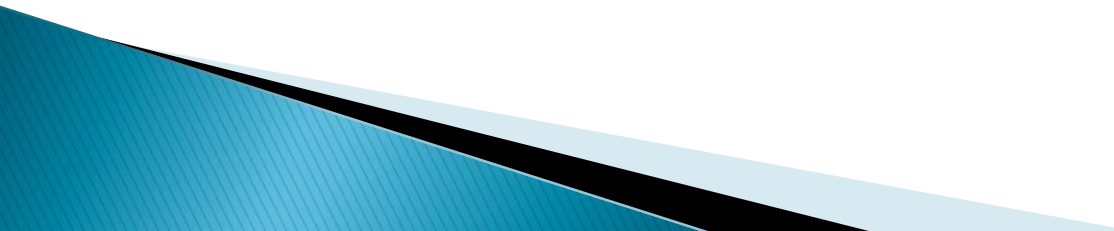


# Breakout Groups

Automotive Secure and High Confidence Platforms

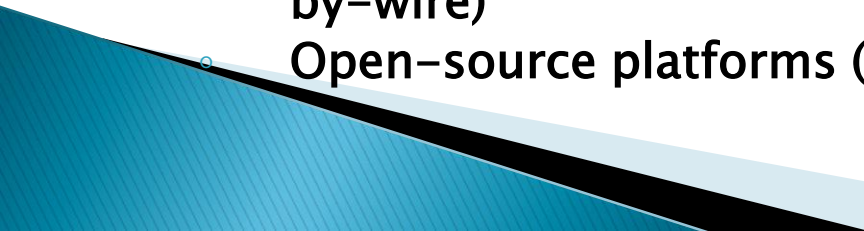
# Automotive Secure and High-Confidence Platforms

- ▶ Lead: **Betty Cheng**
  - ▶ Scribe: **Doug Rhode**
  - ▶ Room: **104**
  - ▶ Interested attendee count: 17
- 

# List of Attendees

- ▶ Betty HC Cheng, MSU, *Lead*
- ▶ Doug Rhode, Ford, *Scribe*
- ▶ WassimNajm, DOT
- ▶ MilosZefran, UIC
- ▶ Massimo Osella, GM R&D
- ▶ Tom Forest, GM R&D
- ▶ ShenbingJiang, GM R&D
- ▶ Sumit K. Jha, UCF
- ▶ Tom Fuhrman, GM R&D
- ▶ Patrick E. Lanigan, CMU
- ▶ SandeepKulkarni, MSU
- ▶ SayanMitra, UIUC
- ▶ Dave New, Chrysler
- ▶ KameshNamuduri, UNT
- ▶ AnuradhaAnnaswamy, MIT
- ▶ LinhPhan, UPenn
- ▶ Sam Weber, NSF

# Research Challenges

- ▶ **Software Complexity**
    - Impossible to validate sufficiently through testing as number and complexity of modules increases and need to be integrated
    - New business-models with many suppliers and developers
  - ▶ **Assurance (Safety and reliability)**
    - Cost effective Fail-Operational Systems
    - Moving from Fail-Safe to Fail-Op
    - Protect against common mode of failures (EMC, Power Supply, Lighting, ...)
  - ▶ **Cyber-Physical Security**
    - More connectivity into our vehicles
    - More safety critical controls (towards autonomous driving and by-wire)
    - Open-source platforms (for Infotainment)
- 

# Software Complexity Roadmap (1 / 2)

**3–5 year:**

- ▶ **Model-based / Math-based design**
  - Currently, components are modeled, but full vehicle environment not widely use.
  - Formal methods are needed.
  - Component integration and full vehicle not currently done.
- ▶ **Integration methods including models, tools and data are needed.**
- ▶ **Formal Methods are currently only being used for research.**
- ▶ **Automated Validation and testing**
- ▶ **Run-Time Safety monitors / Safety Goals violation (current:**
  - Current practice does not use full safety monitor model in run time.
  - Separate requirements for safety monitor is still needed. Formal methods are needed.
- ▶ **ISO-26262 Functional Safety deployment in process, but is not a complete solution.**

# Software Complexity (2/2)

- ▶ 5–10 yr:
  - Self-Healing mechanisms
    - This is not fault tolerance, it is low level software to take care of exceptions for example buffer overflow. This is in research. The goal is for each control unit to do self checking to keep alive and fail predictably. Eventually new software uploads uploaded in 10 year timeframe. Ability of the system to apply fixes, predetermined.
    - Fuzzy techniques to break down the system to model the interactions and/or entry points. Not currently used. Possible research topic.
    - Automatic generation of system models from requirements or existing partial models.

# Assurance Roadmap (1 / 3)

## 3–5 year:

- ▶ **Fail Safe Platform with supervisor controller**
  - Some aspects of fail–operational included.
  - Supervisor controller is part of the platform.
- ▶ **System run–time diagnosis and Built in self test**
- ▶ **System Test and Validation**
  - Virtual validation, HIL, etc.

# Assurance Roadmap (2 / 3)

**5–10 year:**

- ▶ **Formal analysis techniques**
- ▶ **Real-time analysis**
- ▶ **Probabilistic techniques**
- ▶ **Model-based testing and validation**
- ▶ **Moving from diagnosis to prognosis**
  - **Predicting failure before it happens to avoid the malfunction of the system/network.**



# Assurance Roadmap (3 / 3)

10–20 year:

- ▶ **Cost effective approach to Fail–operational**
- ▶ **The effects of architectures on Assurance, Safety and Security.**
  - Asymmetric redundancy management and correctness issue.
- ▶ **Dynamic reconfiguration of functions (in distributed systems)**
- ▶ **Reconfigurable Hardware platforms**
- ▶ **Deterministic Redundant Platforms**
  - **Networking (FlexRay , TT–Ethernet)**
    - Synchronization and scheduling
  - **ECU(s)**
    - Lessons learned from distributed world transfer to automotive
- ▶ **Cyber–Physical System Co–design**
  - Combining physics based principles with computer science
  - Resource Aware Control Methods
- ▶ **Formal Methods**
  - Scalability
  - Mixed mode (temporal vs discrete vs continuous)

# Security Roadmap (1 / 3)

- ▶ 3–5 year:
  - Adapt existing IT security techniques to automotive industry.
    - Low hanging fruit
  - Identify threat models (threats, actors, etc...)
  - Domain analysis
    - Physics of problem need to be brought into the analysis.
  - Develop a security specific automotive process
    - Standards,
    - Processes
    - Tools
    - culture

# Security Roadmap (2 / 3)

- ▶ 5–10 year:
  - Adapt existing IT security techniques to automotive industry.
    - Add rigor including more systematic methods (formal)
  - Trusted Hardware and Software Platforms for CPS systems
  - Secure V2x implementation and models
  - Production ready tool chain.
  - Supply chain and maintenance security solutions available.
  - Refine threat models (threats, actors, etc...)
  - Update Domain analysis
  - Refine security specific automotive process

# Security Roadmap (3 / 3)

10–20 year:

- ▶ Predictive Threat tools developed
  - Behavior analysis
  - Systematic at a higher level
- ▶ Continue to follow security community trends
- ▶ Automatic updating of security measures
- ▶ Develop monitor and enforce higher levels of security.
- ▶ Trusted Hardware and Software Platforms for CPS systems
- ▶ Secure V2x implementation and models
- ▶ Production–ready tool chain (support process)
- ▶ Supply chain and maintenance security solutions available.

# Recommendations for Institutions and Cross-Institutional Collaboration

- ▶ Data Sharing
  - Industrial strength data.
  - Action item: NHTSA Visteon Data from ACC field trial.
- ▶ Model Sharing
  - ▶ Action item: add NHTSA links to reports on vehicle models.
- ▶ Benchmarks for evaluating techniques
- ▶ Collaborative projects
  - Website with current issues and problems. NASA has something similar.
- ▶ Funding models:
  - Student support
  - In-kind support (e.g., tools, software, hardware)
  - Faculty/researcher visiting appointments
    - You can also do this with the government as well.
  - How can government agencies support the collaborations?
  - Mutually-beneficial IP agreements between university/industry

# The End

...for now

# Backup / Notes



# 3 Most Challenging Aspects Automotive Secure and High Confidence Platforms

---

## 1. Software Complexity

- Impossible to validate sufficiently through testing
- New business-models with more 2<sup>nd</sup> and 3<sup>rd</sup> parties developers

## 2. Cost effective

### Fail-Operational Systems

- Moving from Fail-Safe to Fail-Op
- Common mode of failures (EMC, Power Supply, Lightning, ...)

## 3. Cyber-Physical Security

- More connectivity into our vehicles
- More safety critical controls (towards autonomous driving and by-wire)
- Open-source platforms (for Infotainment)

*March 17-18 2011*

**NIST**



**USCAR**



- ▶ Security involves a human adversary that modifies or controls the system for what it's not designed.
  - The ability to make the car do something that the driver does not want it to do.
  - Human initiated.

# 3 most promising techniques for dealing with these challenges

## 1. Software Complexity

- **Model-based / Math-based design (current: Components, but full vehicle environment not widely used** Formal methods are needed. Component integration and full vehicle not currently done.)
- **Integration Methods (includes Models, tools, data)**
- **Formal Methods? Current:**
- **Automated Validation and testing**
- **Run-Time Safety monitors / Safety Goals violation(current: Do not use full safety monitor model in run time. Separate requirements for safety monitor is still needed. Formal methods are needed. Component integration and full vehicle not currently done.)**
- **Self-Healing mechanisms (not fault tolerance, it is low level software control unit to take care of exceptions for example buffer overflow. This is in research not currently done. Each control unit self checking to keep alive and fail predictably. Mode switching, if def. Eventually new software uploads uploaded in 10 year timeframe. Ability of the system to apply fixes, predetermined.**
- **Fuzzy techniques to break down the system to model the interactions and/or entry points. Not currently used. Possible research topic.**
- **When can you generate a state space model from UML model? -- Research path. From UML or requirements**
- **Formal Methods (current: research)**
- **ISO-26262 Functional Safety deployment**

March 17-18 2011



# Promising Approaches: Cyber-Physical Security

- ▶ **Security definition:** Security involves a human adversary that modifies or controls the system for what it's not designed.
  - The ability to make the car do something that the driver does not want it to do.
  - Human initiated
  - Malice may or may not be directly involved

# Cyber-Physical Security (contd; AA)

- ▶ **Security definition:**
  - Having a definition may not be necessary
- ▶ Should not design it as a “hard candy with a soft center” in that the design needs to be fool-proof with several layers of defense. At the same time, it should allow information to flow through.
- ▶ Security should be “adaptive” depending on the need.
- ▶ What are the relevant results/tools from general CS that can be applied to automotive systems? Differences?
  - Domain difference: the “owner” can be attacking it and not someone outside. Threats, solutions may be different. But the process of modeling may not be different.
  - The automotive domain is perhaps more an example of security engineering rather than something needs security research.
  - The underlying physics could be used for the security aspects as well.
    - The fault-tolerance principles could be applied to security as well.
    - Natural constraints in the physical dynamics can help in providing security specifications.
  - Methods for mitigating security breaches are dramatically different in the automotive domain.
  - Safety vs. security needs to be dealt with.
- ▶ **Key differences**
  - Environment under which it is built, and maintained.
  - Components come from different, non-validated, vendors

# Promising Approaches: Cyber-Physical Security (contd.AA)

- **Study of economic incentives: how much regulation/mandate is needed? That might drive the approaches.**
  - Highly inter-disciplinary
  - Private sector/Government-directed/etc.
  - Some aspects may be common to safety-related methodologies
- **Threat-models and therefore solutions are different depending on if someone has physical possession or not**
- **V2V/V2I may introduce multiple issues related to security.**
- **What are the carrots/sticks that can be introduced at the development side to help in security?**
  - Security culture in the OEM, etc. instead of being reactive to news-items
  - Methods for assurance in security engineering without having access to the details of the individual components
  - Assurance against failure modes should be expanded to include assurance for security as well.
    - Relevant topic for “science of integration”?

Something similar to ISO662 that occurred in the safety domain needs to happen in the security process as well. Relation between OEMs and vendors was discussed in the safety process –

Is there an easy mapping between “safety” and “security” science/culture/engineering?

Hardware fault-model is central to the safety process.