"Homeland Security" at Home

R. O. "Bob" Stroud, *Raytheon Company, Dallas, Texas, USA*

Homeland Security began at the national level in the United States after the terrorist attacks on 11 September 2001. The concept can be extended to the very basic level of protecting literal homesteads. This paper explores the application of Systems of System concepts developed by the United States' Department of Defense (DoD) to the problem of homestead defense at the homestead level. It outlines the problem, the applications of the DoD concept, the selected solution, and the results and recommendations.

Keywords: Homeland security, system engineering, surveillance.

1 Introduction

In 2008, the Systems and Software Engineering (SSE) Directorate of the Office of the Deputy Under Secretary of Defense for Acquisition and Technology (ODUSD(A&T)) in the United States (U. S. or just US) Department of Defense (DoD) published a guide for systems engineering (SE) of systems of systems (SoS), recognizing that systems engineering is a key enabler of successful systems acquisition, operation, and sustainment in an environment where there are growing numbers of dependent and interdependent systems used to provide war fighter capability. The result was version 1 of the Systems Engineering Guide for Systems of Systems [1] ("Guide").

While the intent of the Guide is to support DoD programs and warfighters, SoS are increasingly a part of contemporary enterprise architecture and engineering. For example, Honour, in his 2008 short course "Systems of Systems" [2] identifies airports as systems of systems. In their 2011 paper on complexity [3], Geraldi, Maylor, and Williams list the enterprises (not necessarily defense related) where systems are comprised of systems, yielding complexity. In their 2009 paper on health care, Hata, Kobashi, and Nakajima [4] show how health care delivery is via a system of systems. In their 2004 paper on public policy decisions, DeLaurentis and Callaway use an example of the next generation national transportation system as a context for their systems of systems discussion [5]. These are collected in Table 1. There are *many* others. In particular, Luzeaux and Ruault [6] in their book Systems of Systems include "zone control and surveillance" as another example of a system of systems. That particular type of system of systems is the subject of this research and report.

2 Zone Control and Surveillance – The Ultimate Homeland Security

Luzeaux and Ruault [6] describe zone control and surveillance in a strictly military context. But since September 2001, especially in the US, this concept has extended to include homeland and perimeter security. In the ultimate sense, perimeter security includes security of the home i.e., domicile, and surroundings.

In particular, the end user has a concern with neighbor unfriendly dog breaking through a chain

Table1: Enterprises Where Systems are Comprised of Systems.

Enterprises Where Systems are Comprised Of Systems	Reference
Airport	[2]
Construction	[3]
Enterprise Resource Planning (ERP) Implementation	[3]
Health Care	[4]
Information Systems	[3]
Plant Engineering	[3]
Product Development	[3]
Transportation System	[5]
Zone Control and Surveillance	[6]

link fence protecting an underlying wooden privacy fence, potentially belligerent vandals, and maintaining a secure environment for yard care and the end users pets. The end user expressed a need for high-resolution video surveillance that would provide objective evidence if legal action was necessary. An incumbent contractor provides monitored security for magnetic door and window alarms on the perimeter of the home. The first approach was to engage the incumbent contractor to orchestrate an upgrade to the existing SoS. That approach proved unworkable, so the end user engaged a second contractor to satisfy the material requirements and a third contractor to install the material solution as detailed below.

3 Application to Problem Under Consideration

Table 2 shows how the principles listed in the Guide [1] apply to this problem of zone control and surveillance. These are discussed in the sections below, considering a row of the table at a time.

Section 4.1.1 of [1], Translating Capability Objectives, is intimately related to Requirements Development. In this example, the objective of monitoring the premises is translated into specific requirements for cameras, field of view/regard, and light sensitivity. Likewise, this requirement needs to be considered in the context of requirements, risk, configuration, data, and interface management in the zone control and surveillance. Interface management has been added to the baseline from the Guide [1] and is shown in italics. Interface management is considered in the context of translating capability objectives because

of the variety of physical and electrical interfaces to be considered (e.g., coax vs Ethernet).

In 4.1.2 of [1], Understanding Systems and Concepts, logical analysis is a method of associating concepts with systems that satisfy those concepts. In this example, the concept of providing home surveillance is realized by surveillance systems, such as cameras and movement detection algorithms that might activate alarms. As noted above, Translating Capability Objectives is concerned with requirements management, so that need would be redundant in Understanding Systems and Concepts. But because surveillance systems that realize concepts span related but different areas in the solution space, Understanding Systems and Concepts also needs to consider risk, configuration, data, and interface management.

Considering 4.1.3 of [1], Assessing Performance to Capability Objectives, the military learned long ago that satisfying the wrong set of requirements perfectly yields a perfectly wrong solution [[7],[8] and many other examples]. Among the many responses to this engineering process flaw is Performance Based Specifications that attempt to focus more on outcome than on details. For example, The Guide for Performance Specifications, SD-15, dated 24 August 2009 [9], states:

> "It is the policy of the Department of Defense (DoD), as required in DoD Directive 5000.01, The Defense Acquisition System, to state requirements in performance terms whenever possible. Part II of the Federal Acquisition Regulation also requires federal agencies to give preference to performance-oriented documents over detailed design

Table 2: Relationships between SoS Core Elements and SE Processes (after [1], Table 3.2).

4.1 Core Elements of SoS SE \ 4.2 SE Process Support for System of Systems Engineering	Technical Processes								Technical Management Processes							
	Requirements Development 4.2.1	Logical Analysis 4.2.2	Design Solution 4.2.3	Implement 4.2.4	Integrate 4.2.5	Verify 4.2.6	Validate 4.2.7	Transition 4.2.8	Decision Analysis 4.2.9	Tech Planning 4.2.10	Tech Assessment 4.2.11	Requirements Management 4.2.12	Risk Management 4.2.13	Configuration Management 4.2.14	Data Management 4.2.15	Interface Management 4.2.16
4.1.1 Translating Capability Objectives	X											X	X	X	X	X
4.1.2 Understanding Systems & Relationships		X											X	X	X	X
4.1.3 Assessing Performance to Capability Objectives							X		X	X	X		X		X	
4.1.4 Developing and Evolving a SoS Architecture	X	X	X						X	X		X	X	X	X	X
4.1.5 Monitoring and Assessing Changes									X				X	X	X	X
4.1.6 Addressing Requirements and Solution Options	X		X						X	X		X	X	X	X	X
4.1.7 Orchestrating Upgrades				X	X	X	X	X	X	X	X	X	X		X	X

documents when describing agency needs. To implement DoD and federal preferential policies on stating requirements in performance terms, DoD 4120.24-M, Defense

Standardization Program (DSP) Policies and Procedures, gives preference to developing and using performance specifications over detail specifications."

An unexpected consequence unfortunately is that the outcomes do not favor adoption of the approach. In Edouard Kujawski's insightful Unintended Consequences of Performance Specifications for the Reliability of Military Weapon Systems [10], he notes

"Reliability data from 1996 to 2000 might be an indicator of negative unintended consequences of the cancellation of military specifications. The acquisition of successful military systems requires a mix of performance and prescriptive reliability requirements that depend on the application, technology maturity, and complexity."

So the first relationship of Assessing Performance to Capability Objectives is that of validation – making sure the requirement actually satisfies an end user need. Likewise, there is a relationship with Decision Analysis because there is a need for traceability – why was the decision made to map a particular performance objective to a particular capability objective[1]. Requirements traceability is a critical aspect in maintenance, for example [[8], [11], and many others]. Next, Tech Planning and Tech Assessment are important to Assessing Performance to Capability Objectives. Tech Assessment has been added to the baseline from the Guide [1] and is shown in *italics*. The author contends it is difficult to address Tech Planning without Tech Assessment. For example, if Tech Planning is proposing to achieve a lower noise figure by a change to Boltzman's constant, perhaps Tech Assessment is needed to assess requirements development by Tech Planning[2]. Tech Planning and Tech Assessment naturally relate to Risk Management: a planned and even assessed technology might still not be ready for use. The Army's Future Combat Systems (FCS) program, for example, spent billions of dollars before it was cancelled because the technology planned for and assessed was still immature [12].

For 4.1.4 of [1], Developing and Evolving a SoS Architecture, this project, though new, relies on current COTS technologies: cameras, network video recorders, change detection algorithms, and others. But this does not mean that evolution should not be considered in design. For example, a large tree on the property and other obscurants indicate the potential need for additional cameras. The video processing system selected comes with eight cameras, was procured with twelve, and is capable of integrating four more cameras (+33% margin for a total of sixteen) to accommodate this possibility. The Guide [1] states

"Ideally the architecture of an SoS will persist over multiple increments of SoS development, allowing for change in some areas while providing stability in others. This ability to persist and provide a useful framework in light of changes is a core characteristic of a good architecture. Over time, the SoS will face changes from a number of sources (e.g., capability objectives, actual user experience, changing CONOPS and technology, and unanticipated changes in systems) [that] may all affect the viability of the architecture and may call for changes. Consequently the SoS systems engineer needs to regularly assess the architecture to ensure that it supports the SoS evolution."

The system selection process for this SoS considered these concepts. As noted above, the potential evolution to sixteen cameras was considered in the evaluation of potential solution systems. Contemporary as well as evolving video protocols were considered. Environmental changes such as growth of trees was considered. Software upgrade and patch application methodology was considered in this context. And in exact alignment to the guide, these changes are considered to be over multiple increments when the end user can afford to or must update and upgrade when needed.

Requirements development, logical analysis, and design solution are all relevant to Developing and Evolving a SoS Solution. Requirements satisfaction is relevant to solution selection.

Solutions and requirements are analyzed with logic, and the design solution is selected based on a logical process. Decision Analysis is relevant because choices are made as a SoS Solution is developed and evolved. Tech Planning is related because, as noted below, technology evolves and solutions will migrate

---

[1]Perhaps Decision Analysis should, in general, be more broadly associated and applied

[2]Author's note: Boltzman's constant is indeed a constant

to evolved technology. Requirements Management, Risk Management, Configuration Management, Data Management, and Interface Management are all relevant to developing, evolving, and sustaining a SoS Solution.

For 4.1.5 of [1], Monitoring and Assessing Changes, technology (including software) is not static. But with each push forward, change introduces risk. For example, upgrading the video monitoring software may make it incompatible with connected monitoring equipment in general and computers in particular. Maintaining awareness of the suppliers plans is helpful, but often suppliers plans are not adequately revealed until the moment of upgrade (or after). Microsoft, for example, announced a schedule for upgrades but not does not reveal content or compatibility concerns. In this context, consumer awareness of supplier compatibilities both present and future are a concern. The end user in this case uses Apple products, from iMac, to Macbook Pro, to iPad, to iPhone. If the current equipment provider elected in the future to be only Microsoft compatible, this would introduce a continuity of service issue. The guide [1] states

> "A core activity of SoS SE is to anticipate changes outside the control of the SoS that could affect the functionality or performance of an SoS capability. This includes changes to the technologies used to support the SoS or changes to the missions of the individual systems as well as external demands on the SoS. To be successful, the SoS systems engineer requires a broad awareness and understanding of trends in enabling technologies, technology insertion, and mission evolution."

In this problem, supplier changes are outside the control of the SoS end user, and this puts the end users investment at risk. A reasonable assessment of this risk determined that the concern is "small" but the risk is real and is not zero. The end user or their representative are delegated this concern.

Decision Analysis applies Monitoring and Assessing Changes because decisions need to be made about changes. Risk Management, Configuration Management, Data Management, and Interface Management are all relevant to monitoring and assessing changes.

For 4.1.6 of [1], Addressing Requirements and Solution Options, eliciting end user needs and deriving associated requirements is essential if the procured and integrated SoS is to satisfy the end user's expectations. In this problem, the end user's expectation of fidelity even at the extremes of the field of view dictated a requirement for a high definition camera. The limited time the end user could devote to examining the recorded video surveillance dictated both media large enough to store a significant amount of collected video and software assisted change detection and screening so that motion caused by wind blowing the pecan tree is not flagged as suspicious but motion caused by a neighbor dropping a limb into the region under surveillance is flagged as suspicious. The target area required analysis as detailed in Results below to determine the number and pointing directions of surveillance cameras.

Requirements Analysis is naturally related to Addressing Requirements and Solution Options. Likewise, the Design Solution is naturally related to Addressing Requirements and Solution Options. Decision Analysis and Tech Planning are related because of the need to have solutions that meet customer expectations. Requirements Management, Risk Management, Configuration Management, Data Management, and Interface Management are all relevant to Addressing Requirements and Solution because satisfaction is not without risk. Configuration Management is part of Solution Options as these are satisfied and evolve. Likewise, Data Management and Interface Management are part of Solution Options as the selected solution must interface with existing user premises equipment.

In 4.1.7 of [1], Orchestrating Upgrades, upgrades are a fact of life in systems of systems. In this case, orchestration must consider a number of providers who (a) assure that upgrades across the system of systems do not degrade performance but (b) who do not necessarily coordinate their upgrades. This means the end user of the SoS, or a hired proxy, must assure that upgraded elements and systems in the system of systems will continue to work as expected after upgrades and recapitalization. In this case, for example, the vendor of the recorder console (Swann) states "The NVR is guaranteed to work with Swann branded network cameras only". This means there is a risk of using other vendor cameras even though Swann states of their cameras that "These NVR IP cameras will only work with NVR (Network Video Recorder) DVR systems that are ONVIF compliant. If using a different brand

ONVIF[3] compliant camera with a different brand ONVIF compliant recorder they may not be 'Plug-n-Play' and some configuration may be needed at setup."

For the all Swann recorder and camera system of systems discussed here, the upgrade risk is minimal until that point where Swann equipment is no longer backward compatible, at which point a recapitalization decision by the end user will be required.

Thus, Implement is relevant as are Integrate, Verify, and Validate. This project is not really a transition of equipment but is a transition of the SoS end user who has no legacy equipment for this function. Thus, Decision Analysis and Tech Planning are relevant as the SoS evolves into the future to assure continued satisfaction of user needs. Tech Planning is not on the original Guide and so has been added in italics. Tech Assessment, Requirements Management, Risk Management, and Configuration, Data, and Interface Management are needed to assure the smooth transition across evolved SoS as a consequence of Orchestrating Upgrades.

4 Requirements

Figure 1 graphically shows the zone requiring surveillance for the problem. Figure 2 shows the plot of the zone to be protected. Figure 2 was required to consider sensor capability and placement and was developed by outlining the home and property boundaries on a scan of the survey acquired for the property at the time of purchase. Discussions with the end user determined that high definition persistent video surveillance over 100% of the threatened property to be the top-level system of systems (enterprise) requirement. Analysis was required to determine the characteristics (distance and pointing capability) of some of the sensors. Most fields of regard (FOR) were determined by inspection, but one required analysis as incorporated into Figure 4. Figure 3 shows the rendering of the plot shown in Figure 2 into a graphic. Measurements using conventional tools (e.g., tape measure) are included in Figure 3 and used in the analysis in Figure 4. Fields of regard (FOR) were developed based on logical camera locations as shown in Figure 4. FOR were determined by inspection except in one case that was

---

[3]Open Network Video Interface Forum (ONVIF), see http://www.onvif.org

determined by trigonometric analysis incorporated into Figure 4.

The requirements derived for this system of systems are shown in Table 3. Since at least one vendor claimed satisfaction of the requirements, achieving compliance is not an issue.

5 Results

The requirements in Table 3 are satisfied in the Operational Viewpoint shown in Figure 5. Figure 5 shows camera emplacements along the eaves of the protected home. In operation, wired Ethernet transfers the collected video surveillance to a central Network Video Recorder (NVR) in the protected home. Software in the NVR processes the collected video to isolate changes, and these are stored in the NVR for end user evaluation.

There are several video surveillance systems of systems that could conceivably satisfy the requirements enumerated in Table 3 above. Trade studies are not the subject of this report (trades are frequently cited in [1]), but major factors involved in the selection of the vendor are, in addition to the cost of the system, the availability of qualified installers, ease of use, compatibility with user premises equipment, and vendor stability.

Camera selection was driven by the requirement for high definition and the need for numerous coverage areas, which in turn drove cost. There was a requirement for ordinary and low visible light sensitivity. The HD aspect of the cameras made wireless connections implausible due to the bandwidth requirements of each camera and the required number of independent channels, combined with a lack of encryption from the point of origin for privacy. Wired options offered were a single Ethernet cable that carries digital video and status from each camera in one direction and power (Power over Ethernet), command, and control in the other direction or multiple wires from each camera carrying video and status in one direction and other wires carrying power, command, and control in the other direction. The single wire option was assessed as less risky due to less potentially faulty connections. The end user decided that one wire for data, power, status, and control is preferred over more than one from an installation, reliability, and maintenance perspective. Ultimately, Swann cameras were selected. Swann says their cameras will work with any NVR as long as it is ONVIF

Figure 1: Back view of house requiring Zone Control and Surveillance. Threatened dog shown. Threats absent.
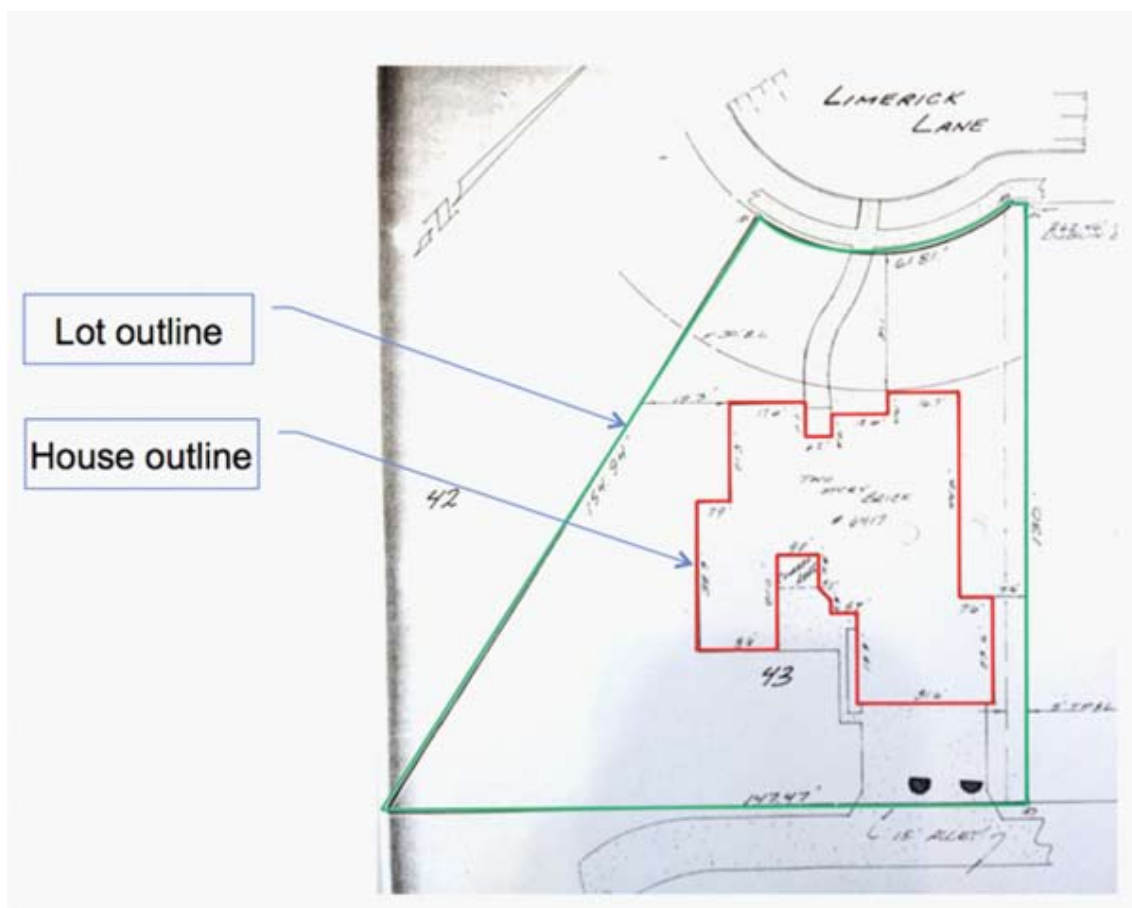

Figure 2: Top view of zone to be protected includes front and back of the home.

compliant (see above), but, curiously, they guarantee success only with their cameras paired with their NVRs. Faced with limited time to consider alterna- tives, the end user decided on a Swann NVR. The purchased NVR and cameras it is packaged with are shown in Figure 6. The NVR comes with a
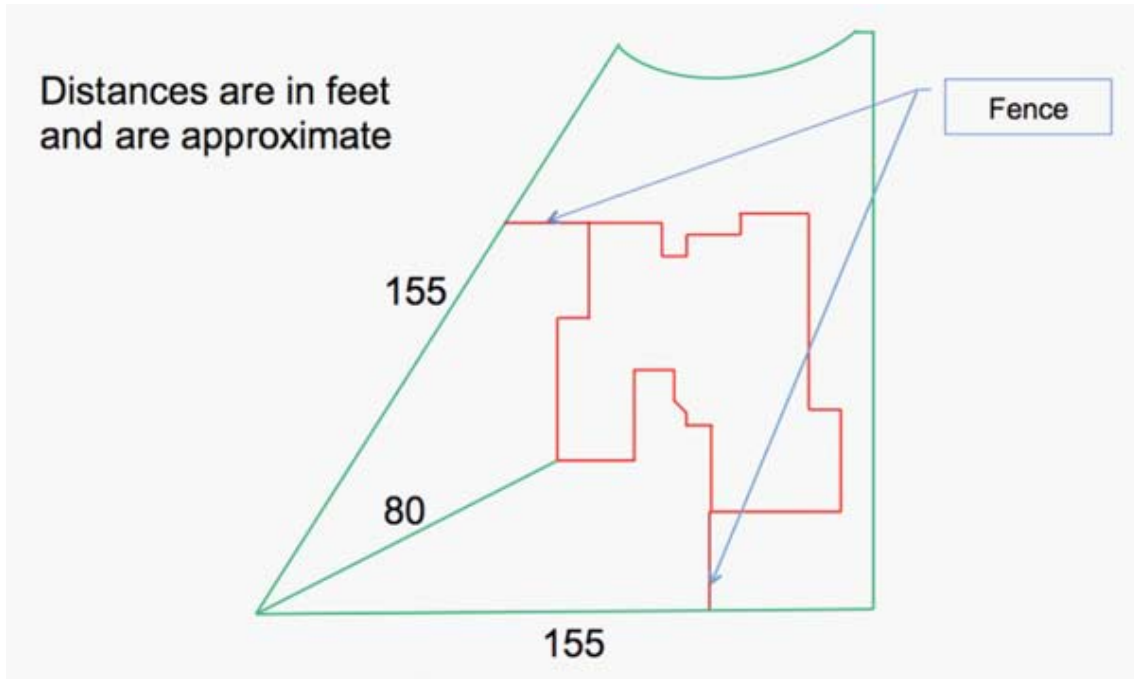
Figure 3: Measurements show the maximum required viewing distance from the camera mount point to be about 80 feet (Measurements, except for the trigonometric analysis, are from the survey).
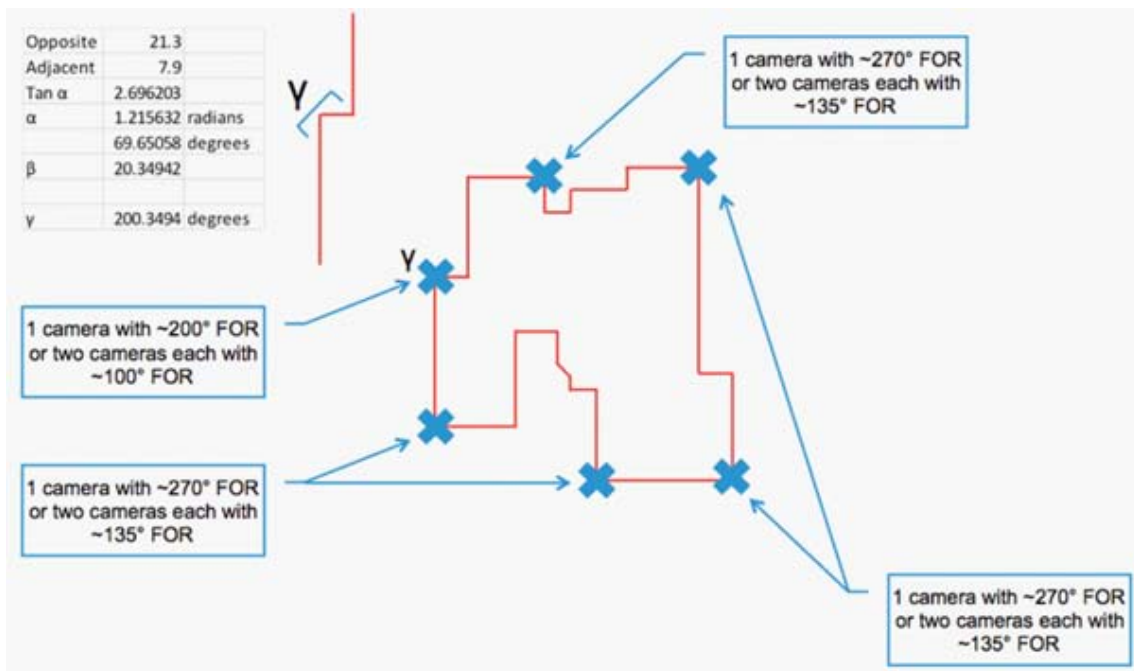
Figure 4: The Field of Regard (FOR) for most sensors was determined by inspection, but one required trigonometric analysis.

wired mouse but no monitor. A monitor is needed to set up the system and to view the recorded video. The NVR has a High-Definition Multimedia Interface (HDMI) output, and the cameras are HD, so a HDMI compatible monitor was selected and added to the ensemble.

The NVR was purchased as a package that included eight fixed mount cameras with no pan or

Table 3: Requirements for the System of Systems solution to the design problem.

Requirement	As Bought
12 cameras, each with Not Less Than (NLT) 135° Field of Regard (FOR, see Figure 4) • Each camera must be able to pan, tilt, and zoom independently • Two cameras autofocus • Frame rate adjust in proportion to activity	12 cameras, each with ±75° FOR, each on a fixed mount • 10 cameras with fixed focus • 2 cameras with variable focus Assessed compliant
Minimum imaging distance 80 feet (see Figure 3)	115 feet imaging distance
HD visible and low light video • Visible in daylight, low light capable in "dark"	1 lux@F1.2, 0 lux with Infrared (IR)
Wired power (or Power over Ethernet, PoE)	PoE
Recorder and monitor/computer interface inside	Compliant
Up to 16 cameras for growth	Compliant
Eight x 24 hour days recording • Lossless compression	"up to 45 days of continuous recording from all 16 channels or record for even longer with motion triggered recording" Assessed as compliant
Processing • Preserves date and time • Selected snapshots conversion to jpeg • Selected clips conversion to mpeg 4 (H.264 Part 10 aka QuickTime)	Compliant Compliant Compliant
Playback at up to 16x real time	Assessed compliant: can jump ahead

"lux" is the metric unit of illumination; lower units represent lower illumination levels and hence better performance in darker environments

"F" numbers are is the ratio of the lens's focal length to the diameter of the entrance pupil; lower numbers generally represent a greater diameter lens (hence improved capability in lower light situations)

Figure 5: Operational Viewpoint (OV-1) for Zone Control and Surveillance. Threatened dog in back yard shown. Threat dog shown, approximately to scale.

tilt. Six of the cameras are fixed field focus and two are variable focus as shown in Figure 7. Geometric analysis showed that four more individual cameras are needed to provide continuous surveillance across the operational area. The variable focus was assessed as not pertinent to the SoS requirements, so four more fixed focus cameras (at slightly lower cost) were selected.

Figure 6: Recorder console requires only installation and connection of cameras and a HD monitor to become operational.

Figure 7: The selected HD cameras use "Power Over Ethernet" so that only one wire is needed to connect the camera to the recorder console.

6 Successes and Challenges

The requirements were successfully satisfied. The end user coordinated the set of requirements in Table 3 with a contractor that provided the material components of the SoS. The vendor recommended another contractor who installed the SoS and trained the end user in its operation.

But this effort was not without challenges. First, the incumbent perimeter monitoring contractor was found to be unequipped or unwilling to satisfy the new requirements. As a consequence, a new contractor was selected and performed the effort.

Cost and time were a second challenge. Satisfying the specified requirements proved to be costly and demanding of the end user's time.

Finally, there were operational challenges that required tuning the installed system for best results. For example, motion sensitive cameras proved to be too sensitive to motion of deciduous tree branches in seasons where the branches had leaves. The contract equipment provided a software capability to selectively edit the area in the field of view where the motion detection capability applied, but this required significant time to set properly. Convenient connection of the end user's computers to the new premises equipment was challenging, requiring installation of new Power over Ethernet (PoE) wiring in the end user's site, use of the end user's wireless access point, and complicated configuration of the end user's wireless devices.

7 Details of Lessons Learned

Ultimately, the end user was satisfied. An important lesson learned is that it is much easier and cheaper to install power, data, and control cabling at the time of construction, even if no monitoring equipment is installed at that time. If a potential end user ever builds a house, this is should be a consideration.

Another lesson learned is the numbers, types, and diversity of systems of systems that claim to satisfy the SoS requirements are so numerous that objective analysis of the possibilities proved to take too much time. The selected vendor was in Australia and simple responses to questions took at least a day. The final selection was based on objective and subjective measures that would never be acceptable in a government or business setting (for example, the selection of contractors for the US government's NETCENTS 2 IDIQ contract took at least three years [13]). The

lesson learned is that "good enough" sometimes is preferred to "flawless" when considering all selection factors.

8 Conclusions

When persistent High Definition video premises monitoring is required, numerous qualified companies and equipment are available to satisfy the requirements. Some vendor offerings are superior to others. Vendor selection, while complicated, does not have to be perfect to be effective. A successful realization, even with challenges, is within reach of the end user by applying the disciplined System of Systems principles developed by the United States Department of Defense. Multiple providers, when reasonably coordinated, can perform an installation of a relatively complicated system of systems. This system is non-commercial in that every constituent system is not provided by the same vendor, with the resulting system of systems requiring integration by the installer and the end user. Collaboration between the provider and the user resulted in a more satisfying outcome, somewhat supporting the claim that performance specifications are superior to prescriptive specifications.

Other conclusions are more nuanced. For example, since the initial installation, one camera of the original twelve has failed. The failure appeared to be connection related, so the end user contacted the installer, who confirmed that the originally installed PoE cables are still connected, leading to the conclusion that the failure lies in purchased products from the equipment vendor. The installer confirmed this and the equipment vendor was contacted, but with thus far unsatisfactory results. The ultimate results are as of now unknown.

Also, the installers were not well trained in setting up the wireless monitoring feature of the vendor product. They were trained on the prior generation product, but that training had limited applicability to this installation. Better training is indicated, complicated by the profusion of available user wireless devices.

A premises video monitoring system is easily available subject to the cautions advanced in this paper.

References

[1] K. J. Baldwin, 2008. Systems Engineering Guide for Systems of Systems. Office of the Deputy Under Secretary of Defense for Acquisition and Technology, Systems and Software Engineering.

[2] E. Honour, 2008. Systems of Systems. Applied Technology Institute.

[3] J. Geraldi, H. Maylor, and T. Williams, 2011. Now, let's make it really complex (complicated). International Journal of Operations and Production Management, 31(9), pp. 966-990.

[4] Y. Hata, S. Kobashi, and H. Nakajima, 2009. Human Health Care System of Systems. IEEE Systems Journal, 3(2), pp. 231-238.

[5] D. DeLaurentis, and R. K. Callaway, 2004. A Syetems-of-Systems Perspective for Public Policy Decisions. Review of Policy Research, 21(6), pp. 829-837.

[6] D. Luzeaux, and J.-R. Ruault, 2008. Systems of Systems, Hoboken. N. J. : John Wiley & Sons.

[7] A. T. Bahill, and S. J. Henderson, 2005. Requirements Development, Verification, and Validation Exhibited in Famous Failures. Systems Engineering, 8(1), pp. 1-14.

[8] J. Xiong, 2011. New Software Engineering Paradigm Based on Complexity Science, New York: Springer.

[9] G. Saunders, 2009. The Guide for Performance Specifications. Department of Defense.

[10] E. Kujawski, 2010. Unintended Consequences of Performance Specifications for the Reliability of Military Weapon Systems. Systems Engineering, 13(4), pp. 405-412.

[11] P. Jayaraman, K. Kannabiran, and S. A. V. Kumar, 2013. A Six Sigma Approach for Software Process Improvements and its Implementation. International Journal of Mining, Metallurgy & Mechanical Engineering, 1(3), pp. 228-232.

[12] P. L. Francis, 2008. 2009 Review of Future Combat System Is Critical to Program's Direction. GAO, ed., p. 4.

[13] DoD. "D – NETCENTS-2 NETOPS AND INFRASTRUCTURE SOLUTIONS," https://http://www.fbo.gov/index?s=opportunity &mode=form&id=5d9d2e50faadc8ae5643d986997a bd19&tab=core&_cview=1.

Mr. Stroud has a BSEE from Texas A&M and MSEE from SMU. He is a Senior Engineering Fellow at Raytheon and has been with the company more than 35 years. He is completing a PhD from Texas Techs Mechanical Engineering Department in the Transdisciplinary Engineering track with a dissertation topic of Complexity Frameworks in Enterprise Design. He is a DoD Architecture Framework (DoDAF) Certified Enterprise Architect.