Autonomy & Transportation: Addressing Cyber-Resiliency Challenges

Andy Lacher, Unmanned and Autonomous Systems Research Lead
The MITRE Corporation
McLean, Virginia

10 June 2015
Presentation to the NIST Information Security and Privacy Advisory Board
MITRE is a private, independent, not-for-profit organization, chartered to work in the public interest. Founded in 1958 to provide engineering and technical services to the U.S. Air Force. Supports a broad and diverse set of sponsors within the U.S. government, as well as internationally.

NSEC
DoD’s National Security Engineering Center
Established 1958

CAASD
FAA’s Center for Advanced Aviation System Development
Established 1990

CEM
IRS’ and VA’s Center for Enterprise Modernization
Established 1998

HS SEDI
DHS’ Homeland Security - Systems Engineering and Development Institute
Established 2009

JEMC
Federal Judiciary’s Judiciary Engineering and Modernization Center
Established 2010

CAMH
DHHS’ CMS Alliance to Modernize Healthcare
Established 2012

NCCoE
NIST’s National Cybersecurity Center of Excellence
Established 2014

MITRE
© 2015 The MITRE Corporation All rights reserved.

Approved for Public Release: Distribution Unlimited. Case Number 15-1841
Increased Automation Moving Towards Autonomy
What’s Compelling the Increase in Autonomous Systems?

Increase safety, security, and prosperity

• Improve Safety
  – Reduce accidents
  – Reduce exposure to danger

• Improve Efficiency
  – Reduce manpower requirements
  – Reduce energy consumption

• Enable New Capabilities
Increasingly Autonomous Systems

• Unmanned Aircraft
• Flight Deck Automation
• Automated Driving
• Driverless Vehicles

Increased dependence upon
  ○ Software
  ○ Data
  ○ Command & Control Links

For safe, efficient, and secure operations

More than Cyber-Security
Think Cyber-Resiliency

Our increasingly complex automation systems must continue to function safely despite design defects, unanticipated situations/data, & deliberate attacks.
Increasingly Autonomous Systems

- More Complex
- Interconnected – Network effects
- Non-deterministic – Not repeatable
- Adaptive – Learning – Evolve over time

Low-end cars have 30-50 Electronic Control Units (ECUs) that talk over Controller Area Networks (CANs)

Source: http://www.informationisbeautiful.net/visualizations/million-lines-of-code/

Lines of Code

Avg High End Car
F-35 Fighter Jet
Chevy Volt
B787
Mars Curiosity Rover
Photoshop CS6
Hubble Space Telescope
F22 Raptor Fighter Jet
Space Shuttle

Source: http://www.informationisbeautiful.net/visualizations/million-lines-of-code/

Approved for Public Release: Distribution Unlimited. Case Number 15-1841
Cyber-Physical Systems

Failure has dire consequences
Consequences

- **Safety** – Increased Operational Risk
- **Efficiency** – Idle fleet
- **Security** – Vehicle Becomes a Threat
- **Privacy** – Unauthorized data access
Deliberate Attacks

• Denial or disruption of service
  – Jamming the C2 or GPS links
  – Malicious code

• Spoofed or false information could be introduced into operations
  – Erroneous navigational information
  – False intruders/collision threats or other obstacles

• Assume control – Third party controlling the vehicle
  – False commands
  – Malicious code

• Access to sensitive information
  – Authorized person with access to info collected during operation
Privacy

• Nearly 100% of cars on the market include wireless technologies.
• Most automobile manufacturers were unaware of or unable to report on past hacking.
• Manufacturers collect large amounts of data on driving history and vehicle performance.
• A majority offer technologies that collect and wirelessly transmit driving history data to data centers (e.g., 3rd-party), and most do not describe effective means to secure the data.
• Manufacturers use personal vehicle data in various ways usually involving 3rd-parties; Retention policies vary considerably.
• Customers are often not explicitly made aware of data collection and, when they are, they often cannot opt out without disabling valuable features, such as navigation.
Example: UAS Connectivity

"Fly-by-wireless" ➔ "Pilotless"

Operating

Non-Operating

Motor Vehicles & Manned Aircraft Have Similar Connectivity Issues
Other Examples

• Tesla Motors Over the Air Software Updates
• Aircraft Line Maintenance Software Loads
• Automotive Automatic Location Logging
• Electronic Flight Bags
• CANBUS / OBD Port Vulnerabilities
• GoGo / Inflight Entertainment
• GPS / ADS-B

…

"Hyundai owners can download the software on to USB drives for use with navigation ports to make their systems Android Auto compatible."

David van der Mark
Connected Vehicles

- Vehicle – to – Vehicle (V2V)
  - NHTSA plans to issue a proposal by 2016 on V2V safety messaging
- Vehicle – to – Infrastructure (V2I)

External Connectivity

Wireless: Key FOBs, WiFi, Bluetooth, LTE, etc.
Ports: OBD-II, CD/DVD Players, USB, etc.
Vulnerabilities

- Unexpected or Erroneous Data
  - Command and Control Link
  - Navigational Data
- Control System Processing Errors
- Unexpected Situations
- Software Updates with Design Defects or Operational Changes
- Malicious Code
- Data Breaches/Spills
Automotive Privacy Principles

- Transparency
- Choice
- Respect for Context
- Data Minimization, De-Identification & Retention
- Data Security
- Integrity & Access
- Accountability

Examples of Sensitive Information: Geolocation, Driver behavior, Biometric information

“...public commitment...”
“...may choose to adopt.”
“...commits to complying...as soon as practicable, but by no later than vehicle Model Year 2018.”
Auto-Information Sharing and Analysis Center (ISAC)

• Public announcement of commitment to create
  - Alliance of Automobile Manufacturers
  - Association of Global Automakers

• NHTSA encouragement

Trusted sector-specific entity that provides a central resource (24x7) for gathering information on cyber incidents, threats and vulnerabilities to critical infrastructure and providing two-way sharing of information between the private and public sectors.
The Government is Thinking About Increasingly Autonomous Systems
“Autonomous Systems are whatever machines haven't done yet”

– Tesler’s Theorem (ca. 1970 aka the AI effect)

Larry Tesler
Expert on human–computer interaction, Stanford, Xerox PARC, Apple, Amazon, and Yahoo!, often credited with designing ‘cut and paste’
Innovation Leadership from Industry Not Government

Brands and logos may be trademarked by their respective holder(s).

Approved for Public Release: Distribution Unlimited. Case Number 15-1841
Clash of Two Cultures

Information Technology

- Innovation
- Revolutionary
- Speed to market
- Entrepreneurial
- Open
- Minimally regulated
- Risk rewarded

Aviation

- Safety
- Evolutionary
- Proven
- Conservative
- Proprietary
- Tightly regulated
- Risk avoided

Small Unmanned Aircraft
Challenges

• Automation (e.g., vehicles, power grid, medical devices, command and control, etc) is becoming increasingly complex and interconnected

• As technology evolves, systems are becoming increasingly intelligent moving towards autonomy where the “machine” perceives, decides, learns, and acts, often without direct human engagement

• Ensuring that these sophisticated non-deterministic software systems are competent and remain resilient to design defects, unanticipated situations, and deliberate attacks is a Federal Government concern

• Our current mechanisms and policies for oversight, T&E, and certification of these systems are not keeping pace with technology change
Third-party Trust

Oversight

Trust Relationship
Framework for Discussing Trust

Trustworthiness

- Competence
- Collaboration
- Content

Trust

- Culture
- People
- Confidence
- Consequence
- Context
- Environment

System

Constraints

© 2015 The MITRE Corporation All rights reserved. Approved for Public Release: Distribution Unlimited. Case Number 15-1841
Cyber-Resiliency – Technical Topics

- Cybersecurity (CS)
- Software Assurance (SW)
- T&E / V&V (Test)
- Trustworthy Autonomy (TA)

Cyber-Resiliency

© 2015 The MITRE Corporation. All rights reserved.

Approved for Public Release: Distribution Unlimited. Case Number 15-1841
Conclusions

• Can’t just think about cyber-security independently of other cyber-resiliency issues

• Need confidence that our cyber-physical systems will function as intended despite:
  − Design defects
  − Unanticipated data/situations
  − Deliberate attacks

• Think about vulnerabilities of the system
  − While operating
  − Not operating but connected
Thank You
Backups
Perspectives on Trust

Insurer
- How do I use this?
- Can I trust it?
- Am I responsible if it makes a mistake?

Operator
- How do I use this?
- Can I trust it?
- Am I responsible if it makes a mistake?

Researcher
- What technology is needed to ensure trust?

Creator
- How should I design and build?
- Will I be liable for problems?

Commander/Supervisor
- Can I reliably use in operations?
- What changes operationally?

Regulator
- Is it safe?

Community
- Do I want this in my backyard?
- Can I count on it?

Acquirer
- How do I express requirements?
- Will it work they way it should?

Patron
- Is it safe?
- Should I use it?
- Can I count on it?

© 2015 The MITRE Corporation. All rights reserved.

Approved for Public Release: Distribution Unlimited. Case Number 15-1841
## Perspectives on Trust

<table>
<thead>
<tr>
<th>Role/Questions</th>
<th>What is at Risk?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Researcher</td>
<td>Reputation</td>
</tr>
<tr>
<td>Regulator</td>
<td>Reputation, Job security, Public trust</td>
</tr>
<tr>
<td>Creator</td>
<td>Reputation, Job security, Employer’s finances</td>
</tr>
<tr>
<td>Insurer</td>
<td>Job security, Employer’s finances</td>
</tr>
<tr>
<td>Community</td>
<td>Personal safety, Personal property/ finances</td>
</tr>
<tr>
<td>Acquirer</td>
<td>Job security, Employer’s finances, Mission effectiveness</td>
</tr>
<tr>
<td>Commander/Supervisor</td>
<td>Job security, Mission effectiveness, Personal safety, Personal finances</td>
</tr>
<tr>
<td>Operator</td>
<td>Job security, Mission effectiveness, Personal safety, Personal finances</td>
</tr>
<tr>
<td>Patron</td>
<td>Personal safety, Personal finances, Personal property</td>
</tr>
</tbody>
</table>
Multi-party Trust
A Network You Can Trust

- Manufacturers
- Pilot
- ATC
- Flight Surgeon
- Insurer
- Airlines
- Regulator (Federal Aviation Administration, Dept of Transportation)
- Maintainer
- TSA
- Unions
- Airport
• Safety by Design
• Third Party Collaboration (Responsible Disclosure)
• Evidence Capture (Forensically secure logging)
• Security Updates (i.e. over-the-air)
• Segmentation and Isolation (Separate safety from entertainment)
Example: Degree of Pilot Control

- **Direct Control**
  - Pilot continuously controls pitch, bank, yaw, and power

- **Direct Guidance**
  - Pilot controls heading, speed, and altitude
  - Auto-stabilized

- **Pilot-Managed Automatic**
  - Pilot Manages Flight
  - Auto T/O Land
  - Waypoint-to-Waypoint
  - Auto Taxi
  - Pilot required

- **Fully Automatic**
  - Pilot Manages Flight
  - Can operate w/o pilot-in-the-loop
  - Auto T/O Land
  - Waypoint-to-Waypoint
  - Auto Taxi

- **Autonomous**
  - Software using perception and judgment to alter flight path
  - Can operate w/o pilot

- **Pilotless**
  - Remotely Pilot

- **Chasm**
Dependability* of Software of Unknown Pedigree (SOUP)

How can the dependability of Software of Unknown Pedigree (SOUP) be assessed so it can be used in aviation safety-critical applications?

SOUP: software item previously developed for which adequate records of the development processes are not available

Approach:

• Analyze and assess processes and techniques from other safety-critical applications where SOUP has been considered or employed

✓ Synthesize, tailor and propose a framework for aviation

• Evaluate framework with case studies

Status

• Reviewed other industries; Completed framework; Peer Review

• Established relationship w/ 3 UAS SW developers for case studies

• Working through 3 case studies in parallel

*Encompass both safety & security aspects
Cyber-Resiliency - Domains

- Automated Driving
- Driverless Vehicles
- Unmanned Aircraft
- Flight Deck Automation

Automated Vehicles
Cyber-Resiliency Research – Masquerading in Other Areas

• Trusted computing
• Cybersecurity
• Reliability
• Software Assurance
• Liability Attribution
• Assured / Trustworthy Autonomy
• Complexity Research
• Software Forensics
• Airworthiness – Safety Cases
• Trusted E-Commerce
• Software T&E / V&V
Trade-off
Teleoperation vs. Automation

- Direct Control
- Autonomous Operations

Safety Critical of System Components

Command and Control Link

Control System SW Reliability

High
Low

Degree of Automation

Notional

Mission Scenario Risk

Degree of Automation

SW Reliability

Safety Critical of System Components

Approved for Public Release: Distribution Unlimited. Case Number 15-1841
How do UAS Differ From Legacy Aircraft?

- No pilot on-board – Fly-by wireless
  - Situation awareness reduction
  - Command and control vulnerabilities
  - Automatic → Autonomous Operations

- Can be smaller

- Often not designed or constructed to established aircraft standards

- Different flight performance and mission profiles
  - Low altitude operations
The UAS Community is Growing Rapidly

Deloitte sees 1 million commercial drones flying [globally] in 2015

The Small Unmanned Aerial Systems (sUAS) market will surpass US$8.4 billion by 2018 ....ABI Research, Small Unmanned Aerial Systems (sUAS) Solutions Ecosystem

- **Authorized Operations**
  - Receive FAA approval via a Certificate of Authorization, Special Airworthiness Certificate – Experimental, or Exempted for a specific purpose; Public agencies (military, law enforcement, academics, test sites) and commercial (section 333); Operating under significant scrutiny
  - Typically flying for the fun of flight; Tend to operate at designated flying fields; Often part of an Aeromodeler club; Sweat equity invested in aircraft

- **New Recreational Flyers**
  - Typically purchased ready to fly or near ready to fly aircraft; Mostly flying aircraft with automated flight stabilization; Flying to augment other interests (e.g., photography, etc.); Tend to be unaware of aviation rules/culture; Not part of an Aeromodeler community
  - Exponential & Exponential Growth
  - Selling >50,000/month

- **Unauthorized Operators**
  - Receiving some form of compensation for flight; Using hobby grade equipment, Mostly flying aircraft with automated flight stabilization

- **Traditional Model Aircraft**
  - 170,000 Members of Academy of Model Aeronautics
  - 1: Academy of Model Aeronautics (http://www.modelaircraft.org/aboutama/whatisama.aspx)

- **Little operational safety data**

---

1: Academy of Model Aeronautics (http://www.modelaircraft.org/aboutama/whatisama.aspx)
2: Privileged discussions with UAS manufacturers
Section 333 Use Cases Above 5%

- Construction Monitoring: 1%
- Training and Education: 2%
- Precision Agriculture: 3%
- Not Specified: 3%
- Infrastructure Inspection: 7%
- Movie and TV Production: 7%
- General Aerial Surveying: 8%
- Real Estate Photography: 11%
- Aerial Photography: 21%
- Mixed Use: 39%
TYPE OF POWER PLANT

- Internal Combustion, 9, 0%
- Not Specified, 14, 1%
- Electric, 2184,
MITRE’s View on the Challenges of Making Autonomy Real

Existing MITRE Engagement

- Design/Architecture
- Perception Technology
- Standards/Requirements
- Reasoning Technology
- Human-Machine Interaction
- Manipulation Technology
- Distributed Decisions
- Cyber-Physical Security
- Trust
- Systems
- Training
- Operations
- Modeling & Simulation
- Regulations
- Analytics & Behavior Diagnosis
- Liability
- Scoring Correctness
- T&E, V&V, Certification
- Practices
- Enablers
Trust vs. Trustworthy

**Trust:** Status of confidence in the mind of human beings based upon their perception and expectation of performance

**Trustworthy:** Inherently secure, available, and reliable; Competent; Does what people expect it to do – and not something else – despite environmental disruption, human user, and operator errors, and attacks by hostile parties.
Resilient Automation System

• “Resilience is the ability to prepare and plan for, absorb, and recover, from and more successfully adapt to adverse events” – *Disaster Resilience: A National Imperative*, National Academy of Science

• Able to continue to function (perhaps slightly degraded) as a result of human errors, automation anomalies, unanticipated inputs/data, missing data, spoofed data, lapses in cyber security, etc.
Aviation Risks

Death or injury of persons:

- **On board**
  - Resulting from a mishap
- **On board another aircraft**
  - Resulting from a mid-air or surface collision between two or more aircraft/ground vehicles
- **On the ground**
  - Resulting from a mishap or collision.

Risks are managed by:

- Certification of aircraft
- Licensing of airmen
- Establishment of operational rules
Thank You