Abstract — Information is the fuel of modern society; from social media to the stock exchange, the ability for individual entities to connect with each other over distance makes everything possible. Similarly, the ability to leverage information across a complex battlespace is one of the key elements that make the U.S. Army such a potent fighting force. At the heart of this capability is a robust and adaptive tactical network that facilitates mission command at every echelon. Though the Army possesses a strong network, continuing efforts to improve it over time is a struggle. Cost and schedule overruns have become normal occurrences as individual systems fail to pass the Army’s rigorous interoperability certification requirements. Without interoperability, the network does not work. The Army’s acquisition community’s shift to focus on a new paradigm of network development, the Common Operating Environment (COE), promised to create a better system for insuring network interoperability in a timely manner. Old habits and practices, however, have threatened the promise of the new paradigm in terms of development, evaluation, and certification. This document examines current practices and issues regarding network development and makes a recommendation for how to approach COE to achieve greater levels of interoperability faster and cheaper. By utilizing an agile based approach, COE can be developed as a system of systems through iterative sprints that focus on developing an interconnected network that works the first time.

Keywords—System of Systems, Systems of Systems Testing and Evaluation, Scrum of Scrums, Common Operating Environment

I. INTRODUCTION

In the post-Vietnam era, the United States Army has focused on developing a lean, agile, and multi-mission capable force through the development of a network of command and control (C2) related capabilities. Unfortunately, the rush to provide the American warfighter with advanced C2, or “mission command” capabilities has funneled such systems into stovepipes of disparate capability. Though additional technical solutions have made these separate capabilities interoperable, they still fail to create the value for the warfighter that an integrated network would provide.

Recently, the United States Army has utilized the concept of a System of Systems in order to improve the development of these networks. A System of Systems (SoSs) is defined as a collection of separate and useful systems that deliver a unique capability [1]. The Army is currently transitioning to a new paradigm of SoS called the Common Operating Environment (COE), which is a System of Systems designed to deliver a unique capability to the acquisitions process. This unique capability definition is vital because it serves as a basis for the requirements of all subordinate systems and for evaluating SoS test objectives [2].

The unique capability that COE offers is two-fold: 1) it allows the commander to access information across the Army tactical network on any device in a standard format, and 2) it offers a modular approach that is scalable and adaptable which allows developers to output capabilities at an efficient rate. This unique capability was developed by consolidating the different views of subject matter experts from across the Army’s acquisition community under the leadership of the Assistant Secretary of the Army for Acquisition, Logistics, and Technology or ASA(ALT). This unique capability has the potential to unite the subordinate systems to synchronize their efforts in support of the overall SoS unique capability [1].

Our work is focused on facilitating the transition to COE and explores the following question: “How do the unique capabilities inherent in the Common Operating Environment change the Army’s Network certification process to reduce total cost, increase interoperability between component systems, and increase the agility of the acquisitions process to respond to the Warfighter’s needs while complying with Federal statutes?”

To answer the question, this document is organized as follows, Section II discusses current issues with the Army’s network acquisition programs. Section III proposes an agile and SOS based approach to developing COE. Section IV analyzes the strengths and weaknesses of such an approach. Finally, Section V concludes the project’s analysis.
II. CURRENT CHALLENGES IN DEVELOPING SYSTEMS FOR THE ARMY TACTICAL NETWORK

Despite adopting several different paradigms over the past twenty years, ASA(ALT) has continually failed to develop the flexible, interoperable network that the American Soldier needs to fight in the modern world. The thinking chart in Figure 1 qualitatively compares the desired “value” of interoperability and timeliness of delivery in the ideal Army network to the value of products developed under ASA(ALT) network paradigms [3, 4]. Even with the new technologies found on the battlefield, the Army network continually falls short of its goal and only makes minor improvements over previous paradigms. Regardless of improvements made to the process, the Army network falls further and further away from the ideal as its value increases exponentially with Moore’s Law [4].

Interestingly, all of the paradigms adopted over the past 2 decades have all failed for the same reasons. Cost and schedule overruns, unmet requirements, and failed certifications all trace themselves back to a system that cannot incentivize the type of adaptive and cooperative acquisition that is required to produce the network the Army yearns for.

A. A Culture of Excessive Quality Engineering

Upon investigation, one of the most obvious causes of the system’s failure to produce timely, adaptive, and interoperable networks is the Army’s general culture of excessive quality engineering. In combat, small flaws in the hardware or software used by Soldiers can often mean the difference between life and death. With such a reality in mind, the Army’s policy is to ensure that “the commander doesn’t integrate the network” [5, 6]. Because of this policy, testing and certification for the Army’s Interoperability Certification (AIC) is incredibly exhaustive, working to test every possible connection and piece of equipment that may be found in any of the Army’s instantiations of the network at the brigade level. The process takes weeks to complete and often stops (at least once per week) due to an error in the proposed network. These errors take up to an additional week to diagnose in most cases and may set an entire crop of field-ready systems back due to one fault. Because of these delays, the Army is continually behind its fielding schedule by at least 1 or 2 years [6]. Currently, the Army is fielding the same set of capabilities designed for Fiscal years 2011 and 2012 (FY 11-12) in FY 15-16.

There is undoubtedly a question of necessity when it comes to the Army’s efforts to certify the network. While battlefield losses due to poor network integration are unacceptable, are not those caused even more by the failure to develop and field key systems? Operational Need Statements (ONSs) circumvent the normal acquisitions process described by DoD 5000.02 in order to procure specific capabilities without a lengthy development and evaluation process. The existence of ONSs in theater suggest that commanders in the field are willing to accept some risk of poor interoperability to secure a capability they feel they need in the moment but may throw away later [3]. During an interview with key members of Program Executive Office Command Control Communications-Tactical (PEO C3T), one of the major issues brought to our attention was the question of how much testing is good enough. With countless variations of the Army’s network (every brigade sets up the network differently), it is impossible to test for every case [5].

Fig. 1 Qualitative Comparison of Ideal Network Value compared to the Army’s Achieved Value from 1990 to Present.
Another major issue with the Army’s acquisition system is the way that capabilities and requirements are funded. Under the current system, the Army funds individual requirements and capabilities directly to project managers (PMs). These project managers then resource the money for specified requirements. The effect of this process creates a series of funding stovepipes which isolate the capabilities being funded from all other capabilities under development. The Army’s current budgeting process brings individual projects into competition with each other for the few dollars available to allocate for development or evaluation. Fierce competition over funding leads each project to develop itself in a way that pushes out other similar projects [4]. The desire to gain a few more dollars also distracts PMs in the short term and prevents them from looking forward to see the big picture of what they are building. Operationally, the lack of cooperation and foresight between PMs has been observed within SoSE&I—the original concept of COE was drafted in order to solve some of these issues [7].

This funding scheme fails to support the spiral development and evolutionary acquisition strategies that the Army desires to practice. Under these strategies, a more aggregated funding process is required to allow similar systems to pool work and negotiate collectively for funding. Collective bargaining is the key to getting the various corporations and developers under contract with the Army to work together with each other and make sure that Soldier gets systems that work together from the start [8, 9].

**C. An Opportunity to Develop Something New**

The Army’s current attempts at developing COE continues the errors present under previously adopted paradigms. To reduce redundancy, the Army is allocating individual capabilities to specific PMs and further enforcing the stovepipe that prevents these systems from working together as well as possible. The modern pursuit of COE will follow in the steps of the paradigms preceding it and only accomplish a minor improvement over them if at all.

Because our work is sponsored by SoSE&I and we do not work directly for them, we have the independence to step outside of the current system and attempt to look forward and develop a plan for an ideal network development tool. By this, we mean to operate on the assumption that our concept of COE occurs no earlier than 2025, when COE’s development and business practices have fully matured. This document describes our plan for this steady-state COE. The next sections will go into more detail.

**III. Future Development and Testing for COE**

The proposed solution for the steady-state development and interoperability testing of COE as a system of systems was developed by synthesizing strategic approaches to SoS test and evaluation and the principles of Agile Project Management (APM). This section will propose a solution to efficiently develop and conduct integration testing for COE in its long-term, steady-state form.

The focus of this solution is on efficiently upgrading the operating systems of each of the Computing Environments (CEs) that make up COE. This solution is broken into 3 tiers of development and interoperability testing to achieve the end goal of an upgraded and interoperable software version every 36 months. The top and overarching tier is the SoS level that is represented by COE as the owner of all subordinate systems. The middle tier is the subordinate system level that is represented by the CEs. The bottom tier is the individual capabilities or applications that are developed within the subordinate systems and are represented by common end-user capabilities such as Chat or Blue Force Tracker.

**A. Systems of Systems (COE) Tier**

The development and test strategy for the SoS tier operates on a 36 month software version update cycle to ensure the COE operating system is kept up to date with technological

![Fig 2. Development and Integration Test Strategy for COE at Steady State as Viewed from the SoS Tier Perspective](image-url)
advances. Using the “sprint” principles of APM, these 36 months are broken into thirty months of individual system development and 6 months of interoperability testing that will be labeled Army Interoperability Certification (AIC). This development and test strategy will be implemented using a staggered test cycle approach. This staggered approach can be visualized in Figure 2 below. In this approach, the COE interoperability standard is set by the other 5 CEs in the environment and the CE presently attending AIC will be responsible to make changes to their own CE to make their operating system interoperable with the rest of the environment. This reduces negative interactions between CEs which waste time that could be spent developing. To develop the COE version software upgrade vision, a COE working group will meet to define the capability functions that will be the focus of the SoS environment upgrade. This working group will assess the capability gaps to ensure each upgrade will meet to define their requirements to fulfill the functional capability requirements set by the COE working group. At the system level, the CE working group will meet to define the capability functions that will be developed for the next software update development bracket.

B. Systems (CE) Tier

The scope of the system tier of the development and test strategy focusses on the CEs and their implementation of SoS capability functions defined by the parameters set by the COE working group. At the system level, the CE working group will meet to define their requirements to fulfill the functional capability requirements set by the COE working group. The requirements definition will take place within the 30 months of development and integration testing of the previous software update. This way, once the integration testing is complete and approved, development can commence immediately following the event. This will maximize the material solution development for the short 30 month period allotted for each CE. The time and effort proportions are illustrated in Figure 3.

The first block will be dedicated to solution design based on the requirements developed by the CE working group. The successful completion of this solution design structure will set the conditions for a smooth and efficient material solution development. Following the solution design generation, the effort will shift to developing the material solution. These solutions should be developed using the “sprint” principles of APM using version build cycles. In the software development sector, APM techniques have been wildly successful because it delivers high value technical quality in a world with adapting reality [10]. Under these principles, the program managers should focus on developing and delivering successful capability updates (Build 1), inter-CE interoperability (Build 2), then intra-CE interoperability (Build 3). At the conclusion of each sprint, the developers will conduct a test to ensure the builds match what the intended stakeholder goals required. These sprint iterations will culminate in an integration and interoperability event (I2E) which will serve as a “pre-test” for AIC and to verify its success in fulfilling its requirements set out by the CE working group. Time must be allotted to refine some flaws revealed during I2E. After this final sprint to develop the solution, the CE must present its operating system software upgrade to AIC and verify its interoperability with the other CEs in COE. CE developers will make necessary changes to ensure interoperability across the environment. Only the CE presently attending AIC will make changes to their software to limit friction generated between different CE programs. After the CEs operating system has been approved by the G6 authority as interoperable, the CE will then proceed to develop the next COE software version upgrade.

C. Component (Applications) Tier

The final tier of the COE software update strategy is the individual capability that appear as applications built on top of a CE’s operating system. The focus of this SoS development and test strategy is not on capability development, but on the integration of the operating systems. Therefore, these capabilities will be developed on the CE level under the guidance of the functional capabilities defined by the COE working group. This means that the CE program manager will be given the authority to develop capabilities on his or her own speed as long as he or she can justify the capabilities’ interoperability with the CE operating system. One of the assumptions declared in this paper is that the CEs will have their own independent operating system that must be interoperable with all other CE operating systems. In theory, an application will be interoperable with the entire SoS if it is built within the protocols of a CE’s operating systems. This logic is founded by the Transitive law [11]. The component update must be tested and justified by the CE program manager in a memorandum document to the G6 who has the authority to declare COE interoperable.

IV. SOLUTION ANALYSIS

This section will explain the evaluated strengths, weaknesses, and opportunities with the proposed COE development and integration test strategy solution.

A. Strengths

The proposed staggered SoS development and integration test strategy brings many strengths to the ASA(ALT) organization. At its heart, COE is a software platform and many similar software platforms such as Microsoft Windows or Apple iOS use APM strategies to quickly develop
 interoperable capabilities to the user. This strategy brings those strengths to the Army Acquisition community by synthesizing APM and SoS test strategies. One strength that this solution offers is the ability to embrace change quickly and adaptively. As Karlesky and Voord note, “change is an inherent characteristic of any growing entity” [12]. COE is most definitely a growing entity with an increasing demand for new, integrated capabilities at all echelons of command. Through the “sprint of sprints” view of pushing all CEs through integration testing at 6 months each, each software update is able to publish a flexible response to the capability gaps that are identified. Another strength is that APM sets the conditions for the software developers to fold user feedback into development early and often [12]. Even from the sprint view on the CE perspective, ensuring test feedback on each capability, inter-CE interoperability, and intra-CE interoperability sprints will give the material developers a greater awareness of how much value the operating system upgrade is giving in relation to the initial requirements. Instead of one test point to evaluate the system’s value, 4 small tests are conducted to ensure the solution is adding the most value possible and does not waste time following an ineffective tangent.

The development and test staggered schedule is beneficial in that it limits the interactions between CE program managers which reduces organizational friction. By isolating one CE and directing it to integrate with the rest of the existing COE network, the COE governance does not have to manage individual CE’s responsibilities for changing their operating system to make the network interoperable. Another benefit of this staggered strategy is the independent interoperability test certifiers have continuous experience testing these CE operating systems instead of only conducting testing every 3 years. This gives the test certifiers experience and recent knowledge of how to most efficiently conduct these interoperability tests and how best to troubleshoot issues.

B. Weaknesses

As no architecture is without its weaknesses, this subsection will discuss several risks associated with this proposal, then offer ways to mitigate those risks. The major risks identified are scheduling and budgeting.

The first major scheduling risk that this proposal could encounter is the unreliability of predicting the tactical network’s operating environment 36 months in advance of the first AIC. Improperly defining the capability goals at an early stage risks those capabilities not being prepared to operate in the future environment. Time and resources can be hard to estimate and with such a large organization, the magnitude of uncertainty is great [13]. In the current scheme of network development, our research has shown that a capability takes about 7 years between the capability requirement definition and when it gets fielded to the Soldier [14]. While the COE working group session would still have to assume the risk associated with predicting the operating environment 36 months in advance, the assumed risk is significantly less than the risk of predicting the operating environment 7 years in the future. To assist in more accurately defining the operating environment, the COE working group should contract analysts to use predictive analytic techniques based on past performance and behavioral model theories. Though not a perfect solution, these techniques can aide the COE working group in a more accurate picture.

Another scheduling risk that this proposal could encounter is the inability of some CEs to complete their AIC within the allotted 6 month window. Due to the rolling nature of the proposal, a delay in any one AIC for a CE will delay the entire project by that amount of time. This impact can be reduced by the COE governance requiring that all applicable contracts for vendors include incentives for achieving the AIC deadline. To further incentivize a timely AIC completion date, the COE governance can also offer monetary bonuses to CEs that complete their AIC earlier than scheduled. This can be offered on a scaled basis so that the earlier a CE’s operating system is certified, the more incentive for the vendor. An internal forcing function of the cost plus contracting is the singularity of a CE attending the AIC. In cost plus contracting, vendors have the flexibility to blame another organization for not completing the contract in time, but with the AIC spotlight on one CE at a time, vendors cannot deflect the blame on another organization. These forcing functions will mitigate much of the risk assumed by ASA(ALT) through this proposed development and integration test strategy.

The main budgeting risk of our approach is connected to the resources necessary to sustain AIC continuously. Under the current proposed plan, COE will attend AIC once every 3 years and all CEs will be tested for interoperability at once [15]. This means that ASA(ALT) will only have to fund a 6 month AIC every 3 years. The issue with hosting an AIC at this tempo is that delay or failure to fully certify the operating system requires paying overtime expenditures and/or the signing of a new contract. The outcome of this strategy could risk uncertainty in the budget and borrowing against resources allocated for competing requirements. With the continual, rolling strategy of AIC, ASA(ALT) will have more certainty in budget allocation because the interoperability certification agency can be contracted to work for a more concrete period of time. The extra cost of overtime and reorganizing the budget could make the current AIC strategy just as expensive as the architecture this paper proposes. Even so, SoSE&I has proposed a plan to conduct the test in a distributive manner, under the Federation of Net-Centric Sites (FaNS) with the intent to reduce the cost of conducting an AIC [15]. In this construct, interoperability testing will be conducted at-home which will mitigate the costs and logistics associated with shipping resources to an off-site location to conduct AIC. In summary, the costs of conducting AIC in a rolling fashion is largely offset by the benefit the strategy brings of producing a consistently interoperable tactical network for the warfighter. The FaNS concept also reduces much of the cost associated with AIC which reduces the concern budgeting may bring.

C. Opportunities

Approaching SoS development and testing in the proposed strategy offers myriad of additional political and organizational opportunities for ASA(ALT). COE is an environment that is made up of disparate subordinate systems that each have their
own biases and agendas. With our approach, the COE governance has the opportunity to encourage the CEs to become a part of SoSE&I’s initiative by setting the most convenient conditions for the CEs to work under this strategy. COE needs the support of all CEs to be a fully interoperable tactical network. To make this initiative the most convenient option for the CEs, SoSE&I can explore options such as offering a remote software upload system at the CE’s headquarters so that the CE developers can test for up-to-date interoperability with other CEs. SoSE&I can also provide staff members to the CE working groups to ensure the working group is nesting its requirements with the identified capability goals. Above all, the COE governance will be of greatest value by offering resources to the CEs to help contractually incentivize their vendors to succeed in this interoperability initiative.

V. Conclusion

This document has proposed an agile and reliable methodology to answer the question of how to certify the interoperability requirements in an efficient and adaptable manner. To achieve this outcome, this document highlighted the major issues discovered in this team’s analysis of the current system then proposed and explained a flexible architecture of CEs attending AIC one at a time in 6 month iterations. The proposal featured many characteristics of APM to maximize COE’s potential to produce a consistently interoperable tactical network. The focus of this strategy is to make the network interoperable foremost, since that is the focus of COE’s unique capability. COE’s authority is mainly decentralized to allow CEs to develop new capabilities on a lower level, thus enabling CEs to take ownership of developing new capabilities. This document then concluded with analysis of the solution and highlighting strengths, weaknesses, and opportunities the proposed solution presents.

The Army’s tactical network is one of the nation’s greatest assets for applying national power across the world. Regardless of the environment, our network allows the Army to operate as the world’s most technologically advanced force. Despite this, however, new thinking is required to develop the network further to enhance its utility on tomorrow’s battlefields. The Army’s COE needs to be approached as a system of systems with the development process tailored to make the most efficient use of the SoS’s unique capabilities. According to our analysis and assumptions of this model, an agile based process centered on a staggered iterative architecture is the most effective way to develop new capabilities that are able to interoperate on a standard network. By ensuring a more timely return on network builds, the Army can stay adaptive to the future needs of the Warfighter and maintain battlefield information dominance into the future.

VI. References