The ORDERED Process for Improving Agile Engineering Outcomes

Brian P. Gallagher, Senior Vice President, Operational Excellence, CACI International, Inc.

Dr. Kenneth Nidiffer, Director of Strategic Plans for Government Programs, Carnegie Mellon University, Software Engineering Institute

Dr. Ronald M Sega, Director, Systems Engineering Programs, Colorado State University

Abstract. This research explores the use of operational risk identification and mitigation techniques during the engineering process to determine whether this increased focus would have a positive effect on project outcomes. An approach using operational risk considerations to enhance the discovery of end user needs during an Agile engineering process is presented, and the results of a survey are provided.

Introduction

One missing aspect of most engineering processes as implemented on a project is an explicit focus on operational risk — that is, the evolving risk to the needs of the end user. This lack of focus on operational risk allows the creation of a chasm between evolving needs and delivered capabilities. The longer the time between identifying needs and delivering capabilities, the wider that gap becomes. This makes the end user less likely to deem the capabilities operationally effective.

Agile engineering approaches have emerged to help decrease the time between the identified need and the delivered capability by engaging end users actively in various planning and demonstration activities[1]. This active engagement of end-users establishes the groundwork for implicitly mitigating operational risk, however Agile methodologies still fail to explicitly use operational risk as a mechanism to ensure the evolving capability reduces the end user's evolving operational risk. Wrubel and Gross describe this disconnect, stating, "… [R]equirements for any given system are highly likely to evolve between the development of a system concept and the time at which the system is operationally deployed as new threats, vulnerabilities, technologies, and conditions emerge, and users adapt their understanding of their needs as system development progresses." [2]

Operational Risk	*The possibility of suffering mission or business loss.*
Operational Risk Management	*An operational practice with processes, methods, and tools for managing risks to successful mission and business outcomes.* *It provides a disciplined environment for proactive decision making to:* *- continually assess what could go wrong (operational risks)* *- determine which operational risks are most important to deal with, and* *- implement strategies to address operational risk*

Table 1. Operational Risk Definitions

In his 2015 report to Congress on the state of defense acquisition, the Honorable Frank Kendall, under secretary of defense for acquisition, technology and logistics, observed that the Department of Defense was optimizing cost and schedule performance over technical advancement, stating, "… [T]here is evidence that we have been pursuing less complex systems with about the same or less risk since 2009. This aligns with my concern that in some areas we may not be pushing the state-of-the-art enough in terms of technical performance. This endangers our military technical superiority. In my view, our new product pipeline is not as robust as it should be at a time when our technological superiority is being seriously challenged by potential adversaries. Not all cost growth is bad; we need to respond to changing and emerging threats." [3] These emerging threats, vulnerabilities and technology changes increase operational risk.

Operational Risk Management

Operational risk management is widely practiced in the banking industry and in military operations. In the banking industry, operational risk focuses on mitigating catastrophic financial loss and controlling the propagation of that loss to other banks and across international boundaries. In the military, operational risk has an emphasis on safety hazards and their impact on mission outcomes. Both of these applications of operational risk management form a foundation for a more robust treatment of operational risk.

Operational risk within the banking industry is focused on reducing the probability of loss due to events such as fraud, mismanagement, system failures, failed investments or legal considerations. Banks estimate their risk exposure, establish mitigation activities and set aside financial reserves to cover loss. In 1974, the Bank for International Settlements (BIS) established the Basel Committee on Banking Supervision to develop standards for international banking focused on risk reduction. These standards evolved from 1988 through 2010 and were known as the Basel Accord, Basel II and Basel III. The term "operational risk" emerged during this time and became the leading approach for managing banking institution risk in the 1990s. [4]

The U.S. Marine Corps defines operational risk as "the process of identifying and controlling hazards to conserve combat power and resources." [5] The U.S. Navy defines operational risk in OPNAV INSTRUCTION 3500.39B as "The process of dealing with risk associated with military operations, which includes risk assessment, risk decision making and implementation of effective risk controls." [6] The U.S. Air Force defines risk management as "a decision-making process to systematically evaluate possible courses of action, identify risks and benefits, and determine the best course of action (COA) for any given situation." [7] The guidance document emphasizes personnel health, safety and environmental factors. The U.S. Army includes guidance for the management of risk in operational contexts within ATP 5-19 and defines risk management as "The process of identifying, assessing, and controlling risks arising from operational factors and making decisions that balance risk cost with mission benefits." [8] The focus of operational risk in the Marine Corps, the Navy, the Air Force and the Army is on operational hazards rather than on a more general definition of operational risk.

The narrow focus within the banking industry on financial risk and within military operations on safety hazards decreases the potential effectiveness of operational risk activities. To that end, more inclusive definitions of operational risk and operational risk management are provided in Table 1.

With these more general definitions, any risk to the successful accomplishment of mission or business outcomes could be identified and addressed. The operational user community can then participate more fully with the acquisition and engineering communities in helping manage risk during the project life cycle. The more robust risk approach [9] is shown in Figure 1 and would require the acquisition community, the engineering community and the operational community to actively identify risks from their unique perspectives, which can then influence project outcomes.

Operational users identify mission and business needs to the acquisition community based on operational risk and threats. The acquisition community commits to providing enhanced capabilities to the end-user at a certain time, for a certain cost. The acquisition community then translates those needs into requirements which are provided to a set of engineers who develop and delivery enhanced capabilities to the end-user while meeting cost and schedule constraints agreed to with the acquisition community. The end-users participate continuously by providing insight into evolving operational needs and are advocates for the capability under development.

When operational risks are explicitly captured and addressed as part of the project life cycle, the resulting capabilities are more likely to address the evolving operational needs of the end user, increasing the likelihood of operational effectiveness of the delivered capabilities and overall user acceptance.

Figure 1. A Robust Risk Approach

Operational Risk-Driven Engineering Requirements/Engineering Development (ORDERED)

ORDERED is a repeatable method designed to influence engineering activities throughout the project life cycle with the purpose of improving project outcomes [10] through the explicit consideration of operational risk. New or enhanced capabilities are driven by the mission and business needs of diverse stakeholders. [11] Mission and business needs increase operational risk when gaps in current capabilities fail to address these needs. As new capabilities are developed, mission and business needs evolve, increasing the operational risk that the new capability will fail to address these changes. The ORDERED method ensures that program requirements and development activities are enacted with a thorough consideration of operational risk concerns. ORDERED does

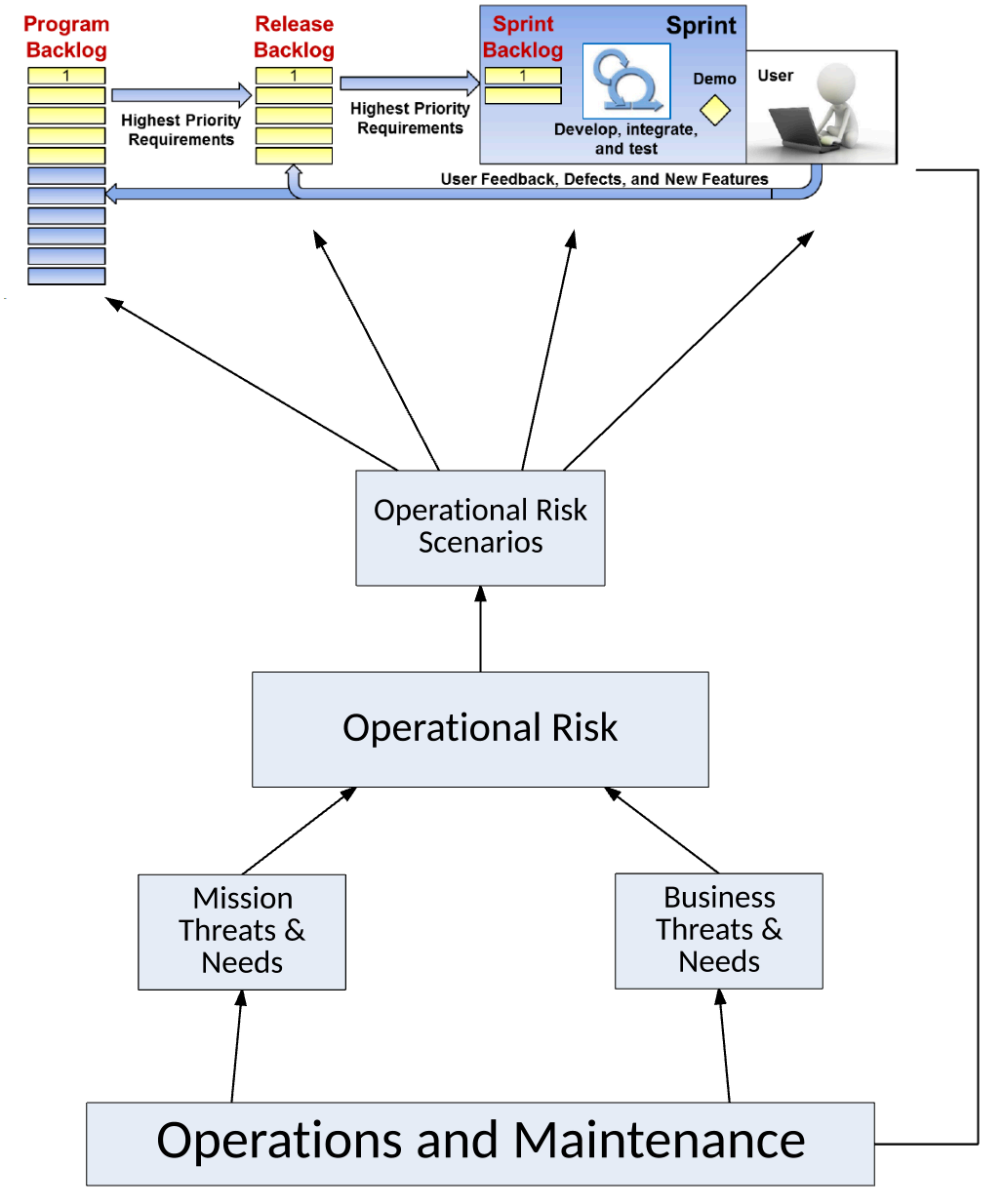

Figure 2. The ORDERED Approach

ORDERED Taxonomy	
A. MISSION	B. BUSINESS
1. Mission Planning a. Stability b. Completeness c. Clarity d. Feasibility e. Precedents f. Agility	1. Resource Planning a. Workforce b. Budget c. Facilities d. Equipment and Systems
2. Mission Execution a. Efficiency b. Effectiveness c. Repeatability d. Agility e. Affordability f. Security g. Safety	2. Governance a. Policies b. Procedures c. Organizational Structure d. Contracts e. Analytics f. Compliance g. Risk Management
3. Mission Outcomes a. Predictability b. Accuracy c. Usability d. Timely e. Efficient	3. Strategic Planning a. Vision and Mission b. Values c. Goals d. Objectives e. Monitoring
4. Operational Systems a. Throughput b. Usability c. Flexibility d. Reliability e. Evolvability f. Security g. Supportability h. Inventory	4. Stakeholder Management a. Identification b. Stakeholder Mgmt Plan c. Engagement d. Controlling
5. Operational Processes a. Suitability b. Repeatability c. Predictability d. Agility e. Security	5. Continuous Improvement a. Problem Identification b. Opportunity Identification c. Root Cause Analysis d. Improvement Planning e. Implementation
6. Operational Staff a. Skill Level b. Training c. Turnover d. Affordability	

Figure 3. The ORDERED Taxonomy

Mission Objectives	Business Objectives
1. Detect, contain, and remediate cyber security threats.	1. Reduce cybersecurity related incidents.
2. Analyze trends, determine root causes, and improve system resilience.	2. Reduce cost of cybersecurity activities.
3. Educate system operators and maintainers on cybersecurity threats.	3. Position for agency organizational consolidation.

Table 2. CSOC Operational Objectives

not replace a program's current engineering methodology, but rather augments current approaches with operational risk considerations. Therefore, ORDERED will work with any life cycle or engineering method. Figure 2 presents a high-level overview of the ORDERED approach as it would apply to a program using an Agile methodology. [1]

Mission and business threats and needs are identified by end-users during operations and maintenance activities. The gap between needs and threats and current systems and operational processes generates operational risk. Operational risk is captured in the form of individual risk statements, which define the potential negative outcomes that could impact mission execution or business operations. Essentially, operational risk is the "loss" that the mission or business may realize.

Operational risk attributes are derived from the risks. These attributes are characteristics of the system or capability. Operational risk scenarios are developed to further describe the risk in terms of the environment or behavior that would negatively impact mission or business outcomes. The scenarios are then used during the Agile engineering process to inform activities such as program and release backlog development and grooming, sprint planning, sprint execution and deployment strategies. As the mission and business needs and threats evolve, operational risks are continually identified, operational risk attributes continue to be identified or refined, and scenarios are developed or updated.

ORDERED uses a taxonomy to help with risk identification. A taxonomy is useful both when exploring sources of risk and when analyzing and classifying identified risks. The ORDERED Taxonomy is shown in Figure 3. The taxonomy was developed and simplified by considering personal experience and several source documents. [12] [13] [14] [15]

Operational Risk and User Stories

Most Agile methodologies capture expected behavior through the use of user stories. [16] User stories are statements of what the end user wants from the system or software. These user stories create the product backlog and are continually updated to ensure the stories represent the end user's prioritized needs. During sprint planning, user stories are moved from the product backlog to the sprint backlog for implementation planning. Active risk management throughout the Agile engineering process is a recognized best practice. The development team shares the responsibility for identifying risks that may impact the sprint, the project, or larger program. The addition of operational risk considerations during risk management activities provides a

Story ID	User Story
S001	As a CSOC analyst, I want to be alerted when an intrusion is detected.
S002	As a CSOC supervisor, I want to be able to evaluate the effectiveness of CSOC analysts.

Table 3. Initial User Stories

valuable mechanism to assist in developing the product backlog and prioritizing user stories for the sprint backlog.

Consider the Cyber Security Operations Center (CSOC) with operational mission and business objectives shown in Table 2.

During planning sessions with end users, the following user stories describing the expected behavior of a new incident detection system could have been captured.

While user stories describe expected or desired behavior, operational risks address unwanted behavior. Using the ORDERED process, the CSOC team conducted a risk identification workshop and identified more than 60 operational risks. The top three are shown below in Table 4, along with their probability of occurrence (P(O)), impact of occurrence (I(O)) and overall risk exposure.

As shown in Table 5, these operational risks were further analyzed by determining their risk attributes using the ORDERED Taxonomy, attribute concerns, and risk scenarios intended to influence Agile life cycle activities.

Scenarios are used routinely in systems and software engineering. The purpose of a scenario is to describe expected results of a system during development in terms of actual behavior. [17] Scenarios describe how the system should behave under certain conditions or when presented with certain stimuli. [18] Operational risk scenarios describe potential future unwanted behavior of the system that would cause mission or business impact to the operational organization. Similar to the concept of anti-patterns, [19] operational risk scenarios describe undesirable outcomes that need to be mitigated because they increase operational risk. The added insight provided by identifying and analyzing operational risks and developing operational risk scenarios can lead to the creation of additional user stories describing capabilities required to mitigate the operational risk. Given the risks in the CSOC example, Table 6 captures additional user stories influenced by a consideration of operational risk.

The addition of explicit identification and analysis of operational risks during Agile planning activities can provide a richer discussion of user stories and improve end user acceptance of the capabilities delivered.

Evaluating the Effectiveness of an Operational Risk Focus

Since few projects explicitly identify and capture their end user's operational risks as

Top "N"	Risk ID	Risk Statement	P(O)	I(O)	Risk Exposure
1	CSOC003	80% of operator time is spent responding to incidents; may not see trends or understand root cause of incidents	4	3	12
2	CSOC001	Incident occurrence is unpredictable; may not have adequate resources to respond during crisis	4	2	8
3	CSOC002	Heavy compliance and oversight make processes rigid; may not be able to adjust quickly to new events	2	3	6

Table 4. CSOC Top 3 Operational Risks

Top "N"	Risk ID	Risk Statement	Risk Attributes	Attribute Concern
1	CSOC003	80% of operator time is spent responding to incidents; may not see trends or understand root cause of incidents	1. Operator: Training, Skill Level 2. Mission Execution: Effectiveness	Inability of inexperienced staff to detect trends and determine causes of incidents
Operational Risk Scenarios 1. Junior staff members become overwhelmed responding to incidents and fail to detect new intrusion within 2 hours 2. During every 8-hour routine shift change, a vulnerability is exploited yet analysts fail to detect the incident or connect the periodic exploitations as related				
2	CSOC001	Incident occurrence is unpredictable; may not have adequate resources to respond during crisis	1. Mission Execution: Repeatability 2. Mission Outcomes: Predictability 3. Resource Planning: Workforce	Ability to predict staffing needs based on expected workload
Operational Risk Scenarios 1. During planning for staffing needs, supervisors fail to account for historical data and seasonal changes 2. During expected upcoming political events, attempts to penetrate the network increase beyond the analyst's ability to respond.				
3	CSOC002	Heavy compliance and oversight make processes rigid; may not be able to adjust quickly to new	1. Operational Systems: Flexibility 2. Operational Processes: Suitability	Inability to adjust the level of controls and reporting in times of crisis
Operational Risk Scenarios 1. During periods of high intrusion activities, required reporting, mandatory system controls, approvals and logging requirements impact the ability of analysis to respond quickly to incidents.				

Table 5. Operational Risk Scenarios

Story ID	User Story
S003	As a CSOC supervisor, I want to be able to predict required analyst staffing based on historical incident activity.
S004	As a CSOC analyst, I want to be able to bypass a set of optional controls during crisis events.
S005	As a CSOC analyst, I want the system to provide trend analysis and alerts.

Table 6. Additional User Stories

part of their risk management process, it is difficult to evaluate the impact of implementing this concept. A survey instrument was developed and administered to explore the relationship between operational risk considerations and project performance. Operational risk considerations were defined as actively eliciting operational risk from end users during the early solution development stages of a project, as well as actively and continually involving end user perspectives during development to identify and mitigate evolving operational risk throughout the project life cycle. Project performance was defined as meeting cost and schedule expectations and delivering capabilities that satisfy the end user's most critical quality attribute requirements and that mitigate operational risk.

The survey was administered to 104 project managers on Oct. 14, 2015. Figure 4 shows how comparing the existence of an operational risk process capability affected project outcomes.

The number of projects exhibiting lower project performance decreased from 50 percent for projects with low risk process capability to 36 percent for projects with medium operational risk process capability and went down to 21 percent for projects with higher operational risk process capability. Projects exhibiting medium project performance increased from 39 percent for projects with low operational process performance to 49 percent for projects with medium operational process performance and increased to 52 percent for projects with higher operational risk process performance. Projects exhibiting high project performance increased from 11 percent for projects with lower operational risk process performance to 15 percent for projects with medium operational risk process capability to 27 percent for projects with higher operational risk process capability. The Gamma score shows a moderately strong to strong positive relationship between the two variables, and the p-value of .006 provides confidence that the relationship is valid.

Given the strength of the relationship and the very low p-value, one can confidently conclude that projects within the sample that focused more on operational risk during the project life cycle also exhibited better project performance than those that focused less on operational risk during the project life cycle.

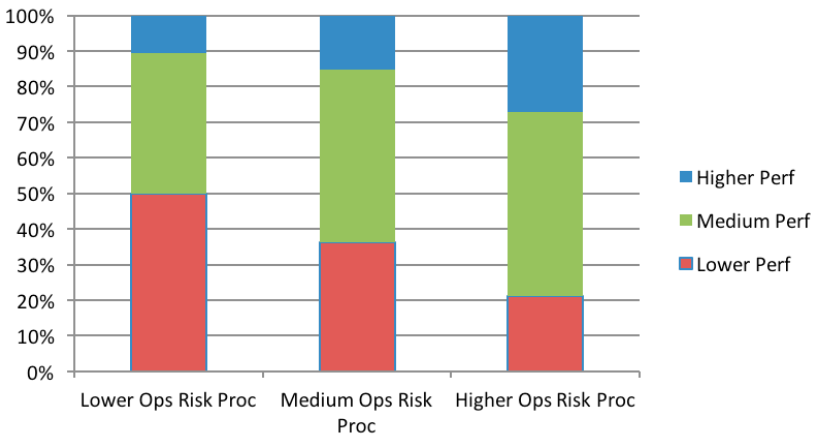

Figure 4. Operational Risk Process Capability and Project Performance

Conclusions

Risk management as an engineering practice is commonplace. However, actively eliciting operational risk considerations during the engineering life cycle is not as common, even in projects using an Agile engineering process. This paper explored the relationship between an operational risk focus during the project life cycle — specifically the use of operational risk to inform the creation of user stories — and improvement in project outcomes. Early results indicate that an explicit focus on the end user's evolving operational risk during the engineering life cycle results in improved project performance. More work is needed to explore techniques to integrate an operational risk mindset into current Agile engineering methods, allowing the explicit mitigation of operational risk and improved project outcomes.

REFERENCES

1. Modigliani, P. & S. Chang. (2014, March.) Defense Agile Acquisition Guide: Tailoring DoD IT Acquisition Program Structures and Processes to Rapidly Deliver Capabilities. McLean, Va. MITRE Corporation.
2. Wrubel, E. & Gross, Jon. (2015.) Contracting for Agile Software Development in the Department of Defense: An Introduction (CMU/SEI-2015-TN-006). Retrieved August 22, 2015, from the Software Engineering Institute, Carnegie Mellon University website. http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=442499.
3. Under Secretary of Defense, Technology, and Logistics (USD[AT&L]), Editor. (2015.) PERFORMANCE OF THE DEFENSE ACQUISITION SYSTEM 2015 ANNUAL REPORT, A.
4. Power, M. (2005.) The invention of operational risk. Review of International Political Economy. 12(4), 577-599.
5. United States Marine Corps. (2002.) MCI, ORM 1-0: Operational Risk Management. Headquarters Marine Corps, Washington D.C.
6. OPNAV, 3500.39 B.(2004). Operation risk management.
7. USAF, Pamphlet 90-803 - RISK MANAGEMENT (RM) GUIDELINES AND TOOLS.
8. Army, ATP 5-19. (2014.) Risk Management.
9. Gallagher, B.P. (2002.) Interpreting Capability Maturity Model Integration (CMMI) for Operational Organizations.
10. Gallagher, B.P. (2015.) Improving Systems Engineering Through Operational Risk Considerations. In the 27th Annual IEEE Software Technology Conference.
11. Susnien, D. & P. Vanagas. (2015.) Means for satisfaction of stakeholders' needs and interests. Engineering economics. 55(5).
12. Gallagher, B.P., et al. (2005.) A Taxonomy of Operational Risks.
13. Gallagher, B., et al. (2011.) CMMI for Acquisition: Guidelines for Improving the Acquisition of Products and Services. Addison-Wesley Professional.
14. ISO, 31000 (2009.) Risk management – Principles and guidelines, in International Organization for Standardization. Geneva, Switzerland.
15. Project Management Institute, Incorporated. (2013.) PMI, A Guide to the Project Management Body of Knowledge (PMBOK® Guide).
16. Cohn, M. (2004.) User stories applied: For agile software development. Addison-Wesley Professional.
17. Mylopoulos, J.; L. Chung & E. Yu. (1999.) From object-oriented to goal-oriented requirements analysis. Communications of the ACM. 42(1), 31-37.
18. Bass, L.; Klein, Mark & Moreno, Gabriel. (2001.) Applicability of General Scenarios to the Architecture Tradeoff Analysis Method (CMU/SEI-2001-TR-014). Retrieved August 22, 2015, from the Software Engineering Institute, Carnegie Mellon University website. http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=5637.
19. Brown, W.H.; R.C. Malveau & T.J. Mowbray. (1998.) AntiPatterns: refactoring software, architectures, and projects in crisis.

ABOUT THE AUTHORS

Dr. Brian P. Gallagher is the SVP of Operational Excellence for CACI, and is responsible for program management and delivery, process effectiveness, and continuous improvement initiatives. Brian has held numerous positions within Northrop Grumman, Carnegie Mellon's Software Engineering Institute, the Aerospace Corporation, and the United States Air Force. He holds a Ph.D. in Systems Engineering through Colorado State University, an M.S. degree in computer science from the Florida Institute of Technology and a bachelor of technology degree from Peru State College.
brian.gallagher@colostate.edu
bgallagher@caci.com

Dr. Kenneth E. Nidiffer has over 53 years of government, industry and academic experience in the field of software and systems engineering. Ken has successfully executed positions as a senior vice president at Fidelity Investments, vice president of the Software and Systems Consortium, and director of technical operations/engineering at Northrop Grumman Corporation. He is currently the director of strategic plans for government programs at the Carnegie Mellon Software Engineering Institute. Ken received his B.S. degree in chemical engineering from Purdue University, Indiana; his M.S. degree in astronautical engineering from the Air Force Institute of Technology, Ohio; his MBA degree from Auburn University, Alabama; and his D. Sc. in systems engineering from George Washington University, Washington, D.C.
nidiffer@sei.cmu.edu

Dr. Ronald M. Sega serves as director, systems engineering programs and special assistant to the chancellor for strategic initiatives at Colorado State University. He is also the Woodward Professor of Systems Engineering. From 2010 to 2013, he also served as vice president and enterprise executive for energy and the environment at both Colorado State University and The Ohio State University. He holds a B.S. in math and physics from the U.S. Air Force Academy in Colorado Springs, an M.S. in physics from Ohio State University and a Ph.D. in electrical engineering from the University of Colorado. Prior to joining CSU, Dr. Sega was the under secretary of the Air Force from 2005 to 2007, where he served as the DoD executive agent for space and led the Air Force team that won the overall Presidential Award for Leadership in Federal Energy Management for 2006. After 31 years in the Air Force, having served in various assignments at Air Force Space Command and as a pilot, he retired from the Air Force Reserve in 2005 as a major general in the position of reserve assistant to the chairman of the Joint Chiefs of Staff. Dr. Sega was director of defense research and engineering (DDR&E), the chief technology officer for the Department of Defense (DoD), from 2001 to 2005. Dr. Sega was a faculty member in the College of Engineering and Applied Science at the University of Colorado at Colorado Springs from 1982 to 2013, also serving as dean from 1996 to 2001. A former astronaut, he flew aboard Space Shuttles Discovery (1994) and Atlantis (1996).