



Escola Politécnica da Universidade de São Paulo
Curso de Pós graduação em Engenharia Elétrica
PSI5121 Sistemas Automotivos



Veículos Autônomos

Aula 4 - Safety

Prof. Leopoldo Yoshioka
11 JULHO 2023



Objetivos da Aula 4:

- Abordar os conceitos segurança funcional de VA
- Analisar os relatórios de auto-avaliação de segurança
- Fechamento e Reflexão sobre a Disciplina PSI5121

Segurança (*safety*) do veículo autônomo

Exemplos de acidentes com veículo autônomo



Exemplos de acidentes com veículo autônomo



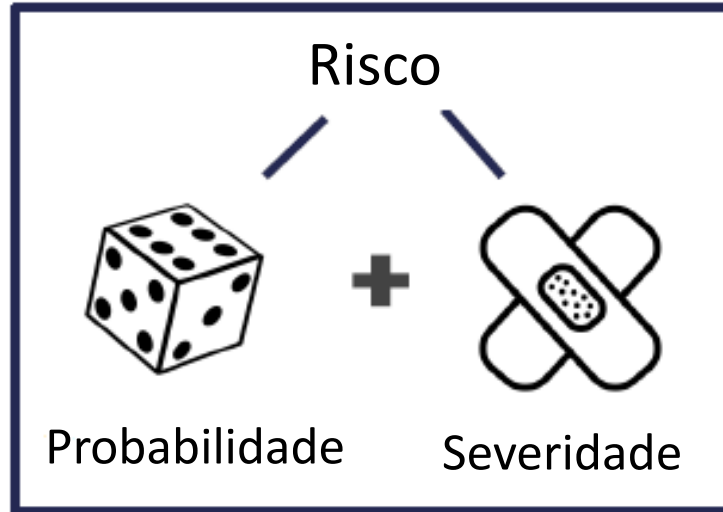
Exemplos de acidentes com veículo autônomo



Acidente com fatalidade envolvendo VA do Uber



Taxonomia relacionado com segurança



Segurança (*safety*) - ausência de risco ou acidente não-razoável

Perigo (*hazard*) - fonte potencial de risco ou acidente não-razoável

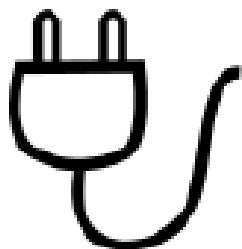
Nesta disciplina vamos definir **segurança de veículos autônomos** como sendo a condição em que:

- O risco de ocorrência de um acidente devido a falhas no sistema, subsistema, componentes, hardware, software seja suficientemente pequena, e tolerável, quando comparado com os veículos convencionais num fator de pelo menos **10 para 1**.
- Por exemplo, nos EUA a taxa de acidentes é de 1 acidente a cada 164 mil milhas (264 mil km).

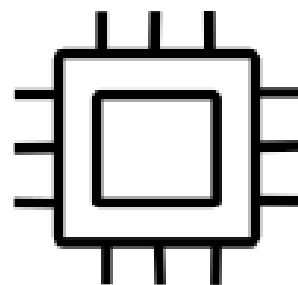
Maiores fontes de perigos e riscos:



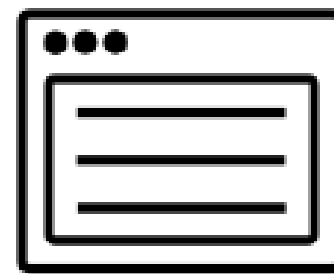
Mechanical



Electrical



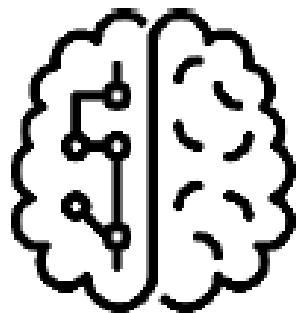
Hardware



Software



Perception



Planning



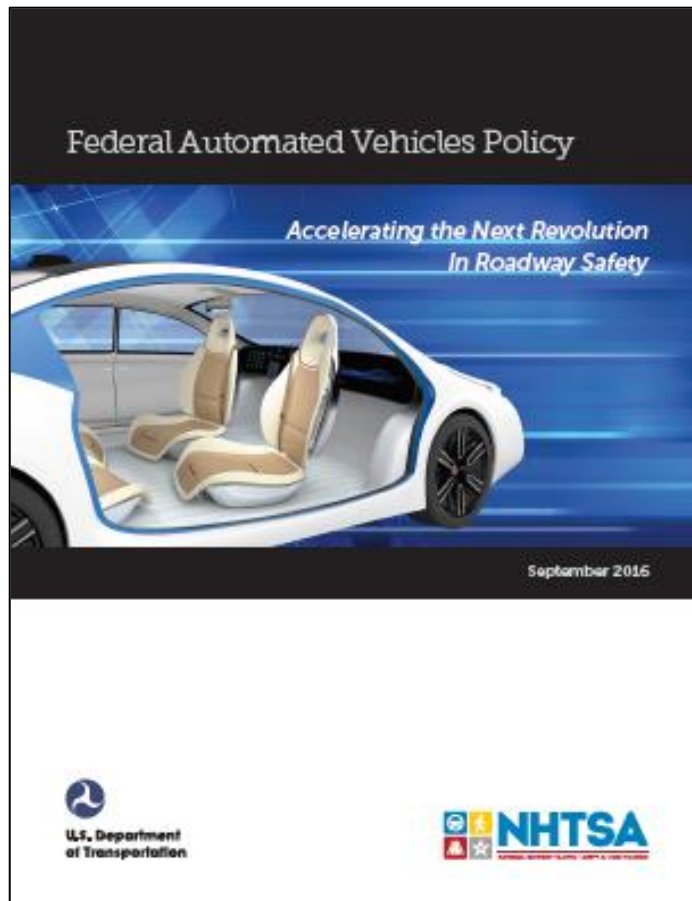
Fallback



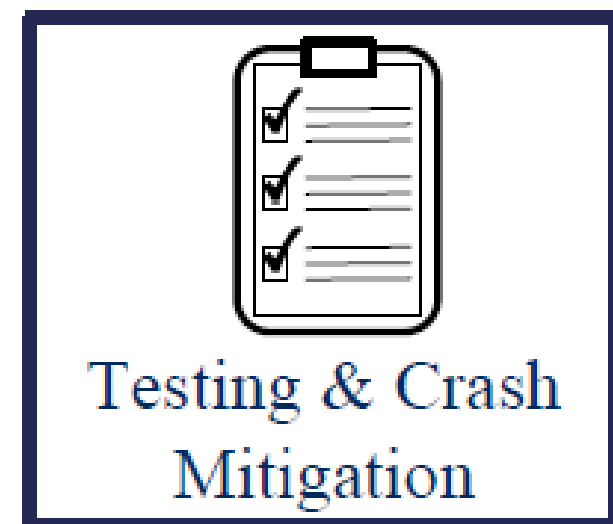
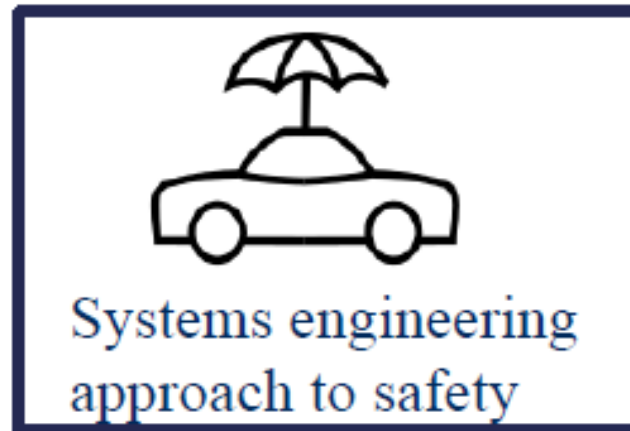
Cyber

Documento de Referência:

US Department of Transit - Safety Framework (2016)



(116 pág)



Aspectos a serem considerados no projeto do VA:



ODD



OEDR



Fallback



Traffic Laws



Cybersecurity



HMI

Testes e mitigação de acidentes de colisão:



Testing



Crashworthiness



Post crash

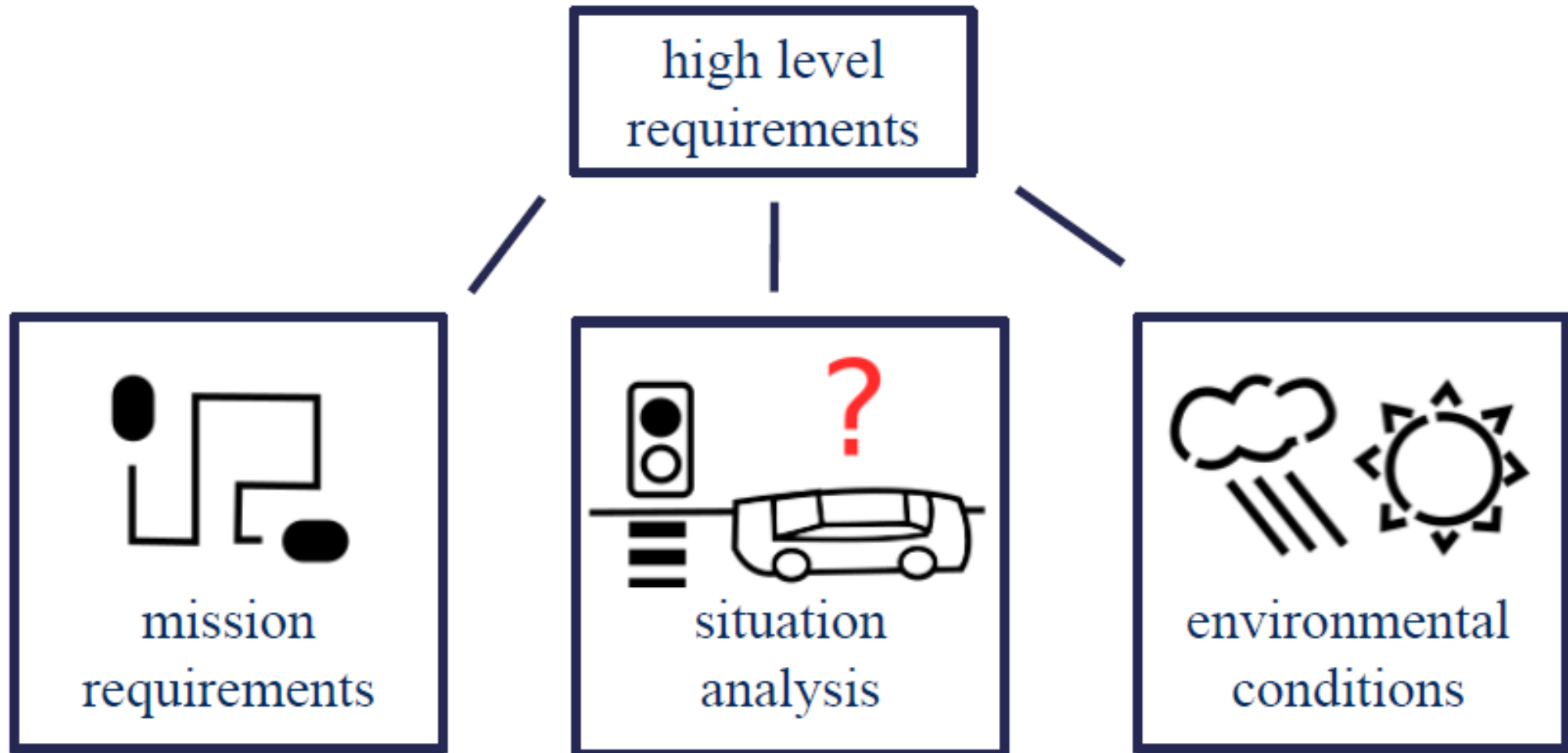


Data recording



Consumer Ed

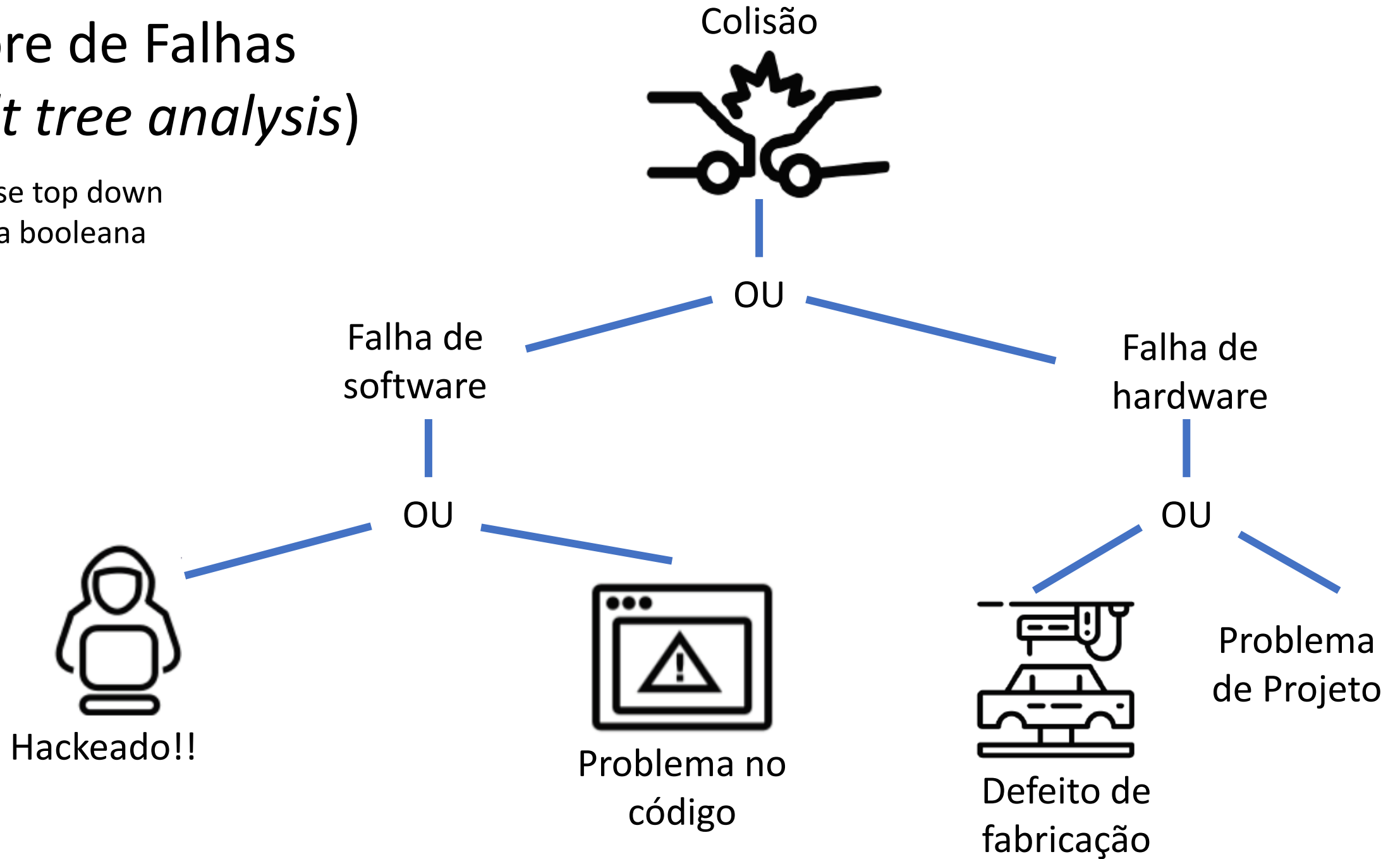
Requisitos de segurança:



Métodos de Análise de Segurança

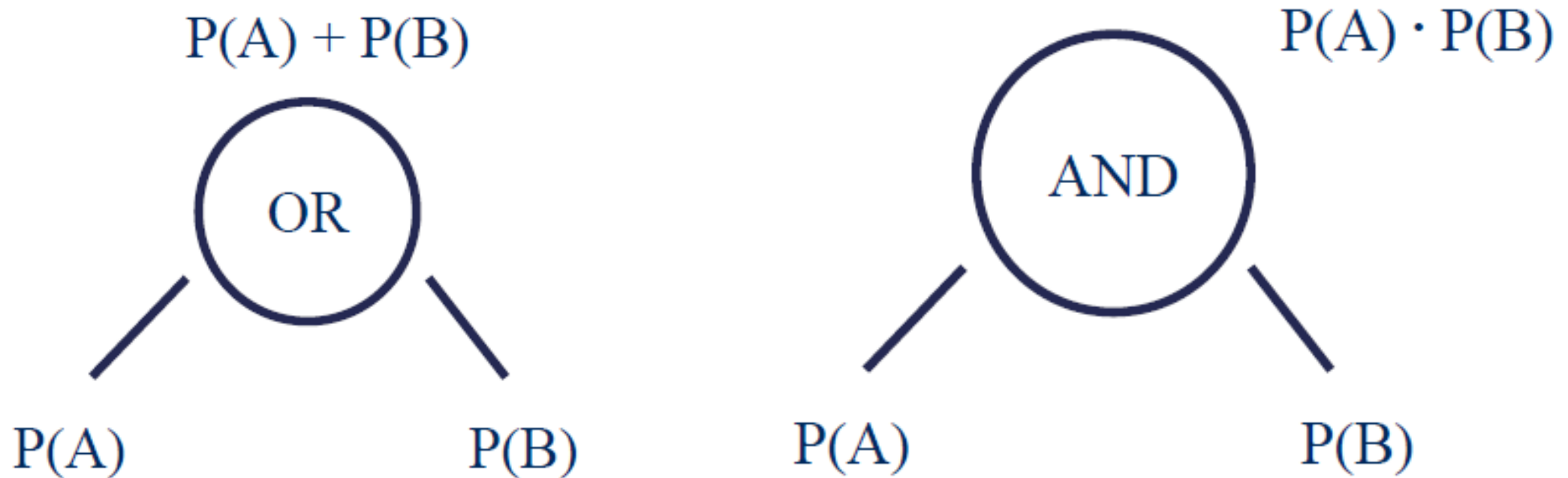
Árvore de Falhas (*fault tree analysis*)

- Análise top down
- Lógica booleana



Análise probabilística de Árvore de Falhas

- Atribuição de probabilidade para ocorrência de falhas
- Uso de portas lógicas para construção de árvore de falhas

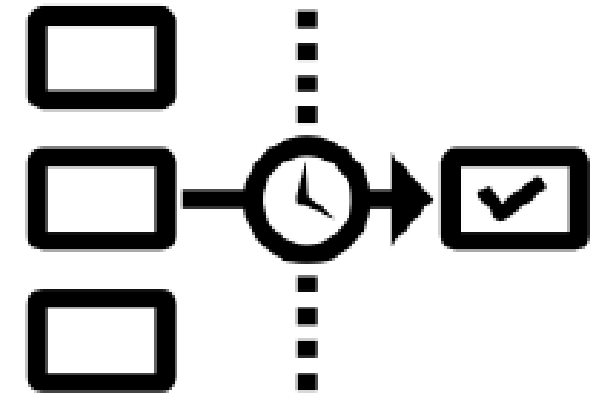


Análise de Modos e Efeitos das Falhas (FMEA)

- Processo *botom up* para identificar todos os tipos e efeitos de falhas do sistema
- **Modos de falha:**
 - Modos ou formas em que um componente do sistema pode falhar
- **Análise dos efeitos:**
 - Análise do efeito das falhas na operação do sistema

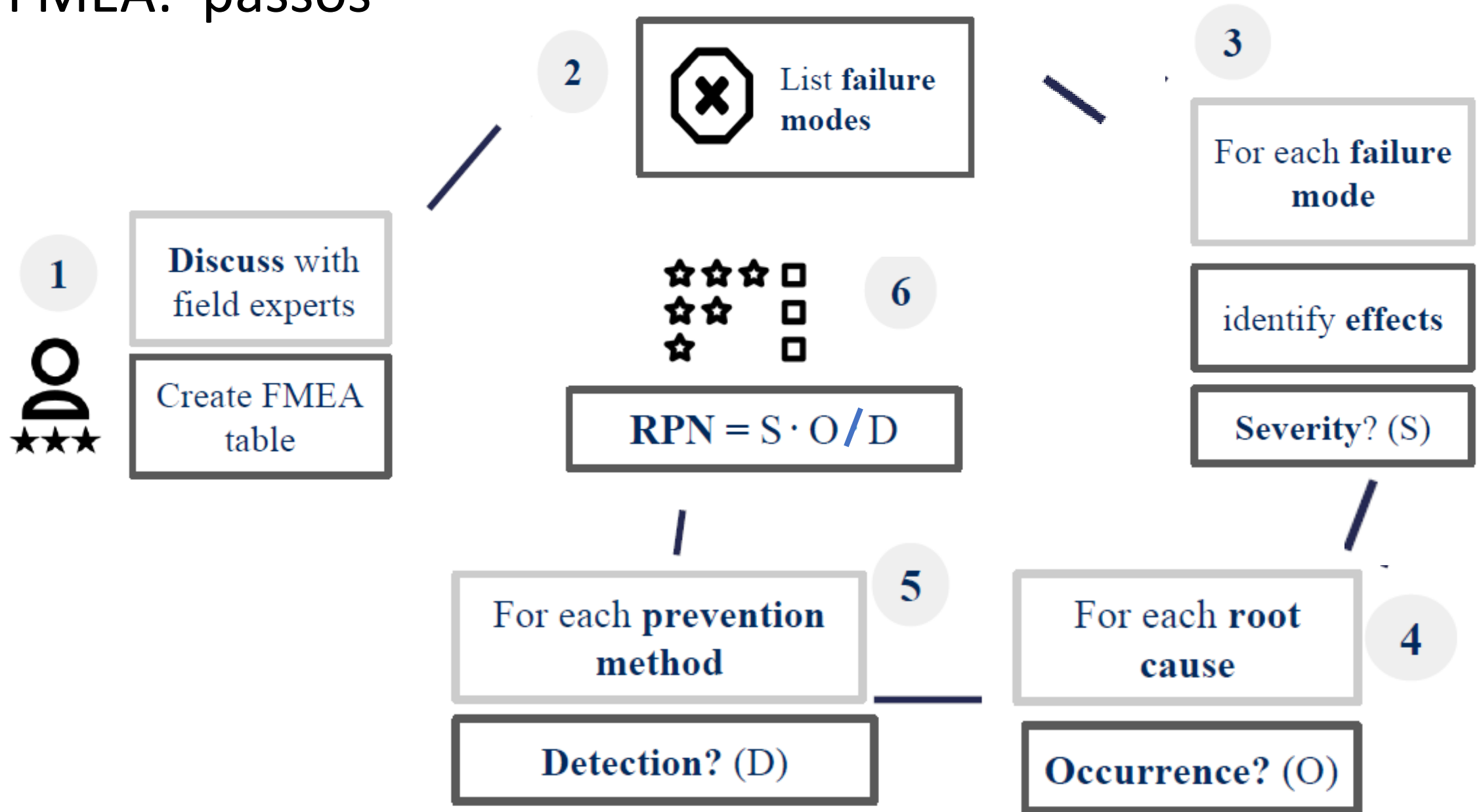
FMEA: qual a ideia?

- Categorizar os modos de falha por prioridade segundo:
 - Quão sério são os efeitos resultantes?
 - Quão frequentemente elas acontecem?
 - Quão facilmente elas podem ser detectadas?



- Eliminar ou reduzir falhas, começando por aquelas com maior prioridade

FMEA: passos



FMEA: Exemplo

- Vamos considerar o seguinte modo de falha:
 - Foi detectada uma falha grave no controlador
 - Severidade: colisão física ($S = 10$)
 - Ocorrência: ($O = 4$)
 - Detecção: ($D = 0,1$)
 - Número de prioridade do Risco: $RPN = (10 \times 4) / 0,1 = 400$

FMEA: Exemplo

- Similarmente pode se analisar outros modos de falhas:
 - Falha de percepção do sinalização: RPN = 100
 - Falha de sincronização do GPS: RPN = 300
 - Predição incorreta da predição de movimento: RPN = 150
- Lista final de RPN:
 - Falha de controle
 - Falha de GPS
 - Predição de movimento
 - Percepção da sinalização

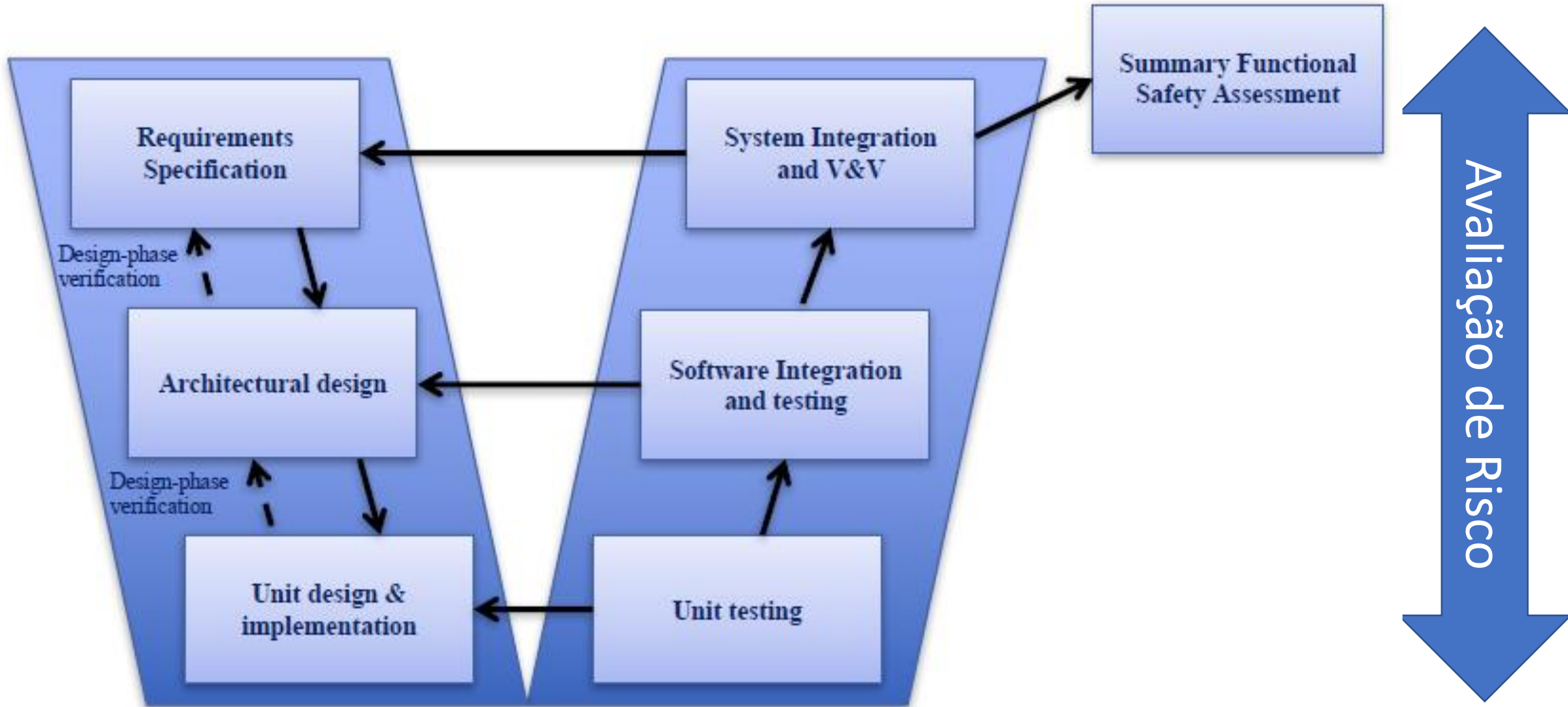
HAZOP – uma variação do FMEA

- Estudo de perigos e riscos (hazard) e da operabilidade
- Processo de brainstorming qualitativo, requer imaginação
- Usa palavras guias como gatilho do brainstorming (não, mais, menos)
- É aplicado para processos complexos
 - Informações suficientes de projeto são disponíveis, e que não estão sujeitos a mudanças significativas.

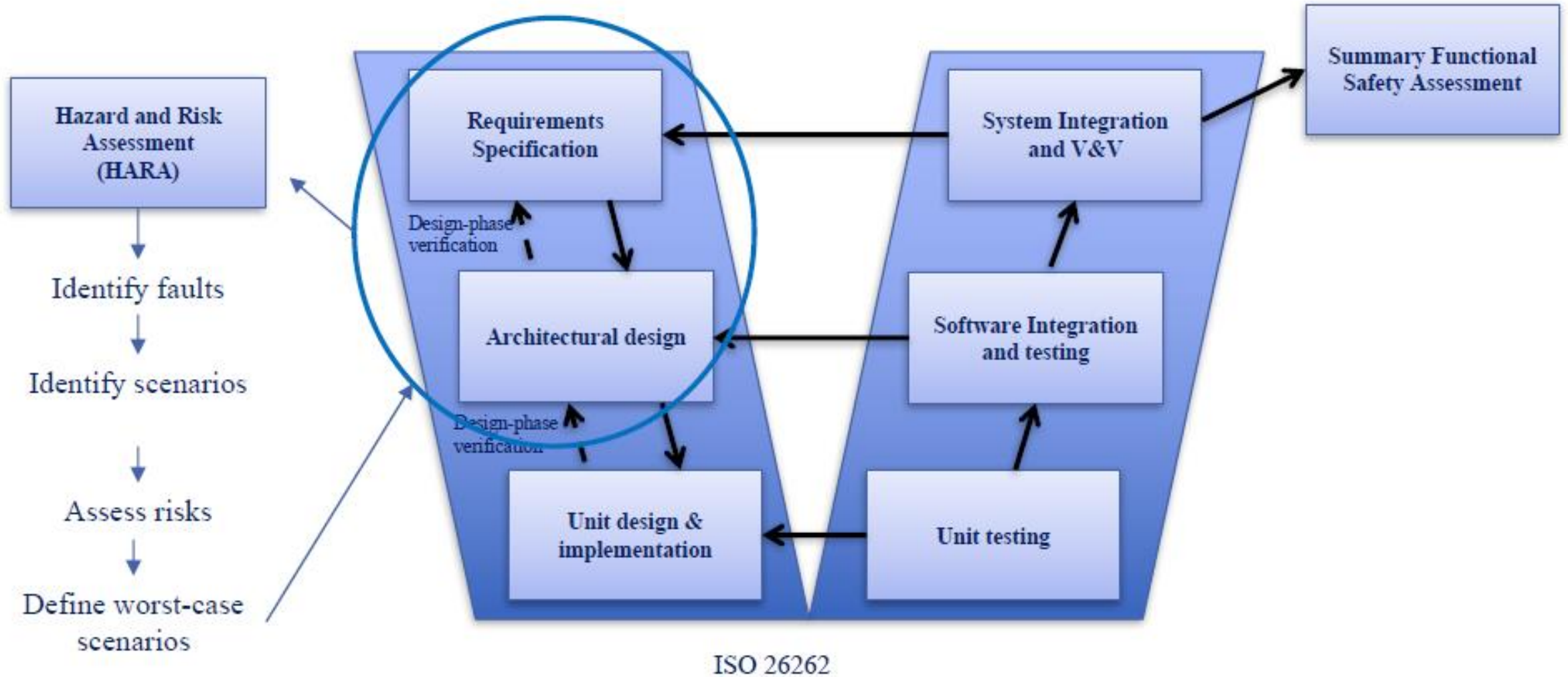
Frameworks automotivo de segurança

- ISO 26.262 – Functional Safety Standard
- ISO/PAR 21.448-1 – Safety of Intended Functionality
- A segurança funcional é definido como:
 - Segurança devido à ausência de risco não razoável
 - Preocupação com a segurança relacionada com o mal funcionamento do sistema
- ISO 26.262 define Níveis de Integridade de Segurança Automotiva (ASIL):
 - ASIL-D (mais rigoroso), ASIL-A (moderado)

Processo de Segurança Funcional – V model



Processo de Segurança Funcional – V Model

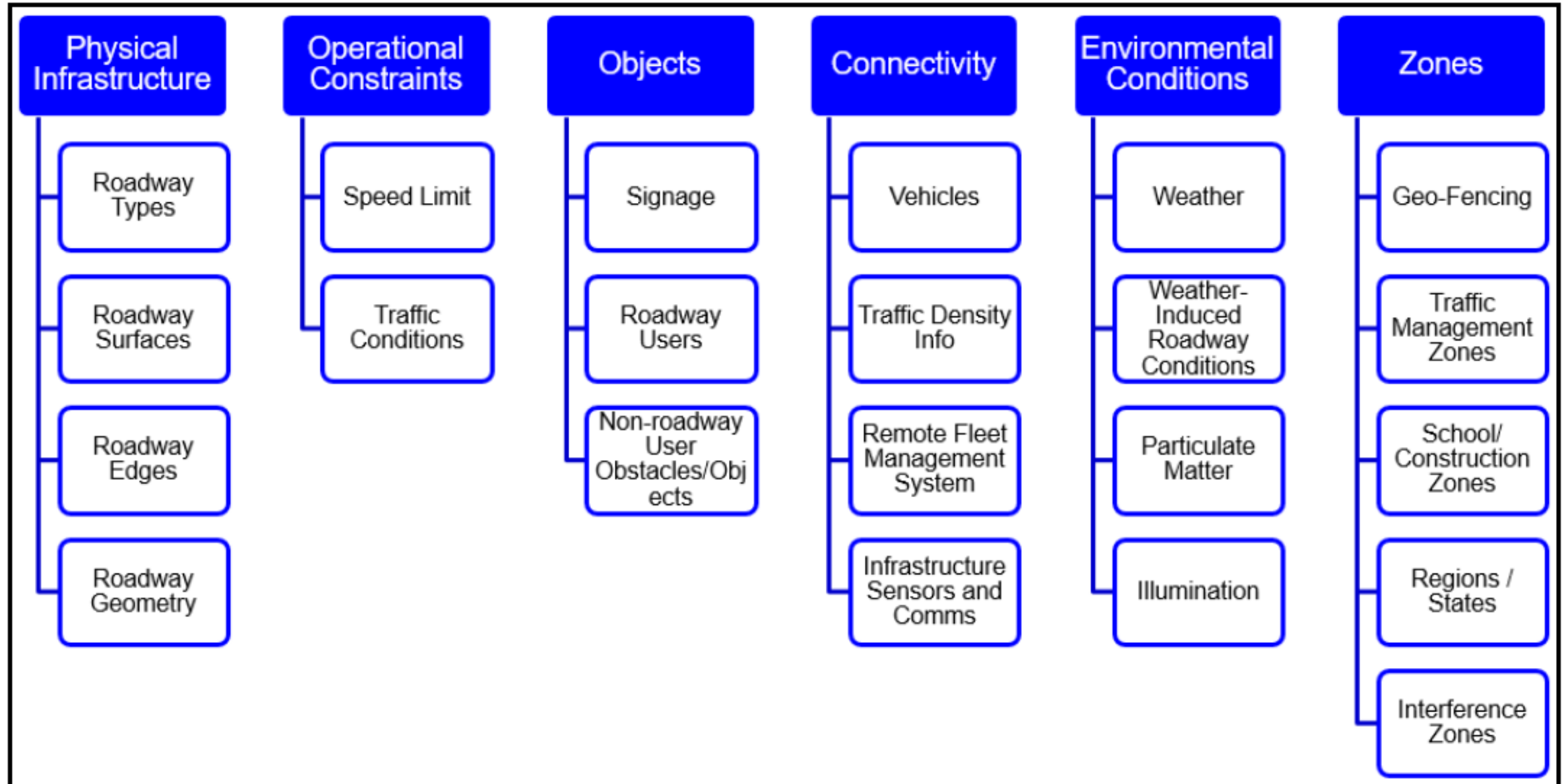


Documentos de referência

US DoT federal policy framework for autonomous vehicle
Autonomous Driving Systems 2.0: A visio for safety

- 12 elementos de projeto de segurança

Classificação de ODD



Estratégias de mitigação de falhas

- Com base nos modos de falha identificados, respostas e estratégias potenciais do modo de falha são identificadas.
- Esse esforço concentra-se nas estratégias de **falha segura** (FS) para os casos em que o ADS não pode continuar em operação devido a uma falha significativa e
- nas estratégias de **falha operacional** (FO) para os casos em que o ADS poderia continuar em operação mesmo diante de uma falha.

Mecanismos de falha segura (FS)

O objetivo principal de uma estratégia de FS é alcançar rapidamente uma condição de risco mínimo (MRC) onde o veículo e os ocupantes estejam seguros.

Três candidatos a mecanismos de FS podem ser considerados:

- Passagem do controle para o usuário pronto para *fallback*
- Parada com segurança na faixa de rolamento
- Saída com segurança da faixa de rolamento e parada no acostamento

Mecanismos de falha operacional (FO)

As estratégias de FO permitem que o ADS continue funcionando, mesmo no caso de uma ou mais falhas. É importante observar que esta operação pode ser suportada apenas por um período limitado ou potencialmente com um conjunto reduzido de recursos. Três mecanismos primários de FO podem ser considerados:

- Redundância de hardware e software
- Compensação adaptativa
- Operação degradada:
 - Redução de velocidade máxima
 - Redução do nível de automação
 - Redução de ODD
 - Redução da capacidade de manobra
 - Redução da capacidade OEDR

Redundância de hardware e software

- A integração de hardware ou software redundante é uma estratégia de projeto que prevê *backups* para peças críticas de equipamentos ou processos lógicos.
- Por exemplo, várias ECUs executando o mesmo algoritmo de controle de direção podem ser instaladas em um ADS. Caso a ECU primária sofra uma falha de hardware, um mecanismo lógico poderá acionar o sistema para começar a responder às saídas da ECU secundária.
- Essa estratégia pode melhorar a confiabilidade e a robustez do ponto de vista operacional, de modo a permitir que o ADS continue funcionando.
- No entanto, essa estratégia aumenta o custo, a complexidade e, potencialmente, o "espaço ocupado" do recurso ADS (por exemplo, precisa de energia e cabeamento adicionais, ocupa espaço adicional).

Compensação adaptativa

- A compensação adaptativa permite que um subsistema ADS compense uma falha em um ou mais componentes, confiando mais em outros componentes ou processos complementares, se disponíveis.
- Por exemplo, se um receptor de GPS sofrer uma falha de hardware e fornecer dados ruidosos ou intermitentes, o sistema de estimativa de estado poderá potencialmente reduzir o peso dos dados do GPS e aumentar o peso de outros sensores disponíveis (por exemplo, IMU, sensores de velocidade das rodas) e continuar a fornecer uma solução robusta e filtrada.
- Essa estratégia pode funcionar particularmente bem para subsistemas que já fazem a fusão de dados de várias fontes (por exemplo, percepção e localização), embora possivelmente não para outras.
- Também é possível que essa técnica de compensação seja eficaz apenas por um período limitado de tempo (por exemplo, o desvio do estimador de estado pode fazer com que o veículo perca a noção de sua posição absoluta ao longo do tempo se o GPS ou outros dados absolutos não forem adquiridos).

Relatórios de Avaliação de Segurança

<https://www.nhtsa.gov/automated-driving-systems/voluntary-safety-self-assessment>

United States Department of Transportation

Search

NHTSA
NATIONAL HIGHWAY TRAFFIC SAFETY ADMINISTRATION

Ratings Recalls Risky Driving Road Safety Equipment

← AUTOMATED DRIVING SYSTEMS

Voluntary Safety Self-Assessment

Company VSSA Disclosures

- [Apple](#)
- [Aurora](#)
- [AutoX](#)
- [Ford](#)
- [GM](#)
- [Ike](#)
- [Mercedes-Benz/Bosch L4-L5](#)
- [Mercedes Benz L3](#)
- [Navya](#)
- [Nuro](#)
- [Nvidia](#)
- [Robomart](#)
- [Starsky Robotics](#)
- [TuSimple](#)
- [Uber](#)
- [Waymo](#)
- [Zoox](#)

Análise do Relatório de Avaliação de Segurança da Waymo

Waymo Safety Reports



Waymo Safety Report
On the Road to Fully Self-Driving

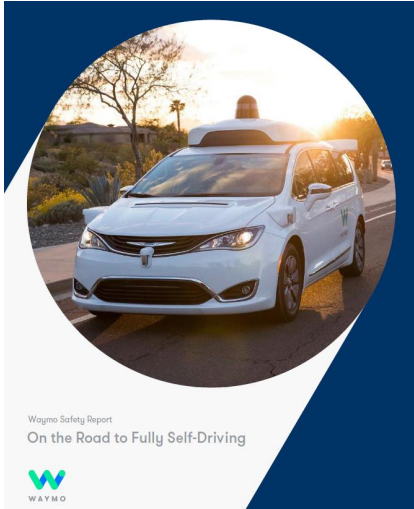


WAYMO

- Safety by design
- Nível dos sistemas, etapas de desenvolvimento, design, testes e validação
- MIL-STD-882E e ISO 26262
- Redundância dos sistemas críticos de segurança
- Capacidade para uma parada segura em caso de evento de falha de componentes do sistema
- Uso de sensores complementares com sobreposição de campos de visão (FoV)
- Extensivo programa de testes
- 5 áreas: behavioral safety, functional safety, crash safety, operational safety, non-collision safety.

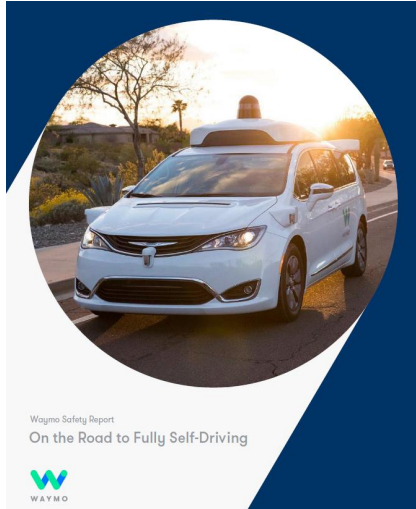
1. *Behavioral Safety:*

Refere-se decisões e comportamento de condução na via. O VA está sujeito às mesmas leis de trânsito que os motoristas e deve ser capaz de navegar de forma segura em uma variedade de cenários esperados e não-esperados. Utiliza uma combinação de análises funcionais, ferramentas de simulação e testes na via para adquirir o domínio sobre o domínio de operação de projeto (ODD) para desenvolver os requisitos de segurança.



2. *Functional Safety:*

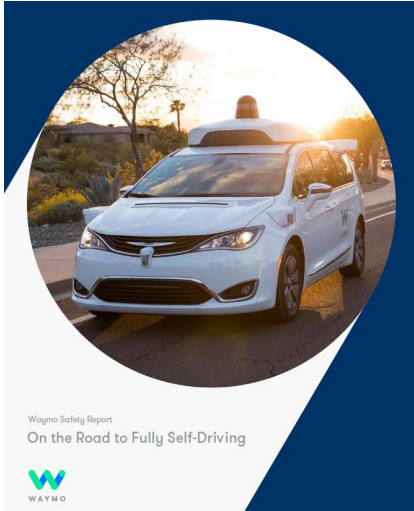
Busca garantir que o veículo continue operando de forma segura mesmo quando ocorrer uma falha no sistema. Isto significa que o sistema possui elementos reservas ou redundâncias para tratar situações inesperadas. O VA está equipado com computador secundário que assume a função quando da falha do computador principal, conduzindo o veículo para uma parada segura (condição de mínimo risco). Possui sistema de direção e frenagem redundante, além de várias camadas de redundâncias em todo o sistema.



3. *Crash Safety:*

Refere-se à habilidade do veículo em proteger o passageiro dentro do veículo por meio de uma variedade de medidas, incluindo projeto estrutural, ajuste de tensão do cinto de segurança e airbag para mitigar a lesão ou prevenir o óbito.

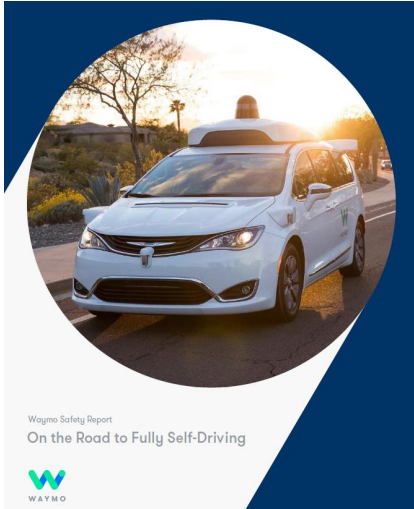
- Certificação do Federal Motor Vehicle Safety Standards (FMVSS)



4. *Operational Safety:*

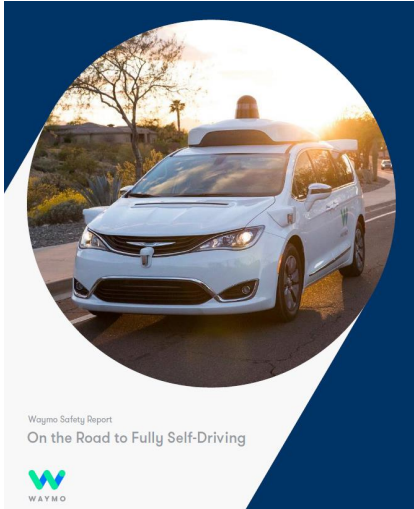
Refere-se à interação entre o veículo e o passageiro do VA. A abordagem adotada para a construção de um produto seguro baseia-se na Análise de Riscos e Perigos (Hazard Analyses), normas de segurança, testes extensivos, e melhores práticas da indústria.

- Testes com o interface de usuário incluindo:
 - Indicação do destino
 - Encostar o veículo
 - Contato com o suporte técnico da Waymo



5. *Non-collision Safety:*

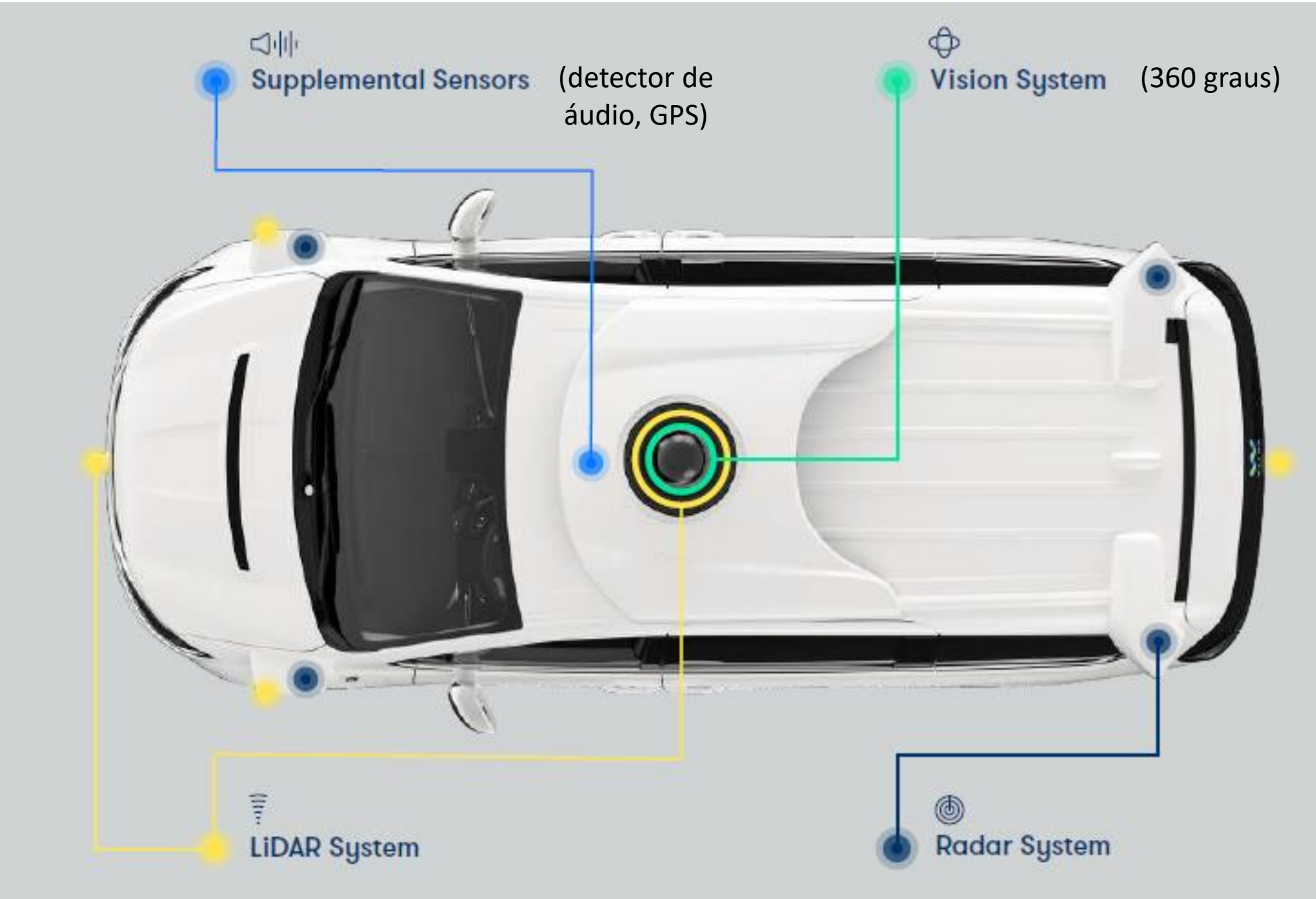
Refere-se à segurança física de todas pessoas que podem interagir com o veículo. Por exemplo, inclui problemas com os sistemas elétricos ou sensores que possam causar danos aos ocupantes, técnicos automotivos, motoristas de testes, socorristas ou curiosos.



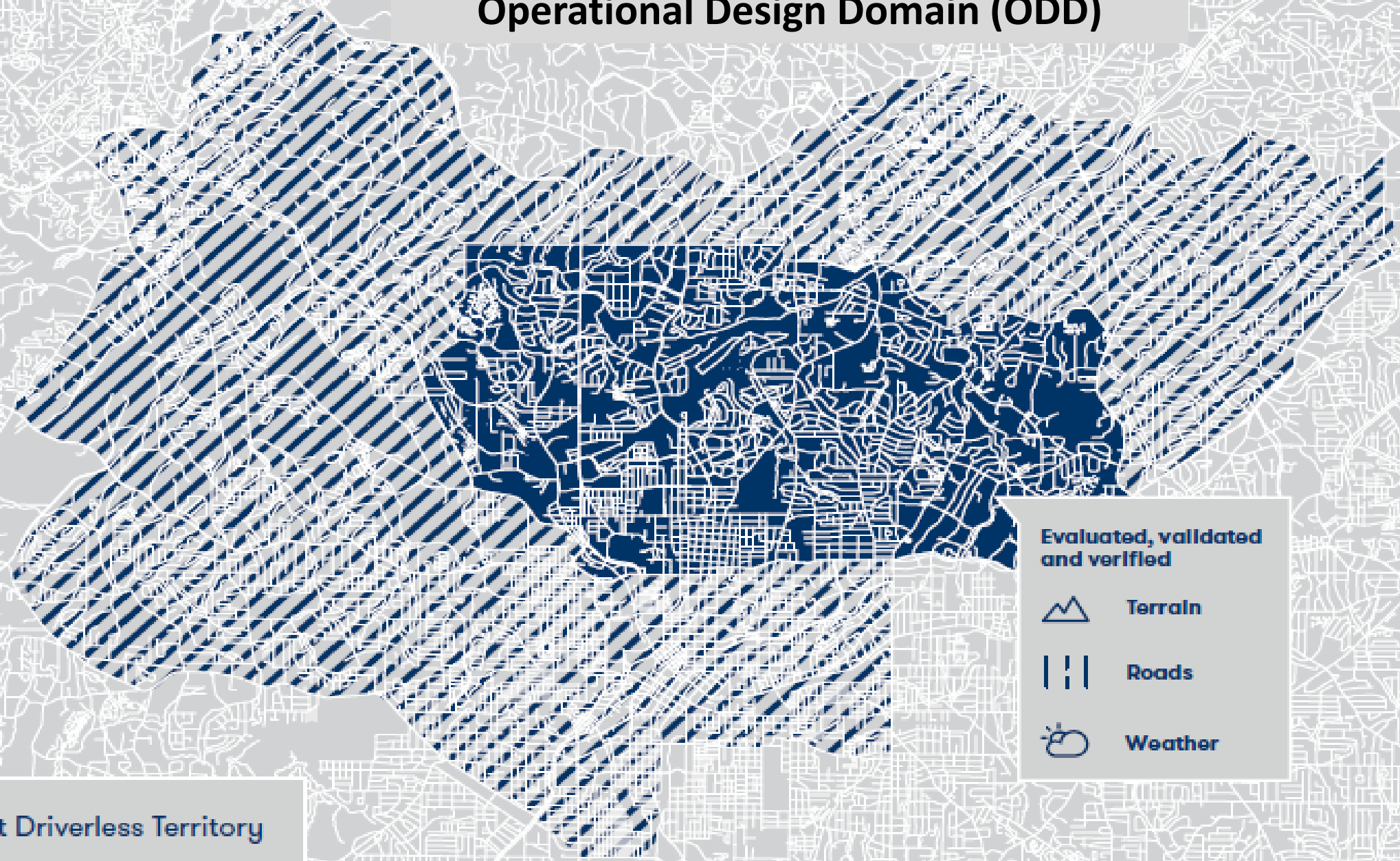
Processo de Segurança



- Estabelecer requisitos de segurança que reduza os potenciais riscos e perigos de acidentes, capturando-os internamente e tratá-los no projeto, e então validar para demonstrar que o risco de segurança foi reduzido para o nível identificado na análise.
- Requisitos de segurança de hardware e software; recomendações de projeto; e procedimentos de controle
- Métodos empregados: *preliminary hazard analysis, fault tree, and Design Failure Modes and Effects Analyses (DFMEA)*







Operational Design Domain (ODD)



-  Current Driverless Territory
-  Future Expansion Area

- Evaluated, validated and verified
-  Terrain
 -  Roads
 -  Weather

Abordagem de segurança do Waymo

1

Build Verifiable Software and Systems

2

Encrypt and Verify Channels of Communication

3

Build Redundant Security Measures for Critical Systems

4

Limit Communication Between Critical Systems

5

Provide Timely Software Updates

6

Model and Prioritize Threats

Testes e Validação

O VA consiste de três subsistemas primários:

- **O veículo base:** certificado pelo OEM (Fiat Chrysler - FCA)
- **O hardware:** fabricação própria, incluindo sensores e computadores
- **O software de direção autônoma** toma as decisões de condução do veículo

Testes de hardware do VA:

- Realizados em colaboração entre Waymo e FCA



Testes de software do VA:



Testes de simulação

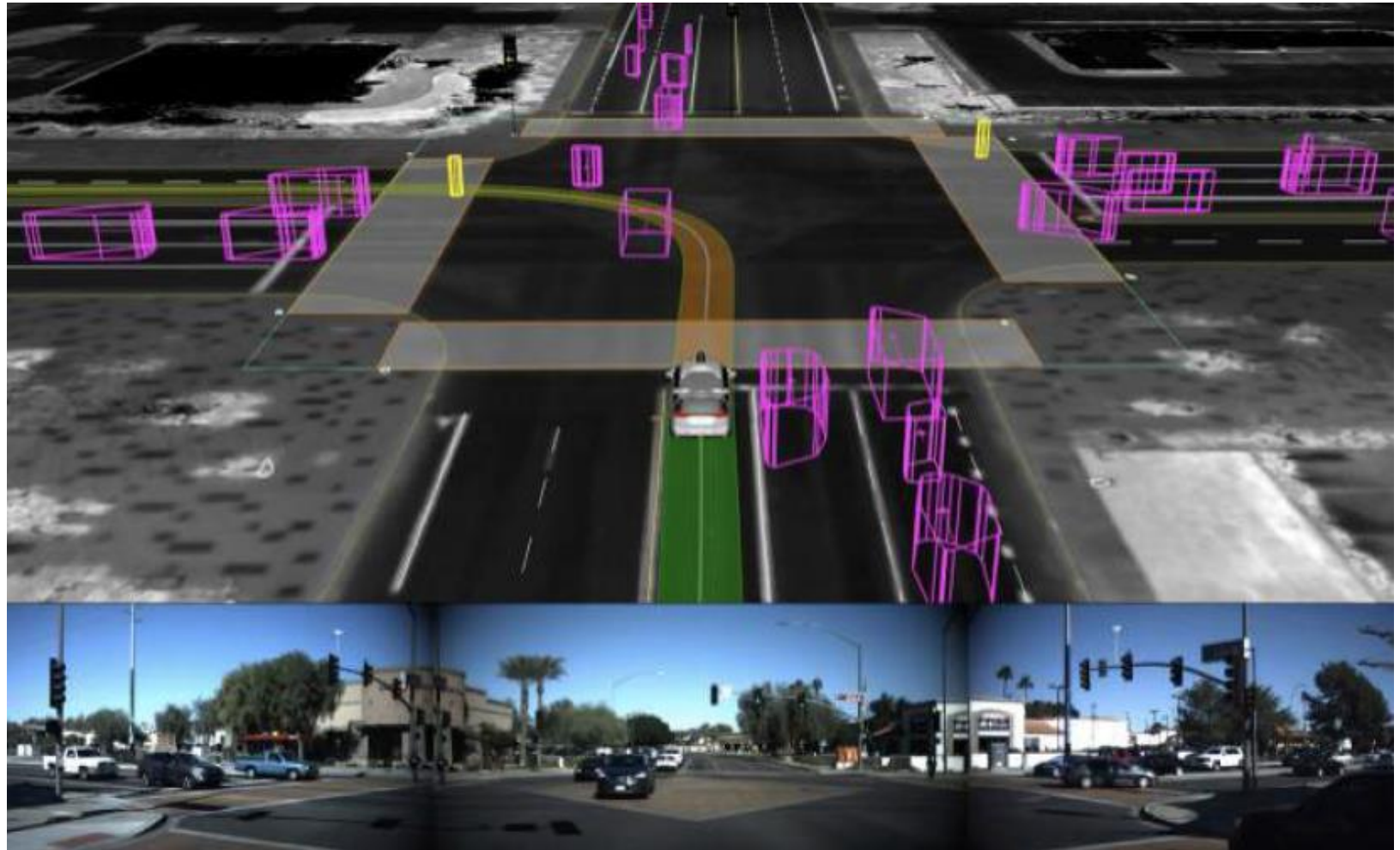


Testes em percursos fechados
(pistas de testes)



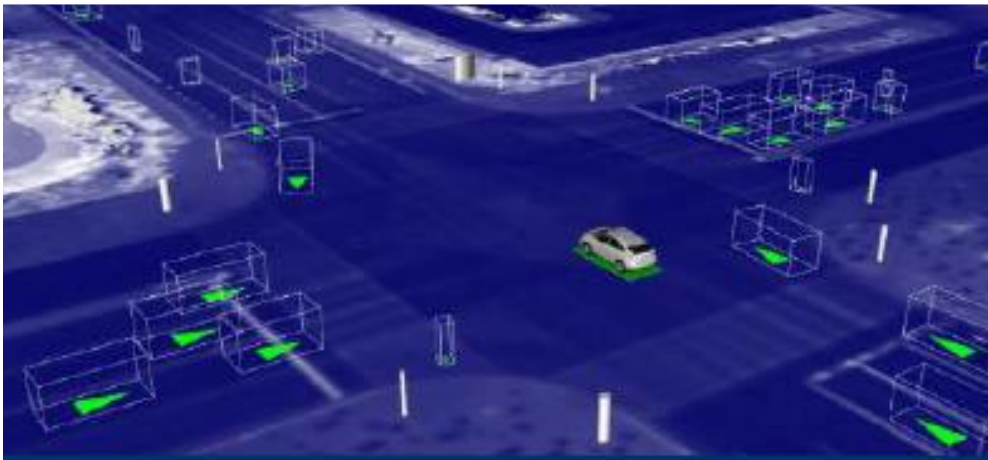
Testes de condução no mundo real
(vias públicas)

Simulação: o mundo virtual ajuda os carros a aprenderem as habilidades para dirigirem no mundo real



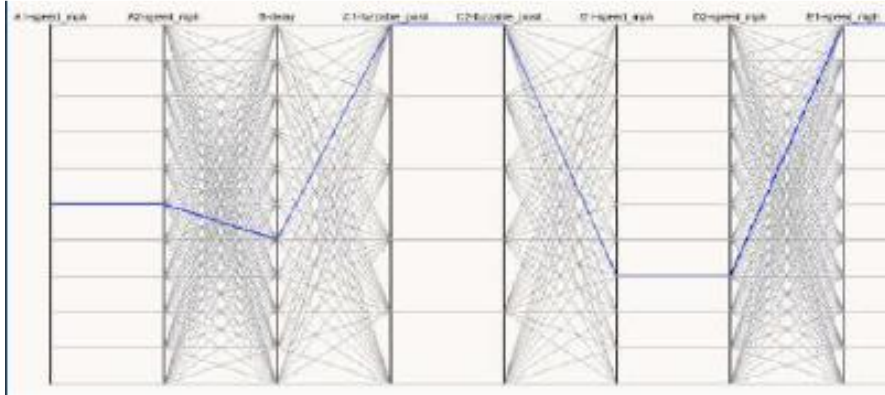
Por dia, 25 mil veículos autônomos realizam viagens virtuais percorrendo 13 milhões de quilômetros

Como é realizado a simulação?

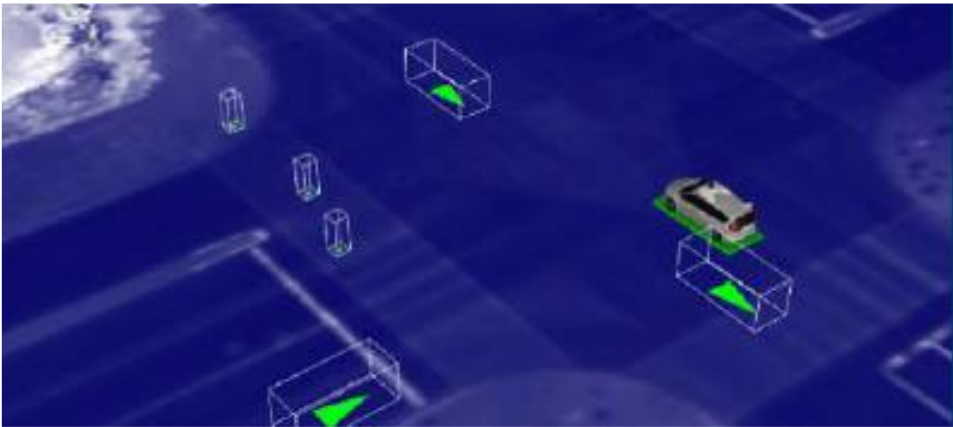


- **Passo 1:** construção de uma visão altamente detalhada e realística do mundo
- **Passo 2:** dirigir dentro do cenário digital milhares e milhares de vezes, treinando a habilidade do veículo em dirigir.

Com a simulação o veículo pode praticar a passagem na mesma intersecção milhares de vezes, com veículos da frota.



Usando um processo fuzzy, pode-se alterar a velocidade, trajetória, e posição dos objetos dessa avenida virtual



Para tornar o cenário mais complex, pode-se adicionar veículos, pedestres e ciclistas que não existiam no cenário original.

- **Passo 3:** criar milhares de variações da condição de tráfego.
 - Cria-se novos cenários para testar casos de “o que fazer se?”.
 - Alterando-se a velocidade dos veículos concorrentes e temporização dos semáforos pode-se assegurar que o veículo é capaz de encontrar uma lacuna segura no tráfego.
 - O cenário pode se tornar carregado e complexo adicionando pedestres, motocicletas ou veículos em zigue-zague.



Testes em circuitos fechados (pista de teste)

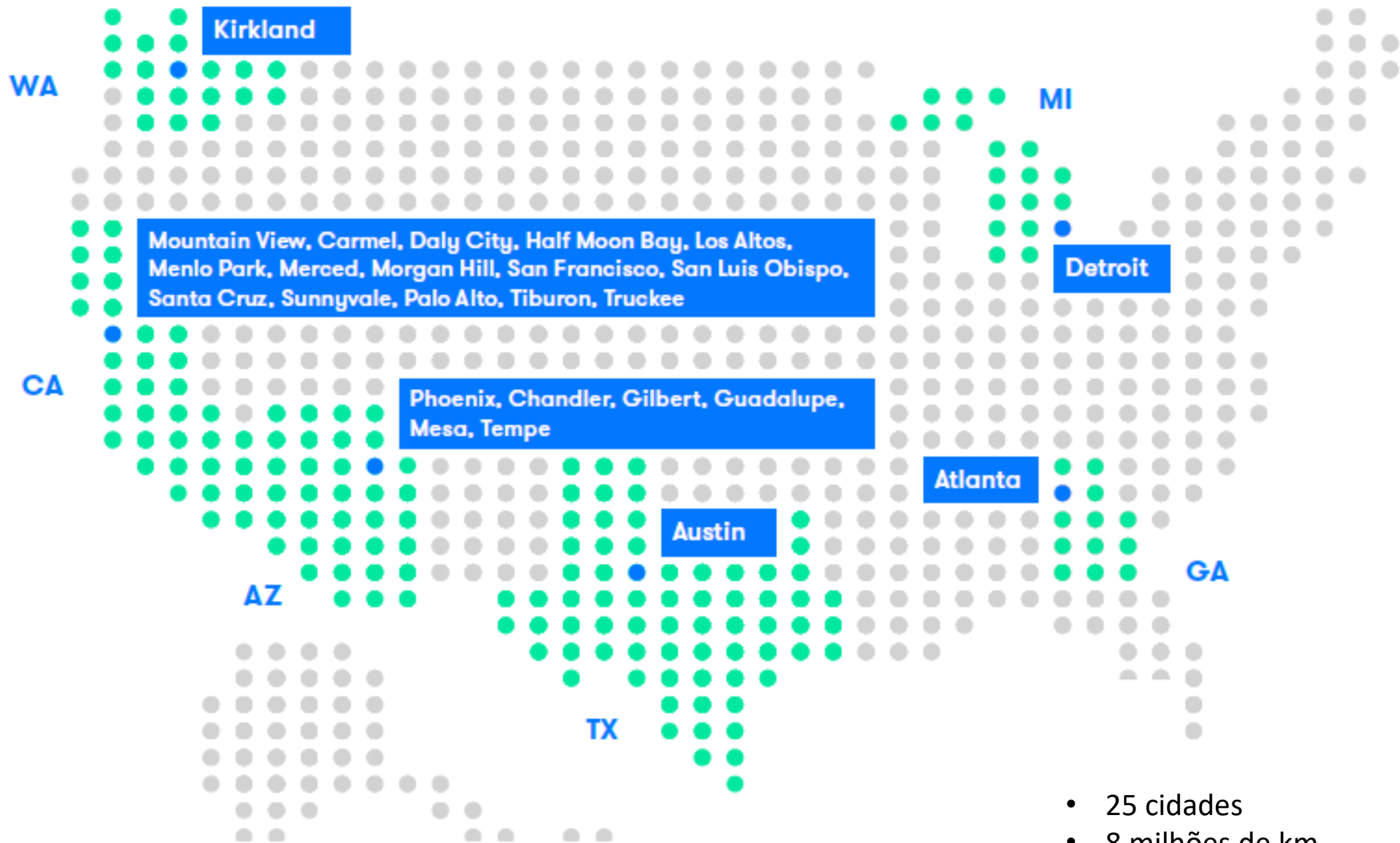


Testes em vias públicas

- **Passo 4:** Validar e repetir o ciclo
 - Uma vez que o VA aprendeu como atravessar ou fazer uma conversão num cruzamento no mundo virtual, vai-se a campo para testar e validar a nova habilidade.
 - Uma nova habilidade aprendida passará a fazer parte de uma base permanente de conhecimento. E, será compartilhada por todos os veículos da frota.

Testes em vias públicas





- 25 cidades
- 8 milhões de km



Reflexões

- A condução autônoma pode ser resumida em três etapas: 1) sensoriamento; 2) planejamento e 3) ação
- Por trás existem hardwares sofisticados e software de navegação extremamente complexo.
- Bancos de dados de simulação e de dados de campo, gigantescos, estão sendo construídos pelas empresas que estão desenvolvendo os veículos autônomos.
- A simulação realística é uma ferramenta importante no processo de desenvolvimento. A Waymo tem uma frota virtual de 25 mil veículos rodando 8 milhões de milhas/dia.