1ª CONFERÊNCIA

Veículos inteligentes

Como eles irão afetar a nossa vida, os negócios e o transporte público?

Segurança Cibernética

Rodolfo Saboia Lima de Souza

APOIO:

cooperação alemã DEUTSCHE ZUSAMMENARBEIT

Por meio da: giz Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH

REALIZAÇÃO:

UFLA UNIVERSIDADE FEDERAL DE LAVRAS

Firjan SENAI SESI IEL CIRJ

45 anos INMETRO

MINISTÉRIO DA INDÚSTRIA, COMÉRCIO EXTERIOR E SERVIÇOS

BRASIL GOVERNO FEDERAL

INTERNET DAS COISAS

“É a rede de objetos físicos ou "coisas" com eletrônica, software, sensores e conectividade de rede incorporados, que permitem a esses objetos coletarem e trocarem dados.”

É a conexão do mundo virtual com a realidade física.

PLANO NACIONAL DE INTERNET DAS COISAS – BNDES e MCTIC

Define os Ambientes e prioriza ações governamentais

- Cidades
- Indústria
- Agricultura
- Saúde

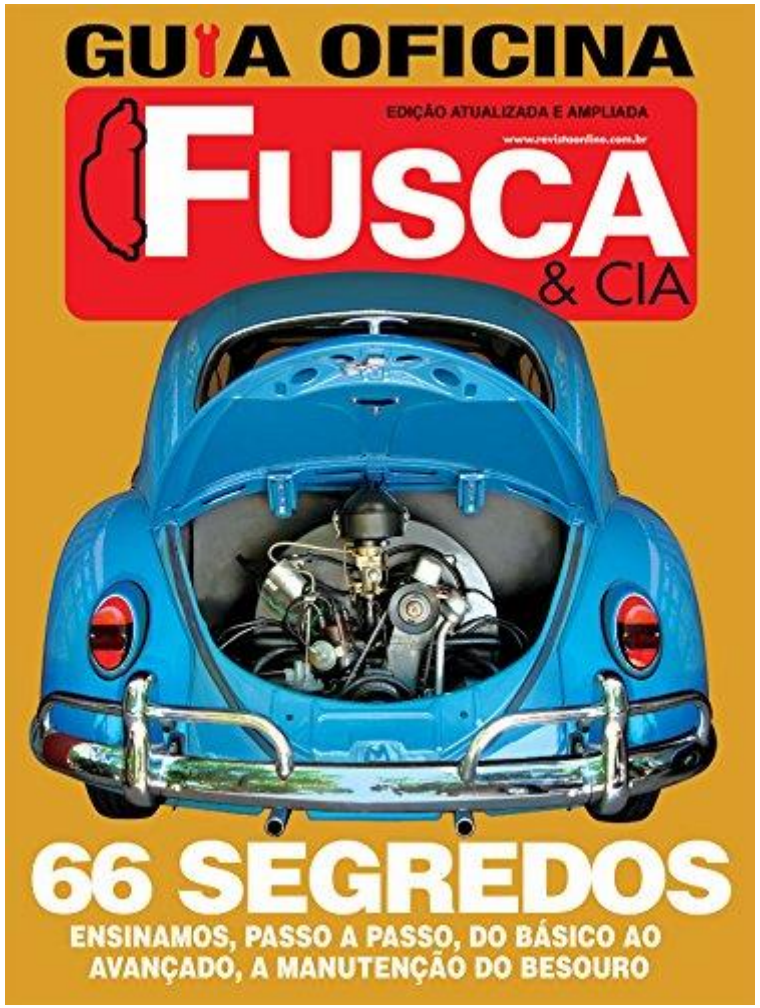
- Residência
- Escritórios
- Etc....

- Automóveis

VOLTANDO AOS AUTOMÓVEIS

ATÉ 1980

- Sofisticado equipamento eletro mecânico
- Ignição – Bobina, Distribuidor e Platinado
- Injeção – Carburador (Bernoulli)
- Buzina conectada diretamente ao volante
- Luzes conectadas ao botão interruptor
- No máximo um rádio AM-FM com poucos transistores
- Uma antena que sobe manualmente



HOJE

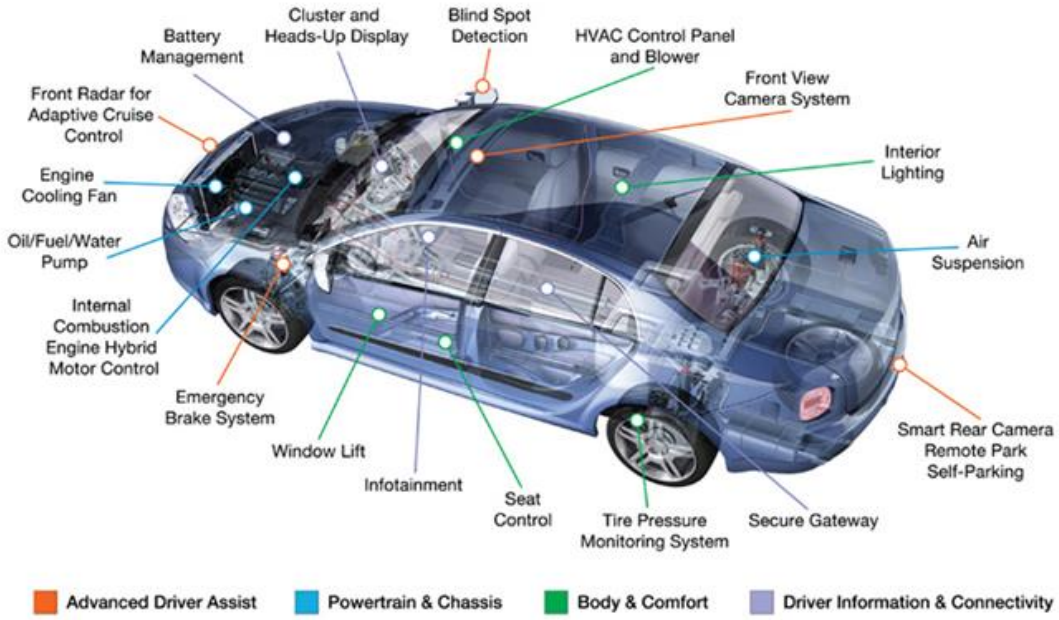
Centralina Eletrônica

Sensores ⇒ Centralina ⇒ Atuadores

- Sensores (também designados Transductores de Entrada): Convertem as grandezas mecânicas em sinais eléctricos.
- Centralina: Recebe dos sensores, os sinais elétricos correspondentes a grandezas físicas, processa esses sinais, e envia para os actuadores os sinais eléctricos correspondentes a acções que os actuadores devem executar.
- Atuadores (também designados Transductores de Saída): Convertem os sinais elétricos recebidos da centralina para grandezas físicas, correspondentes às acções mecânicas e/ou elétricas que devem executar.

A centralina, por sua vez, é constituída pelos seguintes módulos

- Conversor A/D
- Processador Digital de Sinal (DSP - Digital Signal Processor)
- Memória EEPROM ou FLASH
- Memória RAM
- Portas de E/S (entrada e saída)
- Conversor D/A
- Porta de Conexão c/ dispositivo externo



BARRAMENTO CAM

- Rede de dados conectando os diversos dispositivos do veículo

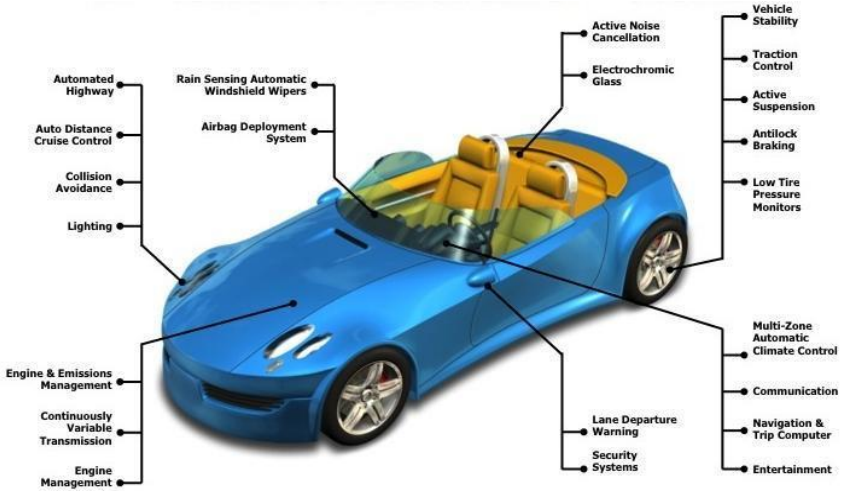
E NO FUTURO

Veículo Inteligente

- GPS
- Lidar
- Radar
- Vários barramentos
- Várias centrais de processamento
- Software complexo

Comunicações

- Veículo - Veículo – V2V
- Veículo - Infraestrutura – V2I
- Veículo - Rede – V2N
- Veículo – Qualquer Coisa – V2X



INFRAESTRUTURA

HOJE

- Rua, Rodovia – asfalto, paralelepípedo, terra, concreto
- Pintura no asfalto
- Olho de gato
- Sinal Luminoso (semáforo)
- Placas de sinalização
- Postes de iluminação
- Câmeras de Monitoramento
- Medidores de excesso de velocidade, e avanço de sinal
- Cronotacógrafo (caminhão)

FUTURO

- Rua, Rodovia – asfalto, paralelepípedo, terra, concreto
- Pintura no asfalto – tinta especial
- Olho de gato com RFID ou outro tag eletrônico
- Sinal – dispositivo eletrônico
- Placa de sinalização – dispositivo eletrônico
- Postes de iluminação – Conexão RF (Wifi, Celular, etc)
- Câmeras de monitoramento
- Drones de monitoramento
- “Caixa Preta” veicular

AMEAÇAS!

Até 1980

- Cortar o cabo de freio (filmes de James Bond)
- Por uma bomba no carro acionada pela Ignição (filmes de Máfia)

Até Agora

- Trocar o “chip” para “envenenar” o carro
- Falsificar resultados de testes de emissões com utilização de software malicioso
- Automóvel sofrer efeitos negativos de interferência eletromagnética

No Futuro

Só Deus sabe!!!!!!

QUEM PODE ATACAR?

Pessoas, organizações ou governos

- na Internet
- em um carro próximo
- nas proximidades com sistemas de interferência eletromagnética
- de dentro do veículo

MOTIVOS?

Precisa enumerar?

Tipos de Ataques

- Cibernéticos
  "Um ataque, via ciberespaço, com o objetivo de interromper, desativar, destruir ou controlar maliciosamente um ambiente/infraestrutura de computação; ou destruindo a integridade dos dados ou roubando informações controladas."

- "Guerra" Eletrônica
  "O conjunto de ações que utilizam a energia eletromagnética para destruir, neutralizar ou reduzir a capacidade de combate do oponente"

PONTOS VULNERÁVEIS

Ataques Cibernéticos

- Central de Controle do Veículo
- Central de armazenamento de dados do veículo – “Caixa Preta”
- Um veículo próximo conectado
- Qualquer dispositivo com microprocessador na Infraestrutura
- A “Nuvem” ou o “Fog”
- Esqueci algum?

Guerra Eletrônica

- GPS
- Lidar, Radar, etc...
- Interferência em redes de comunicações

PRIORIDADES DE SEGURANÇA

- Segurança física dos passageiros, pessoas na rua, e objetos urbanos
- Fluxo de veículos
- Privacidade dos dados
- Conteúdo da Caixa Preta

TUDO ESTÁ PERDIDO?

Os mecanismos de segurança para equipamentos e redes de dados já existem. Precisam ser adaptados, e desenvolvidos para a nova situação.

- Avaliação de riscos
- Estudos de casos de ataques reais e hipotéticos
- Definição de ferramentas adequadas
- Balanço adequado da segurança e dos “custos” decorrentes
- Decisões técnicas e políticas (ex: grau de privacidade)
- Estabelecimento dos requisitos de segurança nos dispositivos e na rede (avaliação de conformidade)

PROTEÇÃO DOS SISTEMAS EMBARCADOS

Análise dos dispositivos por metodologia de “caixa preta”

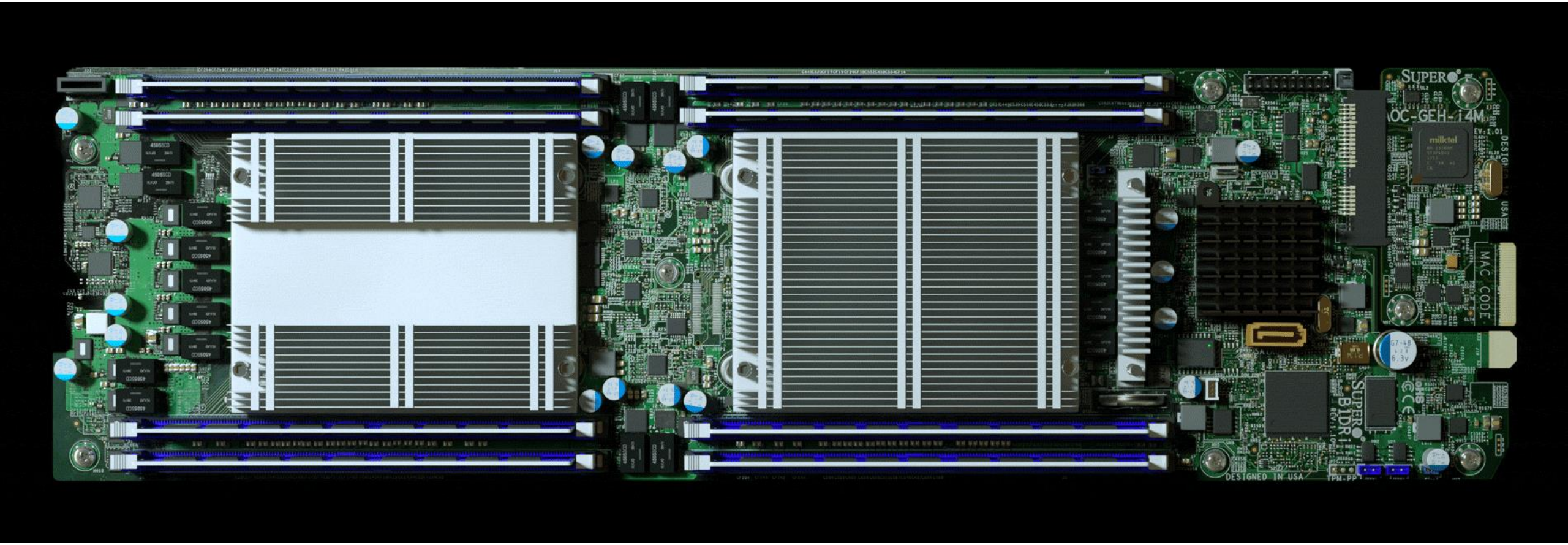
- Provocar ataques conhecidos nos sistemas embarcados e verificar os efeitos

Análise dos dispositivos por caixa branca

- Obrigar fabricante a fornecer toda documentação do hardware, firmware, e software utilizados
- Analisar o produto em um laboratório acreditado, e verificar conformidade com o dispositivo documentado, e com os requisitos de segurança

1º CONFERÊNCIA

Veículos inteligentes



VANTAGENS E DESVANTAGENS

- Método de “caixa preta” é menos seguro, porém menos complexo
- O fornecimento do código pode comprometer sigilo industrial
- Método de “caixa branca” incentiva o desenvolvimento de sistemas mais seguros
- Conceitos como legalmente relevante devem ser usados, mas com cuidado
- Nenhum método GARANTE segurança
- NÃO É SÓ O VEÍCULO QUE DEVE SER TESTADO, MAS PRATICAMENTE TODOS OS DISPOSITIVOS

AUTENTICAÇÃO DOS DISPOSITIVOS CONECTADOS

- Necessidade de autenticação dos dispositivos para prevenir entrada de componente malicioso
- Pode-se utilizar assinatura digital Objetos Metrológicos (IoT) - ICP BRASIL
- Outras cadeias de certificados digitais podem igualmente ser utilizadas
- Um mecanismo semelhante ao Blockchain pode vir a ser utilizado
- Outros métodos de autenticação podem envolver parâmetros físicos do local onde o objeto deve estar

PROTEÇÃO DA REDE DE DADOS E DOS DATACENTERS

- Firewall
- DMZ
- Deteção de Intrusão
- Vlan
- Isolamento de tráfego
- VPN
- IPV6 – com IPSEG
- Proteção de camada 2

PROTEÇÃO DOS SISTEMAS RF

GNSS é especialmente vulnerável (spoofing)

- Utilização de métodos de posicionamento alternativo (Tags de posição, E-Loran, acelerômetro inercial)

Radar e Lidar

- Utilização de método alternativo de sensoriamento (imagem)

Interferências nas comunicações

- Entrar em modo de segurança

Chamar polícia

VÁRIAS DECISÕES TÉCNICAS E PRINCIPALMENTE POLÍTICAS

- Grau de risco tolerável
- Níveis de requisito de segurança para cada dispositivo envolvido
- Nível de privacidade dos usuários
- Modelo de análise de conformidade para os dispositivos embarcados
- Método de autenticação dos dispositivos
- Modelo de segurança de rede de dados
- Modelo de segurança da “nuvem” e datacenters

O QUE TEMOS QUE FUGIR

Modelo de segurança do Windows PC

- Antivirus
- Se o vírus ou malware entra no PC pode fazer tudo

O QUE TEMOS QUE PERSEGUIR

Celular tem modelo de segurança mais confiável

Caixa automática bancária