SEPTEMBER 2019

AUTONOMY AT SCALE

Intelligent Machines Advancing Technology to Improve our Future

noblis®

For the best of reasons

NOBLIS.ORG

TABLE OF CONTENTS

CHALLENGE: ENSURING INTEROPERABILITY AMONG AUTONOMOUS SYSTEMS

Mile Corrigan

The rapid advancement of the Internet of Things (IoT) connects our world and multiplies our collaborative force. It creates a data-rich environment where the integration of autonomous systems—IoT devices, sensors, artificial intelligence, and robotics—becomes increasingly more complex. Despite significant technological advances and disruptive autonomy innovations, a growing need for interoperability remains within and among autonomous systems, operators, and command and control networks.

"Interoperability has historically been, and continues to be, a major thrust in the integration and operation of unmanned systems … A robust interoperable foundation provides the very structure that will allow for future advances in warfighting."

Without interoperability, the technology's full potential cannot be realized, and the delivery of enhanced value and reduction of operational risk cannot be achieved. In the Unmanned Systems Integrated Roadmap released by the Office of the Secretary of Defense (FY2017–2042), "Interoperability has historically been, and continues to be, a major thrust in the integration

Figure 1: Complexity of interoperability across heterogenous environments

and operation of unmanned systems … A robust interoperable foundation provides the very structure that will allow for future advances in warfighting." Autonomous systems must be able to collaborate with machines and humans to operate effectively in highly complex and contested environments and, ultimately, to derive benefits from their collective synergies. Figure 1 depicts the complexity of interoperability across heterogenous autonomous operations.

Interoperability Challenges

Interoperability applies to both intra-system and inter-system components and represents both physical/logical interconnections and external interactions between multiple systems. The National Institute for Standards and Technology (NIST) provides a working definition for interoperability: "The ability of software or hardware systems or components to operate together successfully with minimal effort by the end user ... Facilitated by common or standard interfaces"[1].

With the ongoing, rapid advancement of systems, interoperability between new and legacy systems will become a major concern for large enterprises in both the government and commercial sectors. In the world of "high-assurance autonomy," systems must operate functionally while satisfying rigorous safety and security properties to ensure the success of safety critical missions. The challenges facing high-assurance autonomy, interoperability, and integration mainly stem from:

1. Lack of consensus on and adoption of a common set of IoT standards
2. Insufficient verification and validation (V&V) methods
3. Proprietary software and hardware interfaces
4. Lack of trust between systems, operators, and networks

Challenge 1: Lack of consensus and adoption of a common set of IoT standards and protocols

Without standardization, services cannot be exchanged among systems efficiently, impeding our ability to:

- improve connectivity/communication protocols and end-to-end quality control protocols
- apply common processing and programming interfaces and languages
- deliver orchestration and automation platforms for effective operations
- reduce lifecycle costs of hardware and software investments

As multiple stakeholder organizations offer new standards, the need for government and private industry collaboration on the adoption of common standards and protocols grows. Industry most widely uses the Open Systems Interconnection (OSI) model, which decomposes communications across seven functional layers for implementation of interoperable networks (Figure 2)[2]. The IoT-centric model focuses

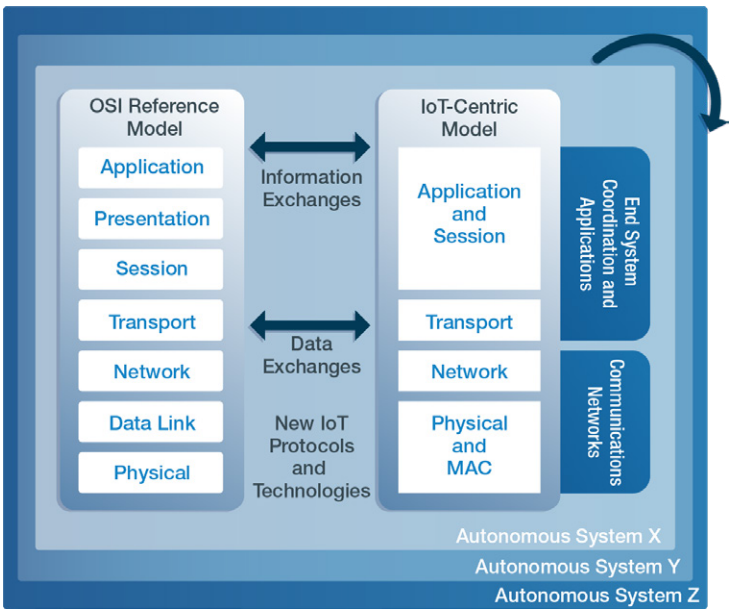


Figure 2: The OSI reference model aligned to IoT-centric communications

"The industries have built standards for the IoT, but it's been implemented in a fragmented, ad-hoc sort of basis. What we're going to see is industry adoption of standards, that includes cellular and IoT, and then you'll see a scaling that will overwhelm many of us."

on four layers of the OSI reference model stack for communication, data transmission, and end system coordination.

With competing economic incentives, firms have begun implementing their own data exchange and information formatting standards and practices—often overlapping with existing offerings and challenging industry and government efforts to adopt common, universal information sharing standards. Across the IoT space alone, the Institute of Electrical and Electronics Engineers (IEEE) identifies over 80 applicable standards, many focused on specific vertical markets[3]. While various IoT alliances, consortia, vertical markets, and vendors offer current solutions, new technologies and architectures continue to be developed at a rapid pace—all of which still need to be secured and standardized. Ericsson's IoT Chief Jeff Traver's recently said, "The industries have built standards for the IoT, but it's been implemented in a fragmented, ad-hoc sort of basis. What we're going to see is industry adoption of standards, that includes cellular and IoT, and then you'll see a scaling that will overwhelm many of us[4]."

Consensus and standards adoption for interoperability face hurdles that include:

- **Economic advantages** that can incentivize the development of proprietary systems for increased market share and to achieve vendor lock-in. Vertical initiatives drive the variation in standards to suit an industry's specific needs, such as data transport protocols to enable information exchange between "communities of things," versus mobile ad hoc network (MANET) routing communications protocols for Unmanned Aerial Vehicles (UAVs).
- **Competing standards**, such as the wide range of communications standards for low-range and medium-to-low data rate IoT communications (e.g., ZigBee, Bluetooth, IEEE 802.15.4), that can complicate the decision-making and selection process.
- **Lack of reference and architectural models** that adequately address interoperability and standardization objectives and gaps. The Department of Defense (DoD) has called for open architecture structures designed to facilitate modification to evolving requirements and technology advancements.
- **Fear of obsolescence** that can delay adoption as new technologies, together with evolving and competing standards, are developed and launched with increasing speed. Adopting the wrong standard could result in a system that becomes obsolete (think VHS vs. Betamax).

Many large organizations like Cisco, Intel, IBM, and GE are joining IoT standards bodies (e.g., the Industrial Internet Consortium, IPSO Alliance, the Open Connectivity Foundation) to stay ahead

of the adoption curve. Technology companies like Google and Amazon, however, have taken a different approach to gain a competitive advantage, by developing their own technologies and interoperability solutions[5].

Challenge 2: Insufficient V&V methods

With increased autonomy comes unpredictability. As autonomous systems execute both coordinated and uncoordinated actions in new and unforeseen ways, they are failing differently than could be predicted with a human in the loop—driving the need for robust software V&V methods. Software V&V, a technical discipline of systems engineering, employs a rigorous methodology for evaluating the correctness and quality of a software product through the software lifecycle. Validation confirms that the software meets the user's needs: "Are we building the right system?" Verification confirms that the system is well engineered: "Are we building the system right?[6] Today, V&V activities account for nearly 25% of development costs—a figure anticipated to increase disproportionately with other development costs as the unpredictability of autonomous systems grows[7].

Validation confirms that the software meets the user's needs: "Are we building the right system?" Verification confirms that the system is well engineered: "Are we building the system right?

Traditional approaches, designed for testing manned systems, will not be enough to meet the key V&V challenges presented by highly adaptive and non-deterministic systems:

- **Dynamic and Unpredictable Environments** to which context-aware autonomous systems react to dynamically drive the need for a much larger decision space that can produce unanticipated events and failures. Plans and deliberations are intertwined with actions that can be both proactive and reactive. With adaptive systems, behavior across all working conditions is not known at design time, making fault tolerance methods difficult to implement.
- **Emergent Behavior**, dependent on the acquired knowledge of each system, prevents the inclusion of fault avoidance methods in the formal verification process. System interactions can often produce unintended consequences. Testing adaptive systems that learn, adapt, self-diagnose, and apply intelligence in decision-making is often highly labor intensive, making it costly and time consuming to comprehensively observe the full range of simulated fault scenarios for a given mission.
- **Lack of Test Repeatability**, a necessary condition for establishing and maintaining reliable test methods. The complexity of the operating environment coupled with adaptive software characteristics can produce different results even when a system is supplied with the same set of inputs. Fault removal through extensive testing and debugging is difficult to achieve since an autonomous system's behavior changes and learns over time.
- **Lack of Reliable and Certifiable V&V Methods** complicates efforts to prevent errors in autonomous system development. Test and evaluation (T&E) requirements imply formal methods for system assurance based on past

failure conditions of similar systems, not readily available for newly developed autonomous systems[8]. Recognizing this challenge, Former Chief Scientist of the U.S. Air Force, Werner Dahm asserts, "Developing certifiable V&V methods for highly adaptive autonomous systems is one of the major challenges facing the entire field of control science, and one that may require the larger part of a decade or more to develop a fundamental understanding of the underlying theoretical principles and various ways that these could be applied"[9].

These challenges all demonstrate the high cost, complexity, and difficulty of achieving V&V results by applying classical software testing methods such as fault avoidance, fault removal, and fault tolerance testing to autonomous systems.

Challenge 3: Proprietary software and hardware interfaces

With such a wide array of commercial software and hardware products deployed across large enterprises today, proprietary interfaces present a major barrier to system integration and interoperability. Organizations holding a large portfolio of commercial-off-the-shelf (COTS) systems—like the DoD does—cannot maintain pace with changing conditions of unmanned systems due to their proprietary nature and lack of data rights and need for more timely software updates.

Unlike open source software and interfaces built using common data standards and protocols, proprietary software and hardware interfaces raise major issues, including:

- **Vendor Lock**, which deepens reliance on the vendor for upgrades, enhancements, maintenance, and support versus open source software and interfaces built using common data standards and protocols.
- **Innovation Lag** that slows the pace of innovation and evolution of autonomous system capabilities, as system owners must negotiate with the vendor for required software changes.
- **Integration Stall** caused by closed interfaces and proprietary software that inhibit integration and data-sharing among systems, typically exacerbated by lack of user access to source code or the ability to make modifications or fixes.

Closed software is not without its potential advantages such as extensive technical support for maintenance and, oftentimes, higher product stability due to a smaller feature set. These advantages, though, may not outweigh the drawbacks for large enterprises that desire to keep pace with reliable, interoperable, high-assurance autonomy. In acknowledgment of this tradeoff, the Defense Science Board Task Force has recommended that each U.S. military service initiate at least one open software design project to decouple autonomy from the vehicle—deploying proven technology to reduce manpower, increase capability, and adapt more swiftly to future missions[10].

"Developing certifiable V&V methods for highly adaptive autonomous systems is one of the major challenges facing the entire field of control science, and one that may require the larger part of a decade or more to develop a fundamental understanding of the underlying theoretical principles and various ways that these could be applied".

Former Chief Scientist of the U.S. Air Force, Werner Dahm.

Challenge 4: Lack of trust between systems, operators, and networks

The notion of trust, implying a human psychological trait characterizing assurance or certainty in human-to-machine (H2M) interactions, reflects a key challenge in the context of implementing and operating autonomous systems. The research paper "The Trust V – Building and Measuring Trust in Autonomous Systems"[11], defines two types of trust for a user to accept an autonomous system:

- **System trust**, or human confidence that the system behaves as intended. Achieving this trust requires a high level of assurance that the system satisfies its requirements, (i.e. the traditional V&V challenges).
- **Operational trust**, or human confidence that the system helps the user perform the assigned tasks. Achieving this trust requires a high level of assurance that the scenarios for which the system was designed are useful. A lack of human confidence in the system or its operations impedes high-assurance autonomy, integration, and interoperability.

People tend to respond to technology in human and social ways. Unclear or uncertain decision-making of an autonomous system negatively influences a person's level of reliance in complex situations. Whether trust means sending a loved one on the road in a self-driving car or sending machines or drones into battle with humans, prioritizing the establishment of H2M trust in the design process can ultimately create better interactions for the end-user and reduce the chance of misuse.

The Air Force Research Laboratory (AFRL)[12] identifies five human-machine teaming technology challenges that must be addressed to establish trust between systems, operators, and networks to maximize performance in complex and contested environments:

- **Human State Sensing and Assessment** to measure and assess the human's state (e.g., physiological, performance, behavioral).
- **Human-Machine Interaction** to enable humans and machines to communicate and share information.
- **Task and Cognitive Modeling** to allocate workload and decision-making balance.
- **Human and Machine Learning** to adapt, learn, and extend mutual training between humans and machines.
- **Data Fusion and Understanding** to integrate human and machine data (e.g., context, time, format) for a shared world model.

Any human operator must be able to trust their interactions with an autonomous system to achieve greater levels of interoperability and mission assurance between other systems, operators, and networks. Shared understanding is key to overcoming the H2M trust barrier.

Current and Evolving Approaches

Standards and Open Architectures for Interoperability (Challenge 1 & 3)

IoT network protocols and standards continue to evolve as quickly as new industries and use cases emerge across business and government. Enterprises must choose the right network topology for the use case and consider the market in which the capability will be deployed. Most IoT-enabled autonomous systems comprise a multi-tier architecture spanning devices, gateways, data systems, and services as depicted in Figure 3.

With no universal model to describe the collection of protocols, standards or technologies, developers face the challenge of selecting the right subset

of protocols, drawing from competing standards and minimizing risk of obsolescence. Further complicating these decisions, large enterprises need to reduce lifecycle costs, ensure vendor conformance to open standards, and guarantee the commonality of components across autonomous platforms. Figure 4 depicts the Open Standards reference model for IoT communications, highlighting the ever-evolving network and data protocols available in the marketplace today[13].

Integration across different layers to perform data and information exchanges requires alignment of appropriate protocols as defined by the different Standards Developing Organizations (SDOs) (i.e., the IEEE, IETF, ITU, etc.). The SDOs, alliances, and forums develop IoT protocols based on the physical interfaces already established in the industry. For example, the Wi-Fi, VX2 protocols used in the PAN and LAN networks are found in IEEE 802.11, while protocols like ZigBee, Thread, Wireless HART, etc. are built over IEEE 802.15.

To exchange messages and data across multiple sensors and systems, the application layer supports multiple protocols which in most cases use the publish/subscribe models. An IoT architect must carefully select the right protocols across the different layers appropriate for the type of network to ensure interoperability as well as scalability and performance of the solution.

To meet interoperability challenges head on as new protocols and standards emerge, the DoD launched an initiative to develop an Unmanned Ground Vehicle (UGV) Interoperability Profile (IOP)[14] for the acquisition of future programs, the upgrade of fielded systems, and the evaluation of commercial products. The IOP created by the U.S. Army Robotic Systems Project Office, approved for public release through the National Advanced Mobility Consortium (NAMC), specifies interoperability across several levels:

- **OCU/UxV(s):** Between Operator Control Units (OCU) and one or more Unmanned Vehicles (UxV(s)).
- **Intra-OCU:** Between and among OCU hardware and software elements.
- **Intra-UxV:** Between and among UxV subsystems, payloads, and platforms.
- **OCU/UxV/C2:** Between OCUs, UxVs and external C2 systems to exchange command and control, battlespace and audio/video information.

The IOP, designed to support a wide range of missions, vehicle classes, controller classes, payload classes, architectures, and interactions with external systems, presents a strong case towards realizing “open architectures, reusable, interchangeable components and common, publicly defined interfaces between individual subsystems," said Heidi Shyu, Former Assistant Secretary of the

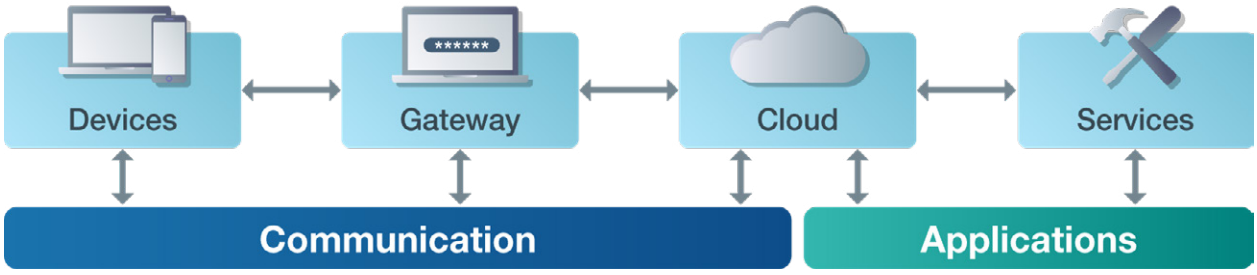


Figure 3: IoT Stack Simplified

OPEN STANDARDS REFERENCE MODEL FOR IOT COMMUNICATION PROTOCOLS

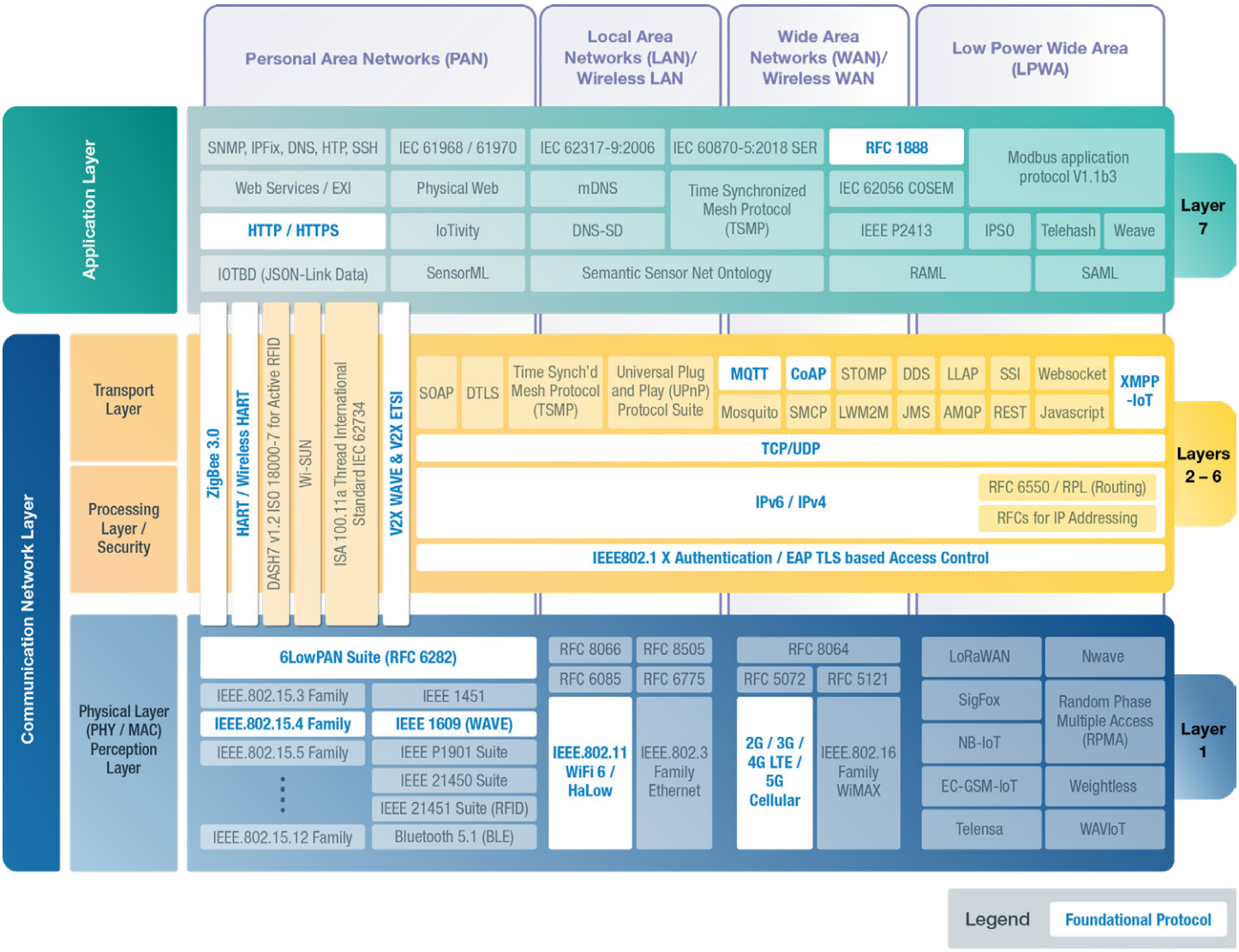


Figure 4: Adapted from the Open Standards Reference Model - Graphic from: David E. Culler (https://www.cs.berkeley.edu/~culler/).

Army for Acquisition, Logistics and Technology[15]. Specifying messaging and transport protocols to support the scope of the IOP will accelerate adoption of standards.

Looking ahead, organizations should dictate the use of open architectures, open standards, and open source software to reduce the reliance on closed and proprietary technologies over time.

Emerging V&V Approaches for Autonomous Systems (Challenge 2)

Several approaches have emerged to address the complexity of verifying and validating autonomous systems. These include model-based approaches, evolutionary test algorithms, simulation-based methods, and virtualization tools that often combine several advanced V&V techniques already in place. Intelligent Systems Division (ISD) researchers at NASA Ames Research Center are applying many of these advanced V&V techniques such as static analysis, model checking and compositional verification to gain trust in model-based autonomous software systems[16].

Classical development processes and methods work well when requirements are easily understood; however, traditional approaches provide limited insight into issues discovered during the test phases of a highly autonomous and open-ended system. This results in an inability to test for all known conditions. Table 1 highlights current test approaches and use cases attempting to address testing challenges for autonomous systems operating in a safety-critical environment.

"Open architectures, reusable, interchangeable components and common, publicly defined interfaces between individual subsystems, said Heidi Shyu, Former Assistant Secretary of the Army for Acquisition, Logistics and Technology."

While most solutions do not extend end-to-end for an entire autonomous system, a few testing and V&V trends have gained wider acceptance across the various approaches:

- **Modeling and Simulation:** Applying model-based testing methods can find failures and reduce defects early in the process, as models can be used to simulate or communicate intended behavior, helping to build trust and acceptance of the system. Simulation-based approaches such as Adaptive Stress Testing (AST) can find failure paths more quickly, using sequential decision processes that can be further optimized with reinforcement learning[17].
- **Virtual Testing:** Applying virtual methods to a representative model of the intended operational environment can reduce costs compared to live testing and poses less risk since the virtual hardware and test environment can be used repeatedly for test experiments.
- **Transparent Engineering:** Systematically engineering systems that provide transparency into weaknesses and defects can handle emergent nonrepeatable behavior. By building transparency into the design and operation of the system, engineers can identify failures early in the design process, improve safety, and provide accountability[18]. Engineers can't

TABLE 1 – TESTING APPROACHES FOR AUTONOMOUS SYSTEMS

Testing and V&V Approaches		Description / Use Cases	Advantages	Work to be Done
Model-Based Test Approach	• Model-based Test Approach • Run-time monitoring • Predictive Analysis	• Model-based testing automatically generates test cases from models • Autonomous Satellite System (AGATA project) employed model-based specifications to produce the RT-Java code of the AGATA onboard software[19] • Autonomic Service-Component Ensembles (ASCENS) combined a model-based approach with run-time monitoring and predictive analysis[20]	✔ Reduces complex systems to logical components, enabling abstraction and componentization ✔ Enables incremental development to initiate software validation earlier in the process ✔ Performs model debugging and automatic code generation ✔ Defines adaptation, awareness, and emergence properties through mathematical models ✔ Generates build ensembles that are more adaptive, reliable, and usable	• Integration of monitoring techniques with runtime verification to bridge testing and formal verification
Evolutionary Test Approach	• Evolutionary Algorithms • Agent-based Software Engineering • Software Abstraction	• Approach to testing autonomous agents that uses evolutionary optimization to generate demanding test cases • Soft goals are transformed into evaluation criteria and tests are generated with evolutionary algorithms suited to multi-objective optimization	✔ Evaluates autonomous agents as a means of building confidence in behavior and greater agent dependability since quality functions are derived from requirements	• Development of design and programming constructs for agent interactions that work towards shared system goals

TABLE 1 – TESTING APPROACHES FOR AUTONOMOUS SYSTEMS, CONTINUED

Testing and V&V Approaches		Description / Use Cases	Advantages	Work to be Done
Adaptive Stress Testing	• Simulation-based test approach • Adaptive Stress Testing (AST) • Markov decision process (MDP) • Reinforcement Learning	• Approach to stress testing that finds most-likely failure scenarios by formulating a sequential decision-process (e.g. MDP) and then uses deep reinforcement learning to search for most likely failure paths[17]	✔ Deep Reinforcement Learning produces more likely failure scenarios compared to other methods (e.g. Monte Carlo tree search) ✔ AST finds failure scenarios efficiently	• Incorporation of more realistic models with tighter constraints on the events of interest
Virtual Test Approach	• 3-D/4-D Modeling & Simulation • Early testing of embedded software via software-in-the-loop virtual integration • High-resolution physics based simulation of robotics platforms	• Virtual testing environment for autonomous aerial vehicles using simulation-based in-the-loop validation of UAV software • Virtual environments for autonomous mobile robot systems using the Mobility Open Architecture Simulation and Tools (MOAST)	✔ Allows for testing without putting the hardware or environment at risk ✔ Allows for the evaluation of using alternative hardware components prior to implementation ✔ Provides a baseline simulation system capable of modeling autonomous systems with the ability to conduct repeatable test experiments	• Development of automated approaches to systematically explore the state-space of the planning algorithm • Development of more realistic simulations • Not everything can be tested virtually to address complexity and noise of the real world • Development of robust algorithms to address rational decision making in an autonomous system

necessarily ensure every corner case is properly handled, but this modern engineering practice can help make every corner case visible.

- **Advanced V&V Techniques.** Static analysis techniques assess code without execution, reducing the potential for dangerous operations that have to be checked by other methods. **Model-checking** efficiently checks that a model of a system satisfies all requirements, providing a robust way to catch system-level errors (e.g. concurrency, deadlocks, etc.). **Compositional verification** – often referred to as a "divide and conquer" approach decomposes properties of a system into properties of its components. Components are model checked separately, guaranteeing the verification of the entire system if each component is verified[16].

Confidence that an autonomous system will operate as intended is critical to its deployment. Developers will progress to more advanced features when they can establish high confidence in lower subsystems, in contrast to low confidence systems where defects are hidden among several layers of the system. The ability to test and verify autonomous systems will continue to be critical to operational deployment, mission effectiveness, and human safety.

Enhancing the Human-Machine Team (Challenge 4)

Numerous evolutions in human-machine teaming are improving communications, comprehension, and control in H2M interactions. Human-robot interaction (HRI), a relatively new field of study, seeks to address the challenge of human-machine trust. HRI encompasses multidisciplinary contributions from human-computer interaction, artificial intelligence, robotics, human factors, operations research, and social sciences. HRI focuses on the understanding, design, and evaluation of robotic systems for use by or with humans—such as fully autonomous machines (classified as robots).

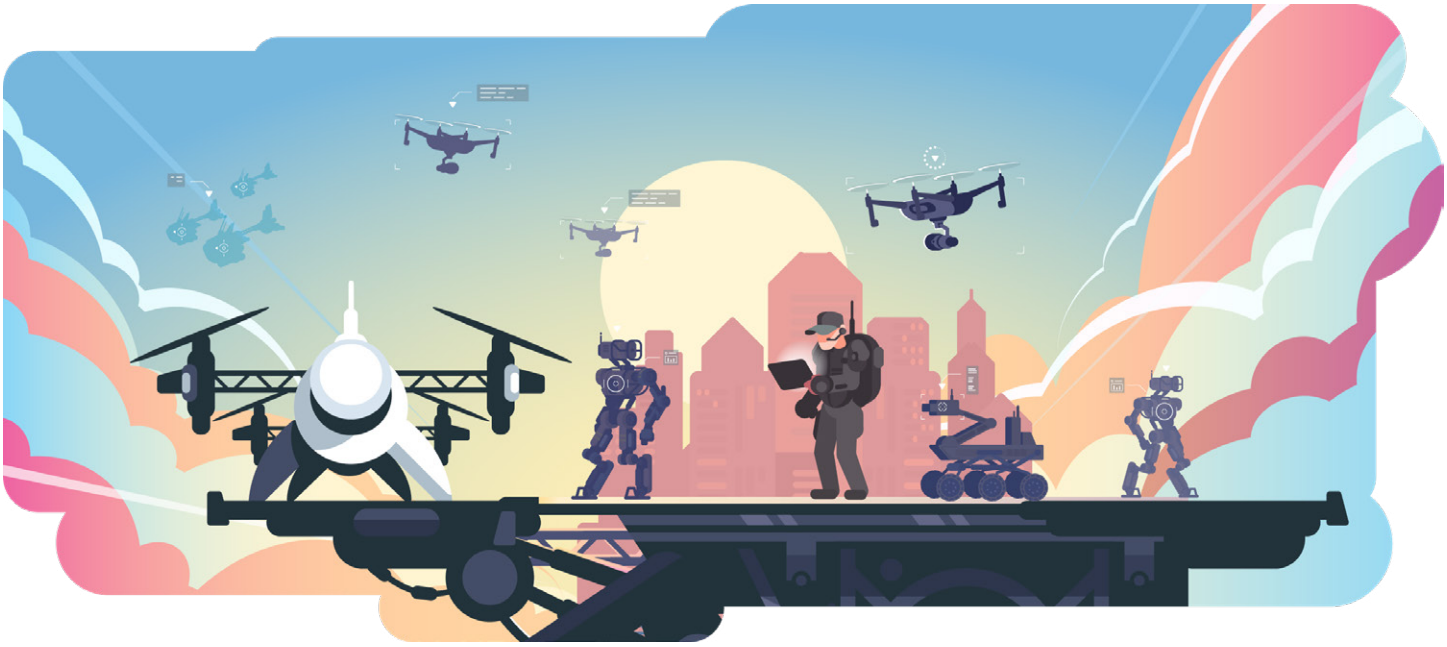


Figure 5: The future of human-machine teaming

TABLE 2 – HUMAN SUPERVISORY CONTROL METRIC CLASSES AND SUBCLASSES

Metric Class	Description	Subclass Examples
Mission Effectiveness	Effectiveness measures relating to the whole human-automation system	Mission performance parameters
Autonomous Platform Behavior Efficiency	Parameters relating to the efficiency of the autonomous platform	Usability, adequacy, autonomy, learnability, errors, accuracy, reliability, neglect time
Human Behavior Efficiency	Parameters relating to how humans sequence and prioritize multiple tasks such as monitoring autonomous platform health and status, identifying critical exogenous events, and communicating with others as needed	Information processing efficiency (e.g., decision-making), attention allocation efficiency (e.g., scan patterns, prioritization)
Human Behavior Precursors	The underlying cognitive processes that lead to specific operator behavior, as compared with the human behavior metric class that captures explicit behavior	Cognitive precursors (e.g., situation awareness, mental workload, emotional state) Physiological precursors (e.g., physical comfort, fatigue)
Collaboration Metrics	Team-level metrics to measure the degree to which the humans and automation are aware of one another and can adjust their behavior accordingly	
	Human-automation collaboration	Trust, mental models
	Automation-automation collaboration	Quality and efficiency of collaboration (e.g., speed of data sharing, quality of system response to unexpected events, etc.)
	Human-human collaboration	Coordination efficiency, team mental model

Source: Evaluation criteria for human-automation performance metrics. In Performance Evaluation and Benchmarking of Intelligent Systems[21]

The scope of HRI addresses H2M communications, shared relationship models between humans and machines to achieve autonomy, enhancements to the human-machine team, and how to capture and express interactions within a given application domain, characterized by the:

- Level and behavior of autonomy
- Nature of information exchange
- Structure of human-robot team
- Training of people and robots
- Design and shaping of tasks for human-robot collaborations

To assess holistic systems, we must establish and validate metrics for evaluation and testing of H2M interactions. To gain an understanding of H2M interactions and how they can be influenced or enhanced to achieve an outcome, the interactions must be measured for improved operations. MIT researchers have defined five metric classes for human-machine interactions, described in Table 2[21].

While we may be decades away from solving all of our human-machine interaction challenges for high-assurance autonomy, system owners can start by exploiting data between H2M and Machine to Machine (M2M) interactions to derive new insights and drive continuous improvements. Improved data collection and data sharing for monitoring, management, and optimization should be conducted early and continuously—especially as data volume and quality increases over time. Valuable information can be extracted from metadata, improving the self-awareness and flexibility of systems. Autonomous system data strategies should adapt situationally with an understanding of unique mission goals and constraints.

Pathway to Improved Interoperability

Interoperability will remain a key challenge for autonomous systems—now and into the future. To exploit the collective intelligence and capabilities of integrated autonomous systems, enterprises must set the foundation for interoperability by establishing an architectural basis for the development of future systems. With so many protocols available in the marketplace today, industry should focus on the most commonly used ones—built on open standards to simplify and accelerate interoperability. Standardizing hardware and software interfaces, requiring the use of open standards, protocols, and architectures, and securing data rights will enable long term sustainability, modernization, and reduced dependency on proprietary system owners—ultimately driving down lifecycle costs.

Autonomous system V&V will require continued advancements in T&E so that run-time architectures can constrain systems to a set of allowable, predictable, and recoverable behaviors, integrated early in the development process. Testing methods will need to integrate development and operational testing and employ new ways to test the whole system whether through virtual testing, transparent engineering, model-based engineering and testing approaches, or new ones yet to be developed. As research in this field evolves and emerging test approaches are applied more rigorously across autonomous systems, organizations will be able to make informed decisions on which test methods will yield the best outcomes.

Finally, human and technological capabilities must be integrated into a well-functioning system to optimize the human-machine team. Constraints should be shared with all parts of a given system so that the autonomous system serves as a creative partner that complements capabilities. To drive the integration and adoption of autonomous systems, trust barriers will need to be overcome. With trust established, the observability, controllability, and partnering between humans and machines improves significantly—enabling enterprises to reap the benefits of high-assurance autonomy.

SOURCES

1 (National Institute of Standards and Technology 2008, 28)

2 Irons-McClean, R., Sabella, A, Yannuzzi, M., IOT and Security Standards and Best Practices, 2019.

3 Internet of Things. IEEE Standards Association. Retrieved from: https://standards.ieee.org/initiatives/iot/stds.html

4 Daws, Ryan. (2019, March) Ericsson IoT chief on AI, 5G, and connecting 'things' instead of 'a thing'. IoT News. Retrieved from: https://www.iottechnews.com/news/2019/mar/01/ericsson-iot-ai-5g-connecting-things/

5 Hughes, Terry. (2016, April) Will industry muscle win in the IoT standards war? [Blog]. Retrieved from: https://internetofthingsagenda.techtarget.com/blog/IoT-Agenda/Will-industry-muscle-win-in-the-IoT-standards-war

6 IEEE Standard for Software Verification and Validation, 1998.

7 Helle, P., Schamai, W., Strobel C. (2016). Testing of Autonomous Systems – Challenges and Current State-of-the-Art

8 Technology Investment Strategy 2015-2018, DoD R&E Autonomy COI TEVV Working Group, May 2015.

9 Dahm, W. J. (2010). Technology Horizons a Vision for Air Force Science & Technology During 2010-2030. Office of the US Air Force Chief Scientist.

10 Department of Defense Defense Science Board Task Force Report: The Role of Autonomy in DoD Systems, July 2012.

11 Zwillinger, D., Palmer, G., & Selwyn, A. (2014). The Trust V - Building and measuring trust in autonomous systems.

12 Overhold, Jim, Ph.D. and Kearns, Kris (2014, April). Air Force Research Laboratory Autonomy Science & Technology Strategy [PowerPoint Slides]. Retrieved from: https://defenseinnovationmarketplace.dtic.mil/wp-content/uploads/2018/02/88ABW-2014-1504_140312v2_-_Autonomy_Strategy_Part_2.pdf

13 Adapted from the Open Standards Reference Model - Graphic from: David E. Culler (https://www.cs.berkeley.edu/~culler/) - The Internet of Every Thing - steps toward sustainability CWSN Keynote, Sept. 26, 2011

14 Robotics and Autonomous Systems - Ground (RAS-G) Interoperability Profile (IOP) (Version 2.0 ed.). Warren, MI, USA: US Army Project Manager, Force Projection (PM FP). 2016.

15 Serbu, Jared. (2014, August) Army turns to open architecture to plot its future in robotics. Federal News Network. Retrieved from: https://federalnewsnetwork.com/defense/2014/08/army-turns-to-open-architecture-to-plot-its-future-in-robotics/

16 Brat, G., Denney, D., Giannakopoulou, J F, Jonsson, A. (2005). Verification of Autonomous Systems for Space Applications.

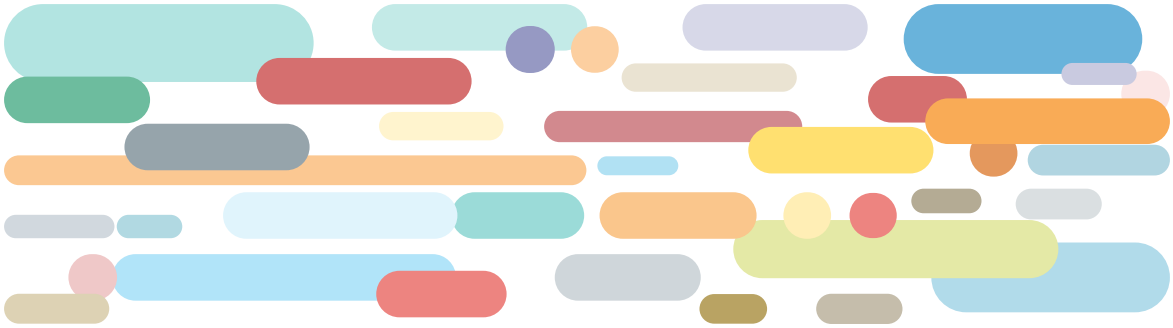
17 Koren, M., Alsaif, S., Lee, R., Kochenderfer, M. (2019). Adaptive Stress Testing for Autonomous Vehicles.

18 Corcoran, William. Transparent Engineering. American Scientist. Retrieved from: https://www.americanscientist.org/article/transparent-engineering

19 Pouly, J., & Jouanneau, S. (2012). Model-based specification of the flight software of an autonomous satellite. Embedded Real Time Software Systems (ERTS 2012).

20 Hölzl, M., Wirsing, M., Klarl, A., Koch, N., Reiter, S., Tribastone, M., et al. (2011). Engineering Ensembles: A White Paper of the ASCENS Project.

21 Donmez, B., P. E. Pina and M. L. Cummings. 2009. Evaluation criteria for human- automation performance metrics. In Performance Evaluation and Benchmarking of Intelligent Systems, R. Madhavan, E. Tunstel, and E. Messina, eds. New York: Springer Science+Business Media. doi:10.1007/978-1-4419-0492-8.



ABOUT NOBLIS

Noblis is a nonprofit science, technology, and strategy organization that brings the best of scientific thought, management, and engineering expertise with a reputation for independence and objectivity. We work with a wide range of government and industry clients in the areas of national security, intelligence, transportation, healthcare, environmental sustainability, and enterprise engineering. Together with our wholly owned subsidiary, Noblis ESI, we solve difficult problems of national significance and support our clients' most critical missions.

NOBLIS.ORG

noblis®

For the best of reasons

703.610.2000 answers@noblis.org @NoblisInc