AUTONOMOUS, ATTRITABLE, COLLABORATIVE DIGITAL TWIN CENTER OF EXCELLENCE

Technology Overview for Component-Oriented Acquisition and Software Confidence on Cyber-Physical Systems

John Launchbury and Aaron MIller

Background

In the context of this document, autonomy is the manifestation of the intersection of sensors, platforms, software and the introduction of artificial intelligence. Autonomy requires the use of data which is generated and used by a collection of sensors operating on computer infrastructure that is integrated into a system. As such, we can think of autonomy, as a collection of often complex software. To effectively deploy autonomous capabilities (i.e., software) on our systems, we must utilize emerging trends in digital engineering and digital twins to find cost effective, time efficient solutions to develop, acquire, maintain, and sustain autonomous, attritable, and collaborative systems.

However, the Department of Defense has long suffered from an outdated acquisition construct that no longer keeps pace with the speed and sophistication of evolving threats to our national security. An aging fleet, the growing cost of new weapon systems, and the rise in rapid technology insertion, specifically in the domain of autonomy and artificial intelligence, make it impossible to build systems under the same 10-30 year acquisition paradigm. Today's weapon systems are made up of embedded computer systems and software which comprise of Cyber Physical Systems. Cyber Physical Systems have capabilities where the hardware and software "are deeply integrated and actively connected to the physical world."[1] Integrating software with hardware greatly extends the capabilities of cyber physical systems and introduces a new level of complexity to their development.. The systems engineering process of today makes systems expensive to maintain and upgrade. It is time consuming, leading to deployments of obsolete capabilities and offering limited reconfiguration of legacy systems.

This issue is a priority of senior leadership within the Department of Defense. Former Under Secretary of Defense for Acquisition and Sustainment, Ellen Lord, reworked the DoD Instruction 5000.02 to address evolving present-day threats and introduced new 6.8 funding lines supporting the acquisition, maintenance and sustainment of software. Former Secretary of the Air Force for Acquisition, Technology, and Logistics, Dr. Will Roper, amended acquisition processes for software and systems to address goals of creating processes to build trusted, reliable software in the Air Force for technological advancements in current and future weapon systems.

---

[1] *American Innovation and Competitiveness Act* (AICA) (P.L. 114-329)

Underlying technologies still limit the effect of the rapid acquisition and the ability to acquire software incrementally against specifications and the Department's approach to software acquisition still trails current industry standards. Modern development approaches to eliminate artisan and craft concepts of software development have the potential to dramatically improve both speed and correctness of software acquisition in the DoD. Critical techniques include the use of digital first approaches in systems engineering and the use of digital twins to support rapid development, test, and deployment approaches. Additionally, principles of software-hardware codesign utilizing digital first approaches offer promise based on recent DARPA programs such as SSITH, HACMS, CASE, VSPELLs and Symbiotic Design of Cyber Physical systems. These digital first approaches offer the ability to speed up both production of new capabilities and the opportunity to inject effective upgrades into legacy systems while also reducing cost. One thing that holds true is Dr. Roper says that "Artificial intelligence (AI) will fundamentally change the character of warfare, so future Airmen must have systems that learn faster than their enemies. To harness this technology from the commercial industry, we must design, acquire, and update software like them."

Through research conducted at DARPA and the DoD services, a new type of acquisition and integration process for software enabled Cyber Physical Systems is possible. In this paper we will discuss how the use of open architectures and standards enables component-oriented acquisition and retrofit with software confidence, how new research in machine learning for runtime assurance and composable system builds is necessary, and the impacts of policy on the implementation of component-oriented engineering.

State of Now

Rapid acquisition has been attempted with mixed success over the years, while we have increased the speed of acquisition, we are incurring significant operations and maintenance costs as well as long-term systems engineering debt when past designs cannot be efficiently reused. A recent use case for the P-8A Poseidon, which was designed to replace the Navy P-3, demonstrates this concern. The Poseidon focused on rapid acquisition using existing Commercial Off the Shelf (COTS) subsystems, basing the Poseidon airframe entirely off of the Boeing 737 aircraft and its supporting infrastructure. A Naval Postgraduate School report finds, "The supportability issues will likely not come from the hardware on the P8; the challenge will be in the software sustainment and software upgrades for the on-board systems supporting a weapon system scheduled to be in the Navy inventory for 20+ years".[2]

Another example is found in the development of the Global Hawk. The Global Hawk yielded quick-to-field prototypes that, while successful, suffered costly overruns in areas of software design and airworthiness certification. In a report studying the results of the Global Hawk Advanced Concept Technology Demonstration (ACTD), it was cited that the Global Hawk ACTD

[2] Brad Naegle and Diana Petross. P-8a Poseidon multi-mission maritime aircraft (mma) software maintenance organization concept analysis. Technical report, NAVAL POSTGRADUATE SCHOOL MONTEREY CA GRADUATE SCHOOL OF BUSINESS AND PUBLIC …, 2010.

achieved prototype to production status in a very short time, yielding 10 low rate production aircraft from the initial prototype in 1998 to 10 block 10 aircraft by 2006. However, the ``military airworthiness certification process was very rigorous and took three years and 77,000 man-hours to achieve''.[3] Thus, of the eight year acquisition process, three years were spent in airworthiness certification.

The examples of the P-8A and the Global Hawk demonstrate that rapid acquisition is here to stay with the goal to enable systems to be designed and built within a fraction of the time. However, these examples also show that the need for quick solutions for fielding warfighter capability often yields design compromises, short circuiting systems engineering best practices and resulting in software that is not composable, defined or able to be reused. The manner in which we utilize systems engineering processes and tools to reuse and build software for weapon systems must change, and we must adapt the methods we use to gain certification to keep up with this rapid acquisition model.

As software becomes more prolific within interconnected cyber physical systems, reconfiguration to meet new mission needs equates to “reusing” software in new contexts and environments. We must find ways to enable the warfighter to reconfigure their systems to achieve mission success with confidence through our acquisition cycle. We must find ways for highly coupled, integrated systems that contain software to perform in new contexts, under new conditions, at all times. Current rapid acquisition models are necessary but faulty. For rapid acquisition to be successful at a broad level, it is necessary to embrace the implicit notion that software, like hardware, must be defined, described and reusable. Just as physical materials and integrated circuits have “data sheets” that describe standard fitness for use, every component of software must also come with an equivalent notion of a “data sheet”. As software can change faster than physical components, static data sheets are infeasible. The current acquisition system of software enabled systems lacks the engineering tools and methods to rapidly argue the fitness for use of that software within new contexts.[4]

State of the Future

Historically, the whole-system focus of embedded software system designs has been critical to designing trustworthy and efficient systems while also managing the limitations of on-board compute resources. Engineers have been able to rely on very tightly integrated hardware and software to perform a specific role within a specific platform, knowing that the systems will be operating in well-defined and isolated contexts. Now that we can no longer accept the cost and extended development timeframes of this approach, we need to upgrade our engineering processes to enable us to build safe and secure systems that are both highly connected and adaptable to evolving mission needs.

---

[3] Bill Kinzig et al. Global hawk systems engineering case study. 2009.

[4] Nancy G Leveson and Kathryn Anne Weiss. Making embedded software reuse practical and safe. In ACM SIGSOFT Software Engineering Notes, volume 29, pages 171–178. ACM, 2004.

Suppose,for example, that a warfighter needs a more capable targeting subsystem for an unmanned aerial system (UAS). Ideally, the squadron commander could authorize a weapon system upgrade and directly purchase and install the new targeting subsystem. However, there is a list of engineering obligations that need to be met. It may be that the new targeting subsystem had been designed for a different UAS with different software attributes, requiring its software to be reconfigured to talk to the new UAS. The new targeting subsystem may have different computational characteristics (timing, error rates, etc), raising issues regarding the overall behavior of the integrated system. In another scenario, the new targeting subsystem software may have a different cybersecurity profile from the previous one, raising questions as to how secure the new integrated system will be.

The State of the Future lies in addressing these kinds of challenges. If we had strong technological approaches to all of these engineering concerns, the warfighter could upload the reconfigured software as a software patch for the existing UAS with confidence that the resulting system will exhibit predictable behaviors, even in a cyber-contested environment. Additionally, ongoing quality control would include warfighter feedback, sharing how the component worked in the field and how it did not, allowing them to upgrade systems only when upgrades are needed and will be successful. This would drive higher efficiency on sustainment and maintenance.

This is a vision of component-oriented systems. Component oriented systems are systems that can be iteratively built and adjusted by replacing components of the system (software and/or hardware). The use of digital engineering and digital twins advances and enables the premise of component oriented engineering. The most promising approach to achieving this vision is a component-oriented systems engineering approach where individual pieces of functionality are created with minimal external dependency and a strong understanding of the attributes of the component itself. Properties of high cohesiveness (clear single purpose) and low coupling (minimal external dependencies) make for a good design of a component and increase its flexibility for reuse and repurposing.

The component-oriented mindset builds on the excellent progress the DoD has made so far with Modular Open Systems Architecture (MOSA), and it takes the next step by adding significant technological automation. Specifically, the behaviors as well as the interfaces of the various components should be well-defined (or learned), and smart integration tools should know what components are available and how to combine them. With effective machine-assisted component-oriented systems engineering we will be able to build composable systems with confidence the software is correct.

To know how to combine components, smart integration tools should leverage the network effect across the DoD enterprise. As components are reused, they will be integrated in new settings. If that information can be learned by the integration tools, it will be able to repeat the task in additional related settings.

To gain understanding of the behaviors of individual components, multiple testing and verification approaches must be leveraged, including verifiable code generation, software verification, traditional test and evaluation, and run time assurance techniques. No single behavioral method is a silver bullet, but smart integration tooling will combine multiple techniques to gain deep understanding of the newly integrated system capabilities and risk profile.

In a future state with component-oriented systems engineering, the needs of the combatant forces on the front lines can directly be translated into rapid acquisition at the highest level. If a system is designed with a modular open architecture involving software and hardware, the combatant forces closest to the mission will be positioned to address a new threat as it emerges incrementally, rather than waiting for the next “block” upgrade. As our warfighters are the most experienced users of our acquired capabilities and tools, we already seek their needs and suggestions to address the most near-term needs. Often these needs are lost in bureaucracy and acquisition of large systems. In a new world of component-oriented systems, our warfighters could rapidly access a market place, search for a specific weapon system, and view the available components that could be installed on this system to achieve the mission utilizing smart integration tooling.

How Do We Get There

While a clean sheet approach is helpful for designing highly trustworthy, and composable software enabled systems, in reality, this approach is not feasible. Most systems are built with existing software that is reused or modified, and often not fully understood. We live with a legacy of large monolithic systems with limited componentization. Component-oriented modularity often takes a backseat to production and deployment deadlines leaving a significant technical debt to be incurred in post-deployment fixes and sustainment.

To realize the future of rapid acquisition at the hands of the warfighter, engineering modernization efforts and additional focused applied research is required. An initial set of proposed projects includes:

- **Legacy Systems Modernization:** Reduce cost and shorten system upgrade cycles by automatically generating assured MBSE models that allow for rapid modification and certification of Airworthy software components. Additionally, the software components can be retrofitted to support Modular Open Systems Architecture guidelines such as Open Mission Systems (OMS) that enable for technological insertion of increasingly complicated autonomy packages. These packages, which require high levels of trust before fielding and use in combat operations, include extensive test artifacts, documentation, and ease the integration of hardware in the loop (HWIL) and software in the loop (SIL) simulators. By leveraging SIL/HWIL and a common Modeling Simulation, and Analysis environment, these capabilities can be rapidly tested, updated, and retested to increase trust in system functionality and behavior.

- **High Confidence Composability Research:** Conduct applied research on leveraging machine learning to aid in increasing confidence rapidly composing systems. The next generation of technologies for composable systems engineering will include advances in the areas of software confidence via self testing, automated decomposition, run time assurance and emergent collective behavior of components.
- **Advancements in Tooling and Techniques:** Develop, prototype, and make available cutting edge and emerging tooling that enables modern digital engineering and digital twinning concepts to support the implementation of complex software such as autonomy into new and legacy systems. This requires an environment to make systems engineering tools and demonstrations accessible to potential users:
    - Develop tools and a process that would allow for the automated assessment of software evidence and provide justification for a software's level of assurance that is understandable. [5]
    - Advance the idea that mathematical models and abstractions of software and hardware components should be used to characterize behaviors, and that reusable system components should be contained in a model-based library. Search functions over this library would leverage cloud-based machine learning to optimize the use of these components in new environments.
    - Create capabilities to verify neural networks in cyber-physical systems by continually monitoring a system's developing behavior which has become an ASTM standard (American Society for Testing and Materials) and is recognized by the FAA as a viable option for the certification of components of unknown provenance.[6] [7]
    - Leveraging advances in machine learning, advance the research for continuous component-oriented confidence, where ongoing monitoring of components enables auto-argumentation and behavioral modeling continuously. A future state must exist where components are embedded with assurance tools and run-time monitors such that the pedigree or technical readiness level of a component automatically increases as it is used; first in the research laboratories, next in test and evaluation, in rapid prototyping and finally in sustainment. This future reduces the burden of manually modeling and verifying systems and leverages a "network-effect" of confidence across different platforms and environments.

Impact on Community

The Dayton Region, Ohio and the Midwest is poised to advance the concepts of component-oriented software-based engineering to the fielding of autonomous capabilities in

---

[5] Graydon, Patrick J., and C. Michael Holloway. "An investigation of proposed techniques for quantifying confidence in assurance arguments." *Safety science* 92 (2017): 53-65.

[6] Clark, Matthew, et al. *A study on run time assurance for complex cyber physical systems*. AIR FORCE RESEARCH LAB WRIGHT-PATTERSON AFB OH AEROSPACE SYSTEMS DIR, 2013.

[7] ASTM International. Astm f3269-17, standard practice for methods to safely bound flight behavior of unmanned aircraft systems containing complex functions. Technical report, ASTM International,West Conshohocken, PA, 2017.

cyber physical systems. Component-oriented software-based engineering utilized principles of mathematical modeling such as those used to build physics based systems. The engineering mindsets, our academic institutions and the demand for rigor resides within our region. The Department of Defense (DoD) led by the Air Force is leading the charge to deploy cutting edge digital first approaches to implement autonomy in CPS. This leadership position evolves from the premise that autonomous, software-based systems operating in contested environments require more rigor than those used in traditional commercial practices.

Dayton is home to the research, development, and acquisition of Air Force systems. Building workforce, companies, and capabilities in the region that will launch the next wave of software deployment in the region protects the value of Wright Patt and the Air Force Materiel Command. Through collaborations with regional academic institutions, businesses and nonprofits, the region is poised to offer the cutting edge capabilities by leveraging our far reaching ecosystem. By serving as the thought leader in the next generation of software, component-oriented engineering for CPS, the region will:

- Build a workforce through collaboration with academia to make relocation attractive for companies looking to build correct CPS capabilities
- Enable additional startups through the commercialization of emerging tools, protocols and procedures created in the region
- Support the growth and modernization of existing businesses and Air Force partners by providing expertise and leadership in CPS assets
- Create opportunities for research and applied learning opportunities for academia in the area of digital, systems engineering.