SYM-AM-19-033

PROCEEDINGS
OF THE
SIXTEENTH ANNUAL ACQUISITION RESEARCH SYMPOSIUM

WEDNESDAY SESSIONS
VOLUME I

Acquisition Research:
Creating Synergy for Informed Change

May 8–9, 2019

Published: April 30, 2019

Prepared for the Naval Postgraduate School, Monterey, CA 93943.

ACQUISITION RESEARCH PROGRAM
GRADUATE SCHOOL OF BUSINESS & PUBLIC POLICY
NAVAL POSTGRADUATE SCHOOL

Acquisition System Design Analysis for Improved Cyber Security Performance

Brad R. Naegle, LTC, U.S. Army (Ret.)—is a Senior Lecturer at the Naval Postgraduate School, Monterey, CA. In addition to acquisition course development and delivery, he is a member of the Navy's software community of practice. While on active duty, LTC (Ret.) Naegle was assigned as the Product Manager for the 2½-ton Extended Service Program (ESP) and USMC Medium Tactical Vehicle Replacement (MTVR) from 1994 to 1996 and served as the Deputy Project Manager for Light Tactical Vehicles from 1996 to 1997. He was the 7th Infantry Division (Light) Division Materiel Officer from 1990 to 1993 and the 34th Support Group Director of Security, Plans, and Operations from 1986 to 1987. Prior to that, LTC (Ret.) Naegle held positions in test and evaluations and logistics fields. He earned a Master of Science degree in systems acquisition management (with Distinction) from the Naval Postgraduate School and an undergraduate degree in economics from Weber State University. He is a graduate of the Command and General Staff College, Combined Arms and Services Staff School, and Ordnance Corps Advanced and Basic Courses.

Abstract

There is ample evidence that cyber-attacks and cyber warfare are a growing concern for the United States. Our warfighting systems and networks have inherent vulnerabilities and so are targets for cyber adversaries. By nature, cyber warfare is an asynchronous strategy, so the danger posed by a cyber threat is not proportional to the size of the entity initiating the attack. The United States' traditional adversaries, state and non-state actors, domestic terrorists, and even individuals can pose an equally dangerous threat.

The various types and astonishing number of cyber-attacks on the DoD has focused efforts to limit exposure to cyber-attacks and mitigate unavoidable vulnerabilities. The most effective way to "harden" systems against potential cyber-attacks is to develop the system with a cyber warfare mindset. To do this, program managers must have an in-depth understanding of their system's cyber vulnerabilities and exercise control over the design and configuration of those vulnerable subsystems.

There are several challenges in both understanding and controlling a system's cyber vulnerabilities, including that the Defense Acquisition System (DAS) is designed to cede most of the design decisions to the contractor. All known and potential cyber vulnerabilities need to be treated as system Configuration Item, so that design and configuration is under government control.

Fortunately, there are tools, techniques, and analyses that can augment the DAS to gain a better understanding and provide more control over the design and configuration of those subsystems presenting cyber vulnerabilities. This research analyzes the integration of these tools and the expected improvement in cyber performance resulting from the implementation. The tools include the integration of the Maintainability, Upgradeability, Interoperability, Reliability, and Safety/Security (MUIRS) analyses; Software Engineering Institute's Quality Attribute Workshop (QAW); Software Engineering Institute's Architecture Trade-off Analysis Methodology^{sm}; and the Failure Modes and Effects Criticality Analysis (FMECA).

Background

Hardly a day has gone by during my tenure at Cyber Command that we have not seen at least one significant cybersecurity event occurring somewhere in the world. We face a growing variety of advanced threats from actors who operate with ever-more sophistication

and precision. —Admiral Michael S. Rogers, Commander, U.S. Cyber Command (Pellerin, 2017)

Threats from cyber-attacks have clearly emerged as one of the most significant threats to the United States and to the Department of Defense (DoD). The sources of attack are varied and include state and non-state actors, traditional adversaries, as well as domestic sources. The emergence of artificial intelligence (AI) cyber-attacks has added to the threat significantly. “Automation and artificial intelligence are beginning to ‘make profound changes to the cyber domain,’ a threat that the military hasn’t yet fully grasped how to counter, Robert Behler, the Defense Department’s director of operational test and evaluation, said” (Capaccio, 2019).

Cyber-attack is an extremely effective, asynchronous warfare tactic, meaning that adversaries that could not possibly face the U.S. military can still be very effective in the cyber environment. While traditional adversaries like China, Russia, North Korea, and Iran are certainly players in the cyber-warfare arena, non-state actors, domestic terrorists, and even individuals can pose a disproportionate threat in the cyber world.

> The relatively inexpensive cyber options being employed today by both state and non-state hacking groups make it an incredibly efficient “leveler” of power. A small group of hackers using simple spear-phishing tactics, for example, can have massive impact on military installations, government operations, critical infrastructure and potentially even weapons systems. (Martini, 2016)

Obviously, this opens up the cyber-threat adversaries list to an unimaginable number that would be nearly impossible to manage or even prioritize.

The types and sophistication of cyber-attacks are growing exponentially. Denial-of-Service (DoS) or Directed-Denial-of-Service (DDoS) attacks have impacts on communications, networks, internet, intranet, and systems using Global Positioning System (GPS) to name a few. Malicious software (malware) is a common cyber-attack methodology that can take several forms from passive collection of data to destructive applications designed to destroy or disrupt operating systems. Spoofing is the introduction of erroneous or misleading information into systems that can dramatically affect operations and can even include voice or video communications assembled by AI that appear to be authentic, but are compilations from available sources. Can you imagine getting verbal commands in the recognized voice of the commander that are realistic in appearance, but totally constructed by AI? Take-over of systems is certainly of concern and in 2011, Iran claimed that it took over a U.S. RQ-170 surveillance drone, although that is disputed by the United States. It was not clear how Iran acquired the drone intact. Some U.S. experts dismiss the possibility that Iran could hack and then take over the drone’s controls, as Iran claims. And yet similar disruptions have proven possible in other battlefields, notably with the Iran-backed Hezbollah militia in Lebanon and drones from Israel.

> “Those jamming capabilities exist, and a lot of them are not as new as we would like to imagine,” says former U.S. Navy electronics warfare officer Densmore. “Anything that has a sensor, that takes communications links—as does the RQ-170, which has two, one for the satellite, and the other is line-of-sight with the ground control station—all it takes is disrupting that.” (Peterson, 2011)

In 2015, the FBI filed a report regarding a United Airlines passenger who had repeatedly gained engine thrust controls of Boeing 737 airliners through the entertainment port:

> During the conversations, [FBI investigating special agent Mark] Hurley wrote, [Chris] Roberts disclosed that he had previously hacked into IFE [in-flight entertainment] systems, manufactured by Panasonic and Thales—which provide video monitors in the passenger seatbacks—about 15 or 20 times on various flights between 2011 and 2014. According to the document, Roberts said he gained access to the systems by plugging his own laptop computer into the IFE system's electronic boxes mounted under passenger seats. Once in the system, he said he was able to access other systems—including the jets' Thrust Management Computer, which is responsible for providing power to the plane's engines. (Ware, 2015)

Software hacking with active systems designed to destroy, take over, or spoof software applications have exploded. In addition, stealthy software attacks designed to gather data, log keystrokes, or lay in wait for a particular event, peer connection, or timing event are more and more common. In short, there appears to be no end to the types of cyber-attacks or the combinations and permeations of those known today.

The methods for conducting cyber warfare appear to be continuing to expand, and with AI-generated attacks, the differing types of attacks are likely to continue to expand. The proliferation of types of cyber-attacks was one of the drivers for the transition from the Defense Information Assurance Certification and Accreditation Program (DIACAP), which tended to be a terminal process once the certificate was issued, to the Risk Management Framework (RMF), which is a continuous risk management process. While this is a logical approach given the constantly advancing cyber threats, it causes more work for the PM as the iterative process will be examined numerous times during the developmental process.

DoD Acquisition Cyber Exposure

An ever-increasing number of DoD weapon systems are leveraging technology that, unfortunately, places them in danger of cyber-attacks. The DoD's warfighting systems have degrees of dependence on GPS, communications, networks, and software, which all have opportunities for cyber vulnerabilities. The DoD is in the process of developing more extensive networks to leverage the inherent advantages with the communication capabilities, as well as the situational awareness that networks can provide. These more extensive networks will include more and more platforms, thus increasing their cyber vulnerabilities, as well. All of these will be extremely valuable cyber targets for adversaries. The advantages of the system technologies and networks will continue to be desired by the DoD, so planning effectively to counter cyber vulnerabilities will be a reality for system and network developers.

This all means that the DoD will continue to develop systems and networks with inherent cyber vulnerabilities, managing those vulnerabilities with a continuous RMF process. This puts the program manager (PM) in a nearly constant state of cyber vulnerability assessment, reacting to the ever-emerging cyber threats from the vast array of entities involved in cyber warfare against the United States. This could potentially require significant time and resources to track and assess every emerging cyber threat and perform a vulnerability assessment on the system under development.

The PM cannot control the emergence of new cyber threats, so must concentrate on what can be controlled: the system's cyber vulnerabilities. Understanding the system's vulnerabilities allows the PM to quickly and efficiently assess any new cyber threat and quickly perform an RMF iteration to verify the severity of the threat and any mitigation efforts available. The PM must identify all system potential or actual cyber vulnerabilities and take control of managing the design and architecture of each one. All cyber vulnerabilities must

be designated as a Configuration Item (CI), placing it under government control, or at least be treated the same way as a CI.

Barriers to Effective Cyber Performance Design

There are significant barriers to achieving a complete understanding of any system's vulnerabilities, but overcoming these barriers is a key to being able to rapidly respond to new cyber threats. Any communications conducted by the system are a potential vulnerability, but especially wireless communications such as those used by unmanned aerial vehicles (UAVs), transmitting intelligence, surveillance, and reconnaissance systems, systems using GPS or other guidance/positioning information, and many autonomic systems that passively transmit system health data. While this seems to be rather straight forward, some commercial components may have communications abilities that are not apparent. For example, virtually all cell phones include an FM radio chip that can be activated: "That's right; today's smartphones have a built-in FM chip that gives them the ability to receive radio signals in your area" (OPB, n.d.). An in-depth understanding of any subsystem capable of transmitting or receiving information is required.

System software development is a particular challenge in ensuring that any cyber vulnerability is known. The software must be engineered carefully to minimize vulnerabilities, and significant design and engineering needs to be included for software-intensive systems to be able to self-check for cyber intrusion attempts. For example, cyber vulnerabilities could be significantly reduced if the software application could detect and immediately report any attempt to modify or add software lines of code, or access to system software at all. Any authorized access or maintenance activities would need to have a rigorous authentication protocol to ensure only authorized access or changes were accepted.

Software engineering needs to be conducted with cyber vulnerabilities as a hard parameter. One of the challenges in software engineering is to keep the software from communicating and interacting with other connected software systems or modules. The Boeing 737 example of accessing flight controls through the entertainment system is a good example of this concept. With all of the engineering discipline needed to reduce cyber vulnerabilities, using commercial software or reused software is extremely problematic, if not impossible. Any existing software to be added to the architecture of a developmental system would have to be thoroughly vetted and the inner working known to a very high degree. With most commercial software, this is not possible as the DoD does not own the data rights and they are most often not obtainable because there is so much of the commercial company's proprietary practices evident in the code. In addition, there are a significant number of coders who code in what is known as a "back door" to the software that allows them access, bypassing the normal security protocols built into the programs.

> The National Grid could be at risk of a cyber attack after a hacker group linked to China create a "back door" in software used by big businesses. Companies at risk from this latest attack include American weapons firm Lockheed Martin, Russian energy supplier Gazprom and French bank Société Générale. (Tarrant-Cornish, 2017)

This means that software reuse and using most commercial software would be nearly impossible when considering potential cyber vulnerabilities unless the engineering structure was completely known and verified to ensure that any potential cyber vulnerabilities associated with the reused code were understood and included in the risk management. While this seems logical, the amount of software engineering needed to achieve this in the reused software may actually exceed the engineering effort in the original

design and build of the app. Again, this presupposes that the original software is even accessible, which is not the case in most commercial software.

The Challenge

The PM must have control and insight to the system architecture, build processes, and verification methodologies that far surpasses the current state of practice in the DoD acquisition environment to gain control of known and future cyber threats.

This challenge is exacerbated by the existing DoD acquisition environment for developing systems.

> Since the implementation of Acquisition Reform in the nineties, detailed specifications have been replaced with performance specifications in order to leverage the considerable experience and expertise available in the defense contractor base. In most hardware-centric engineering disciplines, the expertise that the DoD seeks to leverage, includes a mature engineering environment in which materials, standards, tools, techniques, and processes are widely accepted and implemented by industry leaders. This engineering maturity helps to account for derived and implied requirements not explicitly stated in the performance specification. (Naegle, 2014, p. 8)

The DoD requirements generation system has been designed to provide the contractor with performance specifications to be met within some parameters. In short, the design control and engineering has been placed in the hands of the contractor to leverage the advancements obtained in the commercial sector. In the current and rapidly advancing cyber warfare environment, the DoD now finds that it needs to have much more positive control of the engineering design and build processes that it had significantly ceded to the contractor.

A Way Forward

Fortunately, there are existing analyses, tools, and techniques that can augment the Defense Acquisition System (DAS) to gain more insight and control over the critical cyber design elements. I have previously researched several of these and integrated them into the DAS.

Tools, Techniques, and Processes

The tools, techniques, and processes are briefly described as follows.

- The Software Engineering Institute's (SEI's) Quality Attribute Workshop (QAW)
- The Maintainability, Upgradability, Interoperability, Reliability, & Safety and Security (MUIRS) analytic technique
- The Software Engineering Institute's Architectural Tradeoff Analysis Methodology (ATAM^{sm})
- The Failure Modes and Effects Criticality Analysis (FMECA)

Quality Attribute Workshop (QAW)

The QAW is primarily a method for more fully developing system software requirements and is intended to provide stakeholders' input about their needs and expectations from the software (Barbacci et al., 2003, p. 1). As the system requirements are developed, software quality attributes are identified and become the basis for designing the software architecture. By adding in the desired system cyber performance as a system

quality attribute, software design activities will necessarily include analyses of possible system cyber vulnerabilities as part of the design process.

The Software Engineering Institute's (SEI's) Quality Attribute Workshop (QAW) is implemented before the software architecture has been created and is intended to provide stakeholder input about their needs and expectations from the software (Naegle, 2007). The QAW process provides a vehicle for keeping the combat developer and user community involved in the DoD acquisition process, which is a key goal of that process. In addition, the QAW includes scenario-building processes that are essential for the software developer to design the software system architecture (Barbacci et al., 2003, pp. 9–11). These scenarios will continue to be developed and prioritized after contract award to provide context to the quality attribute identified for the system.

Although the QAW would certainly be useful after contract award, conducting the workshop between combat developers/users and the program management office before issuance of the Request for Proposal (RFP) would provide an improved understanding of the requirements, including cyber performance, enhance the performance-specification preparation, and improve the ability of the prospective contractors to accurately propose the cost and schedule. This approach would support the goals of the System Requirements Review (SRR), which is designed to ascertain whether all derived and implied requirements have been sufficiently defined (Naegle & Petross, 2007, pp. 5–6).

The QAW process is primarily designed to more fully develop system software requirements so that the government Request for Proposal (RFP) is clearer to potential contractors. In turn, the resulting proposals should be more accurate and realistic, reducing requirements and project scope creep. This is critical in communicating the cyber security expectations of the system so that they remain a priority when designing the system (Naegle, 2014, p. 25).

Maintainability, Upgradability, Interoperability/Interfaces, Reliability, and Safety/Security (MUIRS) Analytic Technique

The MUIRS analytic technique is designed to provide a framework for better understanding of essential supportability and safety/security aspects that the warfighter needs and expects, but often doesn't communicate clearly with the capabilities-based JCIDS documents. This analytic technique helps compensate for the immature software engineering environment as the MUIRS analysis illuminates the derived and implied requirements that the immature environment cannot (Naegle, 2014, p. 25).

Much of the software supportability and safety/security performance that typically lacks consideration and is not routinely addressed in the software engineering environment can be captured through development and analysis of the MUIRS elements. Analyzing the warfighter requirements in a QAW framework for performance in each MUIRS area will help stakeholders identify software quality attributes that need to be communicated to potential software contractors (Naegle, 2006, pp. 17–24). The system safety and security (the "S" in MUIRS) would certainly address the cyber performance and vulnerabilities as part of the analysis process. The MUIRS analysis assists the QAW process by focusing on those elements that are, too often, overlooked during the requirements generation process.

MUIRS primarily addresses the immature software engineering environment as it provides an analytic approach for critical sustainment and safety/security attributes that are often missing, weakly articulated, or vaguely stated in the requirements produced. With its capabilities and performance-based requirements processes, the DoD significantly depends on mature engineering environments to "fill the gaps" left from the requirements generation and communication processes, but the software engineering environment is unable to do so.

The MUIRS analysis is also an enabler for the QAW and ATAM[sm] architectural processes discussed next (Naegle, 2014, p. 25).

Architectural Tradeoff Analysis Methodology (ATAM[sm])

The Software Engineering Institute's Architectural Trade-off Analysis Methodology ATAM[SM] (ATAM) is an architectural analysis tool designed to evaluate design decisions based on the quality attribute requirements of the system being developed. The methodology is a process for determining whether the quality attributes are achievable by the architecture as it has been conceived before enormous resources have been committed to that design. One of the main goals is to gain insight into how the quality attributes trade-off against each other (Kazman et al., 2000, p. 1). Obviously, the system's capabilities will necessarily be traded off with their inherent cyber vulnerabilities as part of the ATAM process. Those unavoidable cyber vulnerabilities will then need to be mitigated throughout the design of the system.

Within the Systems Engineering Process (SEP), the ATAM provides the critical Requirements Loop process, tracing each requirement or quality attribute to corresponding functions reflected in the software architectural design. Whether ATAM or another analysis technique is used, this critical SEP process must be performed to ensure that functional- or object-oriented designs meet all stated, derived, and implied warfighter requirements. In complex systems development such as weapon systems, half or more than half of the total software development effort will be expended in the architectural design process. Therefore, DoD program managers must ensure that the design is addressing requirements in context and that the resulting architecture has a high probability of producing the specified warfighters' capabilities described in the JCIDS documents, with increasing emphasis on the cyber performance and vulnerabilities (Naegle, 2014, pp. 26–28).

The ATAM focuses on quality attribute requirements, so it is critical to have precise characterizations for each. To characterize a quality attribute, the following questions must be answered:

- What are the stimuli to which the architecture must respond?
- What is the measurable or observable manifestation of the quality attribute by which its achievement is judged?
- What are the key architectural decisions that impact achieving the attribute requirement? (Kazman, Klein, & Clements, 2000, p. 5)

The ATAM is designed to elicit the data and information needed to adequately address the three questions above. These questions, focused on requirements and quality attributes, are user-centric, and so the ATAM scenarios must be constructed by the user community (Naegle & Petross, 2007, p. 25). The methodology keys on scenario development in three main areas:

- Use Case Scenarios. As the name suggests, these scenarios describe how the system will be used and sustained in the harshest environments envisioned. It includes all interoperability requirements and duty cycles as well. These user-created scenarios convey critical cyber performance information to the system developer including who uses it (and how do we know that it is an authorized user), how they use it (does it involve communication, sensors, GPS, automated inputs, software, etc.), how they maintain it (e.g., would software maintenance be done remotely, which would be a huge cyber vulnerability, etc.), how they use it (does any of the use or maintenance create cyber vulnerabilities, what does it interoperate with, etc.), when and for how long they use and maintain it, and of

course, all of the known ways that the adversary will attack the system, including cyber.

- Growth Scenarios. Growth scenarios focus on known and anticipated system change requirements over the intended life cycle. These scenarios include upgrades and technology refreshments planned; interoperability requirements, such as inclusion in future warfighting networks; changes in sustainment concepts; and other system changes expected to occur over time. For each growth event impacting a cyber vulnerability component, a full Risk Management Framework iteration should be planned.
- Exploratory Scenarios. Exploratory scenarios focus on operations in unusual or stressful situations. These address user expectations when the system is degraded or operated beyond normal limitations due to emergency created by combat environments. These scenarios would necessarily include operations while under cyber-attacks of all sorts. The exploratory scenarios include Failure Modes and Effects Criticality Analyses (FMECA) to identify the essential functions that must not fail. For the DoD, failure modes must include failures that are adversary induced, so understanding all vulnerabilities and how they might be exploited is essential to these analyses. This would obviously include cyber vulnerabilities of all types, which would become the basis for conducting risk analyses on all future types and modes of cyber-attack.

As important to the software engineers, FMECA also identifies those enhancing functions that should not preclude the system from functioning when that enhancing function is degraded or non-operational. For example, the M1 Abrams tank uses the ambient temperature as an enhancer to the main gun accuracy but needs the ability to be fully operational in the case where the ambient temperature sensor is malfunctioning. The software engineers need that information to properly design the software.

Testing

Test cases are developed out of the scenarios, which firmly link the test program with the user requirements in the context of the scenarios. This methodology also helps to ensure that there are verification events for cyber performance, software, and sustainment requirements, which are too often missing from the testing program (Naegle, 2014).

System cyber testing is extremely challenging, requiring specialized skill sets, such as software hackers, communications and sensor experts, and software engineers, to create software viruses, worms, and the cyber-attack artificial intelligence entities. In addition, significant resources are required to perform some of the cyber-attack scenarios like denial of service attacks. The challenges are exacerbated when combining different types of attacks in the same scenario, as cyber-attacks often do.

It is nearly impossible to keep up with the ever-changing cyber threat environments that should be represented in system testing, and the potential threats created by AI-based cyber-attacks is nearly limitless. This makes it imperative that PMs understand and manage their system's vulnerabilities, and not simply react to the latest iteration of cyber-attack.

As shown in Figure 1, the ATAM is an integrating function for many of the tools and techniques discussed here. It is designed to be an iterative process and would be most effective when started in early concept development, then continued through contract award, prototyping, and into the design review process.

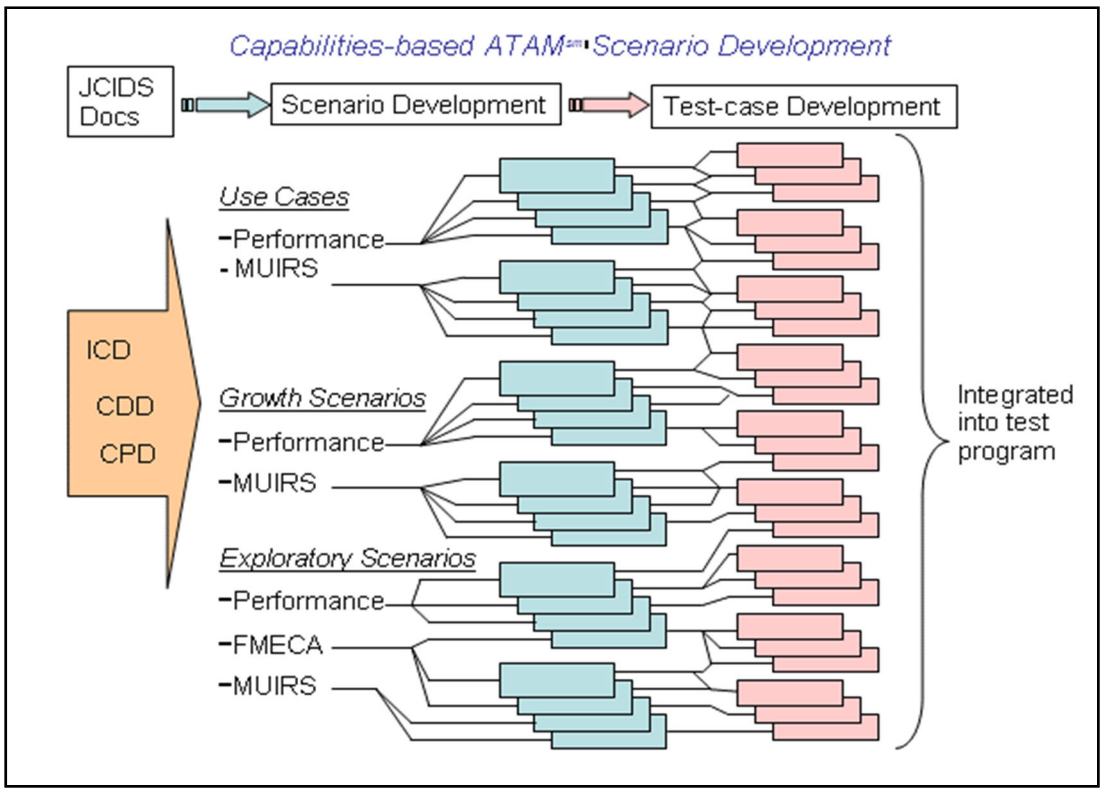

Figure 1. Quality Attribution Workshop and Architectural Tradeoff Analysis Methodology Integration Into Life-Cycle Management
(Naegle & Petross, 2007, p. 25)

The ATAM process addresses four primary problem areas:

- The scenario development provides much more operational context than the typical Operational Mission Statement/Mission Profile (OMS/MP) provides. This level of detail helps to compensate for the immature software engineering environment and is critical for the proper design of the software architecture. The details provided by the ATAM scenarios helps to inform system designers to potential cyber vulnerabilities and is critical to the discovery process and optimizing the cyber design.
- The ATAM serves as a very effective software design metric function. With the software development team using 50% or more of the available resources for requirements analysis and software design before the Preliminary Design Review (PDR), it is critical to have an effective software design metrics function. Any significant redesign is extremely costly in both funding and schedule. If the design is reacting to cyber threats, the design process will be in chaos. Traditional software design metrics focus on the design complexity and do not address whether the design is adequate. ATAM directly links the user requirements to the system architectural design.
- As the testing program is developed from the scenarios, it becomes difficult to omit any critical testing event. In addition, the system developer understands the tests or verification events that must be passed for user acceptance. This would feed the Risk Management Framework the valuable information needed to

assess the system's cyber performance. It would also help identify cyber vulnerabilities and create mitigation actions.

- By integrating the MUIRS analyses into the ATAM scenario development, sustainability and safety/security aspects cannot easily be omitted from the system design. As the testing plan flows from the scenarios, the MUIRS design elements will have corresponding test or verification events identified in the test plan. All of the MUIRS elements need to be considered for cyber vulnerabilities and the safety and security should help drive the cyber performance design (Naegle, 2014, pp. 28–29).

Failure Modes and Effects Criticality Analysis (FMECA)

As the title indicates, this analysis methodology is designed to identify system failure modes, to identify the effects of those failures on the system, and to ascertain the relative criticality of that type of failure. In his book titled *Logistics Engineering and Management*, Benjamin S. Blanchard (2004) describes FMECA as follows:

> Given a description, both in functional and physical terms, the designer needs to be able to evaluate a system relative to possible failures, the anticipated modes and expected frequency of failure, their causes, their consequences and impact(s) on the system overall, and areas where preventative measures can be initiated to preclude such failures in the future. (p. 275)

He goes on to state, "The FMECA is an excellent design tool, and it can be applied in the development or assessment of any product or process" (Blanchard, 2004, pp. 275– 276).

Including ATAM FMECA scenarios with the software systems and subsystems provides architectural design cues to software engineers. These scenarios provide analysis for designing redundant systems for mission-critical elements, "safe mode" operations for survivability- and safety-related systems, and drive the software engineer to conduct "what if" analyses with a superior understanding of failure-mode scenarios. For example, nearly all military aircraft are "fly-by-wire," with no physical connection between the pilot controls and the aircraft-control surfaces, so basic software avionic functions must be provided in the event of damage or power-loss situations to give the pilot the ability to perform basic flight and navigation functions. Obviously, this would be a major design driver for the software architect (Naegle & Petross, 2007).

The primary problem areas addressed by FMECA include requirements clarification and prioritization, and helping to ensure a sound architecture design. This analysis also ensures that the most critical software systems are designed with the requisite reliability and will continue to function in degraded modes (Naegle, 2014, pp. 29–30).

The user needs to describe what is expected from the system when a cyber-attack occurs. For example, does the system actively counter the attack or merely report the attack to operators? How does the system detect and report passive cyber-attacks? What happens to system operations when remote nodes lose user authentication, and how is connectivity eventually restored? What actions will be taken in a denial of service attack? All known system cyber vulnerabilities need to be included in the exploratory scenarios, as this gives a baseline for reacting to emerging cyber threats.

As previously stated, one of the main functions of performing FMECA is to identify those software functions that are not critical, and to ensure that failures or anomalies in those non-critical functions do not preclude or negatively affect system capabilities. Today's systems typically have numerous enhancing functions that improve performance but are not

critical, and the software developers have no way to discern the difference between a critical system and an enhancing one without employing FMECA. In addition to identifying those non-essential functions, cyber vulnerability analyses need to be conducted on these non-essential systems as they are a prime target for cyber-attack. Hackers attempt to find the path of least resistance to affect a system's operations, and this path is often through non-essential functions similar to the hacker going through the in-flight entertainment system to access the 737 engine controls.

Integrating the Tools, Techniques, and Analyses

All of the tools, techniques, and analyses presented in this research must integrate with the existing Defense Acquisition System, or they will not be useful for DoD PMs. Figure 2 depicts how they integrate in the development of the system from the user requirements towards the Critical Design review (CDR).

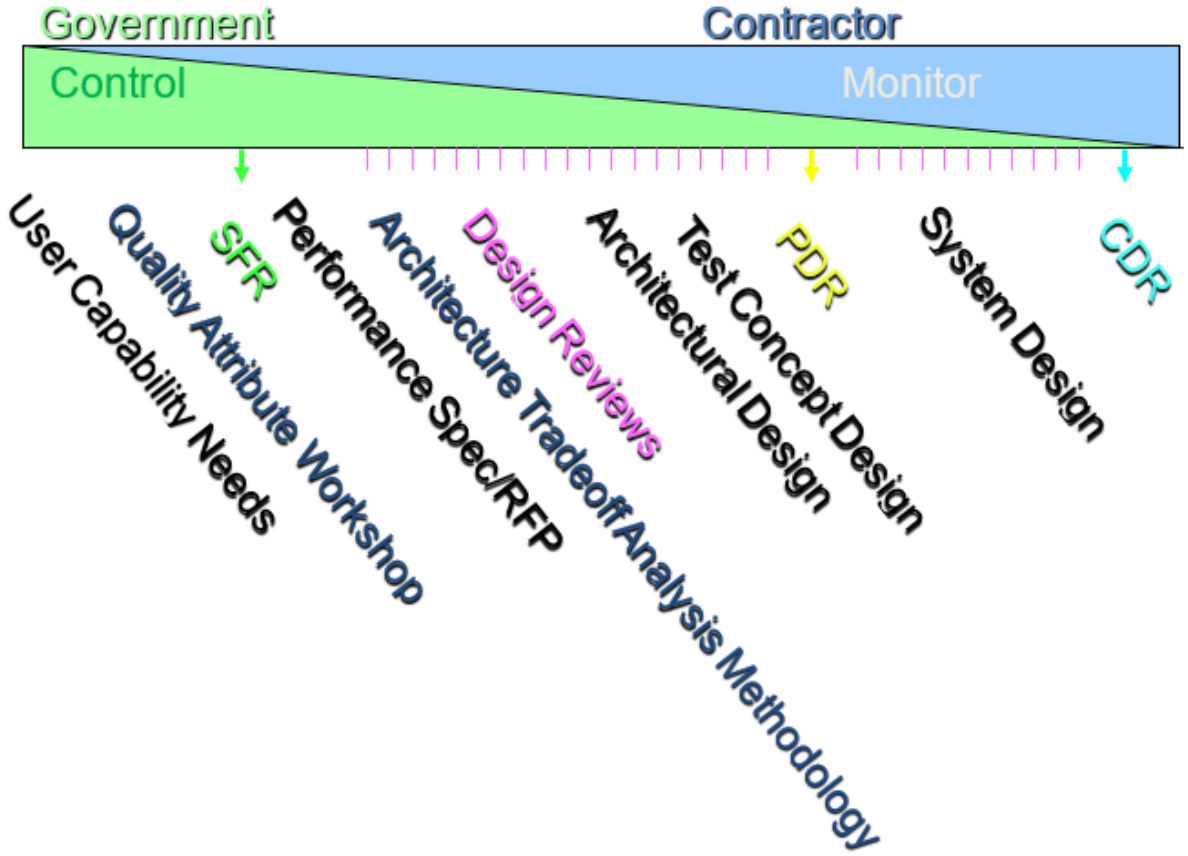

Figure 2. Tools, Techniques, and Analyses Integration Into Design Activities

Figure 2 shows how the government (green) controls the early functions and then monitors the contractor (blue) efforts in the system design process. The QAW is part of the requirements development process and assists in the requirements translation into the performance specification for the Request for Proposal (RFP). The requirements are formally set in the Systems Engineering Process (SEP) at the System Functional Review (SFR) depicted in the figure. The ATAM becomes an integral process within the Design Review (purple) iterative process and serves as the government's input during the early design reviews. The ATAM assists with the contractor's architectural design process and the

ATAM test case development contributes to the development of both the contractor and the government testing concept development. With the proper focus on cyber performance, the system will be designed from the initiation with cyber at the forefront and the testing concept will provide validation of cyber vulnerability mitigation efforts. The purposeful design with traceable cyber elements and associated testing validation fully supports the tenets of the RMF depicted in Figure 3.

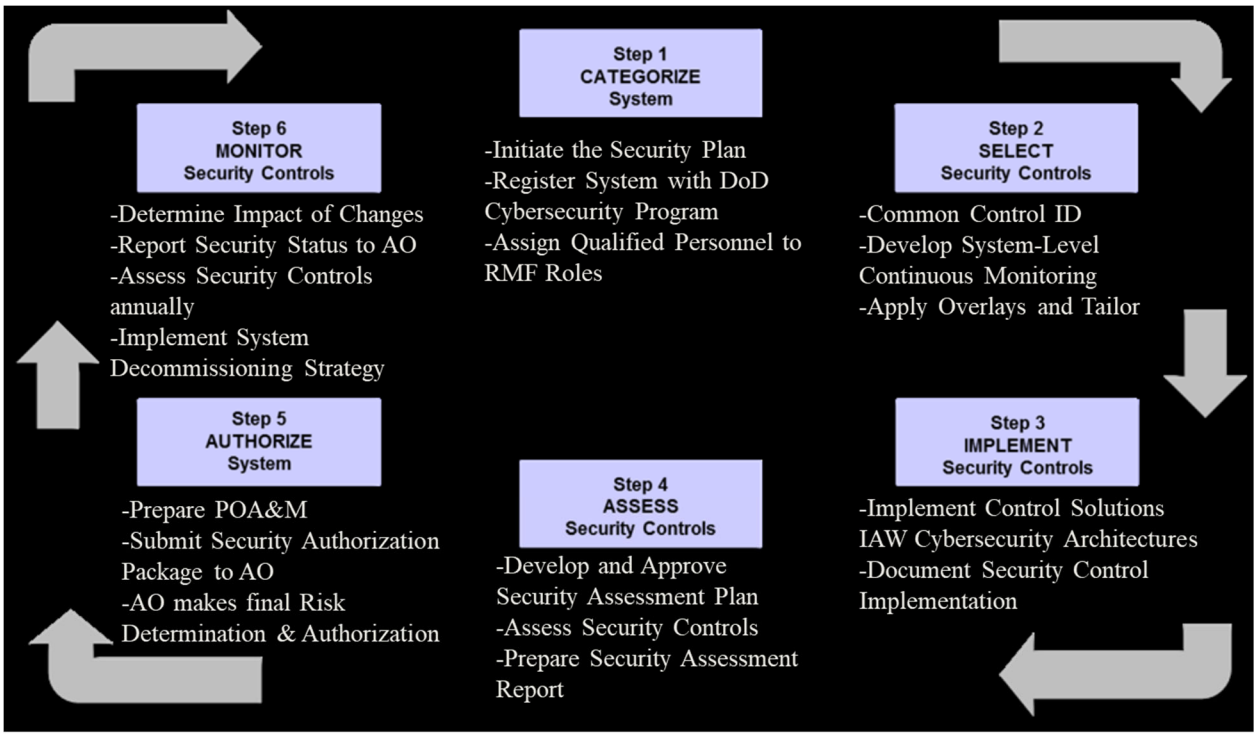

Figure 3. The DoD Risk Management Framework (RMF)
(DoD, 2015, p. 4)

As depicted in Figure 3, the RMF is a continuous and iterative process to continually assess the cyber security aspects of a system. Following the RMF steps, it is clear that the addition of the tools, techniques, and analyses to the DAS provides a method to conduct the RMF assessment from concept to implementation. In step 5, "Authorize," the system's Plan of Action and Mitigation (POA&M) is submitted as part of the security authorization package to the authorizing official (AO), who makes the final cyber risk determination and authorization for the system.

Conclusions and Recommendations

The explosive growth of cyber-attack types and variations, especially with the advent of AI-generated attack modes, makes it nearly impossible to be reactive to new threats. To avoid reacting to every new cyber threat, PMs must thoroughly understand and manage their system's cyber vulnerabilities. To achieve this, PMs must exercise much more control over their system's architectural design than is currently anticipated with the Defense Acquisition System (DAS), which cedes much of the design control to the contractor.

System components that are particularly vulnerable to cyber threats must be designated as Configuration Items and the design and configuration management must be completely controlled by the government. These include any components that have

communications ability, system sensors, virtually all system software, and any other components deemed to have cyber vulnerabilities. This has significant implications for using commercial components and software, or even reuse of software. To understand the system's cyber vulnerabilities, the system component architecture, including software, must be thoroughly understood and controlled. To achieve this in software, the total code architecture must be known and most commercial software will not allow that level of access, as it is considered proprietary. Commercial software data rights are typically unobtainable. Even if data rights could be obtained, the level of engineering effort required to understand the inherent cyber vulnerabilities may exceed the effort to actually build the software from scratch, reducing or eliminating the acquisition cost advantage.

The tools, techniques, and analyses presented in this research augment the DAS to help the PM gain visibility and control of the system design, which is necessary to gain a complete inventory of system cyber vulnerabilities. Effective application of these tools, techniques, and analyses helps inform the Risk Management Framework (RMF) cyber vulnerability assessment techniques, which is what the RMF authorizing official needs to make the final risk assessment and authorization for the system under consideration.

MUIRS (Maintainability, Upgradeability, Interoperability, Reliability, and Safety/Security) Analyses

The MUIRS analyses was designed to help compensate for the DoD requirements generation shortcomings, which too often omit or vaguely articulate performance in each one of these areas even though they are important to the warfighter and impact the system Total Ownership Cost (TOC) significantly. The MUIRS elements also include areas where cyber vulnerabilities may exist and these analyses will likely help identify areas for cyber vigilance.

QAW (Software Engineering Institute's Quality Attribute Workshop)

While the QAW is a software-oriented technique, it is highly effective in fully developing a system's requirements, including the requirements for cyber performance. It was designed to help identify a more complete inventory of requirements, including derived and implied requirements not well identified or defined from the JCIDS and RFP Performance Specification processes. Including the MUIRS analyses as part of the QAW, the resulting requirements inventory is more complete and helps identify potential cyber vulnerabilities to be managed and mitigated.

ATAM (Software Engineering Institute's Architectural Trade-Off Analysis Methodology^{sm})

Another software-oriented methodology, ATAM is designed to more fully develop the system operational and lifecycle context needed to produce a far superior architectural design, especially in software. ATAM is most effective when it integrates the QAW and MUIRS processes. It features user-produced scenarios providing operational context detail not typically provided in the government-generated Operational Mode Summary/Mission Profile (OMS/MP), but absolutely essential for the software engineer to design an effective software system. The scenario development is extremely valuable in identifying potential areas for cyber vigilance including use cases, growth cases that can identify future interoperability needs and technology refreshment events, and exploratory scenarios that identify user expectations while the system is under attack, including cyber-attack. The exploratory scenarios include system FMECA (Failure Modes and Effects Criticality Analysis) scenarios, which can identify both critical and non-critical systems and functions that may reveal potential cyber vulnerabilities.

FMECA (Failure Modes and Effects Criticality Analysis)

The "failure modes" analyses include failure modes induced by adversaries through attacks or intrusion into the systems, so includes cyber warfare as part of the analyses. The "effects" analyses may help in developing cyber vulnerability mitigation strategies. The "criticality" analyses are designed to separate the critical from the non-critical failure modes, but may also help find non-critical systems that pose substantial cyber vulnerabilities as adversaries seek non-critical systems for cyber-attack as they typically have weaker or non-existent cyber defense mechanisms.

Summary

Integrating these tools, techniques, and analyses into the defense acquisition system provides the PM a far superior ability to identify, control, and mitigate the system cyber vulnerabilities in a cost-effective manner. Managing the system vulnerabilities is a better strategy than reacting to the constantly emerging cyber threats and fully supports the DoD Risk Management Framework tenets.

References

Barbacci, M., Ellison, R., Lattanze, A., Stafford, J., Weinstock, C., & Wood, W. (2003, August). *Quality attribute workshops (QAWs)* (3rd ed.) (CMU/SEI-2003-TR-016). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University.

Blanchard, B. S. (2004). *Logistics engineering and management* (6th ed.). Upper Saddle River, NJ: Pearson Prentice Hall.

Capaccio, A. (2019, January) The Pentagon's cybersecurity is falling behind. Retrieved from https://www.bloomberg.com/news/articles/2019-01-28/pentagon-s-cybersecurity-found-unable-to-stay-ahead-of-attackers

DoD. (2015, September). *DoD program manager's guidebook for integrating the cybersecurity Risk Management Framework (RMF) into the system acquisition lifecycle*. Washington, DC: Author.

Kazman, R., Klein, M., & Clements, P. (2000, August). *ATAM[SM]: Method for architecture evaluation* (CMU/SEI-2000-TR-004). Pittsburgh, PA: Carnegie Mellon University, Software Engineering Institute.

Martini, P. (2016, September). Cybersecurity is threatening America's military supremacy. Retrieved from https://techcrunch.com/2016/09/21/cybersecurity-is-threatening-americas-military-supremacy/

Naegle, B. R. (2006, September). *Developing software requirements supporting open architecture performance goals in critical DoD system-of-systems* (NPS-AM-06-035). Monterey, CA: Naval Postgraduate School.

Naegle, B. R. (2014, December). *Gaining control and predictability of software-intensive systems development and sustainment* (NPS-AM-14-194). Monterey, CA: Naval Postgraduate School.

Naegle, B. R., & Petross, D. (2007, September). *Software architecture: Managing design for achieving warfighter capability* (NPS-AM-07-104). Monterey, CA: Naval Postgraduate School.

Organization of Public Broadcasters (OPB). (n.d.). Activate your cell phone's FM chip. Retrieved March 1, 2019, from https://www.opb.org/about/connect/mobilefm/

Pellerin, C. (2017, May). Cybercom: Pace of cyberattacks have consequences for military, nation. Retrieved from DoD website: https://dod.defense.gov/News/Article/Article/1192583/cybercom-pace-of-cyberattacks-have-consequences-for-military-nation/

Tarrant-Cornish, T. (2017, August 17). Chinese hackers 'built back door hack into software to spy on Britain's top businesses.' *Express Online News.* Retrieved from https://www.express.co.uk/news/world/842200/China-hackers-cyber-spying-attack-UK-business

Ware, D. G. (2015, May). Hacker took control of United flight and flew jet sideways, FBI affidavit says. United Press International. Retrieved from https://www.upi.com/Top_News/US/2015/05/16/Hacker-took-control-of-United-flight-and-flew-jet-sideways-FBI-affidavit-says/2421431804961/

ACQUISITION RESEARCH PROGRAM
GRADUATE SCHOOL OF BUSINESS & PUBLIC POLICY
NAVAL POSTGRADUATE SCHOOL
555 DYER ROAD, INGERSOLL HALL
MONTEREY, CA 93943

www.acquisitionresearch.net