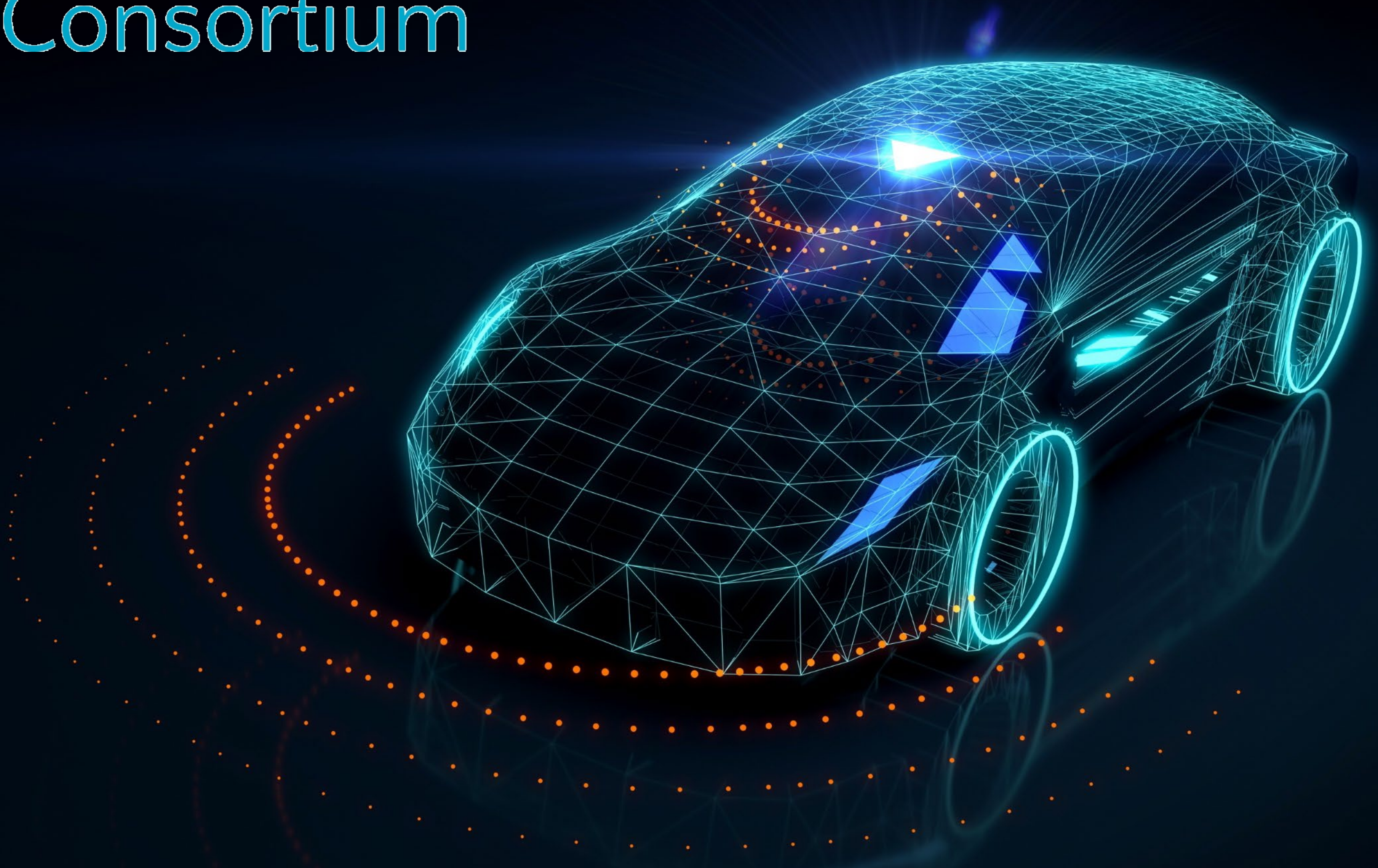
Teleoperation Consortium

Teleoperation Guidelines

Session 253 - Teleoperation for Automated Vehicle Operations

Teleoperation Consortium



The Industry's Forum for
Remote Operation of
Autonomous Vehicles

Scott McCormick

Agenda

- The Teleoperation Consortium
  - Scott J. McCormick, President and CEO, Teleoperation Consortium
- The Teleoperations Challenge
  - Stan Schneider, CEO, RTI, and Board Director, Teleoperation Consortium
- A Focus on Security
  - Chuck Brokish, Director of Automotive Business Development, Green Hills Software, and Board Director, Teleoperation Consortium
- The Evolution of Standards
  - Tao Zhang, PhD, Director of Business Development for Automotive and Transportation, NIST Board Liaison to the Teleoperation Consortium

Scott J. McCormick, President and CEO, Teleoperation Consortium

Scott has degrees in Mathematics, Mechanical and Aerospace Engineering, a Master's in Business Administration, and Doctoral Research in Artificial Intelligence. Prior to the Teleoperation Consortium, Scott was the first President of the VII Consortium and before that the Executive Director of the Automotive Multimedia Interface Collaboration, nonprofit research organizations of the world's largest automakers. Prior to 2000, Scott spent 25 years in aerospace as General Electric's and Williams International's Factory with a Future Program Manager for jet engines.

In March 2012 through 2020, Scott was appointed by the United States Congress to advise the Secretary of Transportation on matters relating to the study, development, and implementation of Intelligent Transportation Systems. In 2016 Scott was appointed as the Chief Transportation Consultant to the Asia Pacific Economic Community for the US State Department.

Scott created the 120 hour Connected Vehicle Professional Credentialing Program in 2015-2016 to help advance knowledge about the entire ecosystem. On June 7th, 2016 Scott was inducted into the Automotive Hall of Fame in Detroit, Michigan.

In 2020, Scott founded the Teleoperation Consortium at the request of the US National Institute of Standards and Technology and is the CEO and President. Scott is also the President of the Connected Vehicle Trade Association, founded in 2005 at the request of the world's largest automakers.

Stan Schneider

stan@rti.com
LinkedIn: Stan Schneider
Twitter: @RTIStan

- CEO Real-Time Innovations
  - Largest autonomy infrastructure software vendor
  - Transportation, Medical, Power, Defense, Industrial Control
- Consortia
  - Teleoperations Consortium board
  - Autonomous Vehicle Computing Consortium board
  - Former Vice Chair, IIC Steering Committee
  - Advisory Board, IoT SWC
- Top-25 Global IIoT Influencer
- PhD, EE/CS, Stanford

Chuck Brokish is the Director of Automotive Business Development at Green Hills Software.

He has over 30 years of experience in the embedded systems, in areas of mobile communications, automotive active noise control, infotainment, ADAS, and V2X.

He has been working on embedded security for over 25 years. Chuck is a registered Professional Engineer, has been active on advisory councils and industry forums and standards committees including ISO, SAE, IEEE, MIPI, and Global Platform.

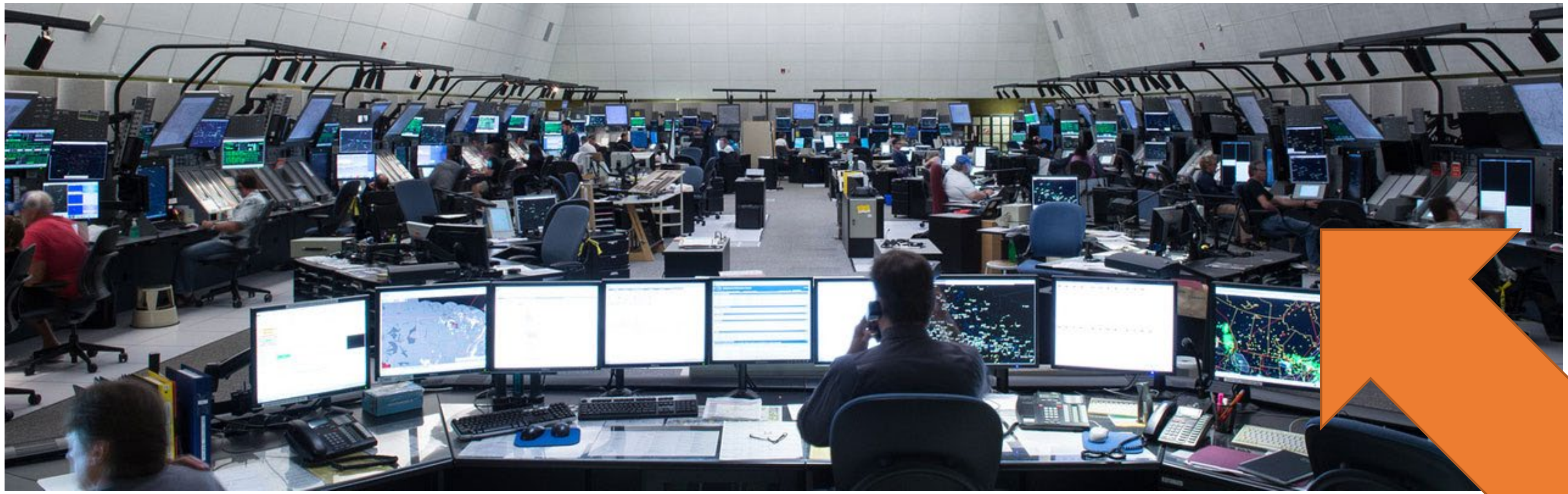
He has patents in the areas of Secure Processor design, Real-time Debug, Active Noise Control, and DSP architecture.

GHS is a founding Member of the Teleoperation Consortium and a Director of the Board.

Dr. Tao Zhang

- Leads Transformational Networks and Services Group in Communications Technology Lab at NIST
  - Advancing technology and standards in areas including automated driving and teleoperation, 6G networks, information-centric networking, cloud computing, edge/fog AI, and wireless localization
- Was CTO / Chief Scientist for the Smart Connected Vehicles business unit at Cisco Systems
- Was Chief Scientist and Director of Research at Telcordia Technologies (formerly Bell Communications Research)
- Cofounded the Open Fog Consortium and served as its founding Board Director
- Elevated to IEEE Fellow for contributions to wireless & infrastructure networking protocols for applications
- Holds ~60 US patents
- Coauthored 2 books ("Vehicle Safety Communications: Protocols, Security, and Privacy" and "IP-Based Next Generation Wireless Networks"), several book chapters, and over 100 peer-reviewed papers
- Served as the CIO and a Board Governor of the IEEE Communications Society and as a Distinguished Lecturer of the IEEE Vehicular Technology Society

What is Teleoperation?



- Teleoperation is the ability to remotely drive or assist a piloted or self-driving vehicle
- Teleoperation requires integrating sophisticated control software, AI-based models, ultra-low latency and reliable communications, and operational vehicle management

Vision: Teleoperation can greatly accelerate the development of safe and efficient mobility by combining remote human intelligence with local autonomous control.

The TC's vision is to foster practical autonomy by providing a forum for global industry, government, and research institutions to recommend approaches and develop an enabling ecosystem.

Mission: Evangelize teleoperation to enable higher autonomy sooner:

- Collaborate on research use cases, categorize approaches, and develop guidelines
- Examine safety, mobility and convenience issues
- Study government and commercial applications
- Identify opportunities for public and private sector participation in the ecosystem
- Maintain an ongoing dialog with public and private decision makers, and
- Educate industry on common issues and opportunities

Members Across Industry, Government, Academia

Corporate

- Autonebula
- Cogenia Partners
- Digital.ai
- Cognizant
- Green Hills Software
- IMS
- Intertek
- Mitsubishi Electric
- Phantom Auto
- RTI
- The Next Education
- VELN

Associate

- American Technology Solutions International Corp. (ATSI)
- Federal Express (FedEx)
- Geotab
- Harris Poll
- KPIT
- Mobile Video Computing Solutions
- Ottopia
- Underwriter's Laboratories

Startup

- 5GVector
- Auve Tech
- Dactle
- Designated Driver
- DriveU.auto
- Eli Technology
- Guident
- Important Safety Technologies
- Interpl.ai
- IP Gallery
- Kilroy Blockchain
- LiveRoad Analytics
- Park My Fleet
- Ridar Systems
- Roboauto
- SmartRemitt
- Strategic Market Services
- Zorya

Affiliate

- British Standards Institute
- Connected Vehicle Trade Association
- COVESA
- Swedish National Road and Transport Research Institute (VTI)
- SAE International

Public Entity

- National Institute of Standards and Technology
- Peach Tree Corners, Georgia
- Volpe Center

Academic

- Clemson University
- International Lisbon School of Engineering – Portugal
- Macomb Community College CAAT
- Royal Holloway, University of London
- Wayne State University

The Teleoperation Guidelines

- Terminology
- Use Cases
- Definition of Approach Categories
- System Software Architecture & Communications
- Key Concerns
- Security Considerations
- Relevant Standards

Teleoperation Consortium

Teleoperation Guidelines Abstract and Outline

June 16 2022 Draft

Teleoperation is a critical accelerator of the coming autonomous age.

Autonomy is progressing quickly across many aspects. Software and computing architecture, a relatively new demand for the automotive industry, is evolving by borrowing from autonomous systems in other industries. Safety, while far from perfect, will eventually meet or exceed human performance. In simple environments like freeways, autonomy will soon be safe and practical.

However, the problem is extremely complex. For many years to come, there will be situations that autonomous vehicles (AVs) can't understand. In these situations, AVs will require assistance. The roads cannot have stuck AVs blocking traffic whenever there is a construction

Goal: publish a Special Publication through the National Institute of Standards and Technology (NIST)

Goals/Objectives/Outputs

The goals of the session are:

- Increase awareness and understanding of Remote Assistance and Teleoperation for Automated Vehicle Operations;
- Share best practices, study results and updates on standardization activities;
- Gather input from the attendees on the Teleoperation Guidelines and Approach Categories that were developed (to be published as NIST special publication);
- Solicit input on relevant areas that guidelines should be developed for that the publication does not address;
- Identify research questions and future research needs.

Audience

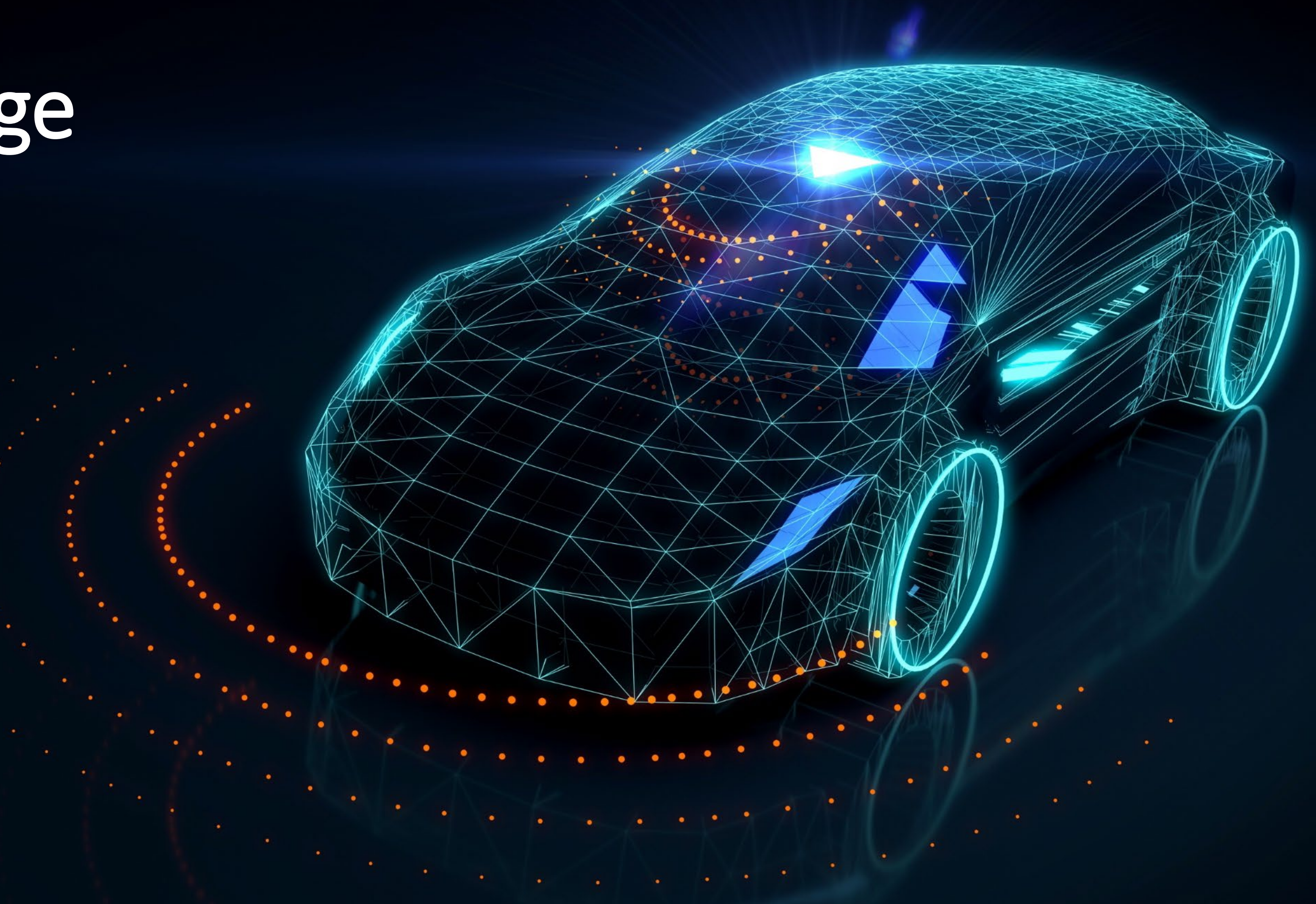
The goal of the Teleoperation Consortium's efforts is to publish this as a Special Publication through the National Institute of Standards and Technology (NIST), an Advisor and Liaison to the Board. The primary audience is industry developers and project managers seeking to implement increasingly autonomous vehicles for road use. The research community, including both industry and academic communities are a secondary audience.

Purpose of the Teleoperation Guidelines Committee

The Members of the Teleoperation Consortium are working to define important areas to address with regards to developing industry guidelines and approach categories.

- Terminology
- Use Cases
- Definition of Approach Categories
- System Software Architecture & Communications
- Key Concerns
- Security Considerations
- Relevant Standards

The Challenge



The Promise of Autonomy & the Need for Teleoperation

Stan Schneider

NUMBER ONE SOFTWARE FRAMEWORK FOR AUTONOMY

RTI enables intelligent systems by connecting AI algorithms to distributed devices

rti

250+ Autonomous vehicle designs

50% of top EV new entrants

40% of largest monitoring & imaging mfgs

~15 surgical robots; incl top 4 entrants

1800+ Designs

~300 Employees

400+ defense programs of record

Most US Navy ships

100s of distributed control systems

25% of N. America renewable power

Western grid balancing system


UMTRI
NT1032
32
NT1032
44

Problem: Getting There is Dangerous and Slow

We have an *obligation* to automate driving

Autonomy is a Matter of Degree

More Autonomy = More Time Without Help

Level 5

F utomation

control

to

ems

Level 4

be available for control

at any time

More Autonomy = More Data, More Complexity

Way More Software

most of the time

Driver expected to be available for occasional control with comfortable transition times

More than one control function is automated

Driver expected to be available for control at all times and on short notice

Level 1

Driver Assistance

Single control functions such as speed selection, braking or lane keeping are automated

Problem: ”Truly Autonomous” Isn’t

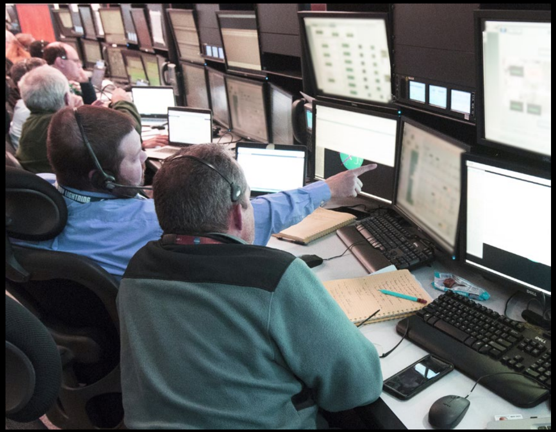
- Real-world autonomy is *hard*
  - Corner cases abound
  - Systems are *complex*
  - Things *change*
  - *Insight* is critical
- Safety cannot be delegated off board
- Connections *must* work
  - Secure
  - Real-time
  - Reliable (when needed)

Autonomy is too hard.
How can we make it work?

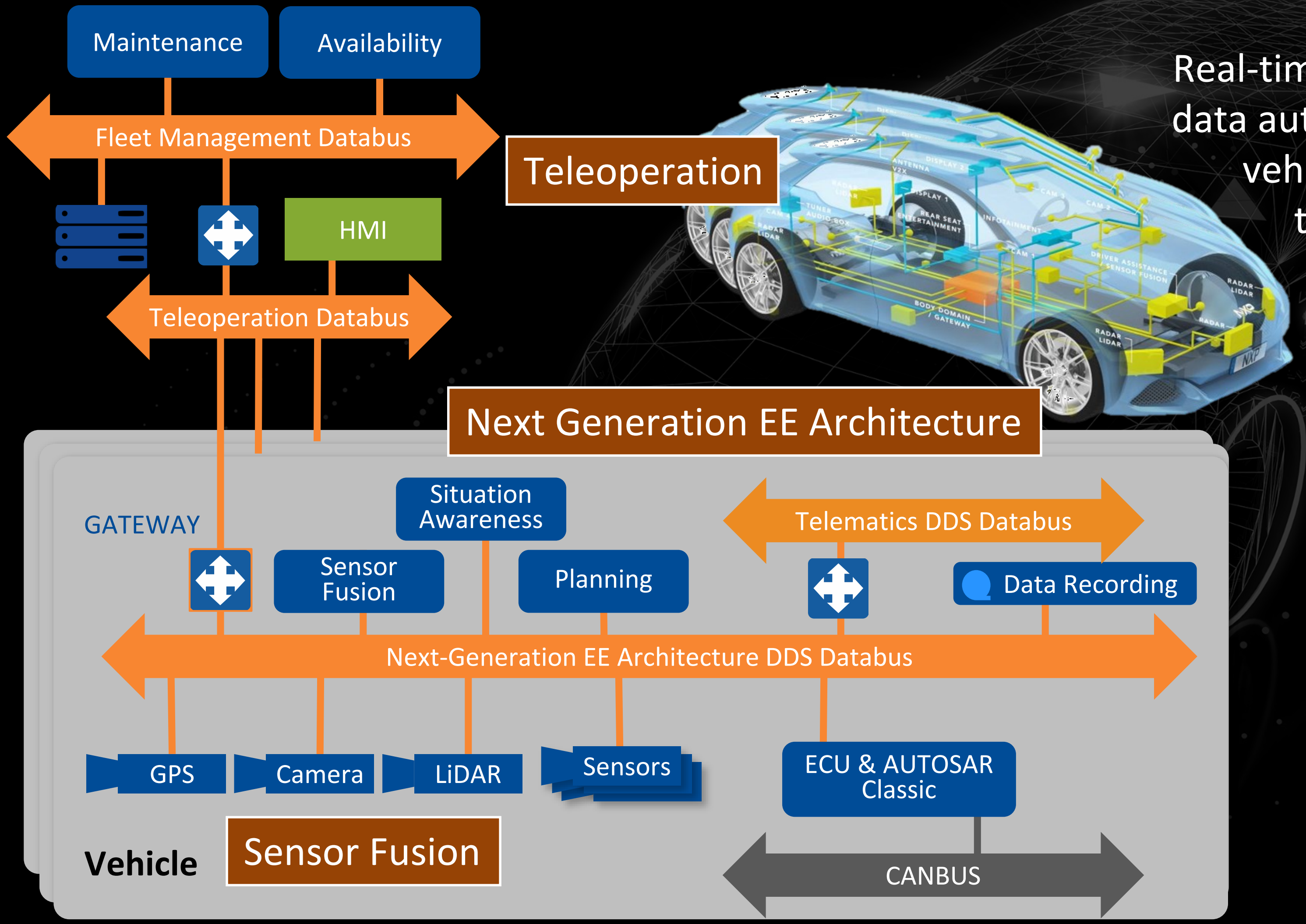
Autonomous Systems *Need* Remote Help

Connect Control Room to Sensor

Unified Data Model



Control rooms for real-time monitoring



Real-time reliable data autonomous vehicles need to operate

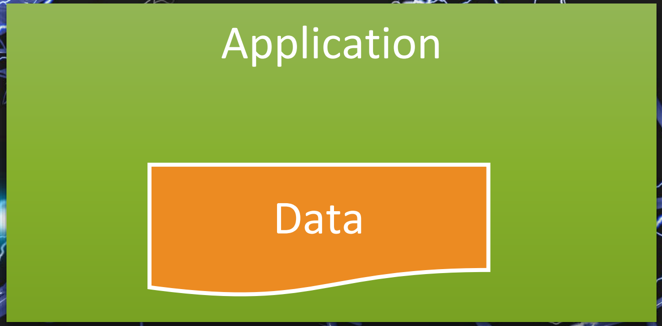
Multiple standards and ecosystems

Autonomy Architecture Needs a New Perspective

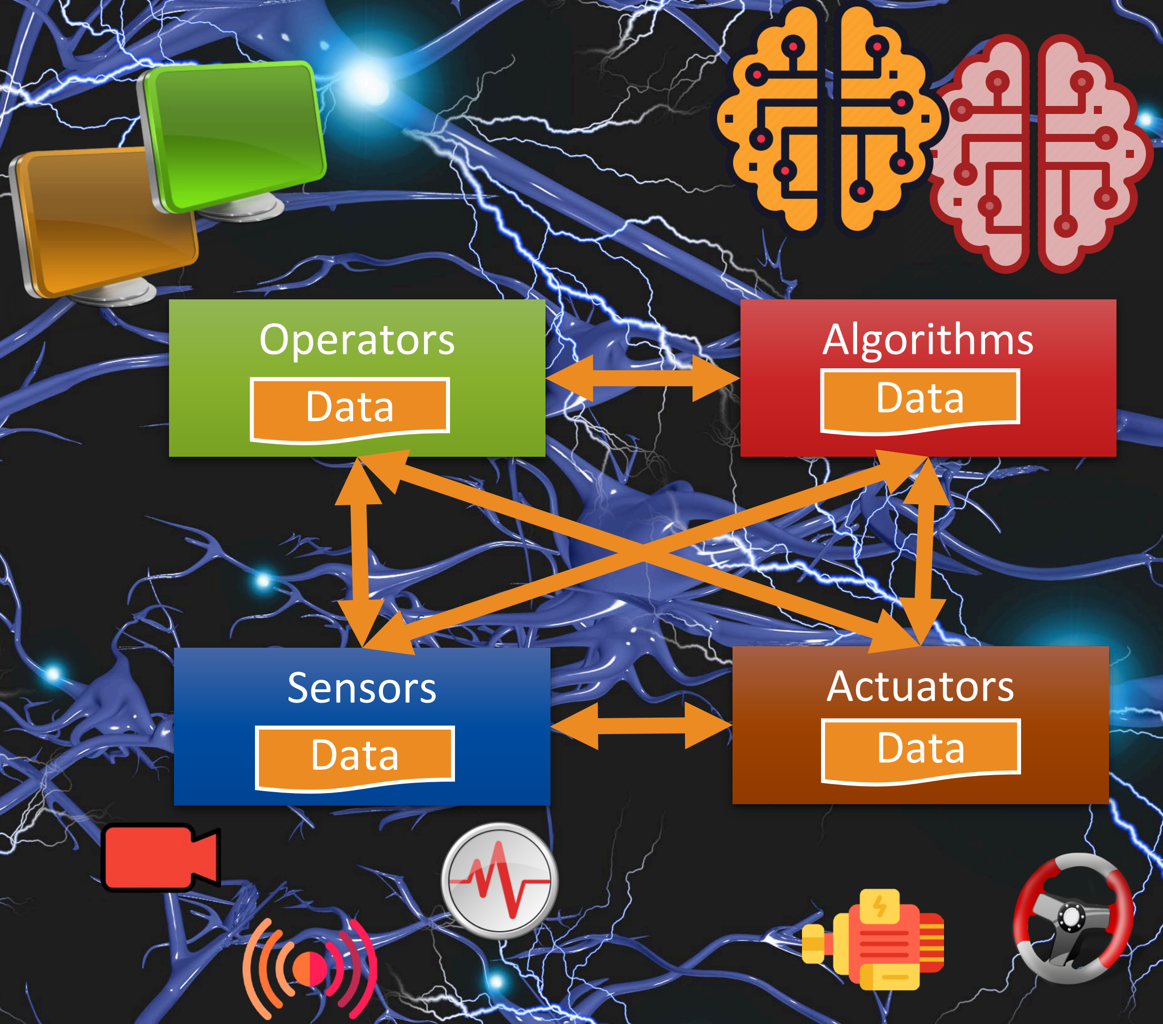
Don't design the data around the system…

Design the system around the data.

Data Centric *Architecture*



Data Centricity Decouples & Shares



- Logically puts all data “inside” every application
- Enables data sharing throughout the system
- Delivers motion, scale, speed, reliability, security
- Ideal for high-bandwidth varied flows…*like AI algorithms that connect to sensors & motors*

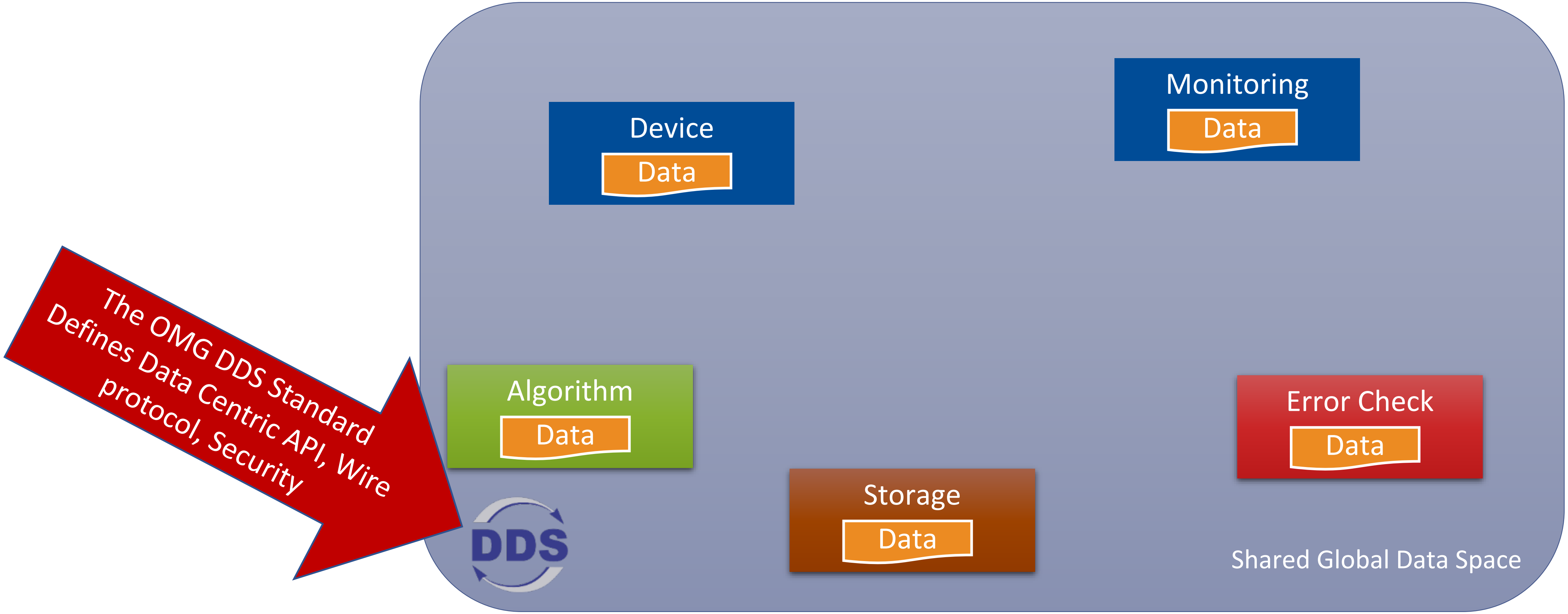
Your Systems. Working as One.

You Need Data Centricity If…

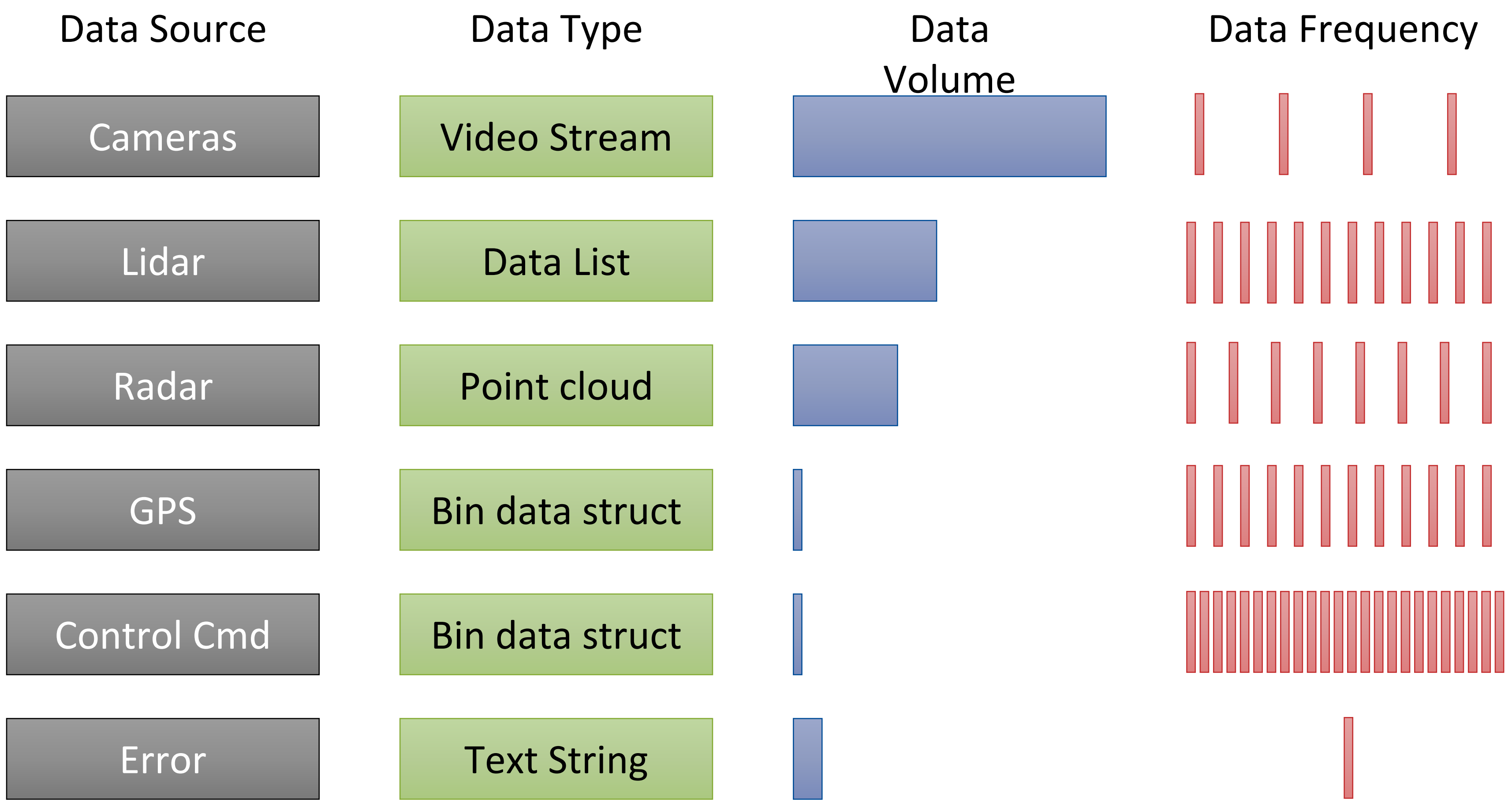
- Are there severe consequences of failure for one minute?
- Have you said “millisecond” in the last 2 weeks?
- Do you have more than 10 software engineers?
- Does your data have many destinations?
- Do you need a new architecture for a smart real-world system?

3+ Yes? → DDS

Data Centricity Makes Mobility Transparent



DDS Data Centricity Unifies Dataflow



- Many different dataflows
  - Volume
  - Frequency
  - Latency
  - Reliability
  - Destination
- ***QoS*** **enables a single databus to handle all**

Quality of Service control greatly simplifies interactions

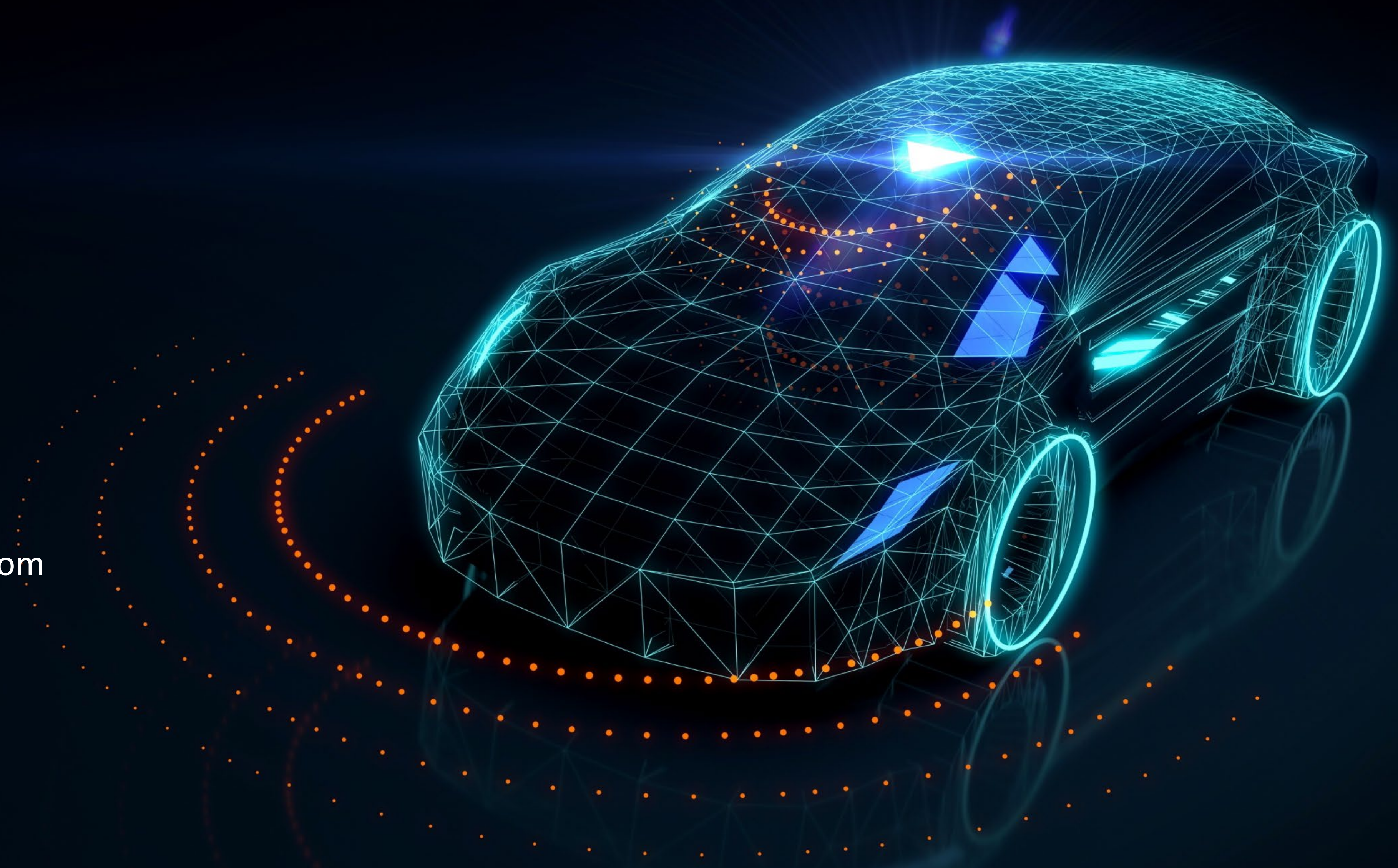
Teleoperation Challenges

Architectural clarity
Intervention triggers
Reliability
Performance & QoS
End-to-end data model
Scale
Fault tolerance
Security
Teleoperation
Stack & platform integration
Ecosystem integration
Evolving designs
Safety
Standards

The Teleoperation Consortium is Defining Why and How to Remotely Assist Vehicles

Teleoperation will accelerate safer, more efficient, fairer transportation

Security



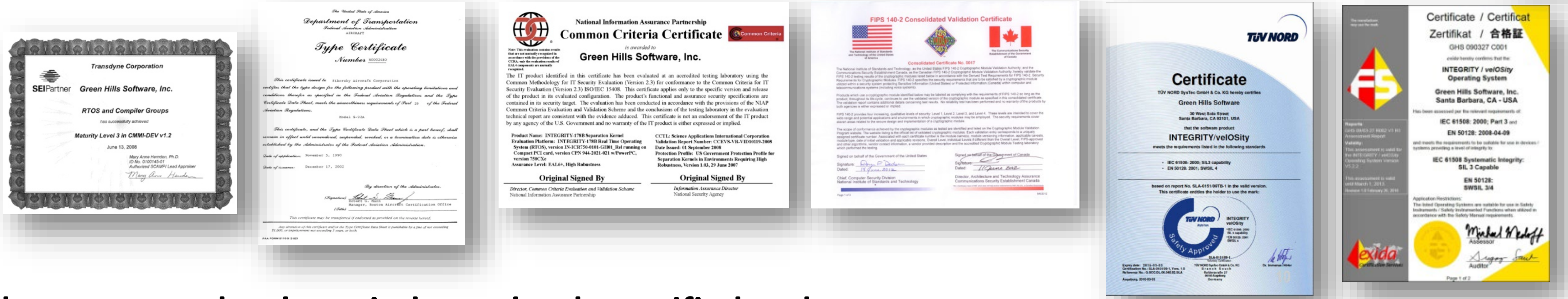
Teleoperation security, from Root of Trust to Remote Operation

Chuck Brokish

What Makes Green Hills Unique?

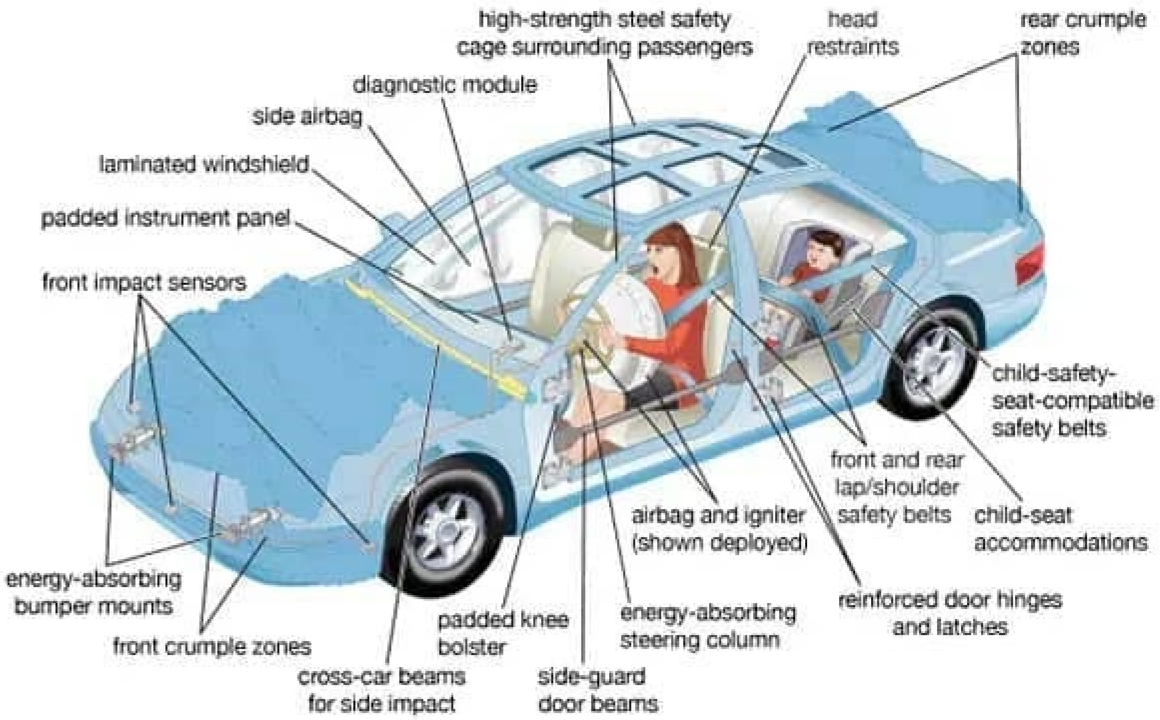
Green Hills Certified at the Highest Levels

Certifying Authority	Industry	Applicability	Certification Level Achieved
NSA, NIAP, NIST	Government	Security (Separation)	EAL6+ High Robustness
NSA	Government	Security (Separation)	Type 1
FAA, EASA	Avionics	Safety (Flight Controls, Engine, Displays)	DO-178B Level A
DIA	Government Network (TS/S)	Security (Separation)	PL4
NIST	All	Security (Encryption)	FIPS 140-2
FDA	Medical	Safety, Reliability	Class II, III
TUV Nord, exida	Automotive	Safety	ISO 26262:2010 - ASIL D
TUV Nord, exida	Industrial Automation	Safety	IEC 61508:2010 - SIL 4
TUV Nord, exida	Rail, Transportation	Safety	EN 50128:2011 - SIL 4
Transdyne	All	Quality	SEI/CMMI Certified
IEEE and the Open Group	All	Open, Interoperable	1003.1 IEEE POSIX Certified



No other company has been independently certified and proven to meet all of these levels of security, reliability and safety

Layered Safety (in Traditional Hardware)



https://www.serramazdaakron.com/5-latest-vehicle-safety-features-youll-be-thankful-for/

Layered Security

Secure External Communication

Message Encryption, Authentication, Certificate Management

Secure Gateways

Mandatory Access Control, Firewalls, Intrusion Detection/Protection

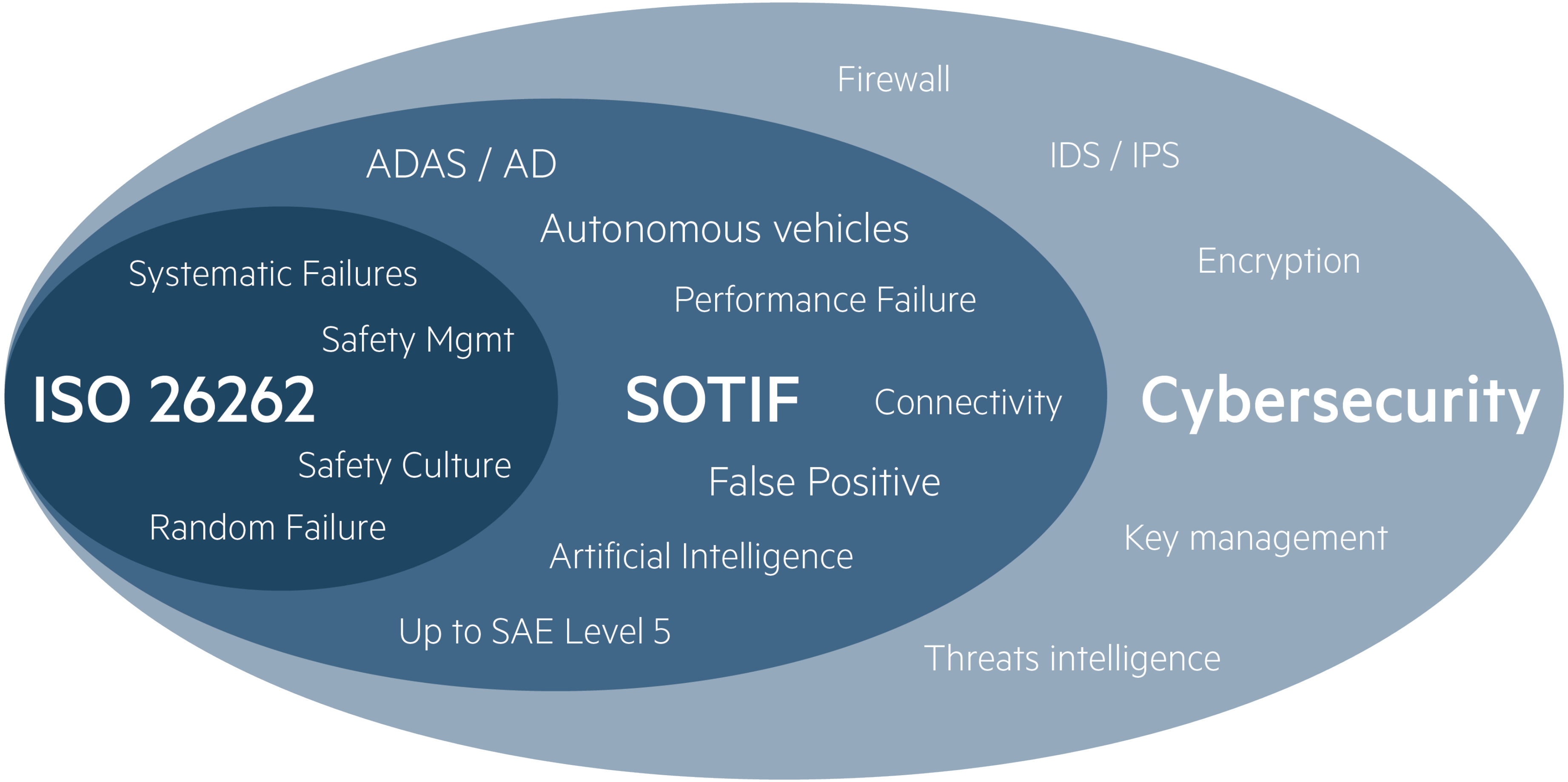
Secure In-Vehicle Communications

Confidentiality, Integrity, Authentication

Secure Harware Platform

Secure Boot, Hardware Security Module, Crypto Engines

Layered Safety and Security in Software



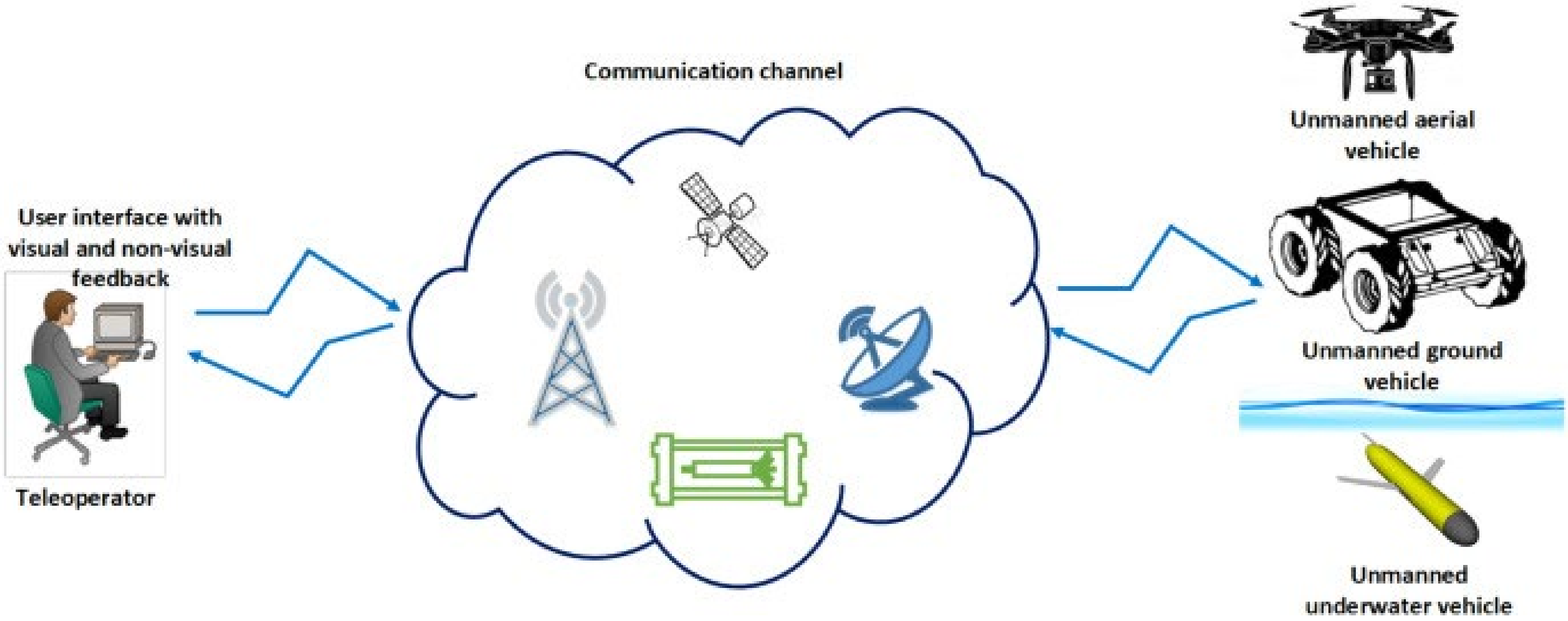
https://certx.com/automotive/

Key Concerns - Security

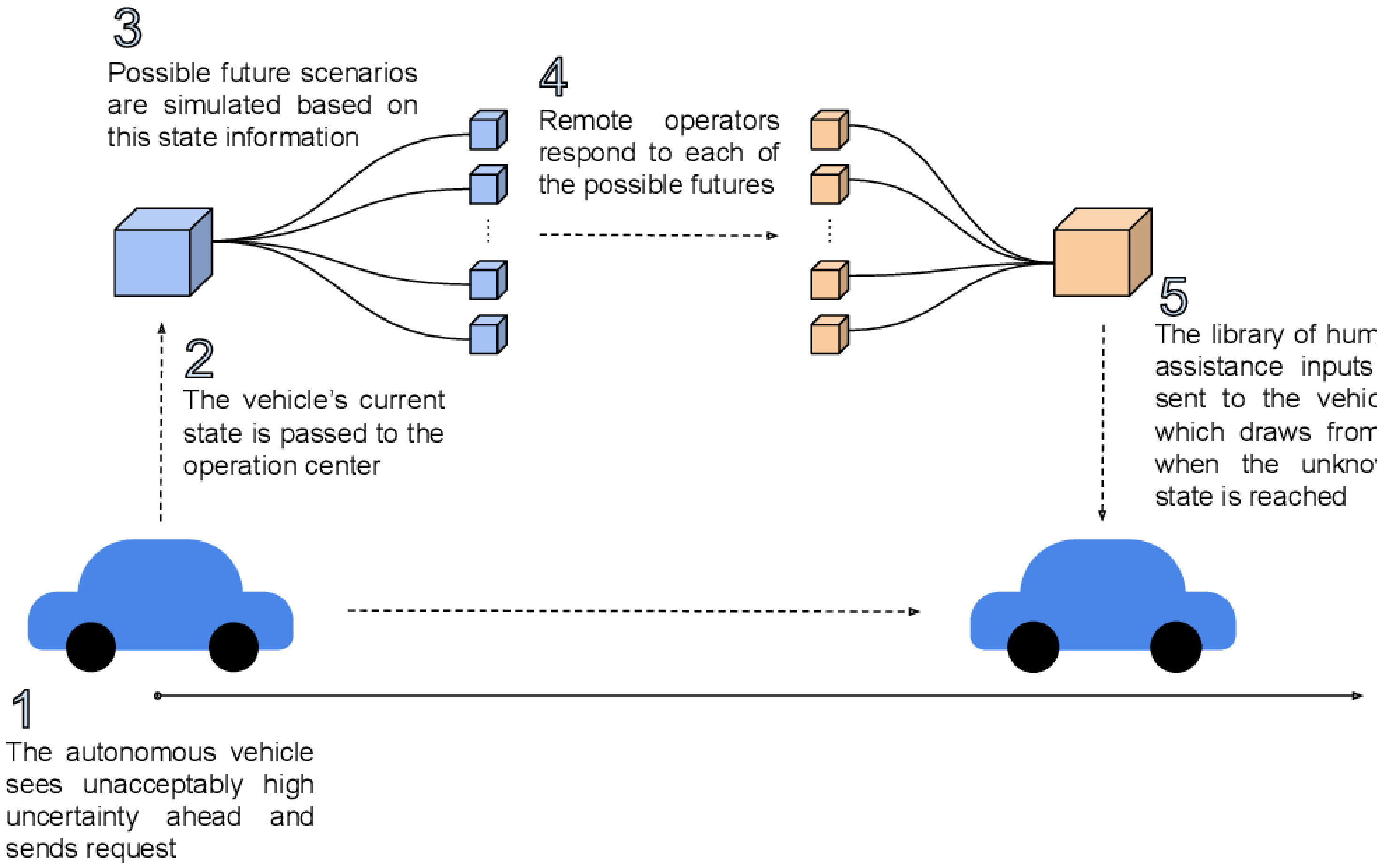
Security considerations

- Targeting the three major teleoperation components: The control station, in-vehicle teleoperation software module and the cloud.
- A vehicle can be taken over by a compromised control station.
- Compromising the teleoperation software module in the vehicle allows control of the vehicle and /or a denial of service (DOS) attack.
- Denial of Service attacks may overwhelm a teleoperation center and block part or all communications between the vehicle and the control station, denying teleoperation services.
- Compromising a teleoperation center may allow the attacker to impersonate a teleoperation center, corrupt and steal its data, and more.
- Blocking all communications between the vehicle and the control station, denying any vehicle assistance.
- An attacker can gain access to teleoperation capabilities via the interface between the in-vehicle AV software stack and the in-vehicle teleoperation module.

Teleoperation Ecosystem

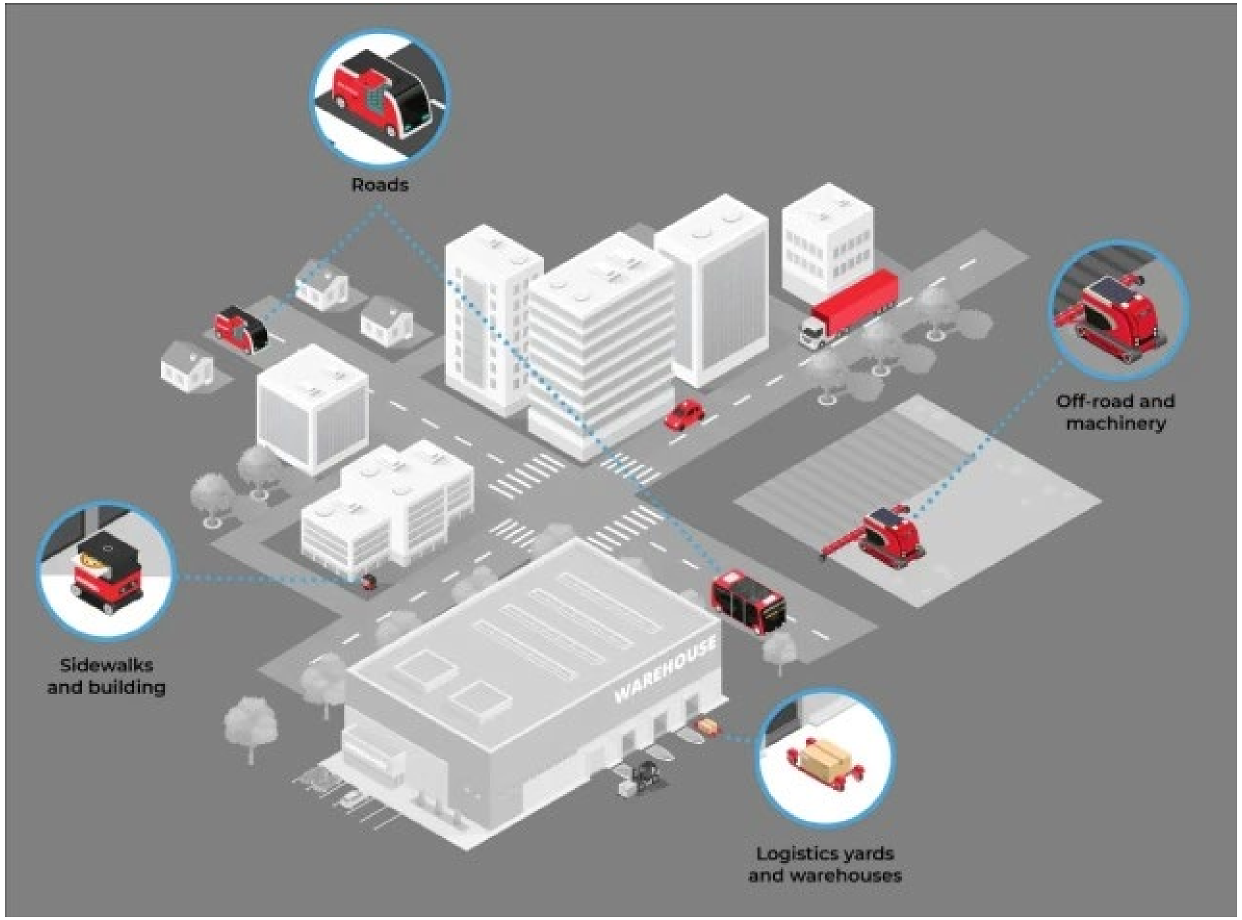


https://www.sciencedirect.com/science/article/pii/S0921889021002414



https://www.semanticscholar.org/paper/Beyond-Safety-Drivers%3A-Staffing-a-Teleoperations-Daw-Hampshire/2b284829aeee5acebcd1839e2ce714f8607d1c2c

Teleoperation Ecosystem



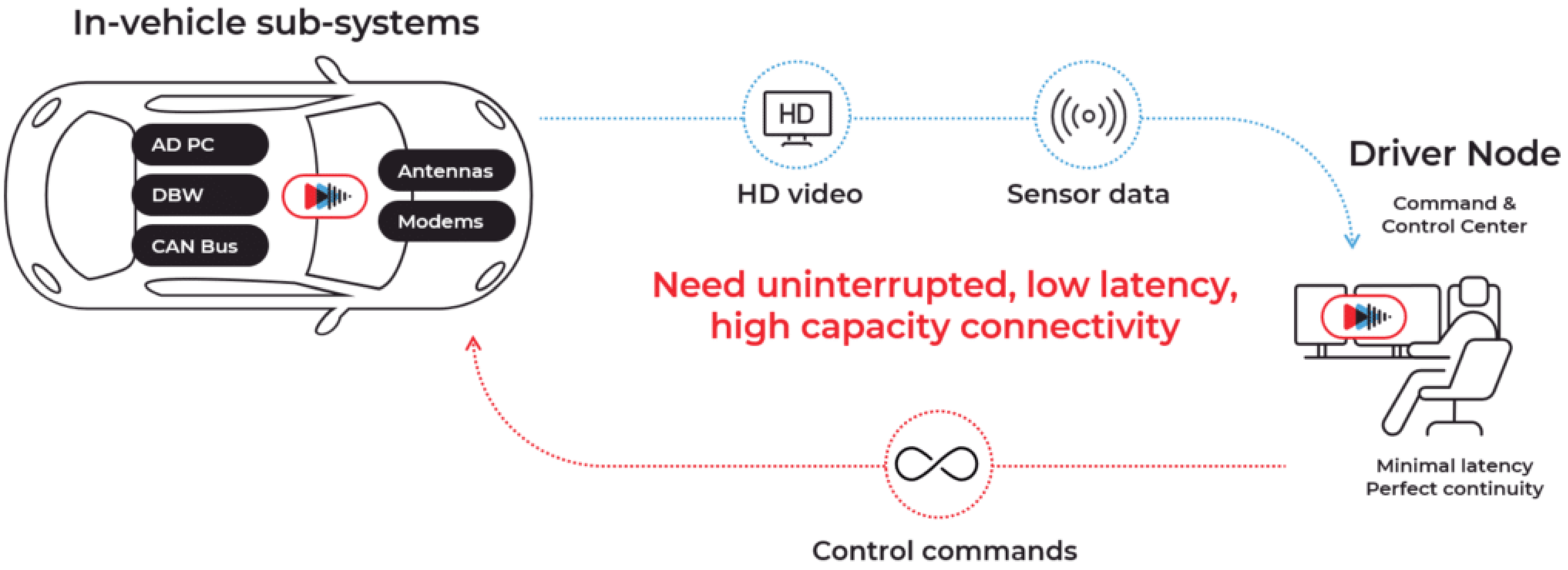
https://www.eetasia.com/why-autonomous-vehicles-will-need-teleoperation/

Key Concerns – Security, continued

Teleoperation cyber-risks clearly exceed the boundaries of a conventional automotive cybersecurity solution. Only when cybersecurity is an integral design element, rather than a third-party solution, can a solution be secure.

Here are a few examples of how such an architecture can provide the security needed:

- Only the vehicle can initiate a teleoperation session when it detects an attacker pretending to be a control station.
- Minimize and supervise the AV stack API to reduce access gained through other software components.
- Use a mediating component between the in-vehicle module and the control station to reduce risk of anomalous usage of the platform.
- Privacy by design to address data privacy. Automotive industries need to adhere to the privacy by design (PbD) approaches in Vehicle-to-everything (V2X) communication to proactively ensure the privacy of passengers, vehicle owners, and operators.



https://driveu.auto/blog/autonomous-vehicle-teleoperation-is-one-network-enough-for-remote-driving/

Key Concerns – Security, continued

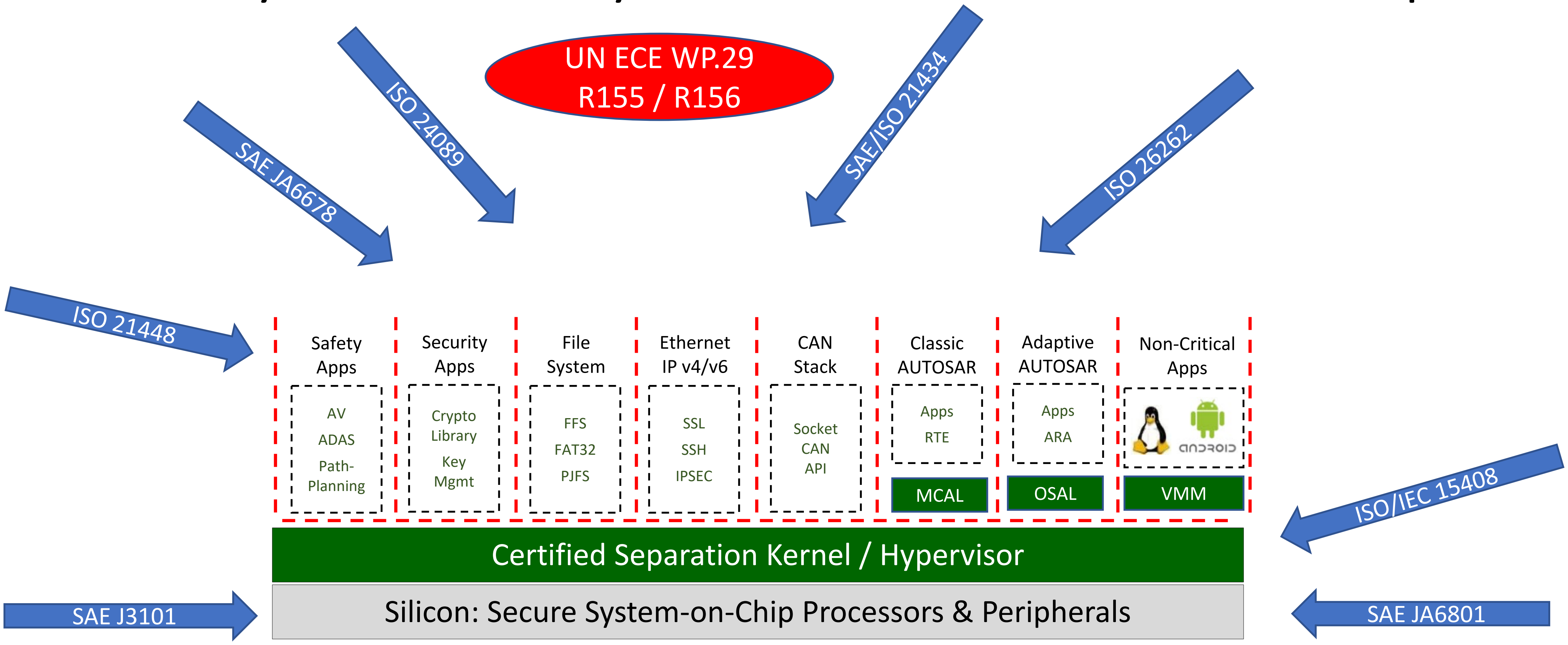
Attack/Vulnerabilities

- Gaining access to computers in the teleoperation center. The attacker can access the computer in the control station via outdated software installed in the computer. In this attack, the attacker runs malicious code on a teleoperation computer to control all the vehicles served by this computer.
- Sensor jamming, spoofing, and blinding/saturation. Sensors may be blinded or jammed. The blinding and auto control attack disables the functionality of the vehicle's camera sensors. Moreover, malicious hackers may add perturbation to the camera-captured images. In this way, the attacker may manipulate the AI model of the vehicle and make the vehicle confused so that it cannot ask for human assistance when required.
- Attacks targeting communication channels. Communication channels' security should be paramount in AV teleoperation. The main types of cyberattacks on communication channels are Denial of service (DoS) attacks, blocking all communications between the vehicle and the control station. An adversary may modify or drop transmitted video signals, sensor readings, and messages coming from road infrastructures or other vehicles.

Security from the Inside-Out

- Many security architects approach the problem of securing a system from the outside looking in
  - Look for entry points into the system
  - Establish a perimeter
  - Layer additional defense strategies in case the outer layers are defeated
- Inside out security starts by identifying the critical components in the design and isolating those components from non-critical components
  - Assume that non-critical components will be compromised
  - Utilize strong separation principles
    - Hardware separation
    - High robustness software separation
  - Minimize Complexity

Security and Safety from the Foundation-Up



Key Concerns – Security, continued

Attack/Vulnerabilities

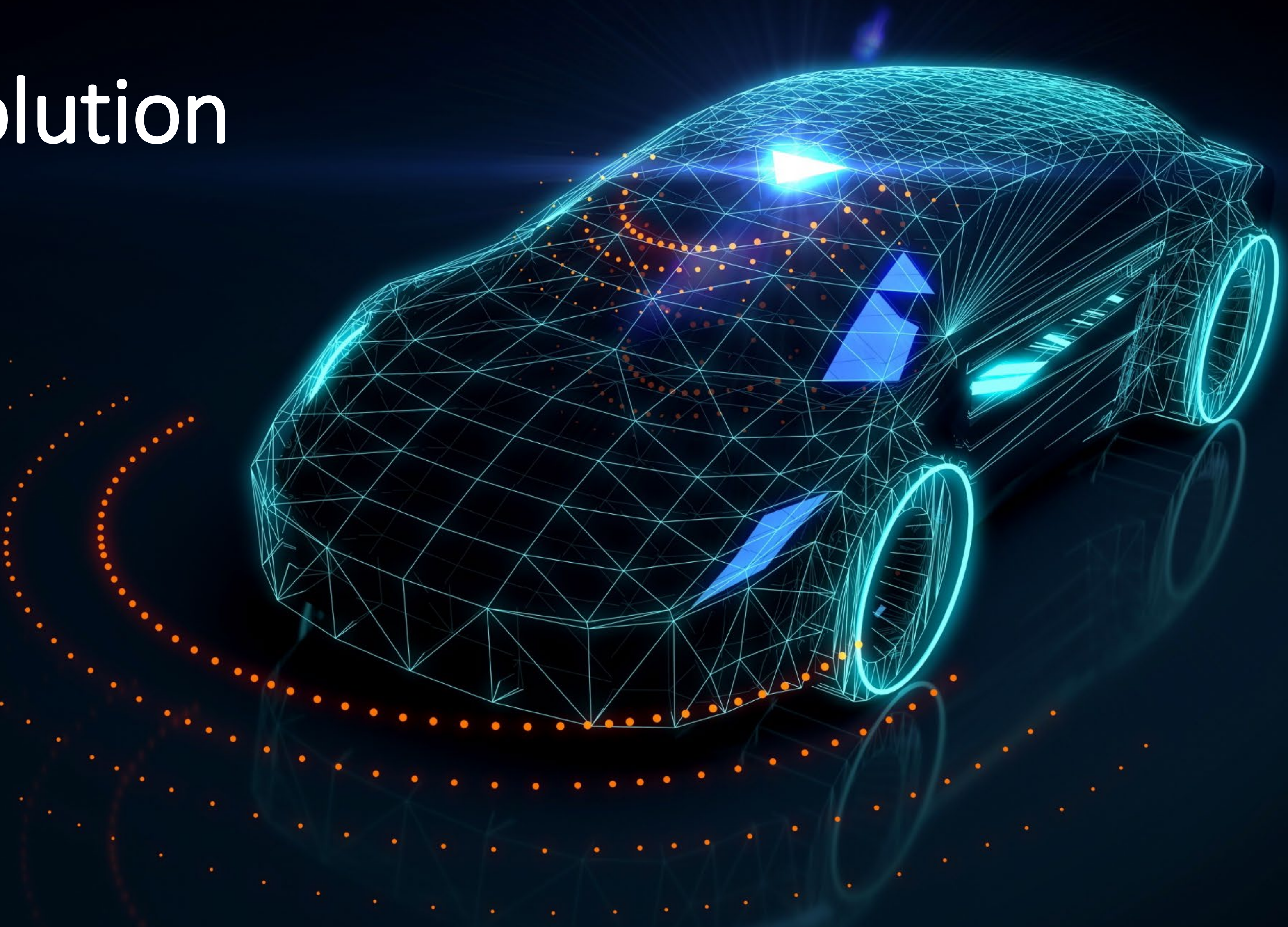
- Gaining physical access to the vehicle network. An attacker may gain physical access to the vehicle network during car maintenance. Afterward, a malicious piece of software can be installed in the vehicle computer to apply small perturbations to the captured images that may result in misclassification during object detection.
- Gaining remote access to the vehicle network. An attacker may remotely exploit the vulnerability of the vehicle head unit (HU) and get access to the vehicle’s internal network.
- Information disclosure. Since the teleoperated vehicle collects sensitive and personal data and shares this data with various stakeholders, an adversary may be motivated to gain access to this confidential data and cause a data breach.
- Ensuring robust communication. The communication between vehicle and teleoperation control center should be strongly protected, using proper encryption authentication to prevent different types of attacks such as DoS, the Man in the Middle, information spoofing, etc.

Key Concerns – Security, continued

Attack/Vulnerabilities

- Managing risks in the supply chain for an extended period. The entire supply chain includes OEMs, all levels of suppliers, subcontractors, and third-party vendors who provide software, firmware, hardware components as well as different services should be supportive of responding to continuously evolving threats and vulnerabilities.
- Systematic security validation and testing. The automakers or software developer updates the AI model with new trained data. Hence, systematic security validation and testing are required throughout the vehicle’s life cycle to combat newly developed cyber-attacks and security vulnerabilities created by updating the vehicles’ AI models.
- Require preparedness and incident response capabilities. Due to the increased connectivity of the vehicle with infrastructures and stakeholders, it is impossible to predict future attacks. Therefore, it is prudent to have a precise and established cybersecurity incident handling and response plan to handle incidents effectively.

Standards Evolution



The need for and evolution of standards for teleoperation

Tao Zhang

Teleoperation is a critical accelerator of the coming autonomous age

- The Teleoperation Consortium is *the* industry forum for remote operation of autonomous vehicles
- Our goal is to accelerate practical autonomy by providing assistance to vehicles in challenging situations
- We are developing a comprehensive Guidelines Document to outline the problem, approaches, and standards
- Join us! Email sjm@teleoperation.org to request information on the TC or the guidance document

Teleoperation Consortium

Call to Action

- Wireless standards
  - These are developing well, and should provide sufficient functionality. We should recommend where different technologies can work.
- Define a data model for teleoperation
  - This is different from in-vehicle or environmental modeling
  - A consistent end-to-end data model is critical (remote operation data model)
- Ensure evolving V2X standards address (and don't preclude) higher-level data modeling
- Specify requirements for a V2X Software Connectivity Framework Standard (does not exist). For example, DDS as a good base for a V2X communications architecture. Can provide a common developer interface for DSRC and C-V2X.

Teleoperation Consortium

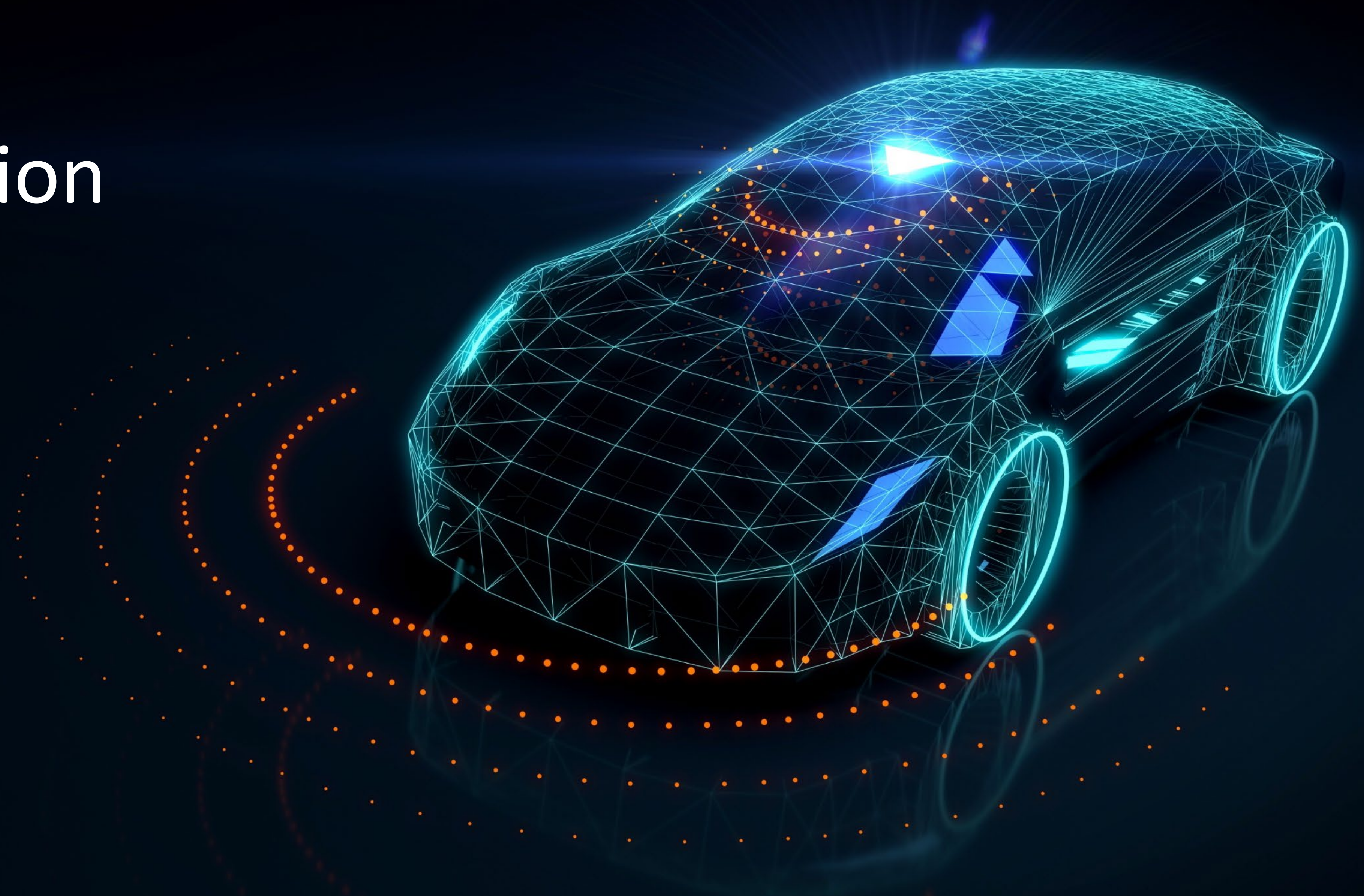
Scott McCormick sjm@teleoperation.org

Stan Schneider stan@rti.com

Chuck Brokish cbrokish@ghs.com

Dr. Tao Zhang tao.zhang@NIST.gov

Discussion



ADDENDA 1

(not presented)

Acronyms and Terms

Addenda – Acronyms and Terms

- **ADAS** - Advanced Driver Assistance System
- **ADASIS** - Advanced Driver Assistance Systems Interface Specifications - The interface for exchanging information between the in-vehicle map database, ADAS and automated driving applications
- **AI** - Artificial Intelligence
- **AV** - Automated Vehicle BSI British Standards Institution
- **CAV** - Connected and Automated Vehicle
- **Data Gateway** — a vehicle side hardware and software module that enables connecting to and using the vehicle's drive-by-wire system or a retrofitted actuation system.
- **DDT** - Dynamic Driving Task
- **DGNSS** - Differential GNSS - A kind of GNSS Augmentation system based on an enhancement to primary GNSS constellation(s) information using a network of ground-based reference stations
- **Direct Control** — a teleoperation method of control that allows an operator to drive the vehicle as if she was in the driver's seat.
- **DOT** - US Department of Transportation

Addenda – Acronyms and Terms, continued

- **Edge Cases** — road conditions that exceed what the Autonomous Vehicle (AV) is designed or able to tackle, for example road work, accidents, very bad weather conditions, a police officer guiding traffic, an unusual obstacle on the road, etc.
- **EU** - European Union
- **FOV** — abbreviation: field of view. The observable area a person can see through her eyes or via an optical device. In teleoperation it's the operator's field of view as seen through screens of the teleoperation station.
- **GDPR** - General Data Protection Regulation
- **GNSS** - Global Navigation Satellite System
- **GPS** - Global Positioning System
- **Handoff** — the transfer of control from the AV to the teleoperator, following a request for teleoperator assistance generated by the AV (a trigger). Or, an active action performed by the teleoperator to safely transfer control of the vehicle back to the AV.

Addenda – Acronyms and Terms, continued

- **HMI** - Human Machine Interface
- **IMU** - Inertial Measurement Unit
- **Human Intervention** — an active action taken by the teleoperator to control the AV either via a direct or indirect method of control.
- **Indirect Control** — an advanced teleoperation method that allows the teleoperator to instruct the AV on how to overcome an obstacle, instead of actually driving it. Using this method, the teleoperator utilizes software tools such as Path-Choice or Path-Drawing. Indirect methods of control are safer, more cyber-secure, more reliable and allow for better scalability than any direct method of control.
- **INS** - Inertial Navigation System
- **ISO** - International Organization for Standardization - **ISO 26262** is an international standard for functional safety of electrical and/or electronic systems in production automobiles defined by the International Organization for Standardization. Its goal is a unifying safety standard for all automotive E/E (Electrical/Electronic) systems. Any safe teleoperation system must adhere to the industry's defined standards.

Addenda – Acronyms and Terms, continued

- **Latency** — the amount of time a message takes to traverse a system. Two-way minimal latency, between the vehicle and the teleoperation station, and back, is required to ensure that teleoperators can safely guide the vehicle from remote locations.
- **LIDAR** - Light Detection and Ranging
- **Network Bonding** — a technology that aggregates data streams from several cellular and/or WiFi modems into one reliable, high-bandwidth and low-latency link. It is considered an essential module required for safe teleoperation.
- **Network Survey** — Prior to commencing teleoperation services in any given operational design domain (ODD), the network quality, coverage and latency in the ODD must be surveyed.
- **OEM** - Original Equipment Manufacturer
- **Operational Design Domain (ODD)** — California's DMV defines it as "… the specific operating domain(s) in which an automated function or system is designed to properly operate, including but not limited to geographic area, roadway type, speed range, environmental conditions (weather, daytime/nighttime, etc.), and other domain constraints." A teleoperation Design Domain is the specific operating domain for teleoperated or monitored systems.

Addenda – Acronyms and Terms, continued

- **OTA** - Over-The-Air
- **PAS** - Publicly Available Specification
- **Path-Choice and Path-Drawing** — user interfaces and software tools that enable humans to instruct AVs on a preferable path to overcome an obstacle, which then the AV executes autonomously. Path-Choice and Path-Drawing are examples of indirect methods of control.
- **RADAR** - Radio Detection and Ranging
- **Retrofit** — an aftermarket installation of system/s on a vehicle, such as a teleoperation kit of hardware and software. Retrofit systems can enable a set of capabilities even if said vehicle wasn't originally manufactured with those capabilities in mind.
- **RO** - Remote Operation
- **SAE** - Society of Automotive Engineers
- **Staffing Calculator** — a software solution used to predict and manage the number of teleoperators needed on a weekly, daily and hourly basis inside a teleoperation center to meet demand for teleoperation.

Addenda – Acronyms and Terms, continued

- **Teleoperation** (TO) — the ability to remotely control vehicles, autonomous or not.
- **Teleoperation Center** — an installation, usually in an office setting, that houses teleoperators and one or more teleoperation stations, used for conducting teleoperation.
- **Teleoperation Service Provider** — a company that provides teleoperation services.
- **Teleoperation Station** — a hardware and software solution used by a teleoperator in a teleoperation center to conduct teleoperation missions.
- **Teleoperator / Remote Operator** — the State of California DMV defines a remote operator as "… a natural person or automated teleoperator who: possesses the proper class of license for the type of test vehicle being operated; is not seated in the driver's seat of the vehicle; engages and monitors the autonomous vehicle; is able to communicate with occupants in the vehicle through a communication link. A remote operator may also have the ability to perform the dynamic driving task for the vehicle or cause the vehicle to achieve a minimal risk condition." A broader definition would omit the word "autonomous," i.e. a teleoperator in essence can control any type of vehicle, not just an autonomous one.

Addenda – Acronyms and Terms, continued

- **Trigger —** a request for human intervention initiated by the AV.
- **V2D** - Vehicle-to-Device (cell phone, tablet, gaming device, laptop, etc)
- **V2I** - Vehicle-to-Infrastructure
- **V2P** – Vehicle to Pedestrian
- **V2V** - Vehicle-to-Vehicle
- **V2X** - Vehicle-to-Everything
- **Video Transport** — smart, end-to-end, video streaming and compression technology, especially when working in sync with network bonding technology, guarantees the best utilization of the available bandwidth and minimal latency to ensure safe teleoperation. It is an essential software and hardware module required for safe teleoperation.

Acronyms and Terms

- We recognize that this is an incomplete list, and that others may have different was of defining the terms.
- We invite all qualified and interested parties to send contributions for this document to sjm@teleoperations.org

ADDENDA 2

(not presented)

References

References

- AVC Consortium, Technical Report 001, Conceptual Architecture for Automated and Assisted Driving Systems, April 2021
- Industry IoT Consortium (IIC), The Industrial Internet Of Things Connectivity Framework (IICF), 2022 Jun 08, https://www.iiconsortium.org/IICF/
- Industry IoT Consortium (IIC): The Industrial Internet, Volume G4: Security Framework Technical Report, version 1.0, 2016-Sep-26, retrieved 2022-07-05, *http://www.iiconsortium.org/IISF.htm*
- Object Management Group, DDS Foundation: DDS Portal—Data Distribution Services, retrieved 2022-07-05, *https://www.dds-foundation.org/*
- International Journal of Robotics and Automation (IJRA), Vol. 10, No. 3, September 2021, pp. 235~260 ISSN: 2089-4856, DOI: 10.11591/ijra.v10i3.pp235-260 Control of teleoperation systems in the presence of cyberattacks: A survey
- TRL PPR1011-Remote-operation-of-CAVs - Project-Endeavour – Main Report
- Human-Centered Design for Safe Teleoperation of Connected Vehicles. https://doi.org/10.1016/j.ifacol.2021.04.101
- AVSC00007202107 AVSC Information Report for Adapting a Safety Management System (SMS) for Automated Driving System (ADS) SAE Level 4 and 5 Testing and Evaluation
- British Standards insititue CAV Standards Roadmap 2022