Escola Superior de tecnologia e Gestão

Instituto Politécnico da Guarda

Engenharia Informática 2020

Segurança de veículos autônomos, um desafio interdisciplinar

Trabalho elaborado no âmbito da unidade curricular de Inteligência Artificial

Nome: Vagner Bom Jesus

Professor: Celestino Pereira

Sobre:

Garantir a segurança de veículos totalmente autônomos requer uma abordagem multidisciplinar em todos os níveis de hierarquia funcional, de tolerância a falhas de hardware, aprendizado de máquina resiliente e cooperação com humanos dirigindo veículos convencionais, para sistemas de validação para operação em sistemas altamente desestruturados ambientes, às abordagens regulatórias apropriadas. Desafios técnicos abertos significativos incluem validar a aprendizagem indutiva em face de novos insumos ambientais e atingir níveis muito elevados de confiabilidade necessária para implantação de frota em grande escala. No entanto, o maior desafio pode estar na criação de um projeto ponta a ponta e processo de implantação que integra as preocupações de segurança de uma miríade de especialidades técnicas em uma abordagem unificada.

Introdução:

Uma previsão típica do futuro dos veículos autônomos inclui pessoas sendo aliviadas do estresse de dirigir diariamente, talvez até tirar uma soneca no caminho para o trabalho. Espera-se que seja acompanhado por uma redução dramática nas mortes ao dirigir devido à substituição de motoristas humanos imperfeitos por (presumivelmente) pilotos automáticos computadorizados melhores. A questão não é se os veículos autônomos serão perfeitos (eles não serão). A questão é quando nós vamos ser capazes de implantar uma frota de sistemas de direção totalmente autônomos que são realmente seguros o suficiente para sair humanos completamente fora do circuito de condução.

"Seguro" significa pelo menos a implementação correta de comportamentos no nível do veículo, como obedecer às leis de trânsito (que pode variar dependendo da localização) e lidar com os perigos não rotineiros da estrada, como linhas de energia derrubadas e inundações. Mas também significa coisas como planejamento de missão, encontrar uma maneira de validar estratégias de aprendizagem com base indutiva, proporcionando resiliência em face de prováveis lacunas na implementação inicial requisitos do sistema, e ter uma estratégia de certificação de segurança adequada para demonstrar que um nível suficiente de segurança foi realmente alcançado.

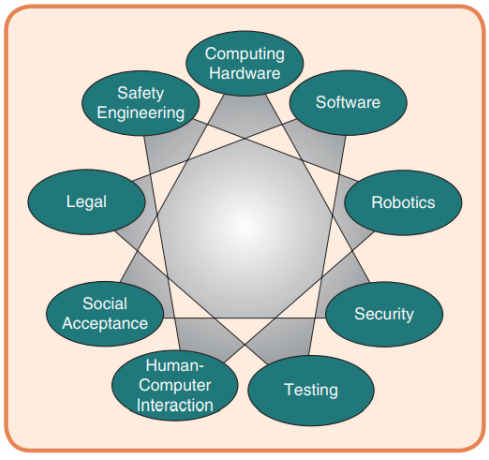

Figura 1. Muitas áreas diferentes requerem uma abordagem coordenada e interdisciplinar para garantir a segurança.

Engenharia segura:

O desafio torna-se gerenciamento de falhas que são muito raros para qualquer veículo, mas vai acontecer com muita frequência ser aceitável à medida que a exposição aumenta a milhões de veículos em uma frota.

Uma preocupação significativa de certificação de segurança é validar qualquer uso por veículos autônomos de sistema auto-adaptativo comportamento. Adaptação irrestrita como como aprendizagem em tempo real de novos comportamentos que um veículo pode ter um comportamento diferente durante a operação do que foi exibido durante o teste e certificação. As abordagens de certificação atuais são essencialmente incapazes de lidar com essa situação, porque exigiam considerando todos os comportamentos possíveis do sistema antecipadamente no processo de projeto e validação. A menos que os limites sejam de alguma forma colocar em adaptação e totalmente explorado durante o projeto do sistema, pode ser impossível garantir a segurança de tal sistema em tempo de design porque o sistema que está sendo testado não terá o mesmo comportamento de um sistema adaptado que é implantado.

Robôs ultraconfiáveis:

Fazendo sistemas autônomos (que são robôs) funcionarem em uma ampla variedade de situações de direção cotidianas, como sempre feito nos protótipos atuais é uma conquista verdadeiramente significativa e impressionante. Uma série de desafios para alcançar o ultra-confiáveis veículos autônomos surgirão, começando com a melhoria robustez do sistema para situações ambientais complicadas (por exemplo, lidar com detritos, desordem e ruído do sensor). No geral, parece implausível projetar um sistema que pode lidar com todas as situações ambientais possíveis perfeitamente, especialmente nos estágios iniciais de implantação de uma frota.

Em outras palavras, esses sistemas precisam ser capazes de auto-monitorar sua confiança em sua própria operação adequada e ser muito bom em saber quando eles não sabem o que está acontecendo. Será difícil conseguir uma deteção confiável de degradação do sistema. Uma alta taxa de falsos negativos levará a veículos operando involuntariamente em um local inseguro maneira. Mas uma alta taxa de falsos positivos deixará muitos carros encalhado na beira da estrada devido a um falso alarme cibernético (com sorte, após ter executado uma missão de segurança bem-sucedida em resposta à falha de autonomia).

Software:

Segurança de software é um tópico de pesquisa de longa data. Dizer que o sistema é seguro porque sua precisão em um conjunto de validação é suficientemente alta levanta a questão de se o sistema realmente funcionará como precisa quando confrontado com a confusão do mundo real.

O que realmente importa é que o conjunto de validação de aprendizado de máquina deve ser abrangente o suficiente para garantir que não há lacunas no comportamento do sistema. O conjunto de treinamento é o mais próximo que temos dos requisitos do sistema, e o conjunto de validação é o mais próximo que temos de um plano de teste. Mas, sabendo que o treinamento e validação conjuntos são bons o suficiente não é tão fácil. Afinal, segurança para tal sistemas, em última análise, dependem da precisão do treinamento e coleta de dados de validação

Hardware Informático:

A razão para isso é que não diagnosticada falhas podem se acumular por toda a vida útil do veículo, então a probabilidade de experimentar várias falhas independentes não diagnosticáveis durante a vida de um veículo é bastante alto em comparação com a probabilidade de várias falhas ocorrendo durante uma única missão de condução para diagnóstico partes do sistema. Assim, será importante criar chips que pode ser auto testado antes de cada ciclo de direção com um nível extremamente alto de cobertura de diagnóstico.

Testando:

O teste rigoroso de autonomia envolve vários problemas, compara um documento de design rigorosamente definido com um sistema para determinar se o sistema corresponde seu design e requisitos. Para sistemas probabilísticos como planejadores, espera-se que o comportamento do sistema seja diferente em cada teste executado, mesmo para condições iniciais essencialmente idênticas. Além disso, pequena mudança nas condições iniciais pode resultar em grandes mudanças no sistema comportamento. Outra dimensão do teste é a injeção e gerenciamento de falhas. Com a implantação de veículos em grande escala, vêm ocorrências diárias de falha do equipamento do veículo simplesmente devido ao grande número de veículos na frota.

Segurança:
A segurança da computação automotiva tem recebido cada vez mais atenção e não mostra sinais de se tornar um problema. Claramente, os veículos autônomos terão de lidar com segurança também.

Além de ataques a veículos específicos, as medidas de segurança precisarão abranger ataques e falhas no nível do sistema. Em particular, pode ser problemático confiar cegamente em a segurança de outros veículos ou até mesmo infraestrutura de beira de estrada ao realizar manobras autônomas otimizadas como tráfego de interseção de fluxo livre. No mínimo, parece prudente garantir que cada veículo autônomo tem a capacidade de perceber quando está sendo alimentado com informações externas incorretas ou maliciosas, detetar que um ataque está ocorrendo e realizar uma missão de segurança se não puder continuar a operação total em face do ataque.

Interação Humano-Computador:
À medida que os veículos autônomos suplantam os motoristas humanos, a capacidade da automação de se comunicar e cooperar com as pessoas se tornará mais importante. Os riscos de desatenção do supervisor humano em sistemas com quase - mas não totalmente – cheio a autonomia deve ser evidente. Mas mesmo totalmente autônomo veículos precisarão pelo menos se certificar de que o ocupante sentir que o comportamento do veículo é seguro se quiserem construir a confiança do cliente e precisarão aprender a antecipar o comportamento de outros veículos também.

Legal:
Um problema inicial significativo na implantação desses veículos será estar lidando com questões legais de responsabilidade. Quando um veículo totalmente autônomo está envolvido em um acidente, pode muito bem ser que o passageiro do veículo esteja justificadamente desatento (talvez até dormindo). Os registos de dados do veículo podem ser a principal fonte de informação disponível sobre o que aconteceu em um acidente. No entanto, o dado de um veículo com defeito não pode ser cegamente confiável. Afinal, se o veículo causou um acidente devido a um mau funcionamento, por que deveria presumimos que quaisquer dados desse sistema com defeito é preciso?

Aceitação social:

A aceitação social dos veículos autônomos, sem dúvida ser um processo complexo. O principal incentivo à adoção é a expectativa de que os veículos autônomos serão, em geral, motoristas mais seguros do que pessoas. no entanto é irrealista, especialmente no início, supor que isso irá significa zero percalços.

Conclusão:

No final, terá de haver uma estratégia de certificação de segurança de algum tipo para veículos totalmente autônomos. Esta estratégia deve abordar as preocupações interdisciplinares de segurança engenharia, confiabilidade de hardware, validação de software, robótica, segurança, testes, interação humano-computador, aceitação social e um quadro jurídico viável.