ifip

WG.10.4

Second IFIP Workshop on Intelligent Vehicle Dependability & Security

June 23 – 26, 2022

Workshop Chair

Dr. Jay Lala
Sr. Principal Engineering Fellow
Raytheon Technologies
San Diego, CA

Organizing Committee

Prof. John Meyer, U Michigan
Dr. Carl Landwehr, U Michigan
Dr. Charles Weinstock, SEI
Prof. Homa Alemzadeh, U Virginia
Prof. Cristina Nita-Rotaru, NEU
Dr. Wilfried Steiner, TTTech, Vienna

https://www.dependability.org/wg10.4/ivds/index.html

IVDS Summer 22 Workshop Overview

WG.10.4

Workshop Focus: How to Survive Cyber Attacks on Safety-Critical Functions of Intelligent Vehicles

Goal: Discuss design solutions, quantitative cyber-survivability measures, and verification and validation with regard to impact on AV safety.

Specific Topics & Issues[1,2]

- Maturity of techniques: Theoretical analysis, modeling, simulation, lab experiments, component and system test & verification, penetration testing, real-world test runs, etc.
- Gaps in capability of techniques and current research in filling those gaps
- Industry use and awareness of existing techniques
- Integration of techniques to provide a holistic safety argument
- Novel system architecture and design solutions for cyber survivability

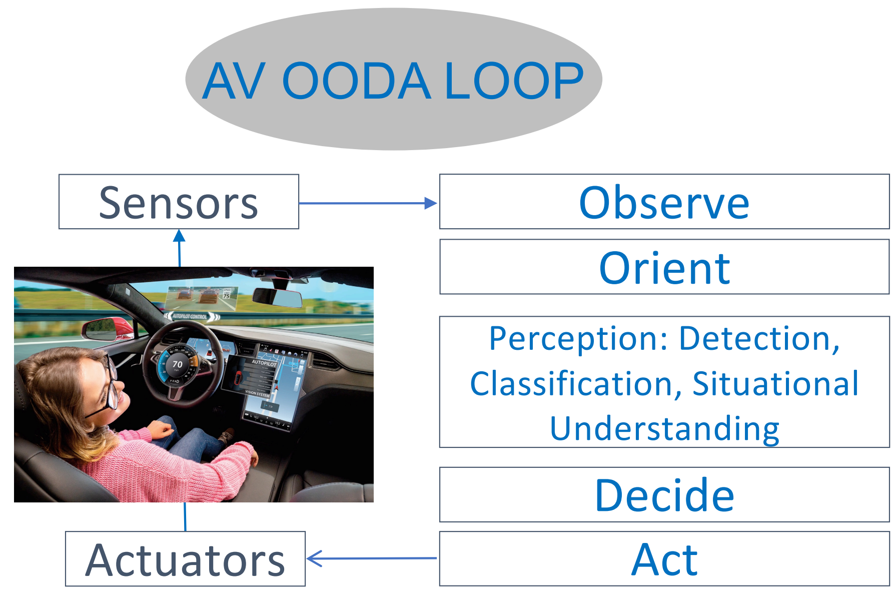
Desired Outcome: A set of specific actions, both short term and long term, to achieve the IVDS project's vision, mission and goals.

1. Physical attacks such as stickers on stop signs, dirty road patches, or poisoning of training data are outside the scope of cyber-related attacks.
2. Deficiencies of AI/ML are also not the focus of this workshop.

Workshop Scope

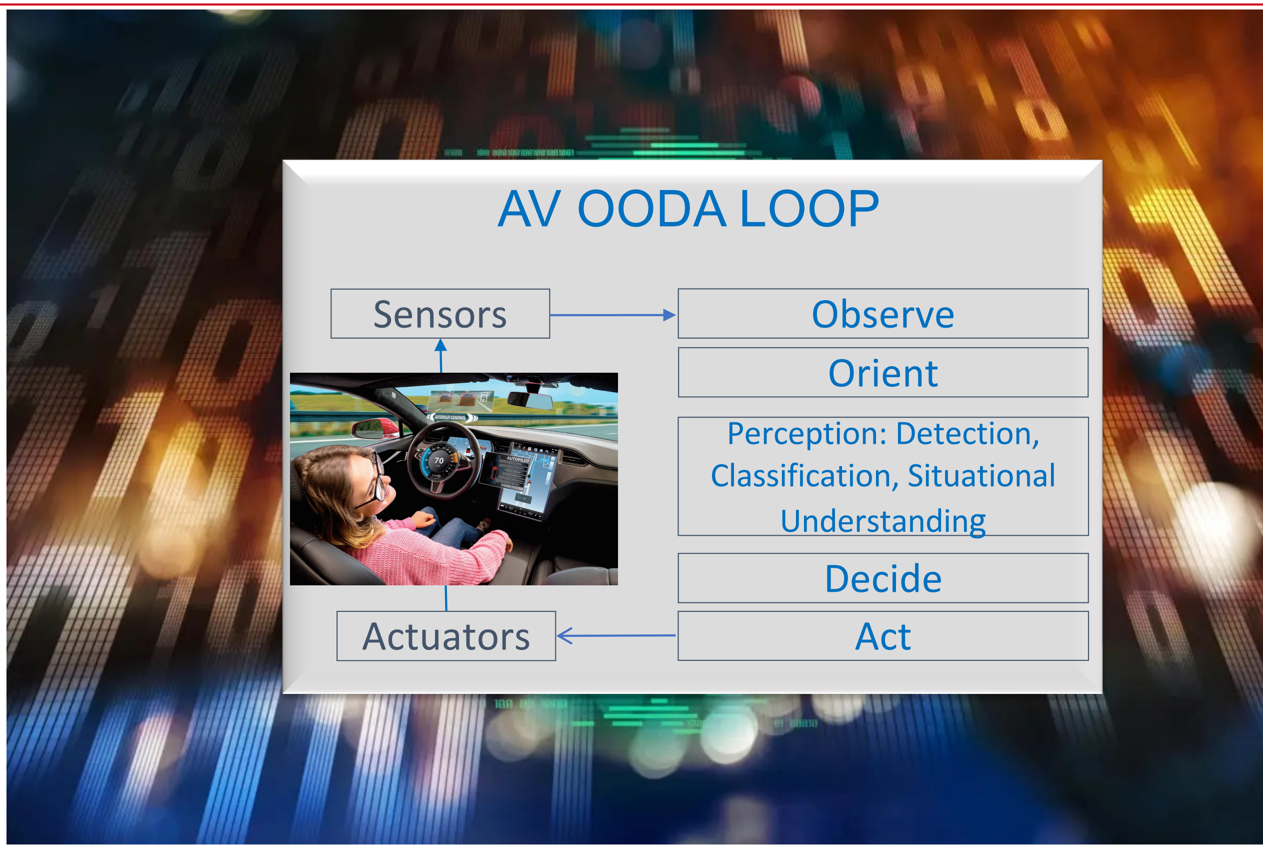
WG.10.4

- Sensors (Observe): Electro-Optical, Infrared, Radar, GPS, MEMS, Vehicle subsystems (Engine/Brakes/etc) performance, health & status sensors
- Algorithms (Orient & Decide): Catch-all for all the Feedback Control System Functions, incl. sensor processing and correlation, situational awareness, decision making, collision avoidance, etc.
- Actuators (Act): Commands to Engine, Brakes, Steering
- Processors: CPUs, GPUs, Software
- Communication: Links to other cars and Traffic Signaling Systems
- Driver Inputs: for L0 – L3 AVs



Current L0-L2+ Functions + Future L3-L5 capabilities

AV Ecosystem Immersed in Digital Sea



AV sensors, actuators, computations, comms are subject to continual cyber attacks

Cybersecurity and Infrastructure Security Agency (CISA) Autonomous Vehicle Cyber-Attack Taxonomy (AV|CAT)

DEFEND TODAY,
SECURE TOMORROW

AV Transportation Sector Guidance

UNDERSTANDING AV SECURITY RISKS AND UNIQUE CHALLENGES

As the CPS threat landscape continues to evolve, organizations will become increasingly vulnerable to attacks that can result in data breaches, supply chain disruptions, property damage, financial loss, injury, and loss of life. CSOs and CISOs should proactively monitor and manage AV technology risks using holistic security strategies that address both enterprise and asset vulnerabilities related to CPS integration with broader connected networks.

CISA's Autonomous Vehicle Cyber-Attack Taxonomy (AV|CAT) tool provides a framework for identifying AV risks based on the **attack vectors, targets, consequences,** and **outcomes** associated with a specific cyber-physical attack. Organizations can use the AV|CAT to understand risks related to AV technology integration, as well as risks to the AVs themselves and other physical assets. The tool offers a baseline for conceptualizing attack sequences and predicting an attack's ripple effects. Security teams can use the taxonomy to trace how a malicious actor can exploit a vulnerability, assess potential impacts, and identify associated risk mitigation strategies to enhance future resilience. The following scenarios use the CISA AV|CAT to illustrate examples of enterprise- and asset-level risks related to AVs:

ATTACK VECTOR
Pathway a malicious actor takes to access a targeted system

TARGET
System a malicious actor seeks to exploit

CONSEQUENCE
Harm resulting from an attack; classifies overall intent

OUTCOME
Real-world result caused by the attack

ifip

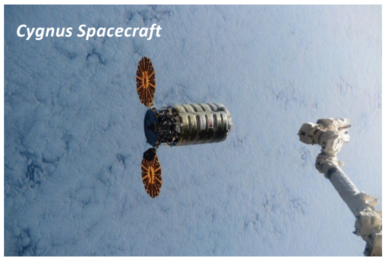
WG.10.4

ATTACK VECTOR *Pathway a malicious actor takes to access a targeted system*	TARGET *System a malicious actor seeks to exploit*	CONSEQUENCE *Harm resulting from an attack; classifies overall intent*	OUTCOME *Real-world result caused by the attack*
ENTERPRISE LEVEL RISK — **COMPROMISING AV NETWORK SECURITY**			
Malicious actor **gains unauthorized access to a network**, such as via a control room, and uses a USB to introduce malware	**Connected AVs and privileged networks** are targeted	**Proprietary and sensitive information could be disclosed** and connected assets could become inaccessible	Compromised company data and connected AV assets could result in **operational impacts and financial losses**
ENTERPRISE LEVEL RISK — **EXPLOITING AV SUPPY CHAIN VULNERABILITIES**			
Malicious actor **works with an insider at a third-party supplier** to nefariously modify data processing motherboards	External device could **remotely load malware** targeting networks and AV driving control, autonomy, and security systems	**Proprietary or sensitive information could be disclosed** and AVs could cease to function properly	Inoperable AVs could lead to **cascading supply chain impacts** and compromised data could result in **security/operational impacts and financial losses**
ENTERPRISE LEVEL RISK — **REMOTELY DISABLING AV FLEETS**			
Cyber criminal **creates privileged credentials to access an AV fleet's anti-theft system** and marks all vehicles as stolen	**Security systems** are targeted	Impacted AVs could become **inaccessible, stolen, or subject to tampering**	Compromised AVs cease to operate properly, causing **operational/supply chain disruptions and financial losses**
ASSET LEVEL RISK — **DISRUPTING AV SENSORS**			
Malicious actor **uses paint and reflective stickers to alter information an AV relies on** to gauge its surroundings, such as a stop sign	**AV hardware sensors and hardware sensor inputs** are targeted and could cease to function properly	**AV could malfunction** and performance could be degraded	AV malfunction could cause **a collision involving people or property, disrupt traffic patterns, or could cease to operate**
ASSET LEVEL RISK — **KEYLESS RELAY THEFT**			
Malicious actor near a corporate facility or AV fleet yard **intercepts the keyless entry signal to an AV** to gain access to the vehicle	**Driving control systems and security systems** are targeted	Impacted AVs could become **inaccessible, unreliable or inoperable due to tampering, or stolen**	Assets could be stolen, resulting in **financial losses**, or AVs could become **inaccessible or cease to operate properly**
ASSET LEVEL RISK — **AV RAMMING ATTACK**			
Malicious actor **gains access to an AV's On-Board Diagnostic (OBD-II) port**, uploads malware to bypass primary systems, and assumes remote control of the AV	**Driving control systems and security systems** are targeted	**Impacted AVs could become inaccessible** and the owner could be unable to regain control to prevent an attack	Compromised AVs could be **stolen, used to cause an accident, used to target public gathering spaces, or used for malicious cargo delivery**

CISA | DEFEND TODAY, SECURE TOMORROW

cisa.gov | Central@cisa.gov | LinkedIn.com/company/cisagov | @CISAgov | @cyber | @uscert_gov | Facebook.com/CISA | @cisagov

Mission Assurance


Cygnus Spacecraft

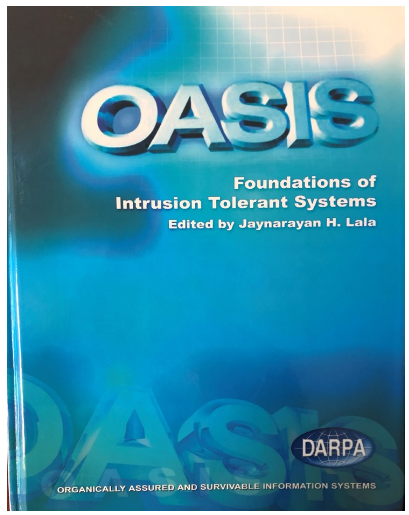

US Navy SSN-21
Nuclear Attack Submarine

DRAPER

ITS
Intrusion Tolerant Systems

Self- Regenerative Systems

OASIS



DARPA


Hypersonic Air-breathing Weapons Concept (HAWC)


Long Range Stand-off (LRSO)
Strategic Strike


Ship-Launched Tomahawk Cruise Missile

Raytheon Missiles & Defense

New Paradigms for Cyber Defense

10 February 2003

Operate Through Attacks!!

Dr. Jaynarayan Lala
Program Manager
Information Processing Technology Office

Self Regenerative Systems (SRS): The Fourth Generation

Prevent Intrusions
(Access Controls, Cryptography, Trusted Computing Base)

But intrusions will occur

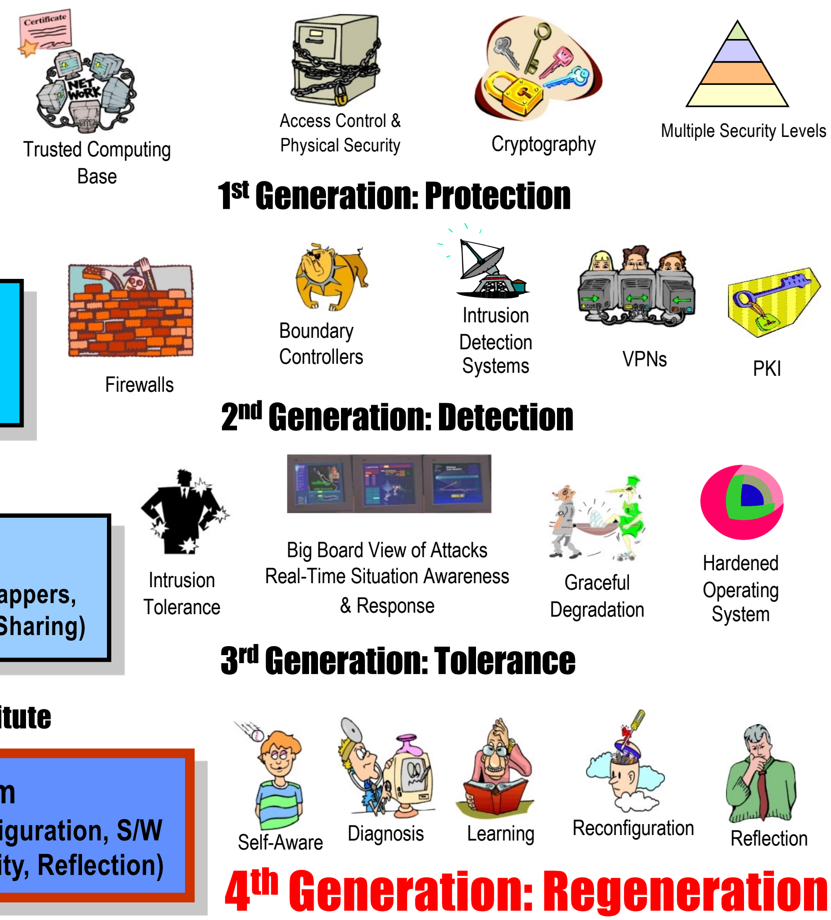
Detect Intrusions, Limit Damage
(Firewalls, Intrusion Detection Systems, Virtual Private Networks, PKI)

But some attacks will succeed

Tolerate Attacks
(Redundancy, Diversity, Deception, Wrappers, Proof-Carrying Code, Proactive Secret Sharing)

So the system must reconstitute

Restore System
(Diagnosis, Learning, Reconfiguration, S/W Rejuvenation, Natural Immunity, Reflection)



DoD Policy: Make Systems Cyber Survivable

1.2. POLICY.

….

c. Programs will employ system security engineering methods and practices, including cybersecurity, cyber resilience, and **cyber survivability** in design, test, manufacture, and sustainment.

Such methods and practices will **ensure that systems function as intended**, mitigating risks associated with known and exploitable vulnerabilities to provide a level of assurance commensurate with technology, program, system, and mission objectives.

"…. Joint Capabilities Integration and Development System (JCIDS) Manual, updated February 12, 2015, implements a robust **cyber survivability requirement** within the **mandatory system survivability Key Performance Parameter (KPP)**. This new requirement will enhance system resilience in a cyber-contested environment or after exposure to cyber threats."

- DoD Program Manager's Guidebook for Integrating the Cybersecurity Risk Management Framework (RMF) into the System Acquisition Lifecycle, September 2015

DoD Instruction 5000.83

Technology and Program Protection to Maintain Technological Advantage

Originating Component:	Office of the Under Secretary of Defense for Research and Engineering
Effective:	July 20, 2020
Change 1 Effective:	May 21, 2021
Releasability:	Cleared for public release. Available on the Directives Division Website at https://www.esd.whs.mil/DD/.
Incorporates and Cancels:	See Paragraph 1.3.
Approved by:	Michael D. Griffin, Under Secretary of Defense for Research and Engineering
Change 1 Approved by:	Barbara K. McQuiston, Performing the Duties of the Under Secretary of Defense for Research and Engineering

Purpose: In accordance with the authority in DoD Directive (DoDD) 5137.02, the policy in Section 133a of Title 10, United States Code, and Directive-type Memorandum S-DTM-19-005, this issuance:

- Establishes policy, assigns responsibilities, and provides procedures for science and technology (S&T) managers and engineers to manage system security and cybersecurity technical risks from foreign intelligence collection; hardware, software, cyber, and cyberspace vulnerabilities; supply chain exploitation; and reverse engineering to:
  - DoD-sponsored research and technology that is in the interest of national security.
  - DoD warfighting capabilities.
- Assigns responsibilities and provides procedures for S&T managers and lead systems engineers for technology area protection plans (TAPPs), S&T protection, program protection plans (PPPs), and engineering cybersecurity activities.

Cyber Survivability is a new Key Performance Parameter (KPP) for weapons systems

Agenda Overview

https://www.dependability.org/wg10.4/ivds/ivds2022/program.html