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 Manages Seven FFRDCs
(Federally Funded Research and Development Centers)

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

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

Increased Automation Moving Towards Autonomy


www.bls.gov


www.cbp.gov


www.panynj.gov


Nyc.gov


www.hood.army.mil

www.fda.gov


www.hood.army.mil


www.dot.gov


www.ct.gov


Af.mil


www.boeing.com

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

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

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

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.

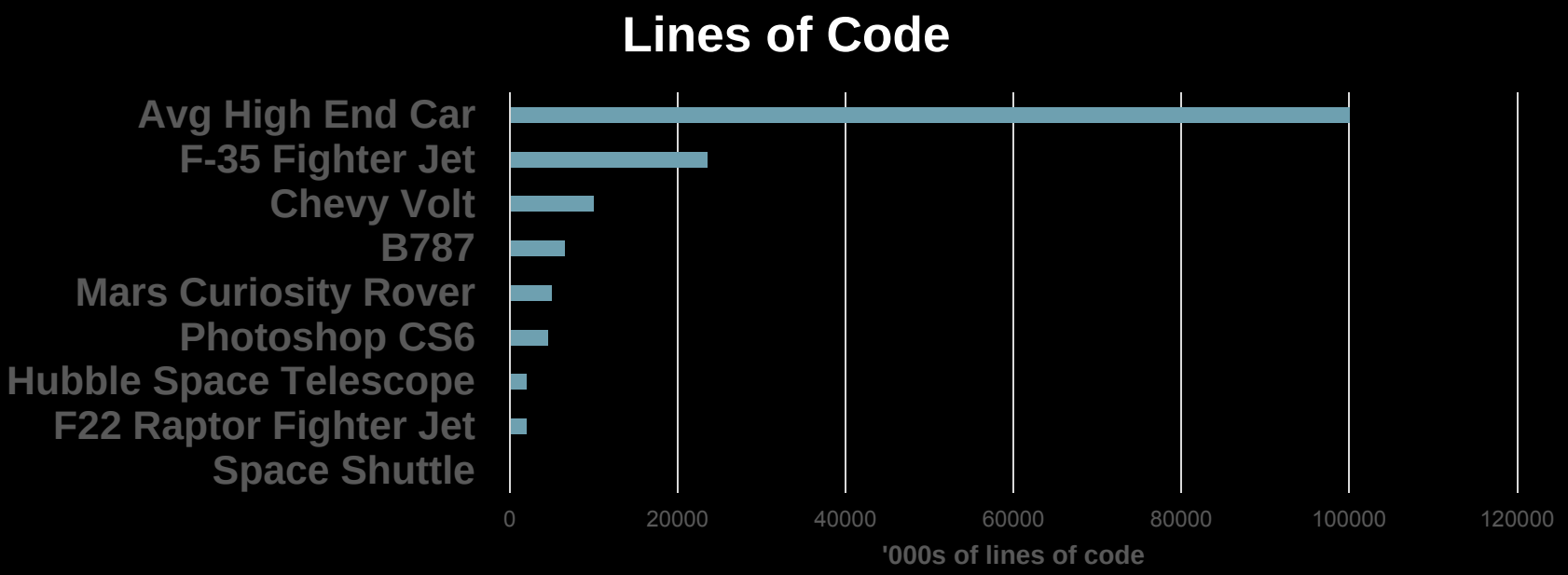
Approved for Public Release: Distribution Unlimited. Case Number 15-1841

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)

www.linkedin.com/pulse/20140626152045-3625632-car-software-100m-lines-of-code and counting



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

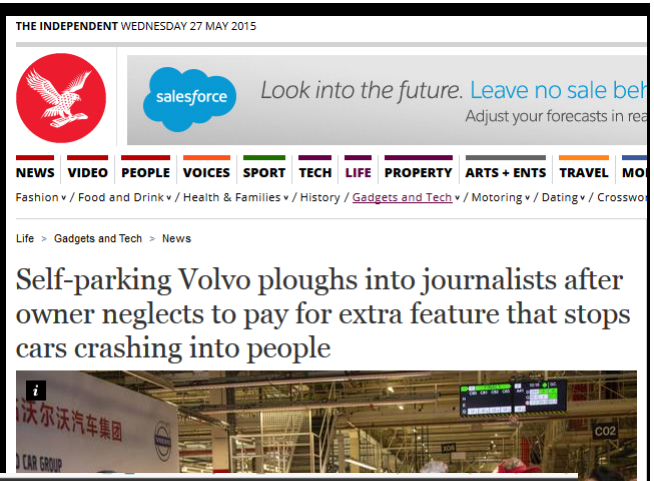
Cyber-Physical Systems

Failure has dire consequences

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

Consequences

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


THE INDEPENDENT WEDNESDAY 27 MAY 2015

NEWS | VIDEO | PEOPLE | VOICES | SPORT | TECH | LIFE | PROPERTY | ARTS + ENTS | TRAVEL

Life > Gadgets and Tech > News

Self-parking Volvo ploughs into journalists after owner neglects to pay for extra feature that stops cars crashing into people


REUTERS

Plane safe? Hacker case points to deeper cyber issues

BY JEREMY WAGSTAFF

May 26 Security researcher Chris Roberts made headlines last month when he was hauled off a plane in New York by the FBI and accused of hacking into flight controls via his underseat entertainment unit.


NTSB


PCWorld

United, American airlines account fraud highlights hacker focus on travel industry

Jeremy Kirk
IDG News Service

More than 20 travel-related websites have experienced data breaches in the past two months, according to a security expert who tracks the trade in stolen data.

Data from those websites is being sold on underground forums by cybercriminals, said Alex Holden, CTO of Hold Security, a company that specializes in monitoring the illegal trade and alerting companies if their data is found


USAF


THE WALL STREET JOURNAL. | THE CIO REPORT

CIO Journal

CIO REPORT | CONSUMERIZATION | BIG DATA

American Airlines iPad App Glitch Traced to Database Software

COMMENTS (1)

CLINT BOULTON

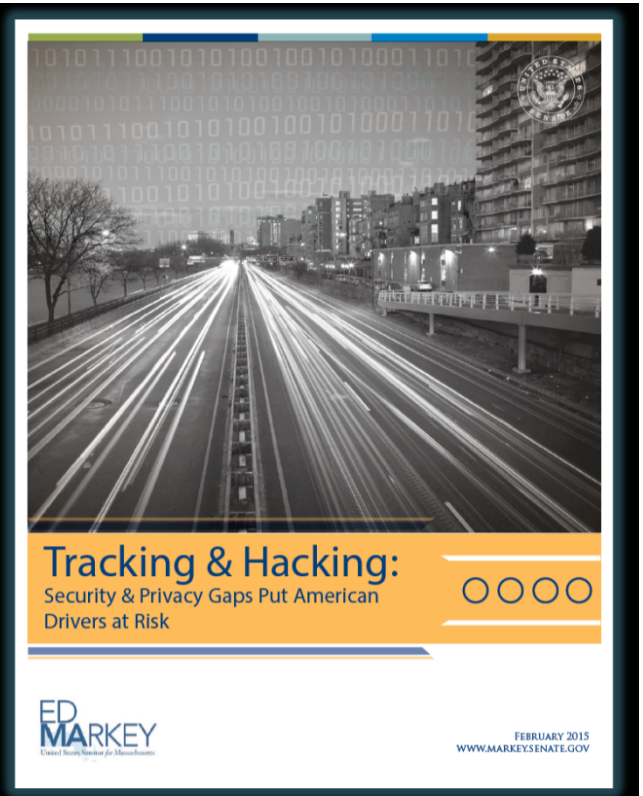
Approved for Public Release: Distribution Unlimited. Case Number 15-1841

Deliberate Attacks

- **Denial or disruption of service** — Safety & Efficiency
  - Jamming the C2 or GPS links
  - Malicious code
- **Spoofed or false information could be introduced into operations** — Safety & Efficiency
  - Erroneous navigational information
  - False intruders/collision threats or other obstacles
- **Assume control – Third party controlling the vehicle** — Safety & Security
  - False commands
  - Malicious code
- **Access to sensitive information** — Privacy & Security
  - Authorized person with access to info collected during operation

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

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.

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

Example: UAS Connectivity

"Fly-by-wireless" → "Pilotless"

Operating

Beyond Radio Line of Sight

Radio Line of Sight

Data Uploads
Software Downloads

Non-Operating

WiFi
Public Internet

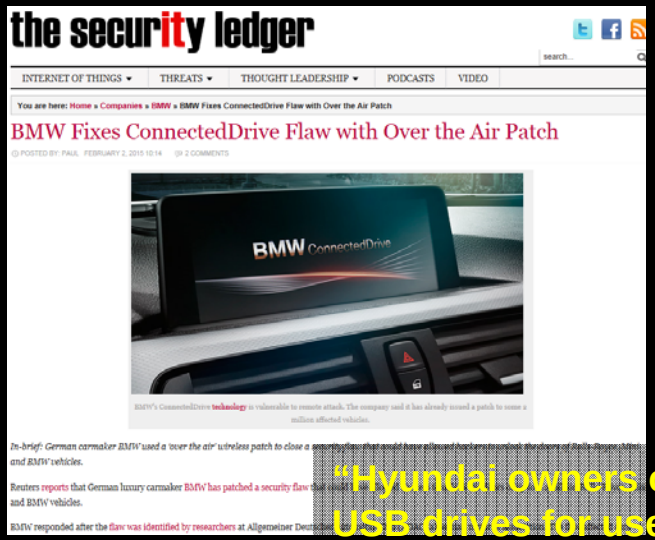
C2 Link

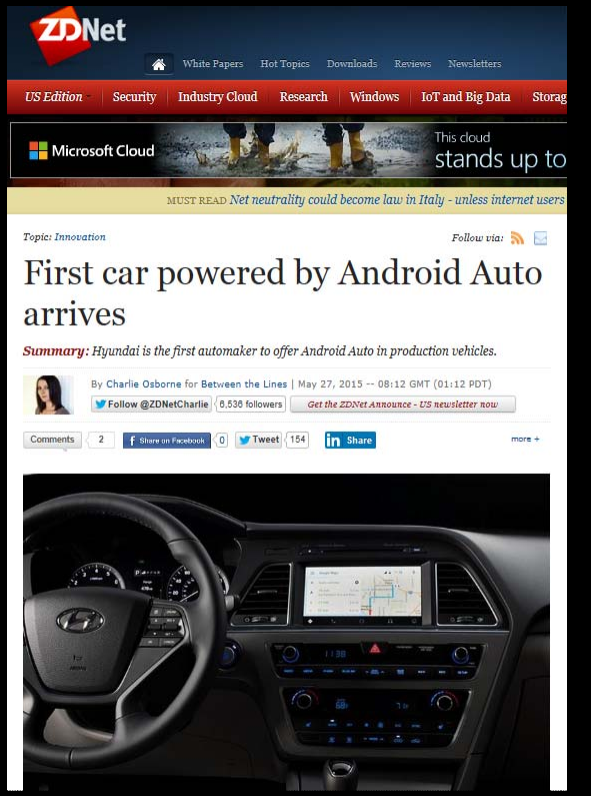
Motor Vehicles & Manned Aircraft Have Similar Connectivity Issues

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

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."

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

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.

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

Vulnerabilities

- Unexpected or Erroneous Data
  - Command and Control Link
  - Navigational Data
- Control System Processing Errors
- Unexpected Situations

Operating

- Software Updates with Design Defects or Operational Changes
- Malicious Code
- Data Breaches/Spills

Non-Operating

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

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

AUTO ALLIANCE DRIVING INNOVATION® GlobalAutomakers

November 12, 2014

The Honorable Edith Ramirez
Chairwoman
U. S. Federal Trade Commission
600 Pennsylvania Avenue, N.W.
Washington, DC 20580

Dear Chairwoman Ramirez:

Re.: Consumer Privacy Protection Principles for Vehicle Technologies and Services

On behalf of the Participating Members of the Alliance of Automobile Manufacturers, Inc. ("Alliance") and the Association of Global Automakers ("Global Automakers"), we are submitting to you Consumer Privacy Protection Principles for Vehicle Technologies and Services. The Participating Members are publicly committing to implement these Principles.

Starting in the Spring of 2014, Members of the Alliance and Global Automakers came together to create a set of privacy principles for vehicle technologies and services ("Principles"), to which members of the Associations and others can agree to as baseline privacy commitments.

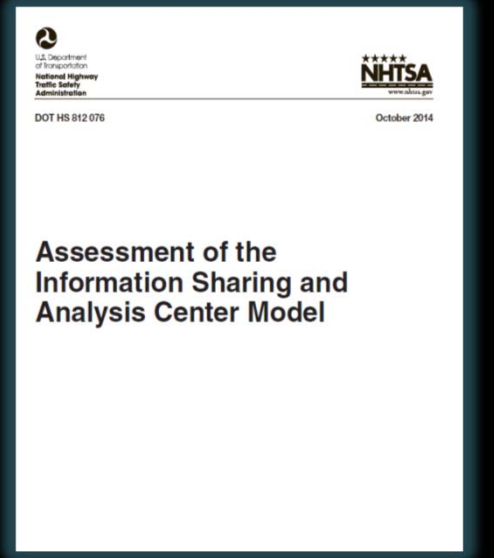
The Principles reflect a major step in the protection of personal information collected through in-car technologies. Although individual Members of both Associations have long protected the personal information under their control, the Principles mark the first industry-wide statement of privacy principles showing a commitment to responsible stewardship of the information used to provide vehicle technologies and services. Sensitive information, like geolocation information and driver behavior information receives heightened protections.

"…public commitment…"
"…may choose to adopt."
"…commits to complying …as soon as practicable, but by no later than vehicle Model Year 2018."

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

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

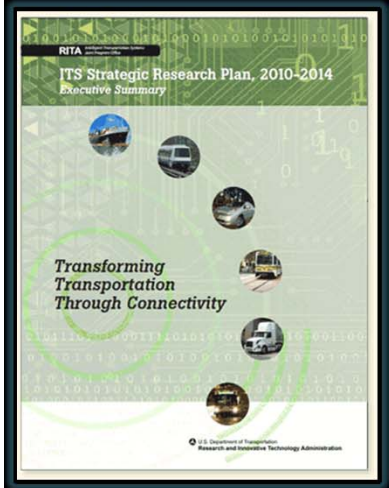
AUTO ALLIANCE
DRIVING INNOVATION®

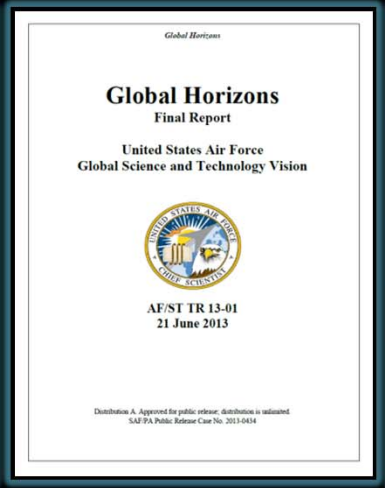
NHTSA
NATIONAL HIGHWAY TRAFFIC SAFETY ADMINISTRATION

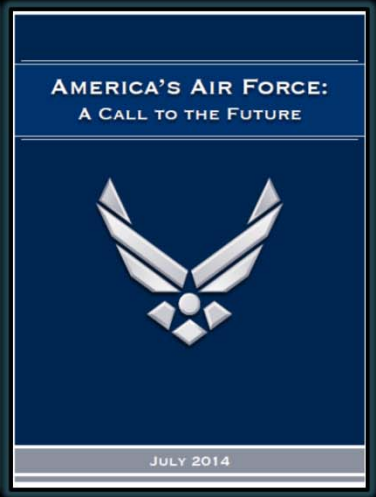
GlobalAutomakers

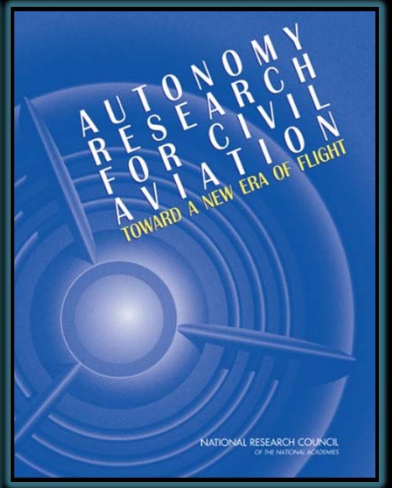
Approved for Public Release: Distribution Unlimited. Case Number 15-1841

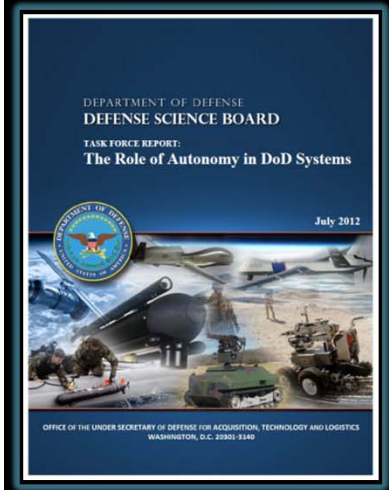
The Government is Thinking About Increasingly Autonomous Systems

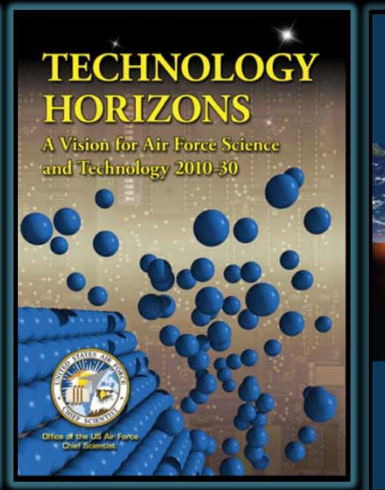


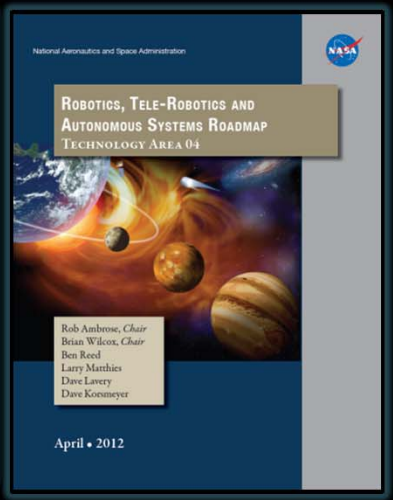


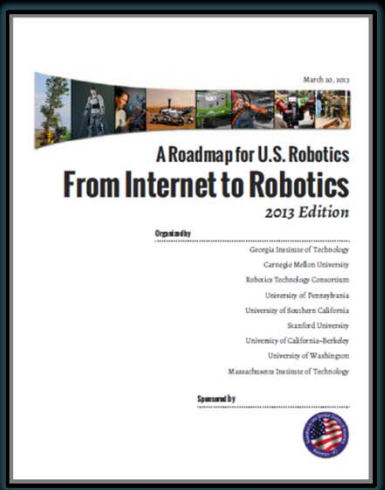


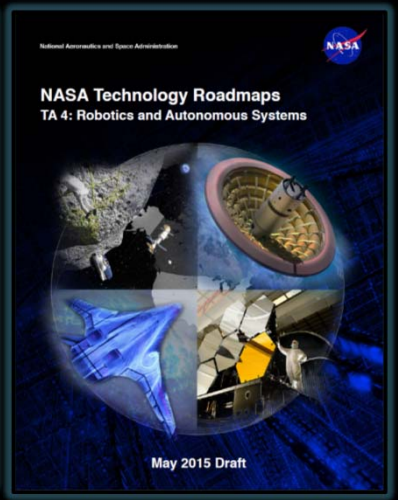












Approved for Public Release: Distribution Unlimited. Case Number 15-1841

“*Autonomous Systems are* whatever machines haven't done yet”

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

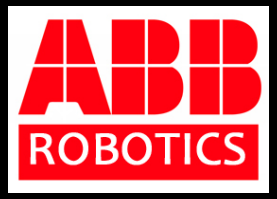
Yahoo via Creative Commons

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

Mercedes-Benz

JOHN DEERE



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

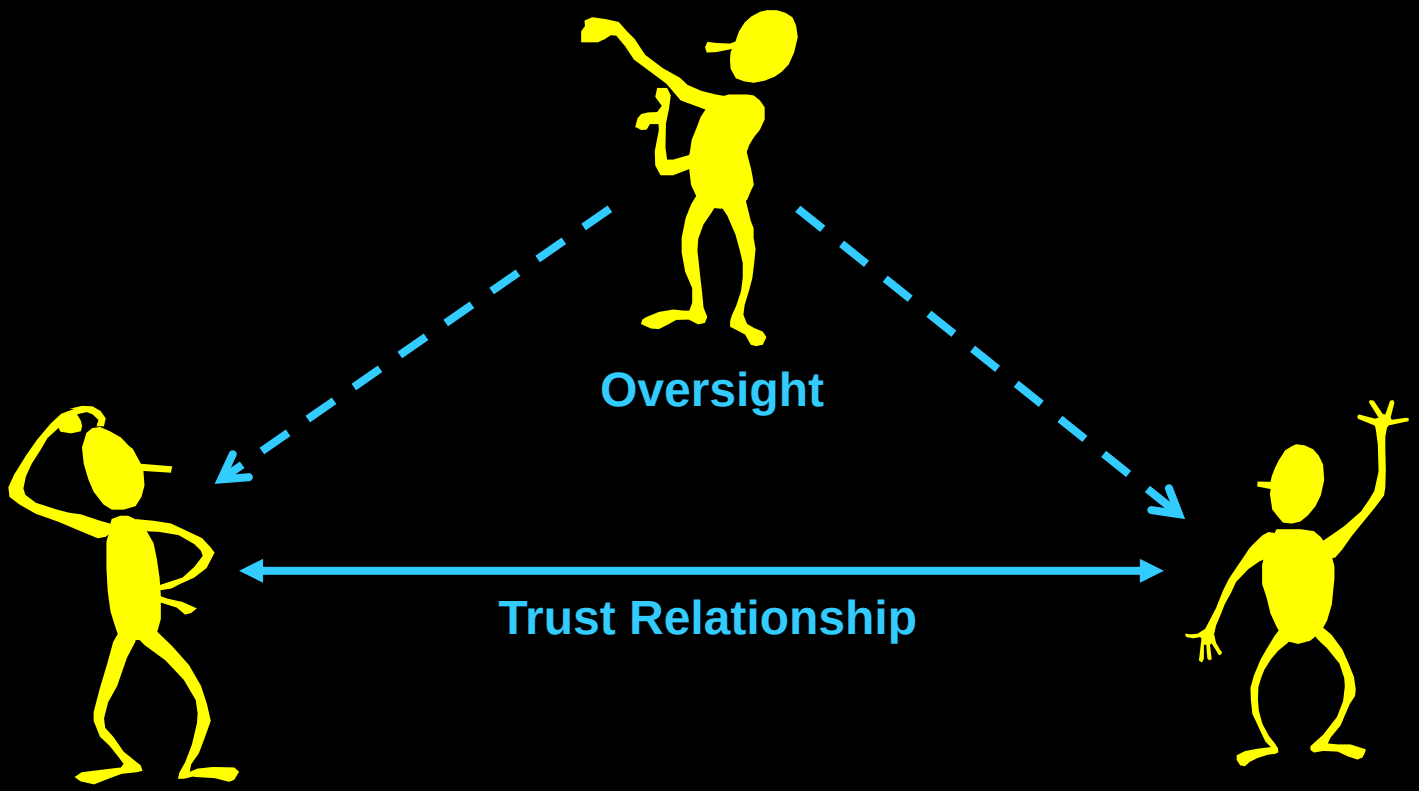
Approved for Public Release: Distribution Unlimited. Case Number 15-1841

Challenges

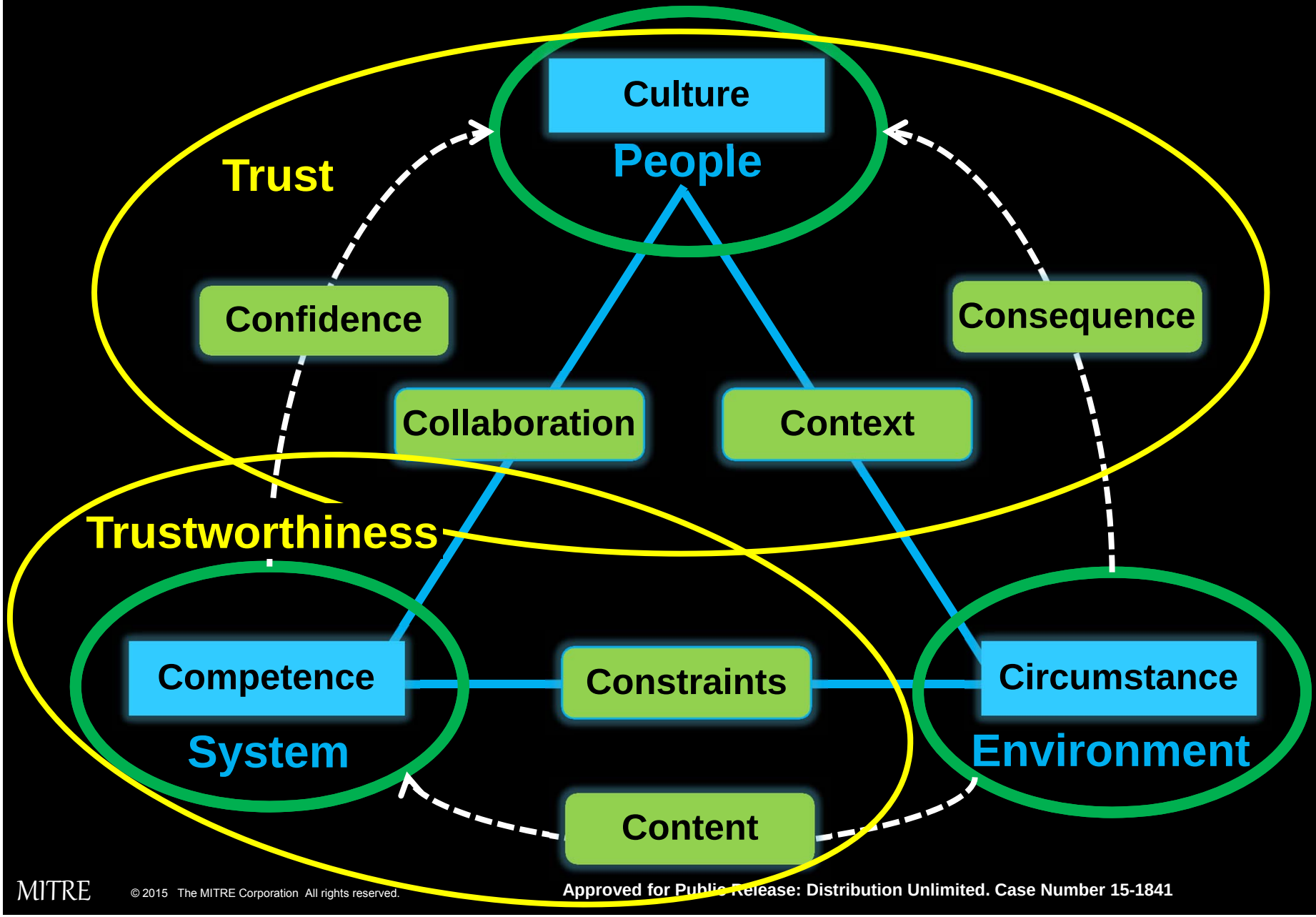
- Automation (e.g., vehicles, power grid, medical devices, command and control, etc) is becoming increasingly **complex** and **interconnected**
- As technology evolves, systems are becoming increasingly intelligent moving towards autonomy where the "machine" **perceives, decides, learns, and *acts*, 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**

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

Third-party Trust

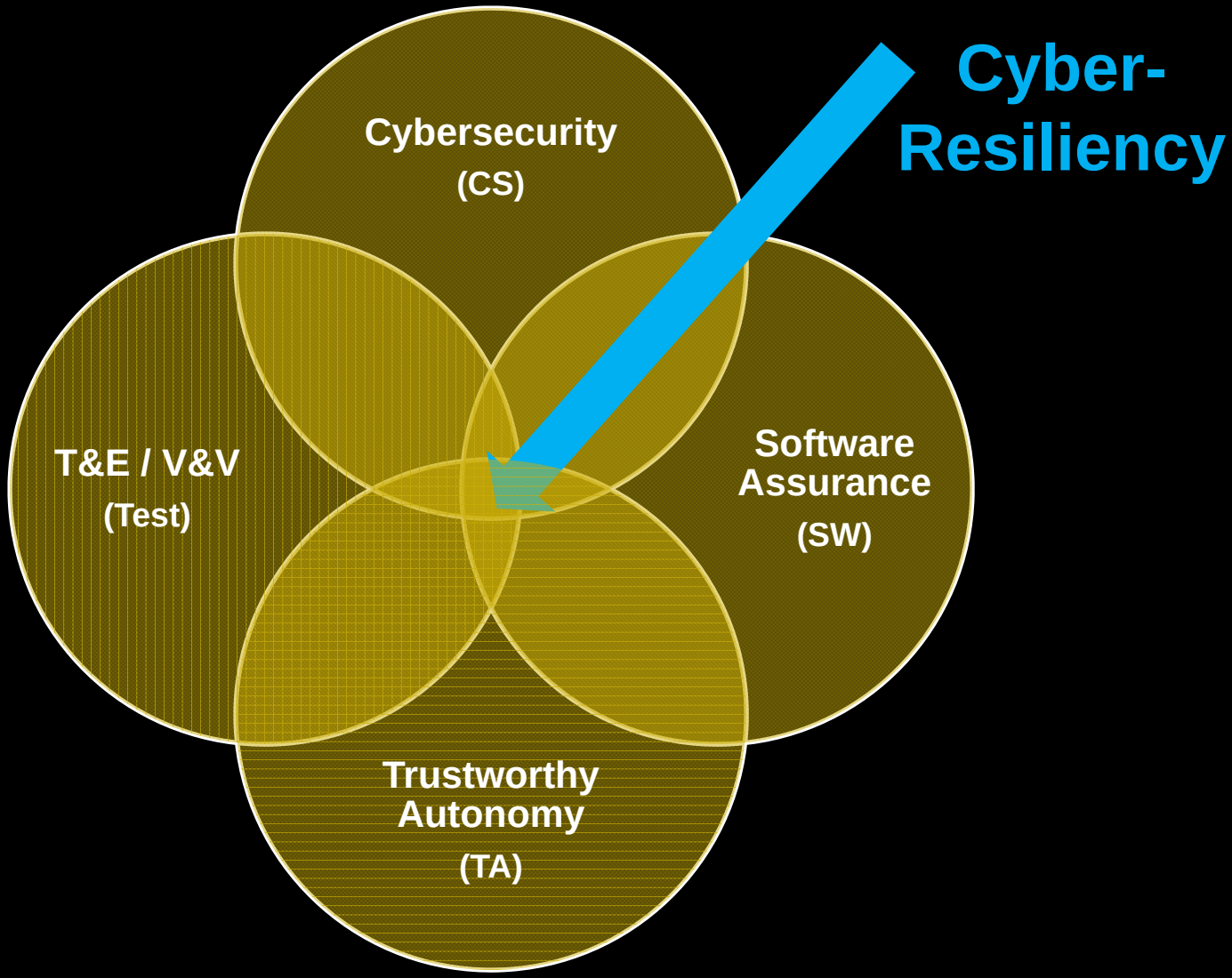


Framework for Discussing Trust



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

Cyber-Resiliency – Technical Topics



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

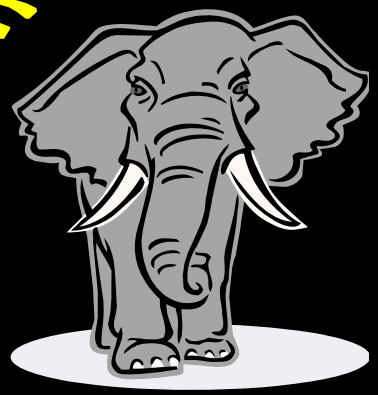
Approved for Public Release: Distribution Unlimited. Case Number 15-1841

Thank You

Audi RS 7 piloted driving concept. Photo by Audi Co

Backups

Perspectives on Trust



Insurer

How do I underwrite?

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?

Commander/ Supervisor

- Can I reliably use in operations?
- What changes operationally?

Creator

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

Regulator

Is it safe?

Community

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

Acquirer

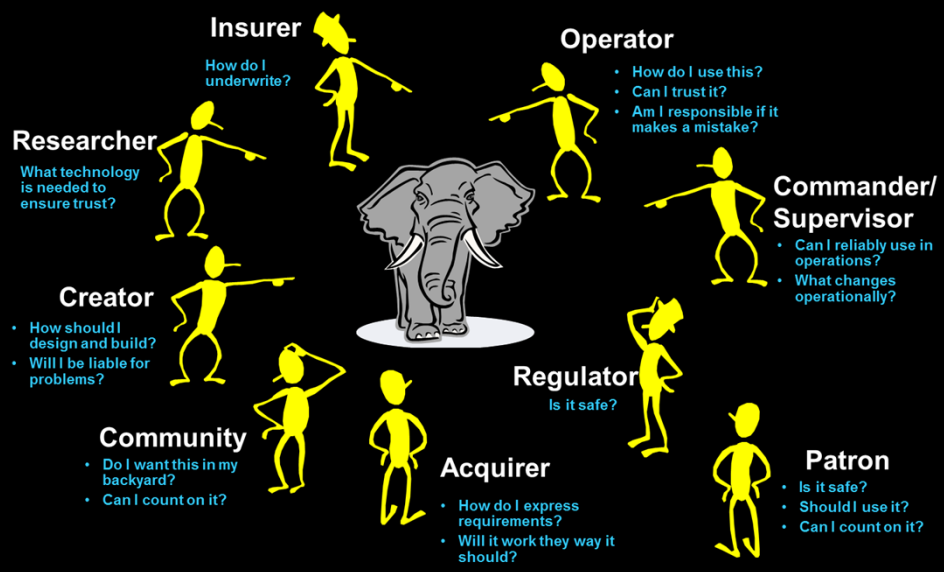
- How do I express requirements?
- Will it work they way it should?

Patron

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

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

Perspectives on Trust

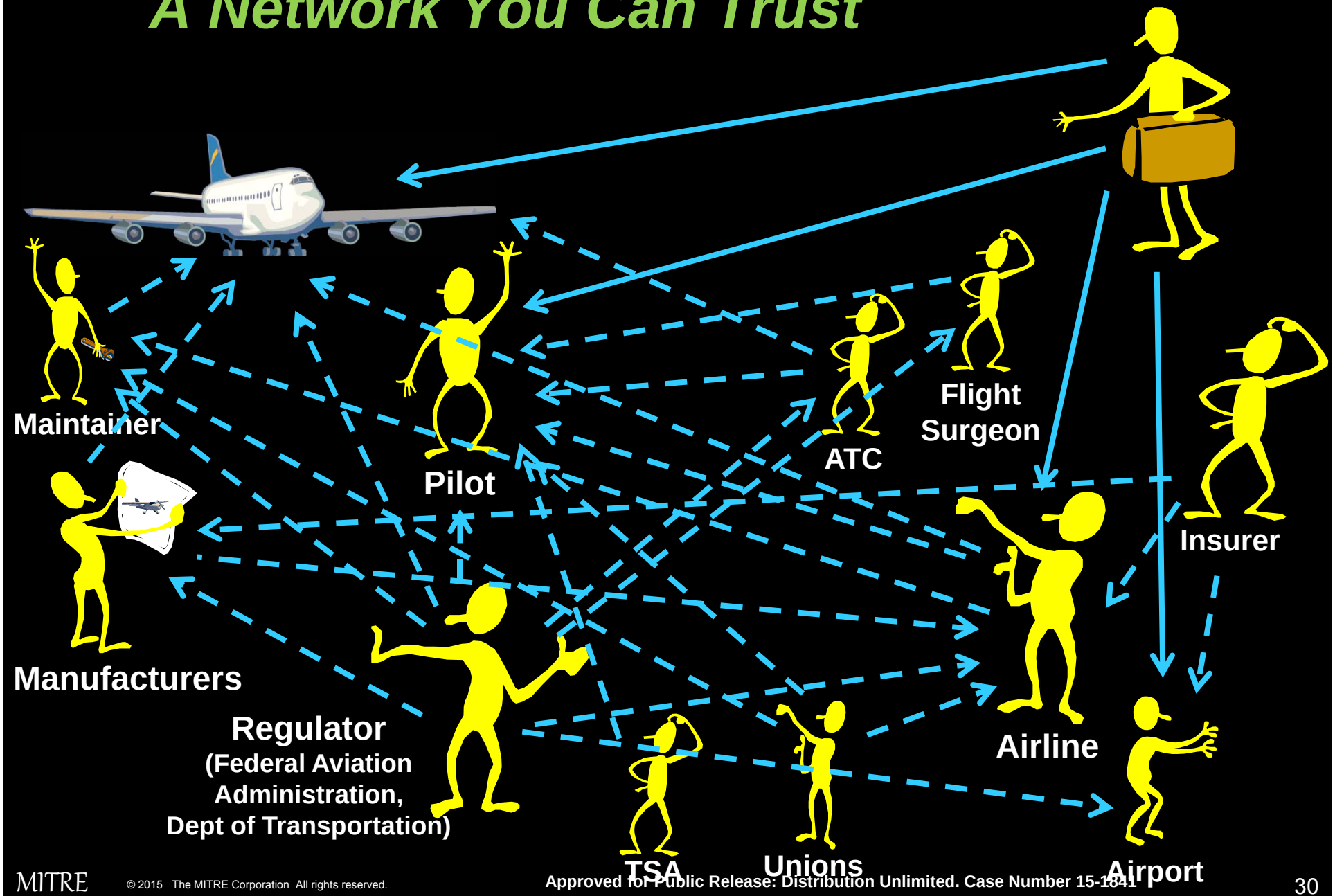


Role/Questions	What is at Risk?
Researcher	Reputation
Regulator	Reputation Job security Public trust
Creator	Reputation Job security Employer's finances
Insurer	Job security Employer's finances
Community	Personal safety Personal property/ finances
Acquirer	Job security Employer's finances Mission effectiveness
Commander/ Supervisor	Job security Mission effectiveness Personal safety Personal finances
Operator	Job security Mission effectiveness Personal safety Personal finances
Patron	Personal safety Personal finances Personal property

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

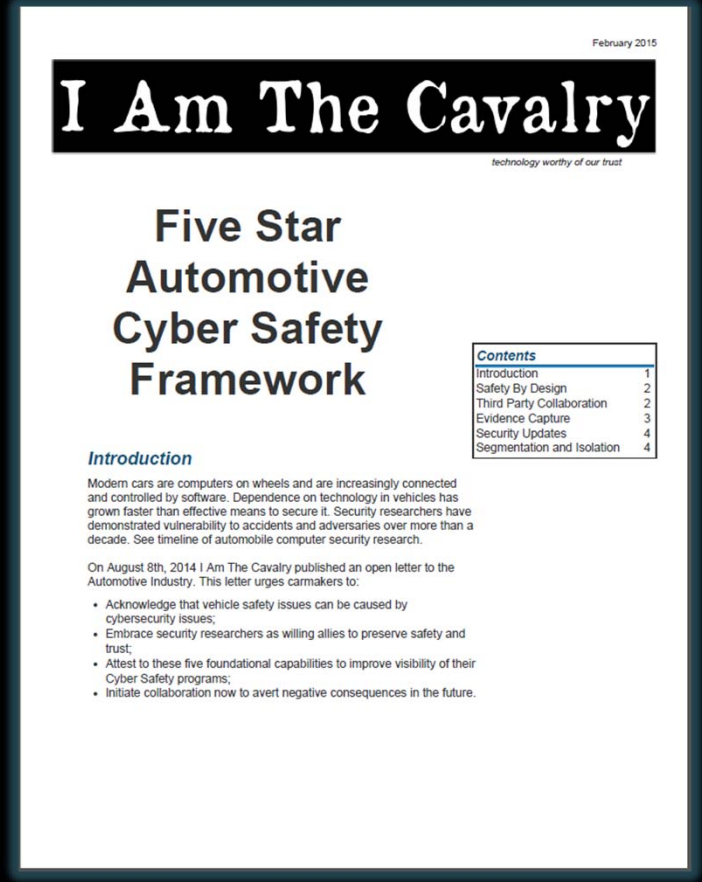
Multi-party Trust

A Network You Can Trust



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

- **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)**



February 2015

I Am The Cavalry

technology worthy of our trust

Five Star Automotive Cyber Safety Framework

Contents

Introduction

Modern cars are computers on wheels and are increasingly connected and controlled by software. Dependence on technology in vehicles has grown faster than effective means to secure it. Security researchers have demonstrated vulnerability to accidents and adversaries over more than a decade. See timeline of automobile computer security research.

On August 8th, 2014 I Am The Cavalry published an open letter to the Automotive Industry. This letter urges carmakers to:

- Acknowledge that vehicle safety issues can be caused by cybersecurity issues;
- Embrace security researchers as willing allies to preserve safety and trust;
- Attest to these five foundational capabilities to improve visibility of their Cyber Safety programs;
- Initiate collaboration now to avert negative consequences in the future.

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

Example: Degree of Pilot Control


Draganflyer X6 Photo: www.PRWeb.com


Photo: US Army


Photo: USCG

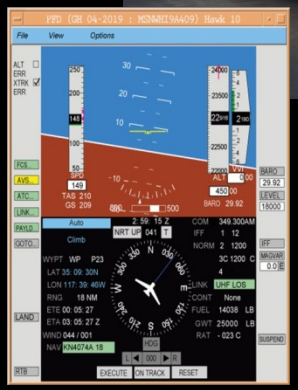


Photo: USAF


U.S. Air Force photo by Airman 1st Class Michael Shoemaker


Photo: USAF

Chasm

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 Flt
- 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

Remotely Pilot

Pilotless

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

Dependability* of Software of Unknown Pedigree (SOUP)

PI: Dr. Steve Cook

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

Category	ID	Level	Assessment	Task	Description	Security	Space	Aviation	Medical	Nuclear	Rail
US - Use of SOUP	US. 1	MINIMAL	QL	Conduct Hazard Analysis	Conduct an analysis to determine the hazards and impacts associated with the potential malfunction, failure, or exploitation of the SOUP. Define the SOUP's intended function. Determine the consequences and possible mitigations for each potential malfunction, failure, threat, or exploitation. Document how the SOUP fails (gracefully or suddenly). The analysis should be conducted in a manner similar to SAE ARP 4761, MIL-STD-882, or equivalent and should address risk associated with potential security and safety vulnerabilities (e.g., RTCA DO-326, Airworthiness Security Process Specification).	BSIMM AM1.3	NASA-STC-8719.13 C, App. A, F	RTCA DO-278A RTCA DO-326 Sec. 2.3.3	IEC 62304; see Section 7.1	European Regulatrs; see Section 2.2.3	DOT/FRA/ORD-03/14 Final Report April 2003; see Figure 3 page 21.

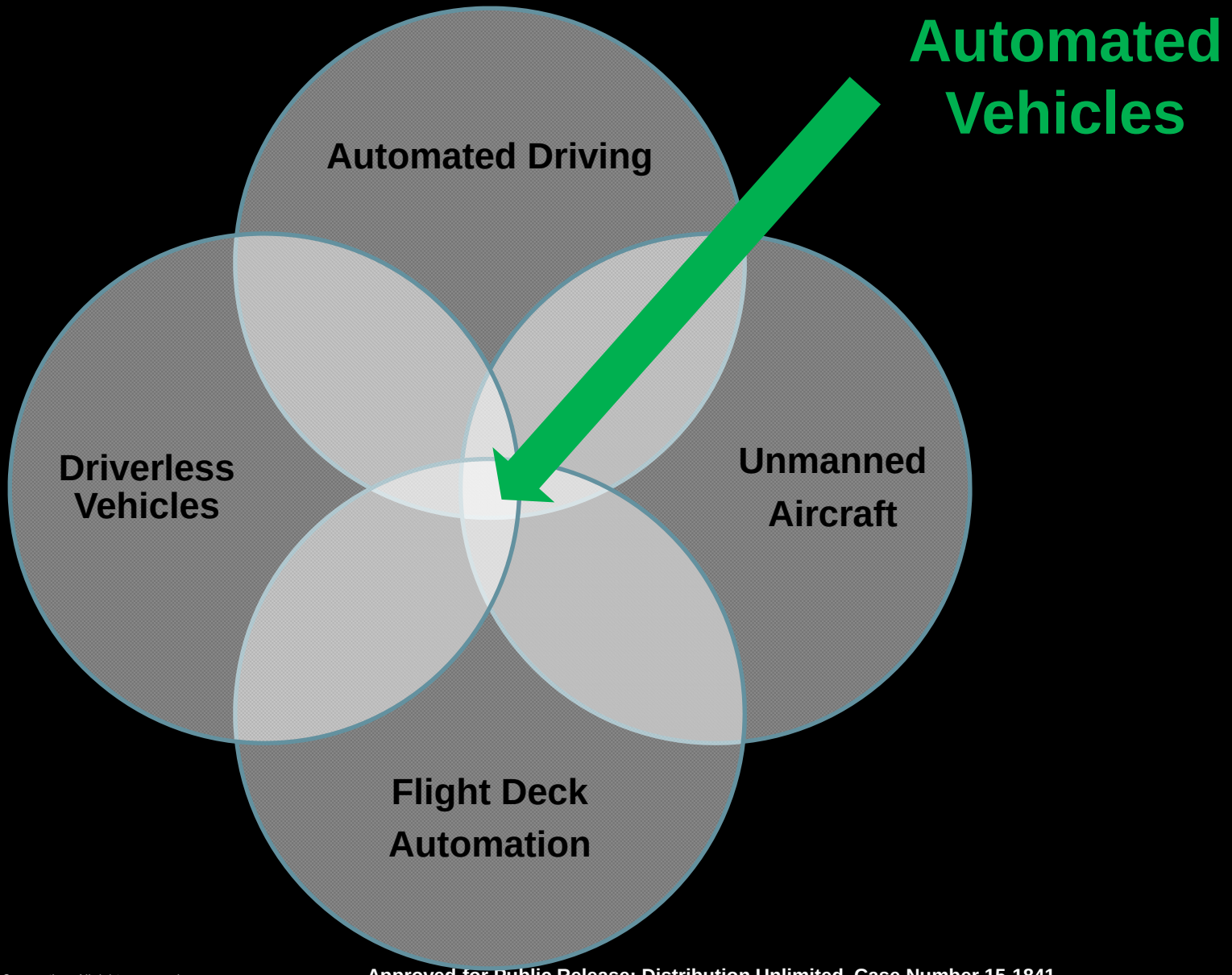
Peer Reviewed

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



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

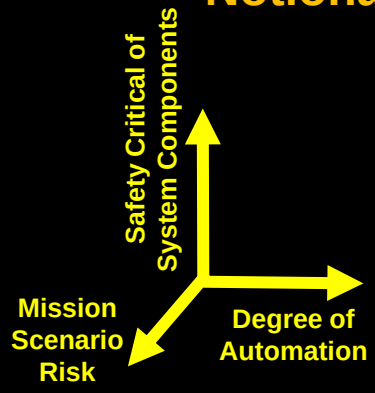
Cyber-Resiliency Research – Masquerading in Other Areas

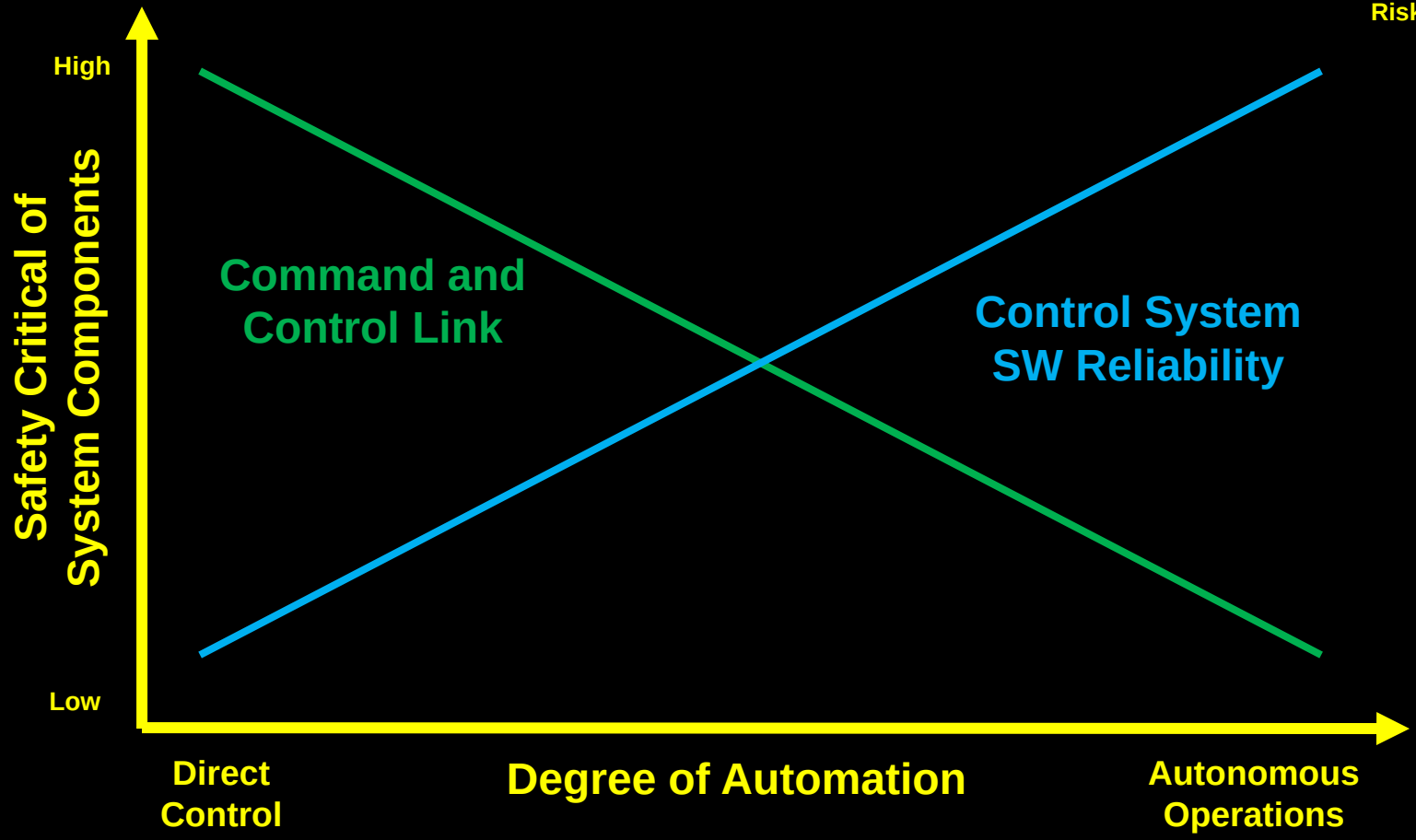
- Trusted computing
- Cybersecurity
- Reliability
- Software Assurance
- Liability Attribution
- Assured / Trustworthy Autonomy
- Complexity Research
- Software Forensics
- Airworthiness – Safety Cases
- Trusted E-Commerce
- Software T&E / V&V

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

Trade-off
Teleoperation vs. Automation

Notional





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

How do UAS Differ From Legacy Aircraft?

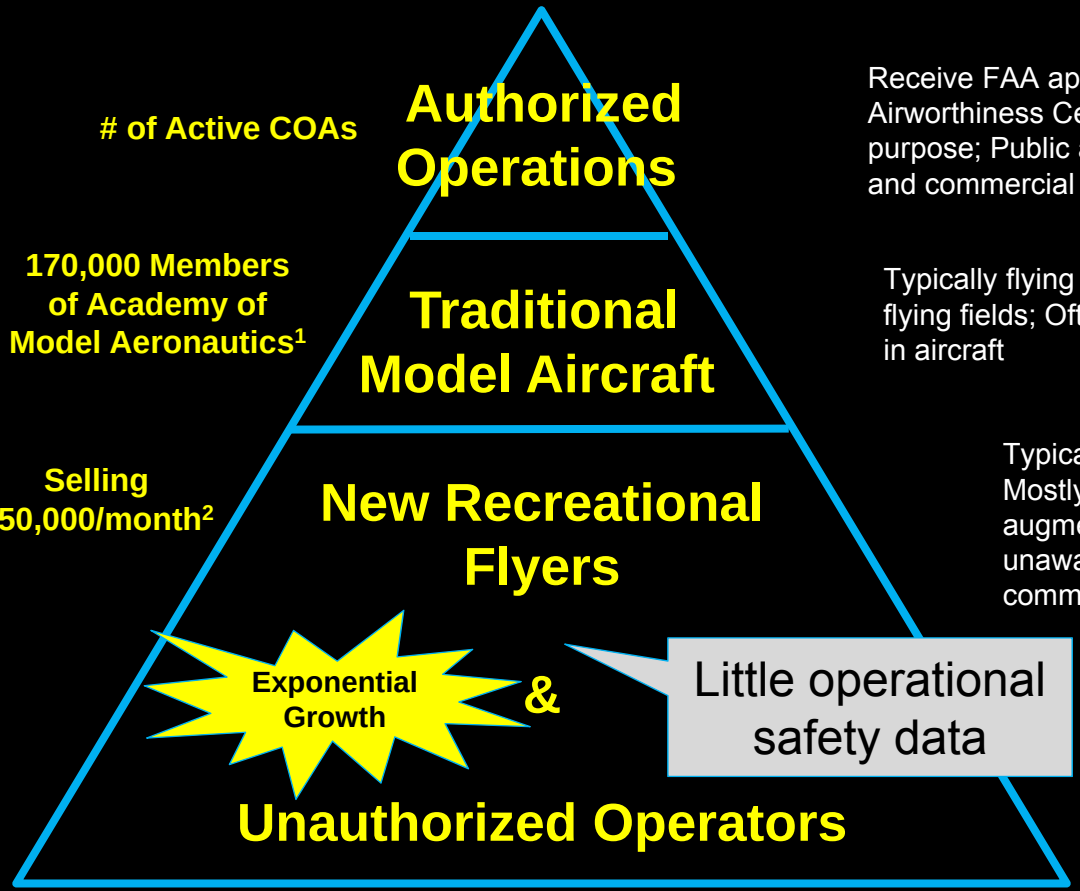
- **No pilot on-board – Fly-by wireless**
  - Situation awareness reduction
  - Command and control vulnerabilities
  - Automatic → Autonomous Operations
- **Can be smaller**
- **Often not designed or constructed to established aircraft standards**
- **Different flight performance and mission profiles**
  - Low altitude operations

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

The UAS Community is Growing Rapidly

Deloitte sees 1 million commercial drones flying [globally] in 2015
http://www.consultancy.uk/news/1362/deloitte-sees-1-million-commercial-drones-flying-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*



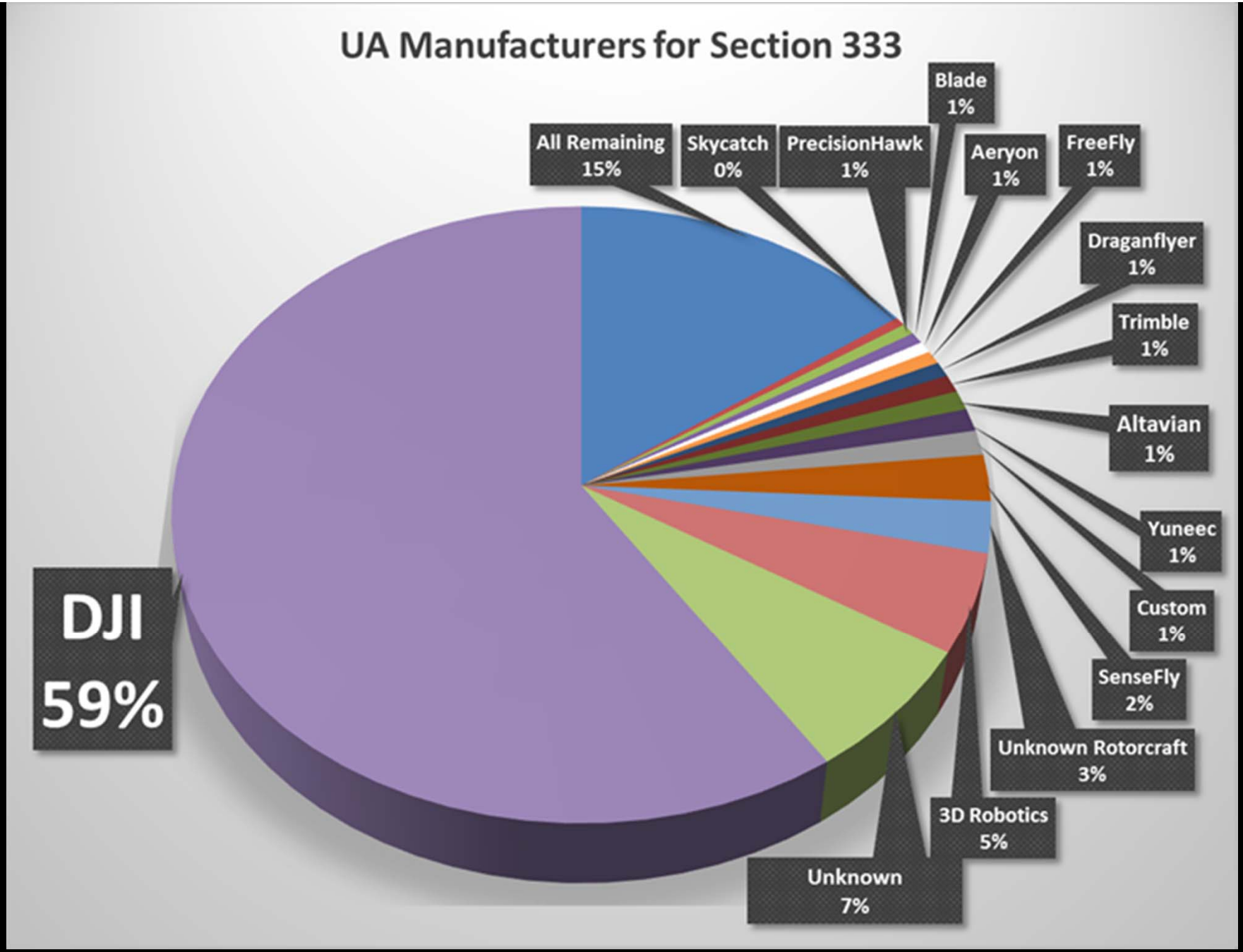
Receive FAA approval via a Certificate of Authorization, Special Airworthiness Certificate – Experimental, or Exempted for a specific purpose; Public agencies (military, law enforcement, academics, test sites) and commercial (section 333); Operating under significant scrutiny

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

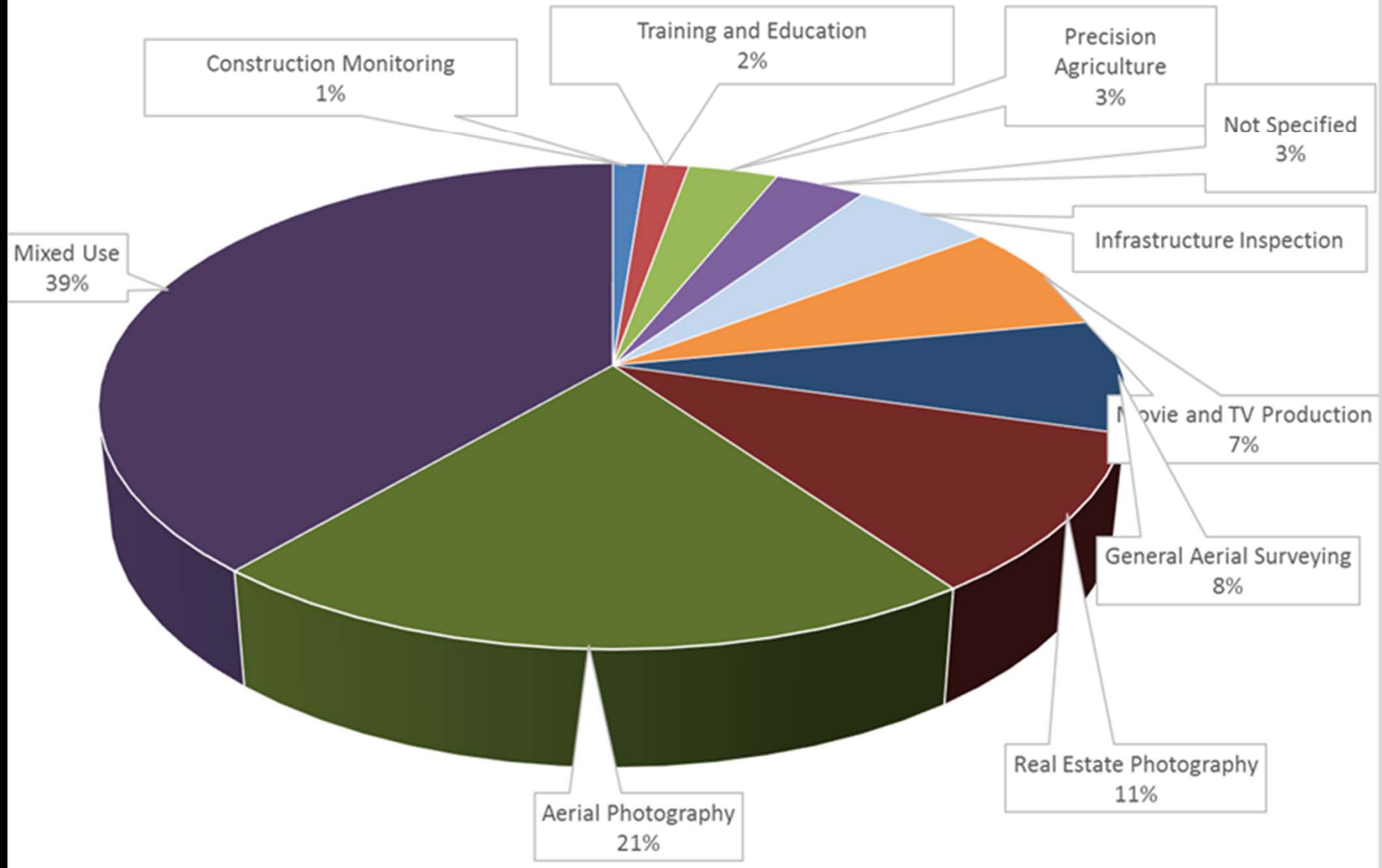
Typically purchased ready to fly or near ready to fly aircraft; Mostly flying aircraft with automated flight stabilization; Flying to augment other interests (e.g., photography, etc.); Tend to be unaware of aviation rules/culture; Not part of an Aeromodeler community

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

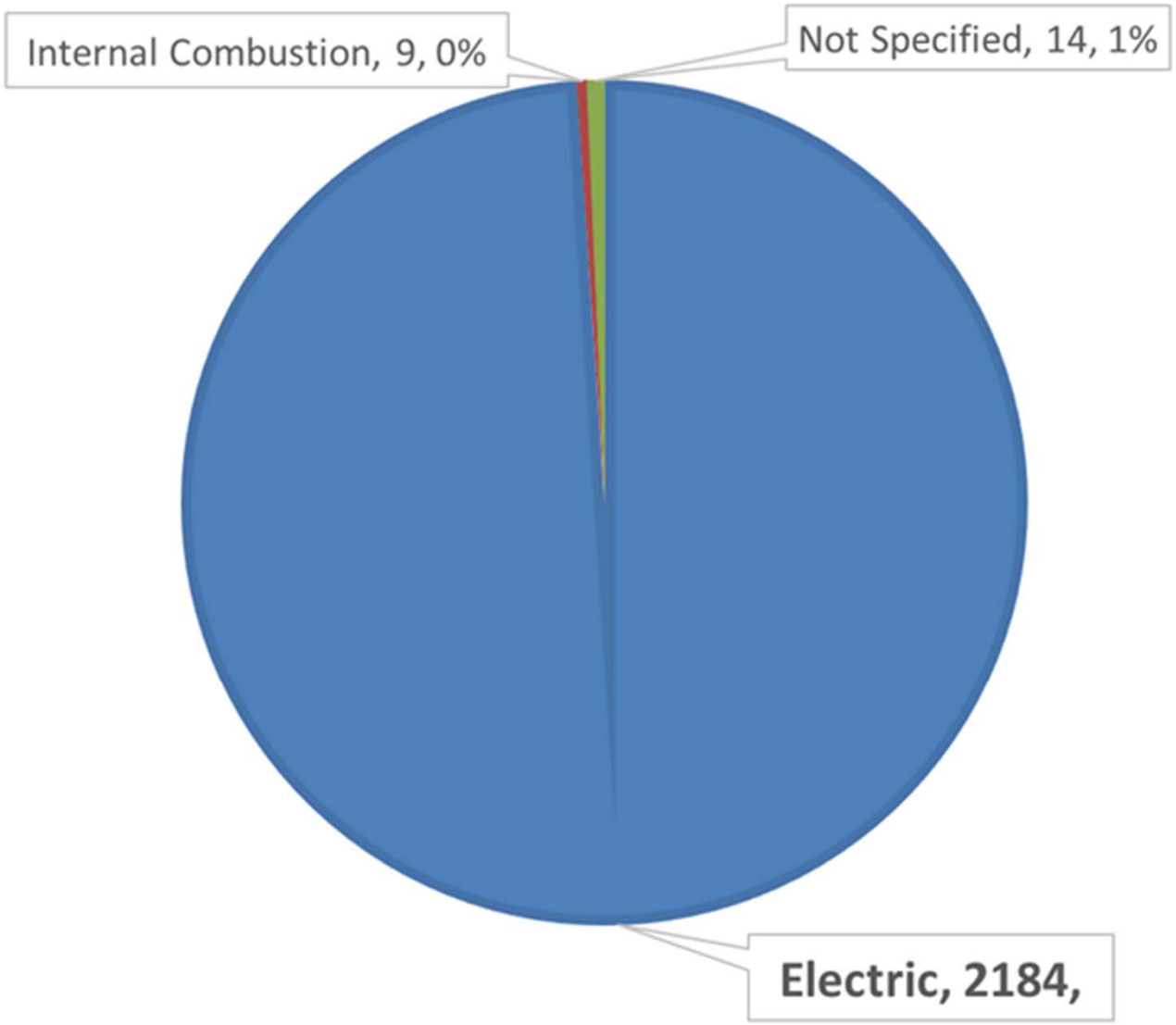
1: Academy of Model Aeronautics (http://www.modelaircraft.org/aboutama/whatisama.aspx)
2: Privileged discussions with UAS manufacturers



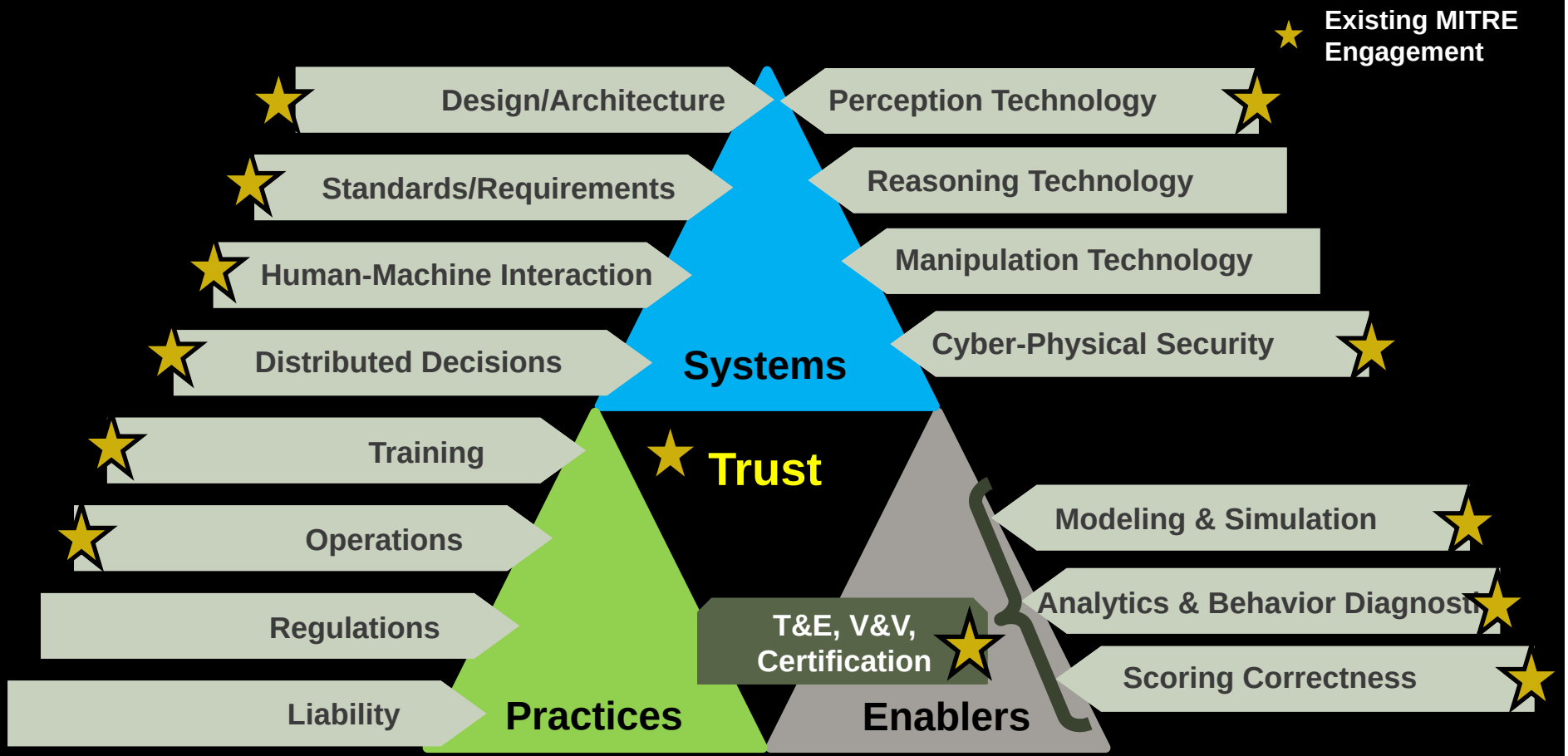
Section 333 Use Cases Above 5%



TYPE OF POWER PLANT



MITRE's View on the Challenges of Making Autonomy Real

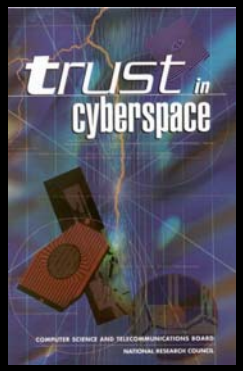


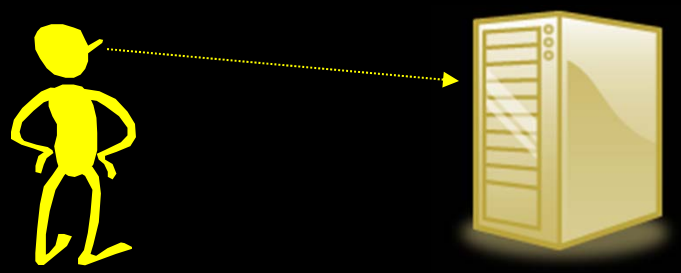
Approved for Public Release: Distribution Unlimited. Case Number 15-1841

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.***





Trust Trustworthy

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

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.**

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

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**

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

Photo: Andrew Lacher