First IFIP Workshop on Intelligent Vehicle Dependability & Security

Jan 29 – Feb 1, 2021

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

Workshop Context

- Promise of safe and secure Level 5 vehicles
- How safe should autonomous vehicles be?
- Human factor challenges of L3

Societal factors present a bigger challenge than technological feasibility

Promise of L5 Vehicles

- Desired end-state of autonomous vehicle evolution is safe and secure Level 5:
  - Totally autonomous vehicles, obviating need for human drivers and even personal autos
- Benefits of transition to 100% L5 fleet on the road include:
  - No human carnage on the roads
  - No drudgery of driving
  - No traffic lights or traffic jams
  - No more hunting for a parking spot
  - Spaces reclaimed for better purposes: home and business garages, parking lots, and on-street parking

Urban planners are already designing clean, green cities with L5 in mind

How Safe should autonomous vehicles be?

WG.10.4

Case	Safety relative to current manual benchmark	Failure Rate (per hour)	Annual Deaths caused by Control System (US)	Deaths/Day (US)
1	Same as	$0.5X10^{-6}$	37,806	104
2	10X better	$0.5X10^{-7}$	3,780	10
3	100X better	$0.5X10^{-8}$	378	1
4	1,000X better	$0.5X10^{-9}$	38	0.1
5	10,000X better	$0.5X10^{-10}$	4	0.01

- As good as an average driver?
  - That will result in 100 people dying everyday (US) due to machine failures.
  - And, yet, this has been proposed as completely acceptable by industry and many government regulators.
- Why should we set the safety bar so low?
  - As a society, we have become inured the auto death toll.
  - We should not let that be the safety standard.

Once-in-a-century opportunity to make land transportation safe

Aviation and Internet Experiences

- FAA mandated 1000X better safety for Fly-by-Wire than an average pilot
  - An average pilot is highly trained and makes fewer fatal mistakes than an average driver
  - And, yet, the FAA raised the bar even higher
- Why would we blow a once-in-a-century opportunity to not save the ongoing death toll on the roads? And, never realize all the benefits cited before.
  - Unlike airplane FBW, autonomous vehicle control systems need only be fail-safe
  - Be able to change to a safe mode and move the vehicle to a safe place and then stop: fail-operational (for a brief time period but not fail-stop)
- Let's not repeat the experience of developing the very insecure Internet
  - Nearly fifty years later, we still have not fixed all the original flaws

Emulate aviation experience to design fail-safe automotive control systems

L3 Human Factors Challenge

- L3 is a mode where routine driving is performed by the control system while human driver intervenes in case of malfunction
- Can one really expect an average driver to stay engaged for a once/yr event?
- Pilots are highly trained to recognize emergencies quickly and take corrective action.
- Do we expect to change driver licensing to do this?
- Why not just skip L3 and aim for L4/L5?

viewpoints

DOI:10.1145/3411053

Jaynarayan H. Lala, Carl E. Landwehr, and John F. Meyer

Terry Benzel, Column Editor

Security

Autonomous Vehicle Safety: Lessons from Aviation

How more than 25 years of experience with aviation safety-critical systems can be applied to autonomous vehicle systems.

AUTONOMOUS VEHICLES SEEM to hold great promise for relieving humans of the boring task of guiding a car through congested traffic or along a monotonous turnpike, while at the same time reducing the annual highway death toll. However, the headlong rush to be the first to market, without adequate considerations of life-critical control system design, could cause irreparable public harm and ultimately set back the promise of autonomous driving. With the current goal of being at least as safe as human driving, espoused by business leaders as well as some regulatory agencies, the annual death toll attributed to automation killing innocent people, just in the U.S., would be approximately 36,500 per year or 100 per day. Think about that for a minute!

This column highlights this important dependability need, the dire consequences of falling short, and how leveraging the knowledge gained by the aviation industry in operating safety-

Numerous automobile companies[2] are racing to be the first to market. Ford says it will have an L5 vehicle in operation by 2021. More ambitiously, Toyota announced in February 2019 that it plans to have a self-driving vehicle ("the most intelligent supercom-

announced it would field a fleet of self-driving vehicles by 2021, and has recently teamed with Ford. As early as 2016, Tesla announced all cars it produces have the hardware needed for L5 driving capability; evidently it is just a small matter of programming.

Moving progressively from L0 to L5 is counter-intuitively less safe

IVDS Project Vision, Mission and Goals

Vision

Safe, secure and dependable operation of intelligent and autonomous vehicles

Mission

Provide thought leadership by engaging stakeholders to increase awareness of dependability and safety requirements, promoting technical solutions, and providing expert help to governance and regulatory bodies in their rule-making and oversight roles

Goals

1. Increase Awareness of Stakeholders: Invite government and industry stakeholders and researchers to workshops; Meet with them in their own environment; Disseminate knowledge at conferences, workshops and via publications.
2. Promote Technical Solutions: Hold DSN & WG10.4 workshops focused on dependability & security requirements, key design challenges, certification & validations, and other relevant topics
3. Engage Governance and Regulatory Organs: Provide Governments and Industry Standards Bodies expert help in defining requirements, standards, and certification methods.

Be Thought Leaders in Intelligent Vehicle Dependability

IVDS Project Background

- **2018**
  - Need for another WG 10.4 project urged by John Meyer
  - Carl Landwehr volunteers to chair ad hoc project committee
  - WG members submit nine proposals
- **2019**
  - IVDS project is approved by the WG at Hood River, OR, USA meeting
  - Jay Lala *"volunteers"* to lead IVDS project
  - White paper distributed at Sept "The Autonomous" meeting, Vienna, AT
- **2020**
  - "Opinion" article (Lala, Landwehr, Meyer) published in CACM, Sept 2020
  - First IVDS Workshop proposed by project team and approved by WG
  - Workshop organizing committee's labor of love brings us here today
    - Alemzadeh, Lala, Landwehr, Meyer, Weinstock

Workshop Goal & Outcome

Goal: Debate and provide arguments on all sides of the following hypothesis:

Level 3 autonomous vehicles cannot be made acceptably safe with current technology and practices.

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

Agenda Overview

Time Zone EST	First IFIP Workshop on Intelligent Vehicle Dependability and Security (IVDS) Winter 2021 *Organizing Committee: Jaynarayan Lala, John Meyer, Carl Landwehr, Charles Weinstock, Homa Alemzadeh* *Host: Charles Weinstock, Software Engineering Institute*
	Friday, January 29
09:00 - 09:05	**Welcome to IFIP IVDS 2021 Workshop** *Mootaz Elnozahy, King Abdullah University of Science and Technology*
09:05 - 09:30	**Workshop Introduction and Objectives** *Jay Lala, Raytheon Technologies*
09:30 - 11:30	**Session 1: Human - Autonomous Systems Interaction** *Session Chair: Kevin Driscoll, Honeywell; Rapporteur: John Meyer, Univ of Michigan*
	Saturday, January 30
09:00 - 11:30	**Session 2: Autonomous Vehicle Industry Perspectives** *Session Chair: Tom Anderson, Univ of Newcastle upon Tyne; Rapporteur: Homa Alemzadeh, Univ of Virginia*
	Sunday, January 31
09:00 - 11:00	**Session 3: Verification and Validation** *Session Chair: Marco Vieira, Univ of Coimbr; Rapporteur: Carl Landwehr, Univ of Michigan & George Washington Univ*
11:00 - 11:25	**Workshop Concluding Remarks** *Workshop Chair & Rapporteurs*
11:25 - 11:30	**Workshop Closing** *Mootaz Elnozahy, King Abdullah University of Science and Technology*
	Monday, February 1
	Session 4: Workshop Wrap-up *Workshop Organizing Committee*
09:00 - 11:00	**Optional session for anyone interested in continuing discussions on workshop topic and IVDS project. The OC will be in attendance as facilitators.**

Today's Detailed Agenda

WG.10.4

Time Zone EST	First IFIP Workshop on Intelligent Vehicle Dependability and Security (IVDS) **Winter 2021** *Organizing Committee: Jaynarayan Lala, John Meyer, Carl Landwehr, Charles Weinstock, Homa Alemzadeh* *Host: Charles Weinstock, Software Engineering Institute*
	Friday, January 29
09:00 - 09:05	**Welcome to IFIP IVDS 2021 Workshop** *Mootaz Elnozahy, King Abdullah University of Science and Technology*
09:05 - 09:30	**Workshop Introduction and Objectives** *Jay Lala, Raytheon Technologies*
	Session 1: Human - Autonomous Systems Interaction *Session Chair: Kevin Driscoll, Honeywell; Rapporteur: John Meyer, Univ of Michigan*
09:30 - 10:00	**Missy Cummings, Duke University: "Tesla Model 3 Reliability in Driver Alerting"**
10:00 - 10:30	**Marjory Blumenthal, RAND: "Approaches to Assessing and Communicating about AV Safety"**
10:30 - 11:00	**Ben Shneiderman, University of Maryland: "Designing for Increased Autonomy & Human Control"**
11:00 - 11:30	**Discussion**