileiro, há ainda outros desafios que devem ser considerados antes da adoção direta das regulamentações R155 e R156. A extensão geográfica, por exemplo, dificulta a implementação ampla de um CSMS e um SUMS. Há áreas com pouca ou nenhuma cobertura de acesso à internet, o que dificultaria o uso de funções de conectividade e/ou o monitoramento de eventos de cibersegurança – ainda que a própria posição geográfica possa ser um fator de redução do nível de risco. Em casos de SUMS que não dependem de conectividade, seria necessário o envolvimento ativo dos proprietários para que as atualizações fossem instaladas com sucesso.

Ainda assim, é essencial que discussões sobre cibersegurança no setor automotivo se tornem mais frequentes e abrangentes, pois o aumento da complexidade e do uso de funções de conectividade já é uma realidade. Enquanto isso, a cibersegurança automotiva ainda está em fase embrionária, com pouca regulamentação em vigor. Há uma janela de oportunidade para observar os casos europeu, sul coreano e britânico, para aprender com as dificuldades por eles enfrentadas e adaptar regulamentações para o mercado nacional.

7 ISO21434

– *ROAD VEHICLES CIBERSECURITY ENGINEERING*



7.1 – INTRODUÇÃO

A Organização Internacional de Padronização (ISO) é uma federação composta por entidades nacionais de padronização. O trabalho da ISO é feito através de comissões técnicas formadas por organizações internacionais, governamentais e não governamentais. A ISO trabalha de forma muito próxima à Comissão Eletrotécnica Internacional (IEC) em assuntos sobre padronizações eletrotécnicas.

A Sociedade Internacional de Engenheiros Automotivos (SAE), com mais de 128 mil engenheiros associados das áreas automotiva, aeroespacial e de veículos comerciais, produz normas utilizadas para o avanço da engenharia de mobilidade no mundo. O desenvolvimento dessas normas conta com mais de 9 mil voluntários no mundo inteiro, cujo processo de desenvolvimento tem a premissa de ser aberto, transparente e colaborativo.

Como referência a norma ISO 26262-3:2018 – "Veículos automotores, parte 3: fase de conceito" – foi utilizada neste documento.

Esta norma tem o objetivo de fornecer diretrizes para fundamentar um conhecimento comum na organização, e em toda a cadeia de suprimentos, a respeito de segurança cibernética através de:

• Definição de políticas e processos de segurança cibernética;

• Gerenciamento de riscos em segurança cibernética;

• Promoção de cultura dotada de segurança cibernética.

Tais diretrizes são aplicáveis nas seguintes fases do produto: conceito, desenvolvimento, operação, manutenção e descomissionamento de componentes e sistemas eletroeletrônicos de veículos automotores, tal qual peças de reposição no pós-venda. Sistemas externos ao veículo, apesar de relevantes, não devem ser considerados como escopo.

As atividades descritas não necessariamente devem ser utilizadas de forma integral em todas as organizações e/ou todos os itens eletrônicos de um veículo. É preciso aplicá-las quando pertinentes, e moldá-las de acordo com o projeto em execução.

Visão geral do conteúdo da norma, dividida por cláusulas:

Cada cláusula é composta por:

- Requerimentos: premissas para desenvolver a atividade em questão;
- Recomendações: de modo a suplementar as premissas;
- Produto de trabalho: entregáveis da cláusula.

7.2 – GERENCIAMENTO DA SEGURANÇA CIBERNÉTICA ORGANIZACIONAL

Para tornar possível a engenharia de segurança cibernética na organização, é necessário uma governança em segurança cibernética apoiada pelo comprometimento da alta gerência, governança esta constituída de disciplinas análogas aos departamentos de desenvolvimento, como: gerenciamento de competências, processos de segurança cibernética passíveis de auditoria, nomeação de autoridades e responsáveis pelas atividades pertinentes, alocação de recursos necessários para executar os processos, gerenciamento de riscos, a manutenção e fomento de uma cultura voltada para segurança cibernética.

São exemplos de uma cultura organizacional rica em segurança cibernética:

• Rastreabilidade das decisões tomadas acerca de segurança cibernética;

• Segurança cibernética deve ter prioridade às questões de custo, performance ou cronograma;

• O pessoal de segurança cibernética leva em consideração as particularidades de cada área no momento de implementar suas disciplinas;

• Análises de segurança cibernética ocorrem de forma independente e sem influência das áreas funcionais;

• Problemas de segurança cibernética são tratados imediatamente ao invés de métodos dependentes de testes no fim do desenvolvimento da solução;

• Estar preparado para possíveis vulnerabilidades, no lugar de reagir somente após algum dano já instaurado;

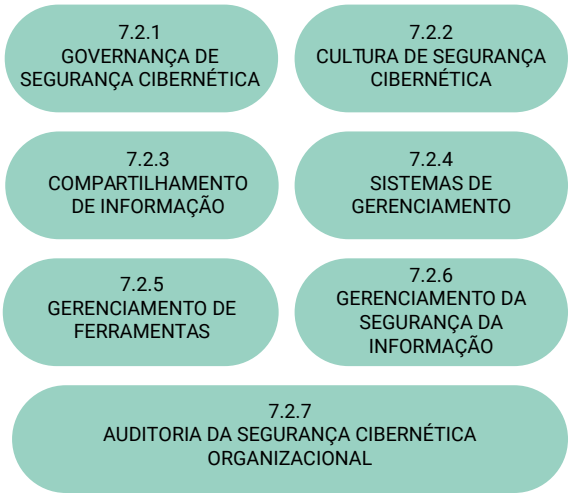
• Recursos competentes devidamente alocados para tarefas de segurança cibernética.

Os processos referentes a segurança cibernética devem abranger o produto em todas as suas fases: conceito, desenvolvimento, operação, manutenção, monitoramento de ameaças à segurança cibernética, resposta à incidentes, melhoria contínua e finalmente o descomissionamento.

A documentação resultante desses processos deve ser armazenada para permitir consultas futuras em uma eventual resposta às vulnerabilidades, como lista de materiais, configuração de software, histórico de alterações do documento (gerenciamento de mudanças). Este suporte deve perdurar durante toda a vida do produto.

Uma tarefa habilitadora de uma cultura de segurança cibernética é a troca de informações entre áreas, e para tal é preciso identificar quais áreas devem estabelecer essa interface e o processo pelo qual se dará essa troca, como por exemplo, o processo de aprovação para compartilhamento de informações e a atribuição de níveis de sensibilidade dos diferentes tipos de informação.

Relação dos entregáveis, ou “produtos de trabalho”:



7.3 – GERENCIAMENTO DE SEGURANÇA CIBERNÉTICA ORIENTADO A PROJETOS

Esta cláusula visa a designação de responsabilidades e o planejamento das atividades de segurança cibernética em um projeto, de forma genérica a ser aplicada a diversos tipos de aplicação, podendo ser pontualmente personalizada para melhor se adaptar ao meio em questão. Exemplos de situações em que a personalização pode ocorrer, fundamentada sempre em um racional documentado:

• Reuso: componentes podem ser reutilizados, mas estarão sujeitos à análise se alguma alteração no componente estiver programada, se o ambiente no qual estiver inserido for diferente do originalmente considerado em seu projeto, ou se novas informações a respeito do componente tenham sido levantadas, mesmo que o componente em si não tenha sido modificado. Além disso, formas de ataques podem ter sido aprimoradas, fazendo-se necessária a análise do componente, mesmo que este ou o respectivo ambiente não tenham mudado.

• Desenvolvimento “fora de contexto”: uma organiza-

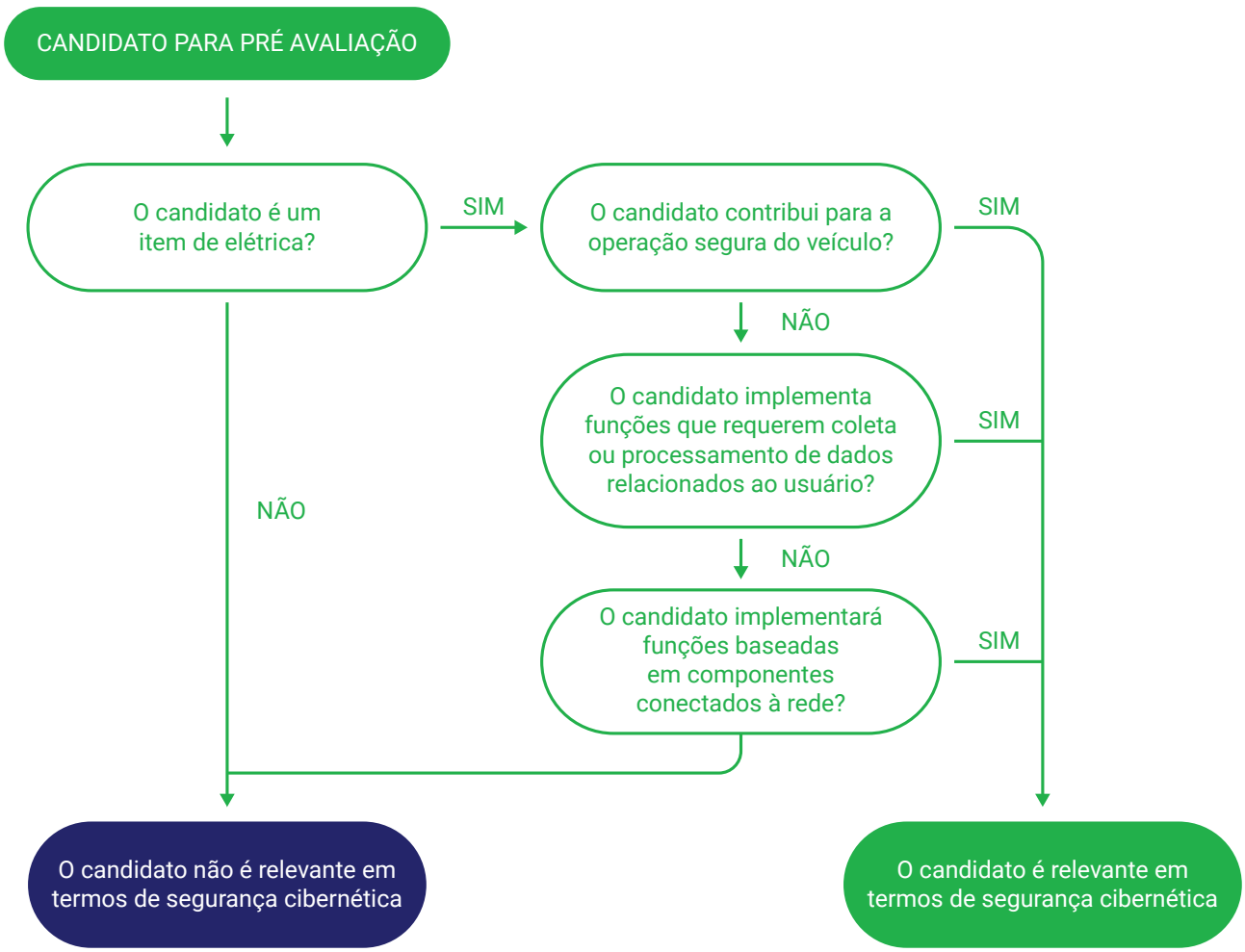
ção pode desenvolver um componente estipulando premissas, antes mesmo de negociá-lo com clientes, de forma a torná-lo versátil o suficiente para diversos ambientes, como por exemplo, um microcontrolador. Este tipo de componente pode ser desenvolvido de acordo com este documento.

• Componentes “de prateleira”: são componentes desenvolvidos independentemente de um determinado cliente, e podem ser utilizados sem alterar seu projeto, como por exemplo, um software comercial. Não é esperado que estes componentes sejam desenvolvidos baseados neste documento.

Em todos os casos é preciso analisar se o componente atende os requerimentos de segurança cibernética e se a documentação é suficiente para suprir as atividades relacionadas do projeto.

Para utilizar tais componentes, é preciso elencar as atividades de integração, e se necessário, atividades de alteração. Um dos entregáveis desta cláusula é decidir se o componente em questão estará sujeito a desenvolvimentos futuros ou não.

Para elaborar o plano de atividades de segurança cibernética, alocar recursos, identificar dependências entre atividades de outras áreas, definir datas e entregáveis, o primeiro passo é determinar se o componente é pertinente. Para isso, seguir o fluxograma:



Tão importante quanto a execução das atividades outrora mapeadas, é a avaliação dessas atividades. A avaliação deve ser feita por pessoal com acesso às informações relevantes e capaz de realizar uma avaliação de segurança cibernética independente. A necessidade ou não necessidade de realizar uma avaliação decorre da análise da complexidade do componente e sua importância identificada na análise de risco de segurança cibernética do projeto. Ao final desta avaliação, é dado um parecer de aceitação, aceitação parcial ou rejeição do componente.

Relação dos entregáveis, ou "produtos de trabalho":

7.3.1 RESPONSABILIDADES DE SEGURANÇA CIBERNÉTICA

7.3.2 PLANEJAMENTO DE SEGURANÇA CIBERNÉTICA

7.3.3 CUSTOMIZAÇÃO

7.3.4 REUSO

7.3.5 COMPONENTES FORA DE CONTEXTO

7.3.6 COMPONENTES DE PRATELEIRA

7.3.7 O CASO PARA SEGURANÇA CIBERNÉTICA

7.3.8 AVALIAÇÃO DE SEGURANÇA CIBERNÉTICA

7.3.9 LIBERAÇÃO PARA O PÓS DESENVOLVIMENTO

7.4 – ATIVIDADES DE SEGURANÇA CIBERNÉTICA DISTRIBUÍDAS

Uma vez que as atividades de segurança cibernética foram designadas às respectivas partes envolvidas, é necessário o gerenciamento da interação entre essas partes, sejam elas fornecedores internos ou externos à organização.

Uma mesma organização pode ser fornecedora de uma montadora e ao mesmo tempo, cliente de seus fornecedores.

Como premissa, é necessário que o fornecedor comprove sua capacidade em atender as demandas de segurança cibernética no desenvolvimento e pós desenvolvimento (se aplicável), seja através de documentos de sua política interna de segurança cibernética, seja através de exemplos do passado quanto à postura da organização frente a um incidente de segurança cibernética.

Uma vez elencado o fornecedor candidato em uma cotação, as responsabilidades entre cliente e fornecedor devem ser designadas, tais como: nome da pessoa responsável pelas atividades de segurança cibernética em cada uma das partes, atividades a serem executadas por cada uma das partes ou por ambas simultaneamente, os requerimentos que tornam a tarefa concluída, como proceder frente a uma vulnerabilidade encontrada.

Ao final desta cláusula, uma matriz de responsabilidades será produzida, será o entregável desta etapa.

7.4.1 CAPABILIDADE DO FORNECEDOR

7.4.2 REQUISIÇÃO PARA COTAÇÃO

7.4.3 ALINHAMENTO DAS RESPONSABILIDADES

7.5 – ATIVIDADES CONTÍNUAS DE SEGURANÇA CIBERNÉTICA

Atividades de segurança cibernética contínuas são aquelas que podem extrapolar um determinado projeto. Nesta cláusula é descrito o tratamento adequado de tais atividades, através de quatro frentes: monitoramento, avaliação de eventos de segurança cibernética, análise de vulnerabilidades e o gerenciamento destas vulnerabilidades.

Monitoramento de segurança cibernética: coleta e análise de informações de segurança cibernética a respeito de gatilhos (palavras-chave, nome de componentes, nomes de fornecedores), pré-definidos. Eventos passados, fontes externas comerciais e não-comerciais, cenários de potencial ameaça.

Avaliação de eventos de segurança cibernética: uma vez definidos os gatilhos e feita a respectiva análise, pontos fracos podem ser identificados e registrados.

Análise de vulnerabilidades: os pontos fracos outrora levantados podem configurar um cenário de vulnerabilidade. Caso um determinado ponto fraco não fique exposto em cenário algum, ou se sua exposição ocorra a uma taxa desprezível, este não se torna uma vulnerabilidade. O racional adotado para classificar um ponto fraco como fonte de vulnerabilidade ou como não sendo uma fonte de vulnerabilidade deve ser registrado.

Gerenciamento de vulnerabilidades: as vulnerabi-

lidades identificadas podem ser tratadas para que seus riscos sejam mitigados ou eliminados. Caso seja necessária a alteração de algum componente, esta será uma atividade parte do gerenciamento de mudanças. A evidência de que a vulnerabilidade foi tratada deve ser documentada.

7.5.1 MONITORAMENTO DE SEGURANÇA CIBERNÉTICA

7.5.2 AVALIAÇÃO DE EVENTOS DE SEGURANÇA CIBERNÉTICA

7.5.3 ANÁLISE DE VULNERABILIDADE

7.5.4 GERENCIAMENTO DE VULNERABILIDADES

7.6 – CONCEITO

Esta cláusula considera como objeto de análise as funcionalidades a nível de veículo inserido no ambiente de operação, o qual chamaremos de "item". Não se trata de uma disciplina com o foco no nível de componente, de forma descontextualizada. É preciso identificar quais as fronteiras do item, ou seja, o que o distingue de seu ambiente de operação, onde está sua interface com demais itens internos e externos. Da mesma forma, é preciso identificar o ambiente de operação pertinente à segurança cibernética e suas interações com o item, pois ao conhecer os elos de comunicação será possível identificar caminhos para sofrer ataques, bem como cenários de ameaça.

A partir dos itens identificados, os objetivos de segurança cibernética, ou "requerimentos para proteger ativos em cenários de ameaça", serão estipulados com base nas disciplinas de análise de risco que veremos a seguir neste documento. O tratamento ao risco pode ser evitar o risco ao remover determinado item, pode ser de mitigação, compartilhamento do risco, ou conceder o risco a cenários limitados.

Uma vez que os itens estejam identificados, os objetivos traçados, o meio pelo qual serão atingidos é formatado pelo conceito de segurança cibernética. Os controles a serem adotados devem levar em consideração a dependência entre funções do item para, por exemplo, limitar a comunicação de uma determinada funcionalidade a um canal seguro ou em função do consentimento do usuário. A descrição dos controles de segurança cibernética somados aos requerimentos de segurança cibernética constituem juntos o conceito de segurança cibernética.

7.6.1 DEFINIÇÃO DO ITEM

7.6.2 OBJETIVOS DE SEGURANÇA CIBERNÉTICA

7.6.3 CONCEITO DE SEGURANÇA CIBERNÉTICA

7.7 – DESENVOLVIMENTO DO PRODUTO

O foco desta cláusula é a especificação dos requerimentos de segurança cibernética e atividades de integração e verificação durante o desenvolvimento, passando por iterações até que os requerimentos sejam atendidos.

A premissa para esta cláusula é ter em mãos as especificações de segurança cibernética do ponto de vista de arquitetura de design macro do projeto, bem como os produtos da cláusula anterior.

Deve-se levar em consideração para a criação de especificações de segurança cibernética: interações entre subcomponentes, cenário pós desenvolvimento (remoção de dados pessoais, por exemplo), capabilidades dos componentes, ou seja, quais seus limites de performance, além da adoção de princípios já estabelecidos para evitar a criação de pontos fracos no projeto. Pontos fracos e vulnerabilidades de componentes conhecidos devem ser avaliados. As especificações deverão sofrer verificação para atestar que estão completas e corretas, e de acordo com as especificações macro antes definidas.

7.7.1 PROJETO

7.7.2 INTEGRAÇÃO E VERIFICAÇÃO

7.8 – VALIDAÇÃO DE SEGURANÇA CIBERNÉTICA

Esta cláusula descreve atividades para validação de segurança cibernética no nível de veículo completo em seu ambiente operacional e sujeito a seus respectivos riscos, configurado da mesma forma que será

quando estiver em produção seriada, de tal forma a confirmar a pertinência dos objetivos de segurança cibernética traçados anteriormente.

Uma vez criadas as especificações, a etapa de verificação e integração se inicia, a fim de garantir que as especificações sejam respeitadas, bem como o conceito de segurança cibernética, através de testes de fluxo de informações de controle e de dados, análises dinâmicas e estática até a aplicação de casos conhecidos, até que os pontos fracos estejam suficientemente mitigados.

O racional que suporte a escolha das atividades de validação deve ser documentado.

7.8.1 VALIDAÇÃO DE SEGURANÇA CIBERNÉTICA

7.9 – PRODUÇÃO

Esta cláusula se aplica ao processo de manufatura dos componentes até o nível do veículo completo, de sorte que produza um plano de controle, a fim de garantir a não inserção de novas vulnerabilidades ao produto se não aquelas previstas em projeto. O plano de controle deve conter:

• Sequência das etapas que aplicam os requerimentos de segurança cibernética para o ambiente pós desenvolvimento;

• Lista de equipamentos e ferramentas necessárias;

• Controles de prevenção a acessos não autorizados durante o processo produtivo;

• Métodos de verificação dos requerimentos, se foram de fato obedecidos.

7.9.1 PRODUÇÃO

7.10 – OPERAÇÕES E MANUTENÇÃO

Esta cláusula descreve a postura frente a incidentes de segurança cibernética e a eventuais atualizações.

Vulnerabilidade é a condição que, a partir de um ponto fraco identificado, oferece riscos significativos ao produto, e deve ser tratada de tal maneira a mitigar o risco ou eliminá-lo ao remover o recurso que carrega aquele ponto fraco.

Atualizações podem ocorrer por diversos motivos, sempre no pós desenvolvimento, pois durante o desenvolvimento as atualizações são designadas no gerenciamento de mudanças. Dentre as razões para uma atualização, estão: correção de vulnerabilidades, fornecimento de novos recursos ou melhoria de recursos existentes.

Para cada incidente de segurança cibernética, um plano de resposta deve ser criado contendo o seguinte:

• Ações corretivas;

• Plano de comunicação;

• Designação de responsabilidades para cada ação corretiva;

• Procedimento para documentar as informações pertinentes ao incidente;

• Um método para mensurar o progresso no plano;

• Critério para conclusão do incidente;

• Ações necessárias para a conclusão.

7.10.1 RESPOSTA À INCIDENTES DE SEGURANÇA CIBERNÉTICA

7.10.2 ATUALIZAÇÕES

7.11 – FIM DO SUPORTE À SEGURANÇA CIBERNÉTICA E DESCOMISSIONAMENTO

Os eventos de fim do suporte à segurança cibernética e descomissionamento devem ser tratados separadamente, pois um componente pode continuar em operação quando o suporte à segurança cibernética termina, o que não ocorre após seu descomissionamento, que pode ser executado sem o conhecimento da organização.

Do ponto de vista de fim de suporte à segurança cibernética, é preciso possuir procedimento de comunicação para informar os clientes deste evento, seja via contrato, seja via anúncios em mídias.

As instruções para descomissionamento devem ser disponibilizadas via documentação acerca do período de pós desenvolvimento, via manual do proprietário, por exemplo.

7.11.1 FIM DO SUPORTE À SEGURANÇA CIBERNÉTICA

7.11.2 DESCOMISSIONAMENTO

7.12 – MÉTODOS DE ANÁLISES DE AMEAÇAS E RISCOS

Esta cláusula descreve métodos para determinar a que ponto um usuário de veículo automotor estará exposto a ameaças. Estes métodos e seus respectivos entregáveis, ou "produtos de trabalho", são conhecidos como "análise de ameaças e riscos", ou TARA – threat analysis and risk assessment, e são executados da perspectiva do usuário. Os métodos desta cláusula podem ser evocados a qualquer momento durante a vida do componente.

Os objetivos desta cláusula estão divididos em 7 tópicos, os quais veremos em detalhes a seguir. A finalidade é a identificação dos ativos, suas propriedades de segurança cibernética, os possíveis cenários de danos causados, qual a intensidade dos danos, e quais caminhos existem para uma ameaça se efetivar.

Cada tópico possui entregáveis que será usado com entrada no tópico subsequente.

7.12.1 – Identificação do ativo

Com a definição do componente em mãos, junto com suas especificações de segurança cibernética, cenários de danos devem ser identificados.

Os ativos (objetos/informações que possuam valor ao usuário) cujos ataques às suas propriedades de segurança cibernética podem culminar em um cenário de danos, devem ser identificados.

O cenário de dano leva em consideração a relação do componente com a consequência adversa, descrição do dano ao usuário, e ao ativo.

Exemplo de cenário de dano: o ativo em questão são as preferências pessoais do usuário armazenadas em um sistema de "infotainment", cuja confidencialidade é uma propriedade de segurança cibernética. O cenário de dano se configura quando essas informações são liberadas para uso sem o consentimento do usuário.

7.12.2 – Identificação do cenário de ameaça

As entradas necessárias são: definição do componente, junto com suas especificações de segurança cibernética, cenários de dano, e lista de ativos com propriedades de segurança cibernética.

Os cenários devem possuir o respectivo ativo sob ameaça, quais propriedades do ativo seriam comprometidas e qual a causa deste comprometimento. Caso haja relações com outros ativos, estas devem ser discriminadas.

A identificação dos cenários de ameaça pode ser obtida através de discussões em grupos, supondo danos como: falsificação de informação, liberação de informação confidencial, negação a serviços, elevação indevida de privilégios.

7.12.3 – Classificação do impacto

As entradas necessárias são: definição do componente, cenários de danos e lista de ativos com propriedades de segurança cibernética.

Os cenários de danos devem ser avaliados acerca das consequências ao usuário nas categorias: segurança, impacto financeiro, operacional e privacidade. Categorias adicionais podem ser incluídas, dotadas do racional que as justificam, com a devida comunicação para as partes envolvidas. (Este documento não cria um método de comparação entre categorias diferentes.)

O cenário de dano deve ser avaliado em cada categoria como:

• Severo; • Importante; • Moderado; ou • Desprezível.

EXEMPLO DE CRITÉRIO PARA A CLASSIFICAÇÃO DO IMPACTO À SEGURANÇA

Classificação do impacto	Critério para a classificação do impacto
Severo	S3: ferimentos que colocam a vida em risco, (sobrevivência incerta), ferimentos fatais
Importante	S2: ferimentos que colocam a vida em risco, (sobrevivência provável)
Moderado	S1: Ferimentos leves e moderados
Desprezível	S0: sem ferimentos

Notas:

Classificação S0 pode se basear na ISO 26262-3: 2018, tabela B1

Critérios tirados da ISO 26262-3:2018

Nível de controle e exposição ao risco de acordo com a ISO 26262-3:2018 pode ser considerado para o impacto à segurança, se o racional for fornecido.

EXEMPLO DE CRITÉRIO PARA A CLASSIFICAÇÃO DO IMPACTO FINANCEIRO	
Classificação do impacto	Critério para a classificação do impacto
Severo	Os danos financeiros levam à consequências catastróficas, as quais o usuário pode não superar
Importante	Os danos financeiros levam à consequências substanciais, as quais o usuário pode superar
Moderado	Os danos financeiros levam à consequências inconvenientes, as quais o usuário pode superar com recursos limitados
Desprezível	Os danos financeiros levam à nenhum efeito, consequências desprezíveis ou irrelevantes ao usuário.

EXEMPLO DE CRITÉRIO PARA A CLASSIFICAÇÃO DO IMPACTO OPERACIONAL	
Classificação do impacto	Critério para a classificação do impacto
Severo	O dano operacional leva à perda de uma função principal do veículo Exemplo 1: Veículo não funciona ou demonstra comportamento imprevisível de funções principais, como o ativamento do modo de segurança ou o deslocamento de um carro autônomo para uma localidade não requerida.
Importante	O dano operacional leva à perda de uma função importante do veículo Exemplo 2: Algo que incomode o motorista de forma relevante
Moderado	O dano operacional leva à degradação parcial de uma função do veículo Exemplo 3: Satisfação do usuário é negativamente afetada.
Desprezível	O dano operacional não leva à perda de uma função do veículo

Notas:

Este critério pode ter ou pode não ter consequências na segurança.

EXEMPLO DE CRITÉRIO PARA A CLASSIFICAÇÃO DO IMPACTO À PRIVACIDADE	
Classificação do impacto	Critério para a classificação do impacto
Severo	O dano à privacidade leva à impactos significativos ou até irreversíveis ao usuário A informação do usuário é altamente sensível e permite a fácil identificação da pessoa sobre a qual a informação se refere.
Importante	O dano à privacidade leva a sérios impactos ao usuário. A informação sobre o usuário pode ser: a) altamente sensível e de difícil identificação da pessoa sobre a qual a informação se refere b) não sensível, mas de fácil identificação da pessoa sobre a qual a informação se refere.
Moderado	O dano à privacidade leva a impactos inconvenientes ao usuário. A informação sobre o usuário pode ser: a) sensível e de difícil identificação da pessoa sobre a qual a informação se refere b) não sensível, mas de fácil identificação da pessoa sobre a qual a informação se refere.
Desprezível	O dano à privacidade leva dano nenhum ao usuário. A informação do usuário não é sensível e é de difícil identificação da pessoa sobre a qual a informação se refere.

Notas:

O conceito de "pessoa sobre a qual a informação se refere" (em inglês, "PII principal") pode ser definido de acordo com a ISO/IEC 29100.

7.12.4 – Análise do caminho para sofrer ataques

As entradas necessárias são: definição do componente, lista de ativos com propriedades de segurança cibernética e cenários de ameaça identificados.

Entradas adicionais podem ser utilizadas, tais como: pontos fracos em eventos de segurança cibernética, pontos fracos identificados durante o desenvolvimento do produto, a arquitetura do projeto, caminhos para ataques previamente conhecidos, análise de vulnerabilidade.

Para identificar os caminhos para sofrer ataques, os cenários de ameaça são analisados. A análise pode ser via abordagem "de cima para baixo", ou seja, a partir do efeito causado até os possíveis caminhos para este efeito; ou "de baixo para cima", ou seja, a partir das vulnerabilidades identificadas.

Os caminhos para sofrer ataques devem ser associados com os cenários de ameaça que podem se consolidar a partir destes caminhos. Adicionalmente, a clareza e a quantidade de detalhes de um determinado caminho para sofrer ataques cresce em paralelo com o desenvolvimento do produto, conforme especificações são enriquecidas e amadurecidas.

Exemplo:

Cenário de ameaça: falsificação de mensagens CAN para a central eletrônica do sistema de freios, resultando em perda de integridade das mensagens CAN e, consequentemente, da função de frenagem.

Caminhos para sofrer ataques:

- A central eletrônica de telemetria é comprometida por interface de celular;
- A central eletrônica coordenadora é comprometida via comunicação CAN pela central eletrônica de telemetria;
- A central eletrônica coordenadora envia sinais de comando de frenagem maliciosos.

7.12.5 – Classificação da viabilidade do ataque

As entradas necessárias são: caminhos para sofrer ataques e análise de vulnerabilidade.

Cada caminho para sofrer ataques deverá ser classificado como um dos quatro níveis abaixo:

É possível executar a classificação através de três abordagens:

CLASSIFICAÇÕES PARA A VIABILIDADE DE ATAQUES E SUAS DESCRIÇÕES

Classificação da viabilidade do ataque	Descrição
Alta	O ataque pode ter êxito com pouco esforço
Média	O ataque pode ter êxito com esforço médio
Baixo	O ataque pode ter êxito com muito esforço
Muito Baixo	O ataque pode ter êxito com muitíssimo esforço

Abordagem baseada no potencial do ataque, que considera os seguintes fatores: tempo estimado para identificar uma vulnerabilidade e desenvolver com sucesso um ataque; habilidade do especialista, seu conhecimento acerca do componente sob ataque, janela de oportunidade e seu equipamento.

Abordagem baseada no sistema comum de classificação de vulnerabilidade (CVSS – “common vulnerability scoring system”), que contempla as métricas de explorabilidade, tais como: vetor de ataque (meio pelo qual o ataque é realizado), complexidade do ataque, privilégios necessários, interação do usuário.

Abordagem baseada no vetor de ataque, que prioriza o vetor de ataque predominante na classificação da viabilidade do ataque.

7.12.5 CLASSIFICAÇÃO DA VIABILIDADE DO ATAQUE

7.12.6 – Determinação do valor do risco

As entradas necessárias são: cenários de ameaça, classificação do impacto, classificação da viabilidade do ataque.

Cada cenário de ameaça terá seu valor de risco. Se um cenário de ameaça pode desencadear mais de um cenário de dano, haverá um valor de risco para cada caso. O mesmo é válido para diversos caminhos para sofrer ataques de um dado cenário de ameaça.

O valor do risco será de 1 a 5, onde 1 significa “risco mínimo”. Exemplo: matriz de risco.

7.12.6 DETERMINAÇÃO DO VALOR DO RISCO

7.12.7 – Decisão para tratamento do risco

As entradas necessárias são: definição do item, cenários de ameaça, valores de risco, especificações de segurança cibernética, decisões passadas acerca do mesmo item ou de itens similares, classificação do impacto, caminhos para sofrer ataques, classificação da viabilidade do ataque.

Para cada cenário de ameaça, uma ou mais formas de tratamento a seguir podem ser adotadas:

a - Evitar o risco;

b - Mitigar o risco;

c - Compartilhar o risco;

d - Reter o risco;

Os itens ‘c’ e ‘d’ devem ser fundamentados em um racional, sendo documentados e sujeitos ao gerenciamento contínuo de vulnerabilidades.

7.12.7 DECISÃO PARA TRATAMENTO DO RISCO

8 CIBERSEGURANÇA DURANTE A OPERAÇÃO DO VEÍCULO

Um conceito chave dentro do contexto da cibersegurança é a capacidade de se detectar vulnerabilidades continuamente e de forma rápida e responder de forma adequada a incidentes, resolvendo de forma dinâmica questões que apareçam em sistemas que já se encontram em operação. Sistemas eletrônicos desenvolvidos de forma adequada têm boas chances de serem produzidos e comissionados com um nível de cibersegurança adequado. Entretanto, ao longo do tempo, vulnerabilidades então desconhecidas podem ser encontradas, técnicas de ataque desenvolvidas ou até mesmo o vazamento de dados sobre tais sistemas podem resultar em um decréscimo no nível de cibersegurança, facilitando a elaboração e execução de ciberataques.

A adição de novas funcionalidades aos automóveis (e demais elementos da mobilidade) os aproxima do cenário descrito no parágrafo anterior. Sistemas de automação e auxílio à condução (ADAS) demandam novos protocolos (PCIe, Ethernet) e unidades de processamento (SoCs). A conectividade pressupõe acesso seguro à Internet, o que possibilita a adição de aplicativos ao veículo e atualizações de software pós SOP requerendo a adoção de criptografia, autenticação e assinatura de software. Naturalmente, novos elementos necessitam ser adicionados à arquitetura eletroeletrônica dos veículos de forma complementar às ECUs embarcadas, trazendo características similares a sistemas computacionais convencionais.

Sistemas com a capacidade de se conectar à Internet, receber atualizações de sistema operacional, bibliotecas, instalação de componentes de software e aplicativos de terceiros, mesmo com o veículo já vendido em circulação, passam a ser uma realidade na indústria automotiva. Essa tendência nos veículos demanda consequentemente a adoção de medidas de cibersegurança para detecção, análise e resposta a incidentes e ciberameaças consolidadas em outros sistemas.

As principais referências de normatização e regulamentação mundiais – ISO/SAE 21434, UNECE R155, UNECE R156 (ver capítulos anteriores) – buscam enfrentar a situação, determinando de forma muito clara medidas para garantir que a cibersegurança veicular exceda sua fase de concepção, desenvolvimento e produção, e permaneça adequada durante toda sua vida útil. Para isso, devem existir elementos que permitam a detecção de vulnerabilidades e ataques, o bloqueio de tais incursões, a capacidade forense para análise das causas originais de tais ataques, a elaboração de modificações de software que façam a contenção de seu impacto e impeçam sua propagação e repetição e, finalmente, capacidade para a atualização do software embarcado no veículo para a implementação de tais correções.

Do ponto de vista de implementação tecnológica, a tendência é a adição de componentes de software aos computadores e ECUs embarcados no veículo para a detecção de anomalias e possíveis ataques, tais como “firewalls” para as redes veiculares (CAN/Ethernet principalmente), agregadores de informações e, finalmente, centros de respostas a incidentes (VSOCs – Vehicle Cybersecurity Operation Centers).

Cibersegurança operacional embarcada em componentes

No nível dos componentes e ECUs, são implementadas medidas que buscam monitorar o comportamento do equipamento e detectar possíveis anomalias. A ideia é analisar em tempo real parâmetros fundamentais, como acesso a regiões de memória, uso de processamento, tempo de resposta, quais componentes de SW estão em execução, entre outras métricas. Caso se detecte atividade anômala, um alerta é gerado e enviado para um sistema de agregação e triagem de alertas, de forma similar a um antivírus clássico. Vale ressaltar que funcionalidades relacionadas ao update de software demandam ainda um “bootloader” seguro, que deve ser implementado para validar e garantir que apenas componentes de software autenticados e de autoria confirmada sejam aceitos na memória da ECU/Computador para serem executados.

Firewalls e medidas de proteção para comunicação e redes

Um veículo moderno possui uma arquitetura de rede própria, com barramentos dedicados para a comunicação entre seus diversos componentes eletrônicos. Tradicionalmente são empregados barramentos CAN e LIN. Porém, buscando atender o crescimento de complexidade e volume de tráfego de informações, observa-se a adoção de redes Ethernet. Técnicas clássicas utilizadas para a proteção de redes podem

ser empregadas no contexto automotivo, como a segmentação de redes, o uso de firewalls e o monitoramento e análise de tráfego.

Centros de respostas a incidentes (VSOCs – Vehicle Cybersecurity Operation Centers)

A adoção de centros de resposta a incidentes, como os VSOCs (Vehicle Cybersecurity Operation Centers), é uma das principais estratégias para lidar com ameaças em tempo real. Esses centros são responsáveis por monitorar continuamente a infraestrutura de TI dos veículos assim como os dados provenientes da própria frota de veículos, permitindo a identificação rápida de incidentes e a implementação de respostas imediatas. A coordenação de ações para mitigar riscos e restaurar a segurança do sistema exige uma análise forense em tempo real, por especialistas dedicados, de dados provenientes de múltiplas fontes, como sensores, módulos de comunicação e dispositivos de diagnóstico.

Além disso, a interdependência entre os sistemas veiculares e as infraestruturas externas, como redes de tráfego e plataformas de dados na nuvem, exige uma abordagem holística para a cibersegurança. Qualquer vulnerabilidade em um desses componentes pode ser um ponto de entrada para um ataque, o que reforça a importância da implementação de medidas robustas de segurança não apenas dentro do veículo, mas também em suas interfaces externas. Dessa forma, a integração de sistemas de segurança com infraestrutura crítica de trânsito e conectividade veicular pode atuar como uma camada adicional de proteção contra ataques que possam comprometer a integridade e segurança dos usuários.

Conclusão:

O fortalecimento da cibersegurança no setor automotivo não é uma tarefa isolada e deve envolver todos os estágios de vida do veículo, desde sua concepção até a operação contínua no campo. A evolução para veículos conectados e autônomos aumenta significativamente a superfície de ataque, tornando essencial a implementação de um ecossistema de segurança integrado e dinâmico. Nesse contexto, a contínua adaptação a novas ameaças, através de atualizações de software e melhorias nos protocolos de segurança, se torna uma prática imprescindível. Ao adotar medidas como firewalls, monitoramento em tempo real e a criação de centros especializados de resposta a incidentes, a indústria automotiva pode assegurar que os sistemas embarcados não apenas atendam aos requisitos de segurança no momento da produção, mas também se mantenham protegidos e resilientes ao longo de toda a sua vida útil, garantindo a segurança de seus usuários frente a um cenário tecnológico em constante evolução.

9 RESUMO EXECUTIVO

Introdução

A cibersegurança no setor automotivo emergiu como uma prioridade crítica, à medida que a complexidade dos veículos modernos e a conectividade aumentaram. Desde os primeiros vírus de computador até os sofisticados sistemas de assistência ao condutor, a proteção de sistemas digitais é essencial para garantir a segurança e a integridade dos veículos. Este whitepaper explora a evolução da cibersegurança, os desafios enfrentados e as regulamentações em vigor, com foco especial no contexto brasileiro.

Evolução da Cibersegurança

A história da cibersegurança remonta à década de 1960, com a criação dos primeiros vírus e antivírus. Com o advento da internet e a crescente conectividade dos dispositivos, os ataques cibernéticos tornaram-se mais sofisticados. No setor automotivo, a introdução de sistemas embarcados e a digitalização dos veículos ampliaram a superfície de ataque, tornando-os vulneráveis a uma variedade de ameaças, como invasões de software, roubo de dados e manipulação de sistemas críticos.

Cibersegurança vs. Segurança Funcional

É fundamental distinguir entre cibersegurança e segurança funcional. A segurança funcional se concentra na proteção contra falhas não intencionais que podem comprometer a segurança do veículo, enquanto a cibersegurança aborda ameaças intencionais e maliciosas. Ambas as disciplinas são complementares e devem ser integradas nas estratégias de desenvolvimento e operação de veículos para garantir a proteção total dos usuários e sistemas.

Dimensão Holística da Cibersegurança

A cibersegurança deve ser considerada em todas as fases do ciclo de vida do veículo, incluindo:

• Análise de Ameaças e Riscos: Identificação de ativos críticos e avaliação de possíveis cenários de ataque.

• Design e Conceito: Desenvolvimento de requisitos técnicos que atendam às metas de cibersegurança.

• Implementação e Testes: Adoção de boas práticas de codificação e realização de testes de intrusão para identificar vulnerabilidades.

• Produção e Operação: Garantia de que todos os processos de produção e operação estejam alinhados com as diretrizes de cibersegurança, incluindo monitoramento contínuo e resposta a incidentes.

A governança organizacional e a conscientização sobre riscos são essenciais para a eficácia das estratégias de cibersegurança, exigindo colaboração entre todos os stakeholders envolvidos.

Normatizações e Regulamentações

O whitepaper analisa os padrões internacionais, como a ISO/SAE 21434 e UNECE R155 e R156, que estabelecem requisitos mínimos para sistemas de gerenciamento de cibersegurança (CSMS) e atualizações de software (SUMS). Essas regulamentações visam garantir que todos os veículos atendam a padrões de segurança cibernética, promovendo a proteção de dados e a integridade dos sistemas. A implementação dessas normas é crucial para mitigar riscos e garantir a segurança dos veículos conectados.

Desafios e Oportunidades no Brasil

O Brasil tem a oportunidade de aprender com as experiências de mercados mais avançados em relação a práticas, normas e regulamentação, como a União Europeia, os Estados Unidos e alguns países asiáticos. A revisão e adoção de práticas recomendadas, o entendimento de lições aprendidas e a colaboração entre reguladores, montadoras e fornecedores são importantes para fortalecer a segurança cibernética no setor automotivo brasileiro.

Conclusão

A cibersegurança é uma questão crítica para o futuro da mobilidade. À medida que os veículos se tornam mais conectados e complexos, a proteção contra ameaças cibernéticas deve ser uma prioridade. Este whitepaper serve como um chamado à ação para que a indústria automotiva, reguladores e stakeholders colaborem na criação de um ambiente seguro e resiliente para a mobilidade do futuro. A construção de uma infraestrutura de cibersegurança sólida não apenas protegerá os veículos, mas também garantirá a confiança dos consumidores e a integridade do setor automotivo como um todo.

APÊNDICE A
– EXEMPLOS DE CASOS

Caso 1

Uma vulnerabilidade emblemática foi encontrada por um hacker em 2024 relacionada às chaves utilizadas para criptografar a imagem do sistema operacional da unidade de infotenimento veicular (IVI) de um sedã híbrido de uma grande montadora, cuja fabricação é do ano de 2021. O hacker descobriu que as chaves foram copiadas de fontes públicas e que estão disponíveis nas primeiras páginas de pesquisas na ferramenta de busca do Google.

O hacker realizou o ataque em seu próprio veículo, algo comum entre entusiastas de cibersegurança de hardware, e divulgou o processo em seu blog pessoal. É muito comum que unidades de infotenimento modernas utilizem sistemas operacionais baseados em Linux, seja na forma do sistema Android da Google ou distribuições proprietárias. O hacker tinha como objetivo obter acesso root ao OS e instalar suas próprias aplicações para uso no dia-a-dia.

Com o uso de ferramentas disponíveis publicamente como bkcracker, o hacker conseguiu extrair a imagem do OS bem como obter acesso à ferramenta de update da montadora. Também foi possível descobrir os métodos de assinatura de software e parâmetros como o IV para criptografia RSA e chaves públicas, informações tais que estavam escritas em texto simples nos scripts de update da montadora. Ao pesquisar a chave pública obtida no Google de forma despretensiosa, o hacker descobriu tratar-se do primeiro exemplo publicado pela NIST para criptografia AES-128bit CBC no documento SP800-38A. Com isso, o hacker é capaz de criptografar e enviar suas próprias aplicações à central IVI.

Este caso deixa claro que apenas aplicar criptografia não é suficiente para proteger informação e garantir integridade e autenticidade. É necessário estabelecer políticas rígidas sobre geração, armazenamento e transporte das chaves e materiais criptográficos, que nunca devem estar prontamente disponíveis no código ou documentação.

Apesar de nesse caso os impactos tenham se mostrado como mínimos, o conhecimento dessa superfície de ataque poderia abrir caminho para consequências mais gravosas, como por exemplo, a instalação de SW maliciosos no IVI que potencialmente levariam

a roubo de dados de aparelhos celulares conectados.

Caso 2

Em 2015, foi realizado um ataque bastante noticiado em um veículo SUV de uma grande montadora. Os profissionais de cibersegurança automotiva Charlie Miller and Chris Valasek descobriram e exploraram uma vulnerabilidade que os permitiu obter controle sobre o carro (prática conhecida como car hijacking, sequestro veicular em tradução livre) de forma remota, utilizando a comunicação via internet do veículo. Os atacantes demonstraram o potencial impacto da vulnerabilidade ao tomar controle do veículo enquanto ele era dirigido a cerca de 110 km/h por um jornalista – que sabia de antemão que passaria pelo ataque, mas não o que os atacantes iriam controlar. O hacker acionou limpadores, controlou o rádio e ar-condicionado e desligou o motor em pleno funcionamento.

O ataque se inicia com a identificação do veículo alvo conectado em uma rede proprietária da montadora. Ao conectar-se na rede como um usuário supostamente autorizado, é possível obter informações e potencialmente comunicar-se com todos os outros veículos conectados. Essa conexão é gerenciada no veículo pelo módulo de infotenimento que, por sua vez, controla também diversas funções de informações e do ambiente do cockpit, tais como ar-condicionado, rádio e aquecimento de bancos.

Em condições normais, não é possível realizar uma ligação direta entre o servidor da rede e o barramento CAN do veículo. Porém, os hackers desenvolveram um firmware específico para a central de infotenimento capaz de sequestrar e manipular a comunicação no barramento CAN e controlar o veículo por meio de diversas funcionalidades. Assim, funções de dirigibilidade como freio de emergência, assistência de faixa e até controle do motor foram comprometidas.

Tais ações não visavam causar risco à vida do jornalista, tampouco obter ganho financeiro pelos hackers. O objetivo era alertar sobre os riscos existentes em veículos que já estão em circulação para que montadoras e fornecedores levem em consideração os riscos aos quais estão expondo clientes e a si mesmos. Medidas de defesa poderiam ser adotadas tanto do lado do servidor (com autenticação forte e monitoramento de atividades suspeitas) quanto do lado do veículo (com verificação de assinatura de dados sendo transferidos, updates de segurança regulares e proteção e isolamento dos barramentos CAN).

Este caso ilustra as possibilidades que um atacante pode explorar ao escalar vulnerabilidades aparentemente simples. Um ataque a uma unidade de infotenimento normalmente não deveria apresentar risco à vida do usuário, porém, ao escalar o ataque, os pesquisadores puderam controlar funções críticas de forma remota, colocando em risco o usuário sem a necessidade de obter contato físico com o veículo. Assim, é indispensável que a segurança seja pensada de forma aprofundada e em diferentes camadas e redundâncias, de forma que uma eventual vulnerabilidade não possa comprometer outros sistemas do veículo.

CASO 3

Na DEFCON em 2019 foi apresentado um ataque proof-of-concept a um modelo de veículo elétrico. O ataque teve como alvo o sistema de destravamento passivo por presença da chave. O grupo de pesquisadores COSIC da Universidade Católica de Leuven foi capaz de identificar e explorar uma vulnerabilidade relacionada à implementação das operações criptográficas no sistema de destravamento por presença de chave e acessar o interior do veículo, ligá-lo e poderiam, inclusive, dirigi-lo.

O sistema de destravamento por presença utiliza um emissor Bluetooth de baixa potência (BLE) embarcado na chave para receber e responder ao desafio criptográfico emitido pelo veículo ao se aproximar. O desafio faz uso do protocolo DST40 que utiliza uma chave de 40 bits para autenticação. Os pesquisadores utilizaram um emissor similar para emitir sinais ao veículo e obter os desafios que seriam emitidos à chave, além de um ID para identificar o veículo, obtido ao capturar os sinais de comunicação.

Ao capturar a comunicação entre chave e veículo, os pesquisadores foram capazes de mapear todas as possíveis chaves e realizar um ataque do tipo brute-force em poucos segundos que testava todas as possíveis chaves até que o veículo se destravasse. Para o ataque, não há necessidade de proximidade com a chave original, foi necessário apenas um modelo da chave para que o algoritmo pudesse passar por engenharia reversa.

Há uma segunda camada de proteção implementada pela montadora na forma de um código PIN definido pelo proprietário que deve ser inserido para que o veículo possa ser ligado. No entanto, essa configuração é opcional e não é ativada na produção. Este caso mostra que protocolos criptográficos devidamente implementados não são necessariamente seguros, podendo estar ultrapassados ou obsoletos. Novos

ataques surgem tão rápido quanto novas tecnologias. Assim, os controles de cibersegurança a serem implementados em um produto devem sempre considerar o estado-da-arte no que tange protocolos de criptografia, métodos de ataque existentes e poder computacional disponível para atacantes. Além disso, patches de segurança devem sempre ser adotados quando novas vulnerabilidades ou métodos de ataque são descobertos.

CASO 4

Sistemas agrícolas como tratores também utilizam tecnologias similares aos veículos on-road, na forma de ECUs, comunicação em barramento ISOBUS (baseado em CAN), sistemas de injeção eletrônica para motores diesel, controles de direção, terminais de infotenimento, etc. Assim, também podem ser alvos de ataques cibernéticos à sua conectividade e/ou hardware. Um exemplo foi apresentado na DEFCON em 2022 pelo hacker Sickcodes, em que foi capaz de obter acesso root na unidade de infotenimento de um trator de uma grande montadora. No ataque desenvolvido por Sickcodes, o sistema operacional e a interface gráfica da central de infotenimento passou a rodar o clássico jogo eletrônico dos anos 1990 DOOM.

Ao obter acesso a alguns modelos de central de infotenimento usados nos tratores da montadora, Sickcodes notou diversas vulnerabilidades e más práticas utilizadas. Por exemplo, o sistema operacional era uma distribuição já em desuso de GNU/Linux desde 2018. Outra vulnerabilidade encontrada foi que para obter acesso privilegiado passando-se por um operador autorizado da montadora seria necessário apenas inserir um arquivo vazio .txt com um título similar a “IAmADealer.txt”.

Sickcodes, obtendo acesso ilimitado ao equipamento, notou ainda que muito do código utilizado incluía ferramentas open-source com uso que violaria as diretrizes de uso propostas pelos seus desenvolvedores originais. O hacker passou então a explorar tudo que seria possível no hardware e, a fim de apresentar o nível de insegurança do dispositivo, fez uma demonstração jogando uma versão temática de DOOM que se passa em uma fazenda, rodando o software no microcontrolador da unidade e utilizando sua interface gráfica. Caso fosse mal-intecionado, o hacker poderia causar ainda mais estrago ao escalar o ataque utilizando as funcionalidades de conectividade para explorar também os servidores da montadora e eventualmente se comunicando com outros tratores conectados em campo.

A simples adoção de boas práticas de cibersegurança neste caso poderiam ter dificultado ou até impedido completamente as atividades demonstrativas do hacker. O uso de distribuições ativas e seguras do sistema operacional, a adoção de métodos adequados de autenticação para obtenção de acesso privilegiado ao sistema e a aplicação de criptografia em dados armazenados são medidas básicas que devem ser adotadas em qualquer sistema.

APÊNDICE B

– REFERÊNCIAS

Capítulo 3

http://repositorio.roca.utfpr.edu.br/jspui/bitstream/1/19820/1/CT_CESEB_III_2016_06.pdf

https://www.iec.ch/functional-safety

Capítulo 5

https://itthub.net/wp-content/uploads/2022/01/Global_Automotive_Cybersecurity_Report_2022.pdf

https://knowledge.bsigroup.com/products/the-fundamental-principles-of-automotive-cyber-security-specification/standard

https://ecs-org.eu/documents/publications/5a31129ea8e97.pdf

https://www.thalesgroup.com/en/worldwide-digital-identity-and-security/iot/magazine/single-automotive-cyber-security-standard

https://qaconsultants.com/blog/automotive-cybersecurity-and-regulatory-standards/

https://ivds.dependability.org/ivds2022/IVDS2022Presentations/SCHMITTNER.pdf

https://upstream.auto/automotive-cybersecurity-standards-and-regulations/

https://capgemini-engineering.com/as-content/uploads/sites/5/2018/01/cybersecurity-in-automotive_position-paper.pdf

https://copperhorse.co.uk/an-overview-of-the-automotive-cybersecurity-standards-landscape/

https://www.enisa.europa.eu/publications/recommendations-for-the-security-of-cam/

https://copperhorse.co.uk/automotive-cybersecurity-standards-a-living-list/

https://www.china-briefing.com/news/china-internet-of-vehicles-new-guidelines-set-framework-for-industry-standards/

https://cybellum.com/blog/intro-to-automotive-cybersecurity-regulations/

https://innovationatwork.ieee.org/u-s-national-highway-traffic-safety-administration-releases-update-to-automotive-cyber-security-best-practices/

ENTRE EM CONTATO CONOSCO:

11 5908 4043 / RELACIONAMENTO@AEA.ORG.BR | WWW.AEA.ORG.BR

ASSOCIAÇÃO BRASILEIRA
DE ENGENHARIA AUTOMOTIVA

@AEA1984_