- 20 Year Vision – Big Trustworthiness Challenges
    - Security, Privacy
    - tradeoffs
    - Roadmap?
    - 5-10 years
    - Standrds need to be developed by forming cyber security groups – like AIAA Jim from Boeing. How to expand to transportation cyber security. Similar group in SAE.
    - Why don't we build systems that focus on cyber security – design time and not run time. People don't believe that they need them.
    - How to measure. Do existing trust models in mobile, internet etc., work in t-cps. Mobility is a factor. Evaluate existing ones and develop new trust models. K-anonymity.
        - How to autneticate with mobility. Physics could be exploited for security
        - How to trust devices that emerge and how to trust peers
    - How to correlate data among big data
    - 10-15 years
    - How to get data to validate the security or trust of a system. New metrics . New attack model. This is a big challenge to CPS security. Can we assess trust degradation over time.
    - 15-20 years
    - Anti virus, malware patching. Model system complexity and abstractions on a more theoretical foundation level.
    - Encryption can be overcome by computing power. Need new strategies are needed to be accepted by public. Key management
    - Data vs. Energy. They don't send a new car.
    - Economic costs. How do we write insurance. Business model
    - Human factors – penetration rejection rate.
- Why are Security, Trust and Privacy in T-CPS relevant
    - Fit with Safety, Performance, Efficiency which are current metrics
    - Do we see design time integration

    - Industry perspective
- Why is Security, Trust and Privacy in T-CPS different
    - What are the unique challenges
    - Ppls or components. The trsut works both ways. Owners can be attacker. Overwirde speed limits. People hack videos. Attacks from isniders. Tamper free hardware.
- What are the technical ramifications of Cyber-Socio-Physical T-CPS
    - Models, Abstractions, Compositions, Verification, Validation

Threats: Prevention or is it detecting an attacks, or reaction to an attack.

Design and run time. attaackers can be subtle. And create massive traffic jams.

Attacks are primarily cyber. If someone manipulates sensor, is it cyber attack. Radar com promise. There is a link here to CPS. Sensors mis reporting information. we trust no vehicle, but there could be. How do we trust these systems. But these are failure models. If it happens by accident, it is tradiotional failure, but if malicious, harder problem.

If we see attacks on sensor, as an important concept to study. Yes. how is it different.

Platoon level attacks. Simple attacks caused by people. Based on applications. False information about an accident. Network level attacks.

Current status – can we create trust profile for roads based on networked vehicles. Infrastructure can also be an asset for creating trust profile. Both system and user perspective.

Threats to privacy – users mobility trace is exposed. How to annymize, but still get service. Privacy-utulity tradeoff. Every activity inside car can be exposed as well. Beyond location. Real-time routing makes it more complicated. Temporal aspects to privacy.

What is fail-safe behavior – no idea yet. Fail safe is not trustworthy. Social contect and location context comes here.theries exist to make redundancy work for dependability. very complicated topic. Trains and sirplanes have this. how does fail safe correspond to security. Vulnerability comes from redundancy management alsgorithms byzantine fault tolerance. Security-privacy rtadeoffs is open issue.who gets to see what information

Humans are a part of the attacks. Report drunk driving.

Humans should know what data is collected; how is it processed. Like an icon on a phone.

Trust visualization for CPS trust. How to design the interface. Increase confidence in the system.

What is usable security? Easy to use?

User penetration/ rejection rate.

How to autneticate with mobility. Physics could be exploited for security