32nd Annual INCOSE international symposium
hybrid event
Detroit, MI, USA
June 25 - 30, 2022

Red-Teaming as a Research Validation Method for Systems Engineering Thesis Students

Timothy L.J. Ferris
Cranfield University
Cranfield, MK43 0AL, UK
timothy.ferris@cranfield.ac.uk

Fanny Camelia
Cranfield University
Cranfield, MK43 0AL, UK
fanny.camelia@cranfield.ac.uk

Tuomas Mattsson
Navy Command Finland
The Finnish Defense Forces
FI-20811, Turku Finland
Tuomas.mattsson@mil.fi

Rogério C. Machado
Life Cycle Management Superintendence
Navy's Program Management Directorate
Brazilian Navy, CEP 20010-000
Rio de Janeiro, Brazil
r.machado@marinha.mil.br

Abstract. All research projects need a forward path method for performing the investigation, making findings and reaching conclusions. In addition, project methodology must include methods that test the truth of the knowledge claimed to have been developed through the project. We address the specific issue of validation in thesis projects in systems engineering (SE) programs where the intended outcome is either an application of SE method or an investigation of a topic in SE. We present red-teaming (RTing) as a validation method for results of SE research. We discuss two case studies of thesis projects which used a RTing method to evaluate a proposed method for doing something. From this we discuss the strengths and weaknesses of the RTing method in thesis projects and provide guidelines for use of RTing as a project outcomes evaluation method. We conclude RTing is a useful method to evaluate a thesis project which generates a design or a method because it uses a method not directly influenced by the student's assumptions in the design of the project. The RTing method is constrained by the challenges of finding willing red-team (RT) members, project schedule, and the RT member's knowledge of the subject.

Introduction

Systems engineering (SE) is understood in various ways, even by people who subscribe to a definition such as the INCOSE definition: "Systems Engineering is a transdisciplinary and integrative approach to enable the successful realization, use, and retirement of engineered systems, using systems principles and concepts, and scientific, technological, and management methods" (INCOSE, 2022). This definition focuses on what SE aims to enable but is agnostic as to what, at a more fundamental level, it is.

There are many universities which offer programs in SE, most often at graduate level. The curricula in most, or all, universities teaching SE rightly teaches methods for performing the tasks associated with the things in the latter part of the definition; graduates need to know about and how to perform the methods to be able to perform the tasks a systems engineer is expected to perform. The published

curricula of courses enable readers to identify which SE methods are taught and, consequently, to determine whether a particular course includes the range of material to be useful for the reader's intended purpose. Addressing this dimension of SE education was one of the motivations, and use cases, for Graduate Reference Curriculum for Systems Engineering (GRCSE) (Pyster *et al.*, 2015).

A second perspective on SE is not elucidated. This is where SE belongs along a continuum between exploring situations and proposing apposite solutions, and the implementation of engineering processes to ensure best possible delivery of a specified systems solution. The former extreme of the continuum views SE as a method of discovery of apposite solutions and the latter extreme views SE as the performance and technical management of engineering tasks that realize a specific solution option. In practice, tasks a systems engineer is expected to perform result in different need for capabilities to contribute at different points along the continuum, so recognition that the continuum exists is observation of fact, not an expression of value of those positions. The finding of apposite solutions view of SE reflects the view that SE itself is a research methodology, that is, that the practice of SE is inherently a research task.

Traditional views of academic research emphasize the development of assured and, preferably, generalizable knowledge about the subject matter, as seen, for example, through the basic teaching of "scientific method" in most undergraduate science courses. Recently, there has been a movement towards acceptance of a wide range of methodologies, particularly in social sciences and investigation of professional practice, which differ from "the scientific method". The traditional "scientific method" is focused on knowledge about the subject of investigation, which often results in abstraction that does not generate practical impact. This suggests a different approach to research may be required if the focus of the work is on achieving a practical effect. We recognize that research in SE may be either research about topics relevant to SE to impact the practice of SE or development of knowledge through the practice of SE (Ferris, 2009).

This paper presents "red-teaming" (RTing) as a validation method in SE research, and investigates its application, particularly, in SE research conducted by thesis students. An overview of research in SE, a review of literature on the RTing method and the application of RTing in two SE theses are presented. This is followed by discussion and lessons-learned from the application of RTing in these projects.

The purpose of this paper is to discuss RTing as an additional method of systems engineering research validation to be added to other methods which are used in research. Other methods include peer review and monitoring by a research degree supervisor. Peer review is generally applied to products describing research, such as papers, reports and theses, to inspect the product, and to determine if the product reports and describes validly what was found, or the product appears appropriate. Peer review is not normally applied to the products developed during a project. Meanwhile, research degree supervisor monitoring of the project is limited by the circularity problem that the supervisor has been involved in the development of the project, advising on approaches that are reasonable to use and therefore does not have the independence of the project that is provided by an outsider to the project development. Further, the supervisor is limited in having seen many iterations of the work at various stages of partial completion.

The appropriate method for validation of research findings depends on the nature and the circumstances of the project. RTing is presented as a method for research outcome validation with a reasonable range of applicability.

Research in or for SE

All research has the purpose of generating knowledge, and therefore, as we consider approaches to doing research and purposes of research, we need to review the nature of knowledge. The classical epistemological view of knowledge is: "*S* knows *p* if and only if: 1. *p* is true; 2. *S* believes that *p*; and

3. *S* is justified to believe that *p*" (Dancy, 1985). That is, knowledge is justified true belief. This general requirement of knowledge has a corollary for research methods, regardless of the purpose or subject matter of the research. To be justified in using something which is claimed to be "knowledge" to do anything the "knowledge" must be developed using a method which ensures it is true and provides justification that belief in that claimed knowledge is reasonable. Without prejudice concerning any other approach to this challenge, one approach which would satisfy this standard in research is to plan a methodology that can generate that about which a knowledge claim is made, and a second, independent, process which tests the veracity of the "knowledge" (Davendralingam *et al.*, 2015).

SE includes concern with the process by which the engineering work is performed and a different set of concerns with the development of the techniques that are used. Research into SE processes often addresses questions of what processes are actually used and the facts about how those processes are implemented, where the research method is often a combination of interviews and surveys of participants to discover the facts on the ground. Research questions in this class of work include the application of standards and methods imposed on organizations. This work often seeks to discover what is done, and how it is done, in organizations. The intent of this research often is a set of recommendations based on facts and findings. The findings can normally be verified using empirical methods and inferential statistical methods are used to validate hypothesized interpretations.

Another subject area of research concerns SE processes themselves, their properties and limitations, or the proposal of new, or variant methods to support SE practice. These topics are likely to be investigated using mathematical methods that explore properties of the methods. Verification may be achieved through either numerical or theorem proof type methods. This work is performed to validate an *a priori* position which is asserted about the process under investigation.

Another subject area of SE is focused on improvement of the system of interest. This research involves the proposal of new methods or solutions, followed by action which investigates the quality of the proposed method or solution. The new process is developed through a reasoned process which builds on knowledge of existing processes, methods and contextual factors and which seems sound using the "forward path" process of a normal development method.

When a research project seeks to improve the system, or systems engineering method, by developing something new, there must be a method of verification and validation of the output. The verification process could be performed by the researcher but a researcher who has already applied their understanding of the situation of interest to develop a concept will be limited by the knowledge of the situation which they used for the method development, which will embed the researcher's assumptions about the challenge in the evaluation of the proposed solution. The effect of the embedding of these biases in the evaluation of the proposed method is that the evaluative process is less likely to identify weaknesses in the proposal and unarticulated assumptions about the scenario are unlikely to be recognized. This problem is likely to also manifest if the evaluative process is performed by another person who has been linked to the project, such as a supervisor of the person performing the project, because of groupthink type processes. A researcher may choose to test a proposed process by development of a model of the process including factors such as formal models of the flow of information and material in the process, but such models, whilst capable of providing quantitative description of the behavior of the process, will not enable discovery of erroneous assumptions about the scenario because the assumptions are embedded in the model through the construction of the analysis. In this case the output of the verification process is objective but the process cannot test whether the correct conceptualization of the challenge is analyzed (Ferris, 1997), that is, validation is precluded.

An alternative to the researcher performing their own validation process, which introduces the potential problems of circularity of reasoning and bias, is to perform the validation using another person who is independent of the "forward path" of the project. The independent person is less likely

to be bound by the same assumption set as the researcher. This point cannot be guaranteed because many assumptions people bring to analysis of situations, and about what may be a reasonable position to take, arise from their background. Therefore, a different person reviewer is likely to share the same deep-seated perceptions about the subject matter as another person from a roughly similar background. A second class of problem that an independent reviewer may have in relation to a project is possession of sufficient knowledge of the situation as to be able to make insightful judgments. This could arise either because of insufficient knowledge of the subject matter or because of lack of common understanding with the proposer of the meaning of the articulation of the idea under test. The effect of these possibilities is that a person chosen to critique a process may be unable to provide suitable validation evaluation. In either case the feedback from the appointed critic would be inadequate.

A further approach to research in SE is to use the SE as a method of performing work, at least as described in broad outlines of SE, and instantiated with a number of specific methods. In this approach to research the goal is to find an appropriate solution to the challenge. The purpose of the verification and validation activities; which are performed as an inherent part of the standard SE process as part of the normal project gate reviews must be performed with the purpose of identifying problems potentially impacting successful completion. This method is, clearly, used where the purpose of the project is to deliver a normal work task. This method may also be used as a method to discover an appropriate solution to a novel need, or a need being addressed for the purpose of finding a suitable solution.

Literature review – Red-Teaming

The term red team (RT) originated from military war games to refer to a team assigned to assume the role of the enemy to test war fighting abilities in opposition to the 'friendly' blue team (Conway, 2012)(Romyn and Kebbell, 2014). As the challenger team, the RT can attack, support or exploit the assumed worst case scenarios, assist questioning the assumptions by thinking "outside the box", challenge the established thinking process and offer alternative thoughts (Conway, 2012)(Romyn and Kebbell, 2014)(Graham and Graham, 2016). Mercer (2017) abstracts the RTing idea as a procedure with which to challenge the dominant thinking about a matter. Mercer traced this conceptualization of RTing to the Devil's Advocate idea developed by the Catholic Church in the 13th century. It has been implemented widely in many areas especially defense and security, cyber security, and information technology.

To challenge the dominant thinking, the RT can take several forms: people with particular expertise such as real soldiers or hackers; paper-based exercises; and computer simulation (Romyn and Kebbell, 2014). Ranjeet et al (2011) proposed using an automated RTing process to test military doctrine. The purpose of automation was to enable both testing of a large number of possible specific approaches and to automate the selection of approaches across a space without the constraint of the mental constructs which could narrow the range of possibilities actually tested based on the challenge of proposing ideas outside one's expectations, as based on training.

We have reviewed RTing by searching Scopus for the term "red team". We reduced the list of items reviewed on the basis of selecting items which by title and abstract communicated that the subject matter was RTing as a means of investigating, or challenging, something. Our review includes a small number of papers in which the RT process itself is the subject, and many papers where RTing was the method used to do the work reported. In the latter case the discussion of the RT ranged from a bare description of what method was used to discussion of the RT methodology in significant depth.

Opportunity of red-teaming

The process of RTing is valued because it enables testing of systems or constructs through the application of a challenge of a kind that the RT choose to apply, rather than a set-piece test or

challenge of a kind designed by the system developers. This provides the opportunity to test the system under a realistic challenge while avoiding the risk of real damage, as may occur in a real attack (Fenton, 2016). A second benefit of RTing relates to the fact that the complex designed systems, or scenarios, which the method is used to test, are usually designed cognizant of some set of potential challenges. Any test of such a system most likely is biased by the set of challenges of which the developers were cognizant. The RT method challenges the system using scenarios which were outside the design-for set. While this enables testing of the system under scenarios different than any anticipated in the design, it still suffers from the philosophical limitation that not finding a vulnerability does not mean that there is no vulnerability, so the method can be used to find and prompt response to specific vulnerabilities but cannot show there is no vulnerability (Baiardi, 2019).

Challenges of red-teaming

While writing in the specific context of information assurance, Wood and Duggan (2000) observe that the RT needs knowledge of a range of specialties related to both disciplines within information systems and the subject matter of the project. This makes a significant resource demand to identify and exercise the RT validation. If the RT members lack appropriate knowledge and skill the findings will be deficient in ways that will not be knowable. The effect of this problem is that RTing in relation to large, complex and distributed systems is likely to be a large and expensive project (Helsinger, Ferguson and Lazarus, 2001). The impact of the reliance on the knowledge and skills of RT members results in the process producing outcomes which are difficult to reproduce and in the class of 'spot' identification of faults rather than assurance that there are no faults (Craft, 2017). Thus, while RTing is a common method in cyber security investigation, the outcomes depend on the skill and diligence of the RT (Clark *et al.*, 2015).

A recognized difficulty in the analysis of sensitive information, such as intelligence reports, where the normal barriers to participation in the analysis work result in all participants having significant acculturation to both the methods and interpretation of data, is groupthink, in which individuals tend to think similarly. A method to address this problem is to use a RT in the analysis, where the members are chosen and instructed so that they will propose significantly different interpretations of the intelligence corpus. This approach is useful for introducing a novel opinion, even if largely to challenge a potentially groupthink viewpoint. However, the method could be problematic, as discussed in Conway's argument concerning the use of a Neoconservative RT in the analysis of Weapons of Mass Destruction related evidence prior to the 2003 invasion of Iraq (Conway, 2012).

Red-teaming as a teaching tool

RTing is a common method in the practice of cyber security, used to discover the vulnerabilities of systems. As such it is natural for educators in cyber security to consider the method as part of their teaching. Deckard and Camp (2016) report using a RT exercise to focus students during training courses. Rege et al (2018) state that it is common in cyber security training to use RT/blue-team exercises, pitting two teams, one defending and the other attacking the integrity of a system so that the learners can learn to think like an opponent and have an experience of how things may unfold an a system attack.

Red-teaming in network intrusion testing

RTing is commonly used in penetration testing of cyber networks. The typical network contains various assets of a variety of attractiveness to penetrate and potentially a variety of protective methods employed. The purpose of RTing is to challenge the systems using methods independent of the network planning and defense development (Kewley and Bouchard, 2001). The major benefit of RTing is that the RT members take pride in their ability to successfully penetrate a network, and therefore will bring to their challenges great diversity of method. However, a weakness of the RT

method is that once the RT has achieved penetration it is unlikely that they will continue to apply equal skill and diligence to seeking other methods of attack (Levin, 2003).

Heckman *et al.* (2013) described an intrusion test experiment in which they established four teams, one of which was the attacking RT, where each team was responsible for one perspective on the system. Their study used various methods of attack and defense to explore the effectiveness of the various strategies.

Tan *et al.* (2014)(Porter *et al.*, 2014) implemented a computationally based RT approach using agent-based modelling. This approach has the advantage of enabling a large plurality of runs through the process, which in turn enables the development of statistical results from the study. A statistical presentation of results provides a basis for confidence in the representativeness of the results obtained, in contrast to the singular results achieved through manual RT processes, in which single cases, only, are executed.

DARPA used RTing to develop malware to exploit weaknesses in the Android operating system. The goal of the RT was to develop the most sophisticated malware while the blue-team had to find means of intrusion detection and provide defenses against intrusion (Holland, Deering and Kothari, 2015). In a RT/blue-team exercise the time required by each team for their tasks is a useful measure of the challenge to attack or defend the system (Rege *et al.*, 2017). Where an organization consistently uses a RT approach it is possible to compare results to estimate the total cost of security (Van Leeuwen, Stout and Urias, 2016).

Kont *et al.* (2017) describe the various teams of people and the supporting software for a large-scale NATO exercise addressing a network defense/attack scenario, demonstrating the significant resource that is expended on the planning for and conduct of significantly large exercises.

Rastegari *et al.* (2013) report using RT methods in the specific challenge of a denial-of-service attack.

Several groups report using RT methods in projects concerned with testing cyber security in various contexts (Rubel *et al.*, 2008)(Farar, Bahsi and Blumbergs, 2017).

Red-teaming in military/security studies

RTing is used in the study of warfare to generate understanding of potential outcomes in various scenarios. However, RTing is personnel intensive, and therefore expensive, and so is used in only a limited number of case investigations (Yang, Abbass and Sarker, 2006). The cost of manual implementation of RTing, and the consequent limited number of cases which can be explored have resulted in attempts to develop automated RTing methods so that a much wider range of scenarios can be investigated (Zeng *et al.*, 2011). Automation of RT methods which enable the systematic exploration of a significant space of options produce a set of results associated with the wide range of scenario variations and consequently enable a much greater generalizability of the results (Lafond and DuCharme, 2011).

RTing can also be used in other security related investigations, with reports of use in criminology to explore how inexperienced members of the public would attempt to proceed with criminal or terrorist actions to determine such things as what might be identified as targets given the common knowledge in the community about the significance and vulnerability of particular sites (Romyn and Kebbell, 2014)(Romyn and Kebbell, 2018).

Red-teaming in hardware design and assurance

One research group has reported addressing the challenge of discovery of Trojan circuits added to logic devices in the manufacturing process. This scenario is a threat because of the separation of

responsibility in the industry between logic and device designers and device manufacturers, enabling modification of circuit designs before manufacture, and also the possibility of manifestation of the insider threat in the design process. This group took an empirical approach involving requiring a blue-team to design the original circuit as robustly as possible, to prevent insertion of Trojan circuits, and a RT who were assigned the task of attempting to insert certain Trojan circuits without the incursion being detected. After the RT incursion attempt the blue-team had the role of detecting the incursion. This work was reported in several papers (Rajendran, Jyothi and Karri, 2011)(Zhang *et al.*, 2013)(Waksman *et al.*, 2014).

Red-teaming to study other threat types

Earlier, in sub-sections "Challenges of RTing" and "RTing in network intrusion testing", of this literature review we have noted mention of the resource intensiveness and potential idiosyncrasies of results in relation to the personnel in the teams, with the suggestion that automation of the process could be a solution. However, there is a distinct advantage of a human driven RT exercise, humans can use methods, such as social engineering, to attempt to penetrate a network through exploitation of insider threats (Moses and Rowe, 2015). The opportunity to use social engineering is a powerful method for discovery of the potential vulnerability of a system through the actions of insiders, not purely technical vulnerabilities. More generally, the RT approach can be used to explore the insider threat vulnerability of a cyber-system (Haigh *et al.*, 2009).

Kraemer, Carayon, and Clem (2009) report a project in which two independent RTs were established and arranged as focus group with the purpose of identifying a range of causal factors for information breaches. This method has the advantage that the RTs function separately, and therefore the range of factors discovered is less constrained than may be the case if a single RT is used, especially if there are social factors which may inhibit free proposal of challenge factors.

Space projects are high risk and produce systems to be deployed in an unusual environment, and therefore are subject to diverse threats to success. NASA employed a RT approach in a project performed by JPL, through sending the RT to the JPL site with the purpose of asking challenging, knowledgeable, questions to review and challenge project decisions (Carrison, 2010).

In a service oriented architecture based system a cooperative RT approach was used in which the RT were provided with information about the system they were attacking and reports of prior attacks on the system (Pal *et al.*, 2012). This approach has the benefit that the RT is informed about what they are attacking, which may help in identifying particular potential attacks, but it may also bias their thinking, constraining their approaches to approaches informed by the design philosophy employed.

Red-teaming in academic research

The preceding sections of the literature review have largely described either situations in which RTing has been used and its method of use in evaluation of particular systems in application as a specific system investigation tool, or observations about the merit or disadvantages of RTing as a system investigation tool. Practical use of RT methods addresses problem spaces which are ephemeral. Use of RTing in academic research is normally understood to require methods which can be reconstructed so that discoveries are repeatable. A further challenge in the use of RTing in academic research in cyber environments, an area of common practical use of the methodology, is that the scale of many academic research projects is small relative to the broad ranging scale of vulnerability exercises in systems and networks of deployed systems scale. The resource limitation of academic research requires academic projects to address specific questions and constrains the permissible RT actions (Mirkovic *et al.*, 2008).

Rosen, Edwards and Suter (2010) report a project in nuclear physics in which two teams were established, one to develop a 'target' and the other to develop a laser to shoot at the target. Both teams

were kept ignorant of the physics model, the method, used by the other to ensure their solutions could be effective in the 'working blind' situation. This is not a classical blue-team/RT construct but applied an adaptation of the concept to suit the project.

Conclusion

The RTing method is one method used to evaluate the resilience of cyber systems and assets, where the focus of interest relates to the avoidance and withstanding of attack, the extent of damage incurred, and the path to recovery (Checkland, 1981). The RT is meant to discover system vulnerabilities before they are found by genuine attackers and is, fundamentally, a tool to support operational planning in any field of practice. The RTing approach is often performed poorly, often focusing on finding specific vulnerabilities, whereas a good implementation of the method would perform systemic analysis to identify systemic issues (Graham and Graham, 2016). RTing focuses on the combination of the asset systems and the organization within which they sit, which contrasts with a simulated attack, in which case the focus is on the response of the asset systems without their interaction with the organization in which they belong (Mansfield-Devine, 2018).

Student Theses in SE

Kinds of project which might be done by students

A Masters level degree in SE in most, or all, universities require the student to perform a project that leads to a thesis. The details of what constitutes an appropriate project and thesis vary according to the particular university regulations. For example, some universities may require a project which investigates a topic relevant to SE in a manner consistent with the classical research methods in engineering, usually collecting data about the subject of interest and analyzing that data to build a conclusion about the research question. In other cases, the project may be to model something, or to design a thing or a process. The local regulations of the university, which may be influenced by accreditation criteria, reflect the intended learning outcomes of the degree, a matter specific to each university.

Regardless of the subject matter and kind of the project there is a pattern which should be present in any project. There must be forward path activity in which the student performs tasks which generate the intended project outcome, referred to here as the "knowledge" intended as the project goal.

Verification & Validation of research

In order that the knowledge generated by the project can be used there must be a process by which that knowledge is tested and demonstrated reliable. The appropriate method of test depends on the nature of the knowledge to be developed. For example, if the project is intended to investigate a topic of interest through an empirical process of observation and analysis the verification and validation of the knowledge is embedded in the project process. The knowledge is posited as a result of preliminary observations and literature review, but it may be expressed in the form of a theory about the subject matter. It is then transformed into a testable hypothesis which could be tested by a set of observations and analysis leading to refutation, or non-refutation, of the hypothesis.

Many projects about how SE is implemented in particular organizations involve either surveys or interviews. These methods have well established test methods, using inferential statistics in the case of surveys and textual interpretation in the case of interviews.

Where a project involves mathematical modelling the verification and validation can be performed using standard mathematical derivation and theorem proof methods for the model itself. The model also can be tested using empirical observations to compare predictions of the model and observed results. However, the challenges introduced by the experimental scenario used to test the model are

constrained by the assumptions which were embedded in the model design. The result is a circularity of reasoning which can only be verified if the implementation is consistent with the originating understanding of the scenario.

At the Masters thesis level it is not unusual for thesis projects to combine some primary data collection and analysis to characterize a scenario, followed by making a proposal to design something, such as a process or possibly a thing, to address a need which prompted the project. This kind of project is justified because it enables the student to demonstrate competence at many elements of the SE process in microcosm. The challenge in this kind of project is that the proposal is the result of the forward path process leaving a need for some means of review before the status of the output can be moved from "interesting curiosity" to "substantiated and suitable for experimental implementation". A validation method for such a proposal is required to make the project outcome at least partially assured.

The evaluation process for a proposed design of a thing or a process could be performed by modelling. The circularity of reasoning effect discussed above undermines the potential effectiveness of any modelling of a proposal. If the proposal is of a thing, the physics models used in the test activity build on the same knowledge of the subject as was used in the design analysis. If the proposal is for a process, the analysis model will include the same assumptions embedded in the forward path work resulting in lack of independence of the evaluation process. A fundamental limitation of modelling as a proposal evaluation method in either scenario is that the models will only include factors of which the modeler is aware. In the case of thesis work this difficulty is considerable because the project is performed by an individual with the result that the evaluation process is not informed by divergence of view of the subject matter. Evaluation of a proposal demands a need for a source of fresh critique on the proposal.

The problem of circularity is exacerbated in the case of thesis projects because the student is still a learner in the field resulting in lack of experience to bring to bear on a proposal to enable a substantial challenge of the proposal.

Proffered Solution - Validation by a Red-team

We propose RTing as an approach for verification and validation of the outcomes of a thesis project proposes a design of a thing or a process. These outcomes are typical of systems engineering project theses. We assert that RTing has properties which overcome the major difficulties which challenge the use of other possible methods to complete the evaluation path in projects to design something through validation.

In a thesis project using a RT approach to validation the student performs the forward path work of design of the thing or process. The proposed design or process is then submitted to a panel of RT reviewers with relevant expertise to perform validation. If the form of the design is a static model it can be validated by individual RT members. If the project has produced an executable model the RT validation might be established as a game with the RT playing against the model.

In the remainder of the paper, we present two case studies of theses, written by two thesis students of an SE course in a UK university, using this methodological construct and we discuss our observations of the effectiveness of the method to provide generalizing guidance for implementation of this method.

CASE STUDIES

Project 1

Project Description The project aimed to plan the method to apply the key principles and values of agile methods to defense acquisition projects in Finnish Defense Force (FDF) (Mattsson, 2018). It is expected that the agile acquisition model proposed would enable adaptation in a rapidly changing global environment. The various agile methodologies share common characteristics and traits that can be seen in their core principles, values and practice, including high collaboration and self-organization of project teams; welcoming change; valuing functionality over documentation; and valuing individuals and interaction over processes and tools. These principles were derived from three agile methodologies, Scrum, Extreme Programming (XP) and Dynamic System Development Method (DSDM).

Project Methods The project applied the first three steps of Checkland's seven-stage Soft System Methodology (SSM) (Checkland, 1981): consider the problematic situation; express the problematic situation; and formulate a root definition; to understand the problem space and the existing acquisition processes. A rich picture capturing key factors, actors, interactions and the organizational context, and a context diagram to further explore the interactions surrounding the System of Interest, were developed to address the first two stages of SSM. A problem root definition, the third step of SSM was formulated using Checkland's CATWOE. The project used flow and sequence diagrams to describe processes and interactions between stakeholders and process products; hump diagrams to show the amount of SE activities during the acquisition lifecycle stages (SEBoK Contributors, 2019). These diagrams were used to model the current, baseline, acquisition process; the recommended acquisition process changes; and the final proposed acquisition process model after RT evaluation.

Red-Team Method Application to the Project The current acquisition process model, and the proposed changes to that model that were represented through flow, sequence and hump diagrams, were evaluated by a RT. This evaluation was performed by email exchange between the student, who developed the models, and the RT members. Each RT member was a project management professional in defense acquisition projects, in the relevant country, with over 20 years of military service and managerial experience.

The student provided a brief description of the model, the proposed changes and the rationale for change to the RT. In reply, the RT member provided critique, written comments, drawings and review notes for each model. In response to the feedback, a refined process was developed and presented to the RT for re-evaluation.

The student developed a baseline and four evolutionary models with embedded agile principles. The RT evaluation of the baseline was performed to familiarize RT members with the process representation and to identify possible errors in the student's interpretation of the baseline process. In the first evolution the student incorporated the "stakeholder involvement and collaboration" principle into the baseline. In the second evolution, the student integrated the "welcoming change" and "functionality over documentation" principles. The third evolution embedded "individuals and interaction over processes and tools". The review of the new proposal was intended to validate it and provide feedback for its application in acquisition. Finally, the student developed a new baseline based on the review and critiques received.

Red-Team Challenge The validation of the agile acquisition proposal relied on the RT members, their expertise in the subject matter and their familiarity with the Rting process. The small number of RT members engaged, their lack experience in the project subject and their unfamiliarity with the Rting process, may have yielded a narrow view of the subject than would be preferable. Organizing the RT based on the principles in the Red Team Guide (Development Concepts and Doctrine Centre, 2013) would improve the validation process.

A validation process that relies on the RT members' experience may limit generalization of applicability. For example, the involvement of RT members in past FDF Land and Sea acquisition projects raises questions about the applicability of the proposed agile model to Air projects.

Project 2

Project Description Performance Based Logistics (PBL) is a contracting strategy in which the supplier provides demanded outcomes and is rewarded based on measured performance (Machado, 2018). By purchasing the outcomes, instead of discrete products or services, through applying proper performance measures the buyer pushes the supplier to act efficiently and effectively, reduce waste, cut cost and improving product/service quality. Successful PBL implementation depends on the buyer supplier interaction to co-create value.

The project aimed to develop a reference structure model for the main elements of a generic fixed price PBL contract between the buyer (navy) and the supplier (contractor) for delivering In-Service Support to warships. The reference model represents the best practice, core elements and relationships, and therefore adaptations can be made to apply the model in the context of a specific navy/country or type of warship. This project identified emergent issues using the model. These and possible solutions were discussed.

Project Methods A literature review was conducted to explore implementation of PBL. In parallel, an exploratory questionnaire was developed and completed by PBL specialists to gain from their experience in both private and public sectors. The information gained by these methods became the basis for the modelling activities and the development of the reference model.

The modelling activities involved development of a context diagram and formulation of the problem definition, the first three steps of Checkland's seven-stage Soft System Methodology (SSM), from both buyer and supplier perspectives. Causal loop, fault tree and use case diagrams, were produced to investigate the inter-relations of the system elements; to identify the root causes of underperforming PBL agreements; and to explore the relationships of key stakeholders and the system; respectively. For each model presented in the thesis the student discussed the elements and relationships, rationale and traceability to literature and/or the questionnaire.

These models became the basis of a set of guideline requirements for a PBL contract. Using the findings of the earlier work in the project the modelling was completed by building a reference model in SysML. The reference model was validated through the RT evaluation.

Red-Team Method Application to the Project A RT was formed of respondents to the questionnaire who had indicated interest in further contributing to the project in order to provide model validation. The RT work was prompted with the questions: Is there something missing?; Is there something that you believe should not be there?; and Do the relationships show the right set of relationships? The model was revised in the light of the critique received and resubmitted to the RT for the final round of evaluation.

Red-Team Challenge Initially four agreed to participate in the RT but only one was able to provide their feedback in time. Therefore, the review of the model was conducted by one specialist, a navy officer with experience in procurement and Integrated Logistics Support; and was limited by that person's viewpoint.

The RT was only involved in the final stage, the development of the reference model, rather than the developmental models and diagramming of the earlier stage of the project. This may lead to the RT only having a partial view of the overall system context, problems and mechanisms. Although the student evaluated the developmental representation models and refined the key elements and relationships from them to derive the reference model, a RT may have had different views. Involving

the RT at an earlier stage would strengthen the final reference model. As emphasized by Wood and Duggan (2000), "timing is everything, and to have an effective impact, the RT must be involved throughout design and development.

DISCUSSION

We now identify the conclusions arising from the two case studies to determine the value of the RT method of validation of student thesis projects.

Observed challenges

Both case study projects were performed by full-time students, whose thesis work, after some preliminary work to identify the topic and plan the project, starts in mid-May and ends ten weeks later. The limited available time severely constrains any project and makes a method involving gaining a considered response from a sympathetic person high risk. This also makes it particularly difficult to have a method which requires multiple rounds of response and modification.

Finding suitable RT members is challenging because of the combination of difficulties: finding people willing to participate; the ability of participants to understand adequately the materials to which they are asked to respond; and participants who can suitably communicate their views. The combination of these challenges introduces another challenge, the tendency to invite responses from a convenient, rather than an expert, sample: an effect we call the "friends and family" challenge, which overcomes the risk of no response at the risk of obtaining response from people lacking the appropriate depth of knowledge of the subject matter.

Observations of red-teaming

The two case study projects have a common characteristic; both were projects to develop a method or process to do something for improving the system under consideration. Both involved preparatory work to discover views of the current situation followed by development of a proposed process or model. The project performer could evaluate the proposed method by a desk process. However, that approach to validation would be limited by not introducing any new idea in the evaluation. Such an approach to validation of a project to create something would represent circular reasoning.

The RTing method is very useful to validate the newly developed method or process, the proposed changes of the system under consideration in SE thesis research. The advantage of the RT approach is that the person entering the project only as an evaluator has an independent view that enables critique independent of how the project produced its products and the scenarios addressed in their development. This enables development of a revised proposal that improves the validity of the method or process proposed. There are two risks to the independence of thought of the RT member: limited competence in the project subject; and common background, ethnic or workplace culture, which makes it difficult for the evaluator to exercise fundamentally independent thought, which therefore reduces the effectiveness of RTing.

Another issue is related to repeatability of the research since different background, experience, expertise and even immediate effects at the time of doing the evaluation of RT members may lead to different critique contributions. Therefore, it is important to plan and form a strong RT with sufficient background and experience in the project subject matter. Having diversity of members' expertise is desirable, since one important assumption is "diverse team members deliver the best result" (Wood and Duggan, 2000), justified on the grounds that diversity of RT members will result in an increase range of ideas of methods to challenge the proposal.

CONCLUSIONS

All research requires a method for validation of what is claimed to be the knowledge developed through the conduct of the project. In some types of projects, predominantly those that attempt to make discoveries about the state or properties of something, the validation is achieved through application of specific data collection and analysis methods.

Another class of project, which is quite common for students who are sponsored by employers who seek to have their students produce something of value in their workplace, is the 'creative' project. A 'creative' project is one in which the intended output is a development of something, a thing or a process, essentially a design. A thesis, of the scale of work that is achievable in a Masters by coursework degree, can only advance 'designs' in the design space, and therefore can result in a forward path exploration of the situation to be addressed, a design process and a distinct review activity of a design review type. There is not time to build and test anything. Therefore, empirical results of the performance of the design are not feasible. Any design review must apply an independent view of the designed entity, which cannot be achieved in the case of a student doing design and their own desk review of that design because of the lack of independent vision of the project.

RTing provides a method for a student to obtain critique of a 'design' from an independent viewpoint in a time constrained project. The RT method is much faster to perform than a method in which the findings are implemented in the form of an executable model that can have response to stimuli tested. The RT generated data is of a kind like the student will receive later in their career, so there is educational value in constructing a thesis project in this form, and the data will be significantly challenging to interpret to represent a significant part of the project.

RTing is a useful validation methodology in the case of thesis projects in which the goal is to design a thing or process to address a specific need.

References

Baiardi, F. (2019) 'Avoiding the weaknesses of a penetration test', *Computer fraud & security*, (4), pp. 11–15.

Carrison, D. (2010) 'Learning risk management from engineers', *Industrial engineer*, 42(10), pp. 42–46.

Checkland, P. (1981) *Systems thinking, systems practice*. Chichester Sussex ; New York: J. Wiley.

Clark, S. S. *et al.* (2015) 'Empirical evaluation of the A3 environment: Evaluating defenses against zero-day attacks', in *10th international conference on availability, reliability and security*. Toulouse, pp. 80–89.

Conway, P. (2012) 'Red team: How the Neoconservatives helped cause the Iraq intelligence failure', *Intelligence and national security*, 27(4), pp. 488–512.

Craft, R. L. (2017) 'Red teaming in the age of IOT thoughts on framing the next generation of technical vulnerability assessment', in *12th system of systems engineering conference*. Waikaloa, Hawaii.

Dancy, J. (1985) *An introduction to contemporary epistemology*. Oxford: Basil Blackwell Ltd.

Davendralingam, N. *et al.* (2015) 'Scitentific foundations for systems engineering - challenges and strategies', in *Proceedings of the ASME 2015 international design engineering technical conferences & computers and information in engineering conference*. Boston, Massachusetts, pp. 1–9.

Deckard, G. M. and Camp, L. J. (2016) 'Measuring efficacy of a classroom training week for a cybersecurity training exercise', in *IEEE symposium on technologies for homeland security*.

Development Concepts and Doctrine Centre (2013) *Red teaming guide*. 2nd edn. Shrivenham, Wiltshire: Ministry of Defence.

Farar, A., Bahsi, H. and Blumbergs, B. (2017) 'A case study about the use and evaluation of cyber deceptive methods against highly targeted attacks', in *International conference on cyber incident*

response, coordination, containment and control.
Fenton, M. (2016) 'Restoring executive confidence: Red team operations', *Network security*, (11), pp. 5–7.
Ferris, T. L. J. (1997) 'The concept of leap in measurement interpretation', *Measurement*, 21(4), pp. 137–146.
Ferris, T. L. J. (2009) 'On the methods of research for systems engineering', in *7th annual conference on systems engineering research*. Loughborough, UK.
Graham, M. N. and Graham, J. L. (2016) 'Thraining the next generation analyst using red cell analytics', in *Proceedings of SPIE 9851, Next generation analyst IV*. Baltimore, Maryland. doi: 10.1117/12.2224077.
Haigh, J. T. *et al.* (2009) 'Trapping malicious insiders in the SPDR web', in *Proceedings of the 42nd Hawaii international conference on system sciences*, pp. 1–10.
Heckman, K. E. *et al.* (2013) 'Active cyber defense with denial and deception: A cyber-wargame experiment', *Computers & Security*, 37, pp. 72–77.
Helsinger, A., Ferguson, W. and Lazarus, R. (2001) 'Exploring large-scale, distributed system behavior with a focus on information assurance', in *Proceedings - DARPA information survivability conference and exhibition*, pp. 273–286.
Holland, B., Deering, T. and Kothari, S. (2015) 'Security toolbox for detecting novel and sophisticated Android malware', in *IEEE/ACM 37th IEEE international conference on software engineering*. Florence, Italy, pp. 733–736.
INCOSE (2022) *Systems engineering*. Available at: https://www.incose.org/systems-engineering (Accessed: 1 March 2022).
Kewley, D. L. and Bouchard, J. F. (2001) 'DARPA information assurance program dynamic defense experiement summary', *IEEE transactions on systems, man, and cybernetics - part A: systems and humans*, 31(4), pp. 331–336.
Kont, M. *et al.* (2017) 'Frankenstack: toward real-time red team feedback', in *IEEE military communications conference*, pp. 400–405.
Kraemer, S., Carayon, P. and Clem, J. (2009) 'Human and organizational factors in computer and informaiton security: Pathways to vulnerabilities', *Computers and security*, 28(7), pp. 509–520.
Lafond, D. and DuCharme, M. B. (2011) 'Complex decision making experimental platform (CODEM): a counter-insurgency scenario', in *IEEE symposium on computational intelligence for security and defense applications*, pp. 72–79.
Van Leeuwen, B. P., Stout, W. M. S. and Urias, V. E. (2016) 'Empirical assessment of network-based moving target defense approaches', in *IEEE military communications conference*.
Levin, D. (2003) 'Lessons learned in using live red teams in IA experiments', in *Proceedings of the DARPA information survivability conference and exposition*, pp. 1–10.
Machado, R. C. (2018) *A systems approach to performance based logistics (PBL) applied to warships support*. Cranfield University.
Mansfield-Devine, S. (2018) 'The best form of defence - the benefits of red teaming', *Computer fraud & security*, (October), pp. 8–12.
Mattsson, T. (2018) *Applying agile principles in the Fiinish Defence Forces aquisition projects*. Cranfield University.
Mercer, G. (2017) 'Reasonable doubts: foreseeing failures in WMD security', *The nonproliferation review*, 24(1–2), pp. 185–193. doi: 10.1080/10736700.2017.1367079.
Mirkovic, J. *et al.* (2008) 'Testing a collaborative DDoS defense in a red team/blue team exercise', *IEEE transactions on computers*, 57(8), pp. 1098–1112.
Moses, S. and Rowe, D. C. (2015) 'The SNAP principle for mitigating privileged account breaches: How secondary non-admin privileged accounts can reduce breach impact', in *World congress on internet security*, pp. 32–38.
Pal, P. *et al.* (2012) 'Cooperative red teaming of a prototype survivable service-oriented system', in *IEEE military communications conference*.
Porter, S. *et al.* (2014) 'Breaking into BIM: Performing static and dynamic security analysis witht he

aid of BIM', *Automation in construction*, 40, pp. 84–95. doi: 10.1016/j.autocon.2013.12.002.
Pyster, A. *et al.* (2015) *Graduate Reference Curriculum for Systems Engineering (GRCSE^{TM}) V1.1*. Hoboken, NJ, USA: Trustees of the Stevens Institute of Technology.
Rajendran, J., Jyothi, V. and Karri, R. (2011) 'Blue team red team approach to hardware trust assessment', in *IEEE international conference on comuter design: VLSI in computers and processors*, pp. 285–288.
Ranjeet, T. R. *et al.* (2011) 'Analysis of key installation protection using computerized red teaming', in *Conferences in research and practice in informaiton technology series, no 113*, pp. 137–144.
Rastegari, S. *et al.* (2013) 'Testing a distributed denial of service defence mechanism using red teaming', in *Proceedings of the 2013 IEEE symposium on computational intelligence for security and defence applications*. Singapore, pp. 23–29.
Rege, A. *et al.* (2017) 'A temporal assessment of cyber intrusion chains using multidiscipplinary frameworks and methodologies', in *International conference on cyber situational awareness, data analytics and assessment*.
Rege, A. *et al.* (2018) 'Predicting adversarial cyber-intrusion stages using autoregressive neural networks', *IEEE intelligent systems*, 33(2), pp. 29–39.
Romyn, D. and Kebbell, M. R. (2014) 'Terrorists' planning of attacks: a simulated "red-team" investigation into decision-making', *Psychology, crime & law*, 20(5), pp. 480–496.
Romyn, D. and Kebbell, M. R. (2018) 'Mock terrorists decisions' concerning use of the internet for target selection: a red-team approach', *Psychology, crime & law*, 24(6), pp. 589–602.
Rosen, M. D., Edwards, J. and Suter, L. J. (2010) 'The National Ignition Campaign (NIC) "blue team/red team" simulated campaigns (Sim-Cams)', in *The sixth international conference on inertial fusion sciences and applications, Journal of physics: conference series 244*.
Rubel, P. *et al.* (2008) 'Effective monitoring of a survivable distributed networked information system', in *The third international conference on availability, reliability and security*, pp. 1306–1312. doi: 10.1109/ARES.2008.188.
SEBoK Contributors (2019) 'Applying life cycle processes', in Cloutier, R. J. (Editor in C. (ed.) *The guide to the systems engineering body of knowledge (SEBoK)*. Hoboken, NJ, USA: The Trustees of the Stevens Institute of Technology.
Tan, Terence *et al.* (2014) 'Computational red teaming for physical security assessment', in *The 4th annual IEEE international conference on cyber technology in automation, control and intelligent systems*. Hong Kong, China, pp. 258–263.
Waksman, A. *et al.* (2014) 'A red team/blue team assessment of functional analysis methods for malicious circuit identification', in *Proceedings - design automation conference*. San Francisco, California.
Wood, B. J. and Duggan, R. A. (2000) 'Red teaming of advanced information assurance concepts', in *Proceedings - DARPA information survivability conference and exposition*, pp. 112–118.
Yang, A., Abbass, H. A. and Sarker, R. (2006) 'Characterizing warfare in red teaming', *IEEE Transactions on systems, man, and cybernetics - part B: cybernetics*, 36(2), pp. 268–285. doi: 10.1109/TSMCB.2005.855569.
Zeng, F. *et al.* (2011) 'High-dimensional objective-based data farming', in *IEEE symposium series on computational intelligence for security and defense applications*, pp. 80–87.
Zhang, X. *et al.* (2013) 'A study on the effectiveness of trojan detection techniques using a red team blue team approach', in *IEEE 31st VLSI test symposium*. Berkeley, California.

Biography

Timothy L.J. Ferris received the degrees B.E.Hons, University of Adelaide, B.Th., Flinders University, B.Litt.Hons., Deakin University, GradCertEd, Queensland University of Technology, and PhD, University of South Australia, 1997. His PhD was in the theory of measurement. He worked as an engineer for Electricity Trust of South Australia and Morrison Court Pty Ltd and University of South Australia. He is currently working with Cranfield University, UK. He has published about 150 papers in journals and conferences and various other items.

Fanny Camelia received the degrees B.Eng, in industrial engineering, Andalas University, Indonesia, in 2003, M.PrjMgmt (Adv) Defence, in applied project management advanced defence, University of Adelaide, Adelaide, South Australia in 2011 and Ph.D. in systems engineering, University of South Australia, Mawson Lakes, Australia. She is currently working as a Senior Research Fellow at the Centre for Systems and Technology Management, Cranfield University, Cranfield University, Cranfield, UK. Her current research interests include systems thinking, systems engineering, engineering education and project management.

Tuomas Mattsson received the degrees MSc in military sciences, The National Defense University, Finland, in 2007 and MSc in systems engineering, Cranfield University, Shrivenham, UK, 2019. He is currently working as a senior staff officer in support for naval strategic acquisition projects, Logistics Sector, Naval Command Finland, The Finnish Defence Forces. Before working in the Naval Command, he was the section chief of Maintenance, supply and procurement with Coastal Fleet Headquarters and Coastal Brigade headquarters between 2012-2017. Earlier in his military career, he has worked as a chief engineer on board several Finnish Naval vessels and taken part in peacekeeping operations as the chief of operational maintenance and logistics.

Rogério C. Machado received degrees B.Eng, in Electrical Engineering, Universidade Federal de Juiz de Fora, Brazil, 2007 and MSc, in Systems Engineering for Defence Capability, Cranfield University, UK, 2019. Having joined the Brazilian Navy's Engineering Corps in 2009, Mr. Machado has been involved in many life cycle processes, including: requirement formulation, procurement, construction, integration, test and maintenance. He is currently working as Integrated Logistic Support Manager within the Navy's Program Management Directorate, Brazilian Navy, Rio de Janeiro, Brazil.

Red-teaming as a research validation method for systems engineering thesis students

Ferris, Timothy L. J.

2022-07

Ferris TLJ, Camelia F, Mattsson T, Machado RC. (2022) Red-teaming as a research validation method for systems engineering thesis students. In: 32nd Annual INCOSE International Symposium, 25-30 June 2022, Detroit, MI, USA, pp. 529-544

https://doi.org/10.1002/iis2.12947