The Stability Model:
An Interactive Framework for Measuring Robustness and Resiliency in Military Command and Control Systems

Madjid Tavana, Department of Business Systems and Analytics, La Salle University, Philadelphia, PA, USA

Dawn A. Trevisani, Resilient Synchronized Systems Branch, Air Force Research Laboratory, Rome, NY, USA

Jerry L. Dussault, Resilient Synchronized Systems Branch, Air Force Research Laboratory, Rome, NY, USA

ABSTRACT

The increasing complexity and tight coupling between people and technology in military Command and Control (C2) systems has led to greater vulnerability due to system failure. Although system vulnerabilities cannot be completely eliminated, the accidental or anticipated failures have to be thoroughly understood and guarded. Traditionally, the failure in C2 systems has been studied with resiliency and the concept of self-healing systems represented with reactive models or robustness and the concept of self-protecting systems represented with proactive models. The authors propose the stability model for simultaneous consideration of robustness and resiliency in C2 systems. Robustness and resiliency are measured with multiple criteria (i.e. repair-recovery times and repair-recovery costs). The proposed interactive framework plots the robustness and resiliency measures in a Cartesian coordinate system and derives an overall stability index for various states of the C2 system based on the theory of displaced ideals. An ideal state is formed as a composite of the best performance values and a nadir state is formed as a composite of the worst performance values exhibited by the system. Proximity to each of these performance poles is measured with the Euclidean distance. The C2 system should be as close to the ideal state as possible and as far from the nadir state as possible. The stability index is a composite measure of distance from the ideal and nadir states in the C2 system. The authors present a case study at the Air Force Research Laboratory to demonstrate the applicability of the proposed framework and exhibit the efficacy of the procedures and algorithms.

Keywords: *Command and Control, Resiliency, Robustness, Stability Index, Theory of Displaced Ideal, United States Air Force*

DOI: 10.4018/jitpm.2013040102

INTRODUCTION

Military organizations are composed of human operators interacting in structured relationships with technology towards the fulfillment of specific objectives. The increasing complexity and tight coupling between man and machines in military Command and Control (C2) systems has led to greater vulnerability due to system failure. Charles Perrow (1984) has described the function of any man-machine system along two clearly distinct dimensions of *interaction* and *coupling*.

Interaction refers to the number and nature of the connections between the components of a system. Linear interactions describe highly structured systems which are logical, sequential and planned. They function as a series of expected events in a predictable sequence. Flaws in one component can be identified and corrected with little disturbance to the overall system. On the other hand, flaws in complex interactions are not visible, and often cannot be comprehended as they unfold. Complex interactions involving unfamiliar, unplanned, unexpected and unforeseeable sequences influence the system's robustness (the ability to avoid failure).

Coupling refers to how quickly and explosively a change in one component of an organization is felt in another. The components of a system are coupled (or joined together) loosely when they are not very dependent on each other. The components are coupled tightly when the parts are highly interdependent. In tightly coupled systems a change in one component rapidly affects the status of other components and influences the system's resiliency (or ability to recover).

The interaction and coupling, whether by design or inadvertently, determine the system's susceptibility to vulnerabilities and make failures not only inevitable but normal. A system accident can be very easy to see in hindsight, but very difficult to see in foresight. Ahead of time, there are simply too many possible action pathways to seriously consider all of them. Therefore, C2 systems are subject to higher failure rates because the complex interactions among their components cannot be thoroughly planned, understood, anticipated and guarded against. In addition, the C2 systems coordinate execution of logically related tasks. Since vulnerabilities cannot be completely eliminated in a C2 system and preventive measures sometimes fail, the C2 system may be subject to intentional malicious attacks. A malicious attacker may create a prohibited task or corrupt an existing task in the C2 systems. This malicious act may trigger some other tasks in the system due to the existence of complex interactions.

Robustness, a *proactive* concept, is the ability of the system to avoid failure, and resiliency, a *reactive* concept, is the ability of the system to recover from failure once it occurs. Although the ability to avoid and recover from failure is important in many complex systems, the idea of self-protecting and self-healing systems is frequently discussed independently in the literature (Dragoni et al., 2009). We argue that typical precautions focusing on robustness *or* resiliency is inadequate and may help create new categories of failures in complex systems. In this paper, we consider both the proactive and reactive concepts and propose an interactive framework for simultaneous consideration of robustness and resiliency in military C2 Systems. The proposed framework plots the robustness and resiliency measures in a Cartesian coordinate system and derives an overall *stability index* for various states of the C2 system based on the theory of displaced ideals. Robustness and resiliency are measured with multiple criteria (i.e. repair-recovery costs and repair-recovery completion times). An ideal state is formed as a composite of the best performance values and a nadir state is formed as a composite of the worst performance values exhibited by the system. Proximity to each of these performance poles is measured with the Euclidean distance. The C2 system should be as close to the ideal state as possible and as far from the nadir state as possible. The stability index is a composite measure of distance from the ideal and nadir states of the C2 system.

This paper is organized as follows. In the next section, we review the literature on resiliency and robustness in organizations in general and in military C2 systems in particular. We then describe the interactive stability model proposed in this study. Following this description, we present a case study at the Air Force Research Laboratory to demonstrate the applicability of the proposed framework and exhibit the efficacy of the procedures and algorithms. The last section presents an overall summary of the study and lists avenues for future research.

LITERATURE REVIEW

A workflow (or process) management system is concerned with the coordinated execution and automation of a set of activities or tasks by different processing entities according to a pre-defined set of rules (Casati et al., 1995). An activity is a logical step or description of a piece of work that contributes toward the accomplishment of a process. While workflow may be manually organized, in practice most workflows involve computer systems that support control, management and collaboration among business processes and activities (Bae et al., 1999). Workflow management is often associated with business process re-engineering where a complex system (i.e. military C2 system) is reduced to a basic form through a categorization procedure. The categorization procedure breaks up work into activities which can then be automated. The processes of categorization and automation have raised numerous challenges in military C2 systems. Workflow systems have been suggested as one way to manage these challenges (Agostini et al., 1994). Different workflow modeling techniques have been adopted by many organizations to: (1) assign the required human resources and artifacts for executing each task; (2) control the business flows of tasks; and (3) effectively monitor the executions of tasks (Tsai et al., 2010).

There are two general categories of workflow management systems including communication-based and activity-based techniques (Mentzas et al., 2001; Liu & Shen, 2003). The communication-based techniques assume that the objective of business process reengineering is to improve customer satisfaction (Winograd & Flores, 1987). In contrast, the activity-based techniques focus on modeling the tasks involved in a process and their dependencies (McCarthy & Sarin, 1993). Jablonski and Bussler (1996) have identified five perspectives for a comprehensive workflow model:

- **Functional:** what has to be executed?
- **Operational:** how is a workflow implemented?
- **Behavioral:** when is a workflow executed?
- **Informational:** what data elements are consumed and produced?
- **Organizational:** who is required to execute a workflow?

Despite their popularity and wide-spread application, workflow management systems still suffer from lack of standards and an agreed-upon modeling method (Salimifard & Wright, 2001). Van der Aalst et al. (1994) have criticized that workflow management systems have: (1) no needed functionality; (2) no clear set of definitions; and (3) no general conceptual framework. The idea of self-protecting and self-healing systems is frequently discussed in relation to computer networks, but it has not been addressed thoroughly in other contexts despite its potential relevance (Dragoni et al., 2009). For example, military operations are highly interactive and complex systems that require efficient and effective C2 to be successful. The interactive complexity and tight coupling between people and technological systems has been increasing in military operations, which leads to unpredictability of operations and inevitably to failures.

Robustness is a property intimately associated with the organizations' capacity to avoid failure while resiliency is the organization's ability to recover from failure. A deep understanding of robustness and resiliency has emerged from the study of many complex systems such as nuclear power production, avia-

tion, space exploration, healthcare, air traffic control and chemical production (Gauthier et al., 2006; Perrow, 1999). The major interest in high-reliability organizations comes from their capacity to achieve high performance while operating in hazardous conditions (Weick & Sutcliffe, 2001). Robustness and resiliency involve both technological and organizational concerns. They are the combination of organizational features such as sense-making and training (Weick, 2001) with technological features, such as redundancy, protection systems, and good engineering design (Leveson et al., 2009). The recent studies on robustness and resiliency emphasize the integration between the organizational and technological views in complex socio-technical systems (Hollnagel et al., 2006; Tavana et al., 2011a, 2011b). A good balance between robustness and resiliency should be envisaged (Nomura et al., 1998). Robustness is important to keep the organization under control; resiliency is necessary to react to hazards.

THE STABILITY MODEL

The proposed stability model simultaneously considers the time and cost attributes in a C2 system. We use the system completion time, with its corresponding repair and recovery times, and the system completion cost, with its corresponding repair and recovery values to measure robustness and resiliency in the C2 systems. The system completion time is the total *repair times* of all the activities when measuring robustness and the total *recovery times* of all the activities when measuring resiliency. There are also costs associated with each activity in the C2 system. These costs may characterize man-hours or computer systems. We consider the repair costs of all activities when measuring robustness and the recovery costs of all activities when measuring resiliency. A C2 system may involve a large number of activities. These activities are generally grouped together and categorized as missions, projects, jobs, etc. We refer to a group of homogeneous activities in a C2 system as a *process*. The algorithm proposed in this study consists of the following steps:

Step 1: Normalize Values

The multiple criteria (i.e. repair-recovery times and repair-recovery costs) are normalized so that each attribute value i over each process j is between 0 and 1. Let the decision matrix X consist of m attribute values over n processes. The normalized matrix transforms the X matrix. We identify the minimum x_i^- and the maximum x_i^+ for processes $j = 1,2,...,n$. Each attribute value x_{ij} for $j = 1,2,...,n$ can be normalized by the following formula:

$$y_{ij} = \frac{x_{ij} - x_i^-}{x_i^+ - x_i^-} \quad (1)$$

which yields values between 0 and 1.

Step 2: Determine Importance Weights

The importance weights in multi-criteria decision making (MCDM) reflect the relative importance of the attributes. These m weights w_i will be between 0 and 1 $\left(0 \le w_i \le 1\right)$ and will have a sum of 1: $\left(\sum_{i=1}^{m} w_i = 1\right)$

Step 3: Calculate Weighted Normalized Ratings

The weighted normalized values are calculated as follows:

$$u_{ij} = w_i \cdot y_{ij} \quad (2)$$

Step 4: Compute Overall Scores

The overall score (i.e. total score for repair-recovery costs and repair-recovery times) of each process is calculated as follows:

$$z_j = \sum_{i=1}^{m} u_{ij} \tag{3}$$

Step 5: Standardize Ratings

The overall scores of the processes are standardized to ensure that each overall score is between 0 and 1. We identify the minimum z_j^- and the maximum z_j^+ for processes $j = 1,2,...,n$. Each overall score z_j for $j = 1,2,...,n$ can be normalized by the following formula:

$$v_j = \frac{z_j - z_j^-}{z_j^- - z_j^+} \tag{4}$$

Step 6: Identify Ideal and Nadir Solutions

The theoretical ideal solution consists of normalized values of 1 over all the attributes and the nadir solution consists of normalized values of 0 over all the attributes. However, in this study, we use the practical ideal and nadir solutions. The practical ideal solution consists of normalized values of the "best process" and the practical nadir solution consists of normalized values of the "worst process" as follows:

$$A^+ = \left\{v_1^+, v_2^+, ..., v_i^+, ..., v_n^+\right\} \tag{5}$$

where v_i^+ is the best value for the $i-th$ attribute among all processes:

$$A^- = \left\{v_1^-, v_2^-, ..., v_i^-, ..., v_n^-\right\} \tag{6}$$

where v_i^- is the worst value for the $i-th$ attribute among all processes.

Step 7: Compute Distances

The weighted distance from the ideal solution (D_j^+) and the weighted distance from the nadir solution (D_j^-) are computed as follows:

$$D_j^+ = \sqrt{\sum_{1}^{n}\left(u_{ij} - v_i^+\right)^2} \tag{7}$$

$$D_j^- = \sqrt{\sum_{1}^{n}\left(u_{ij} - v_i^-\right)^2} \tag{8}$$

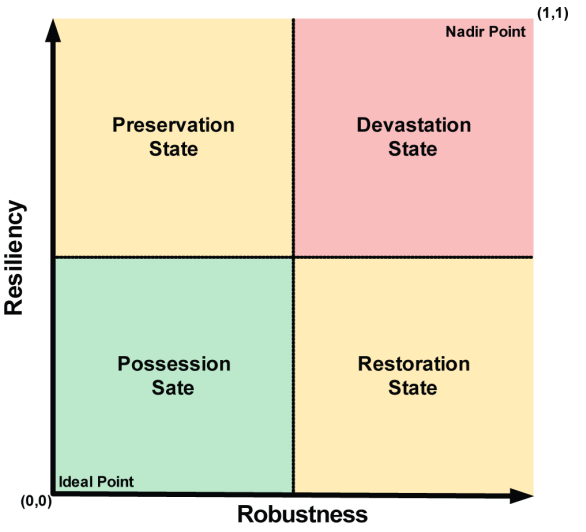
Step 8: Calculate Closeness Coefficient

The relative closeness coefficient, called the sustainability index (S_j) here, considers the distances from the ideal and the nadir solutions simultaneously as follows:

$$S_j = \frac{D_j^-}{D_j^- + D_j^+} \tag{9}$$

The stability index is a composite measure of distance from the ideal and nadir states in the C2 system. The C2 system should be as close to the ideal state as possible and at the same time, as far from the nadir state as possible. With the ideal, nadir, and normal states of the C2 system identified through professional judgment, or available empirical data, all the robustness and resiliency scores are plotted on a Cartesian coordinate system. The robustness scores are plotted on the *x*-axis and the resiliency scores are plotted on the *y*-axis. The normal (threshold) robustness and resiliency scores divide this plane into four quadrants, identified as the Possession, Preservation, Restoration and Devastation Quadrants (see Figure 1).

Figure 1. Stability model



- **Possession Quadrant:** Systems in this quadrant are both robust and resilient. They are unlikely to encounter obstacles that will disable them. However, if they do become disabled, the system can recover without significant difficulties;
- **Preservation Quadrant:** Systems in this quadrant are robust but not resilient. They are unlikely to fail. However, if an unforeseen disaster occurs, the road to recovery will be long and hard;
- **Restoration Quadrant:** Systems in this quadrant are resilient but not robust. They are likely to fail. However, when they fail, they can recover without significant difficulties;
- **Devastation Quadrant:** Systems in this quadrant are neither robust nor resilient. They are very susceptible to failure, and once they have failed, recovery is difficult.

CASE STUDY

In this notional case study, we consider a surveillance operation by an Unmanned Aerial Vehicle (UAV) in the C2 center. In this operation, a flight plan is approved and all the preliminary surveillance activities such as organizing with the Federal Aviation Administration (FAA) and checking the weather conditions are completed. At the execution time, the UAV pilot receives the flight plan and does all the necessary checks. The pilot flies the UAV to the final waypoint (the place that the surveillance target was last seen). The surveillance target is identified and the pilot reports back to the UAV commander to get confirmation that this is the right target for surveillance. Once the target is verified, the UAV commander authorizes the pilot to maintain visible surveillance of the target for a pre-defined period. The UAV pilot maintains the surveillance and the tracking operation of the target for the assigned time period and then returns the UAV to base. Other actors participating in the UAV air operations in the C2 center include: operations controller, order productions officer, duty officer and senior watch officer. The senior watch officer looks for problems and notifies the UAV pilot and commander of these problems. The duty officer and the order productions officer usually come up with a fix and the duty officer is the supervisor who approves the fix.

The non-contested normal environment process presented in Table 1 is composed of six activities (i.e. get flight plan (a), fly to final waypoint (b), acquire target (c), confirm target (d), monitor target (e) and return to base (f)). Activity (a) requires 2 hours of system time on the primary network by the operations controller (1 hour) and the UAV commander (1 hour). Activity (b) requires 3 hours of the UAV pilot to fly the UAV to the final waypoint using the primary system. Activity (c) demands 1 hour of the order productions officer to acquire the target with the primary system. Activity (d) involves target confirmation and requires 30 minutes of the duty officer and 30 minutes of the senior watch officer on the primary network system. In activity (e), the UAV pilot monitors the target for approximately 60 minutes using the primary system. Finally, in activity (f), the UAV pilot uses the primary network to return the UAV back to the base. The entire process requires a total of 11 man-hours and 10.5 primary system hours.

We carefully studied this system with the potential actors and learned that if everything goes well and according to the plans, it is possible to complete these activities with 6.25 man-hours and 6.25 primary system hours as shown in the non-contested ideal environment presented in Table 2. In contrast, we learned that if everything goes wrong, it is possible that we would need 20 man-hours and 19 primary system hours to complete these activities in the fully-contested nadir environment presented in Table 3. The data presented in Tables 2 and 3, established the basis for the ideal and nadir states in this case study.

Initially, we considered two processes to demonstrate the applicability of the proposed framework and exhibit the efficacy of the procedures and algorithms proposed in this study. In Process 1, we study the example presented earlier in a contested environment with off-course UAV due to application malware in the fly to the final waypoint task (Activity (b)). First, we consider the resiliency and the ability of the system to recover from this failure with the manual intervention case presented in Table 4. In this case, the operations controller and the duty officer need to spend 30 minutes of their time to intervene and fix this failure with the primary network. As a result of this manual intervention, the total recovery involves 2 additional primary system hours and 3 additional man-hours. As shown in Table 4, the contested environment with manual intervention requires

Table 1. Non-contested normal environment

Activity	Human System (Man Hours)						Computer System (Machine Hours)
	Operations Controller	Order Productions Officer	Duty Officer	UAV Pilot	UAV Commander	Senior Watch Officer	Primary Network
(a) Get flight plan	1				1		2
(b) Fly to final waypoint				3			3
(c) Acquire target		1					1
(d) Confirm target			0.5			0.5	0.5
(e) Monitor target				1			1
(f) Return to Base				3			3
Total	1	1	0.5	7	1	0.5	10.5 primary system hours 11 man-hours

Table 2. Non-contested ideal environment

Activity	Human System (Man Hours)						Computer System (Machine Hours)
	Operations Controller	Order Productions Officer	Duty Officer	UAV Pilot	UAV Commander	Senior Watch Officer	Primary Network
(a) Get flight plan	0.5				0.5		1
(b) Fly to final waypoint				2			2
(c) Acquire target		0.5					0.5
(d) Confirm target			0.5			0.25	0.75
(e) Monitor target				0.5			0.5
(f) Return to Base				1.5			1.5
Total	0.5	0.5	0.5	4	0.5	0.25	6.25 primary system hours 6.25 man-hours

Table 3. Fully-contested nadir environment

Activity	Human System (Man Hours)						Computer System (Machine Hours)
	Operations Controller	Order Productions Officer	Duty Officer	UAV Pilot	UAV Commander	Senior Watch Officer	Primary Network
(a) Get flight plan	1				1		2
Troubleshooting (a)	0.5	0.5					1
(b) Fly to final waypoint	1				1		2
Troubleshooting (b)				4			4
(c) Acquire target		1					1
Troubleshooting (c)		1					1
(d) Confirm target			0.5			0.5	0.5
Troubleshooting (d)			0.5			0.5	0.5
(e) Monitor target				1			1
Troubleshooting (e)			1				1
(f) Return to Base				3			3
Troubleshooting (f)	1					1	2
Total	3.5	2.5	2	8	2	2	19 primary system hours 20 man-hours

Table 4. Contested environment with off-course UAV in process 1 - manual intervention

Activity	Human System (Man Hours)						Computer System (Machine Hours)
	Operations Controller	Order Productions Officer	Duty Officer	UAV Pilot	UAV Commander	Senior Watch Officer	Primary Network
(a) Get flight plan	1				1		2
(b) Fly to final waypoint				4			4
Troubleshooting (b)	0.5		0.5			1	1
(c) Acquire target		1					1
(d) Confirm target			0.5			0.5	0.5
(e) Monitor target				1			1
(f) Return to Base				3			3
Total	1.5	1	1	8	1	1.5	12.5 primary system hours 14 man-hours

Note: All human operators use computer systems except for the Senior Watch Officer

12.5 primary system hours and 12 man-hours to complete all the activities associated with our example.

Next, we considered the robustness and the ability of the system to avoid this failure with the automated intervention case presented in Table 5. A secondary network system is used to back-up the primary network system and avoid failure. As shown in Table 5, the contested environment with automated intervention requires 7.5 primary system hours, 3.25 secondary system hours and 11.25 man-hours to complete all the activities associated with our example.

In Process 2, we study the C2 system in a contested environment with off-course UAV due to application malware in the "fly to the final waypoint" (Activity b) and the return to base (Activity f). First, we considered the resiliency and the ability of the system to recover from this failure with the manual intervention case presented in Table 6. As shown in this table, the contested environment with manual intervention requires 15.5 primary system hours and 16 man-hours to complete all the activities associated with our example.

Next, we considered the robustness and the ability of the system to avoid this failure with the automated intervention case presented in Table 7. A secondary network system is used to back-up our primary network system. As a result of this automated intervention, we were able to avoid failure. As shown in this table, the contested environment with automated intervention requires 4.5 primary system hours, 6.5 secondary system hours and 11.5 man-hours to complete all the activities associated with our example.

We then studied the resiliency of the system under the two processes presented in Table 8. In the ideal case (if everything goes as planned) the completion of the activities in the case study requires 6.25 Man-hours. Considering an average hourly labor cost of $100, we incur $625 in labor costs. Given 6.25 primary system hours needed to complete all the activities in this case

Table 5. Contested environment with off-course UAV in process 1 - automated intervention

Activity	Human System (Man Hours)						Computer System (Machine Hours)	
	Operations Controller	Order Productions Officer	Duty Officer	UAV Pilot	UAV Commander	Senior Watch Officer	Primary Network	Secondary Network
(a) Get flight plan	1				1		2	
(b) Fly to final waypoint				3.25				3.25
(c) Acquire target		1					1	
(d) Confirm target			0.5			0.5	0.5	
(e) Monitor target				1			1	
(f) Return to Base				3			3	
Total	1	1	0.5	7.25	1	0.5	7.5 primary system hours 3.25 secondary system hours 11.25 man-hours	

Table 6. Contested environment with off-course UAV in process 2 - manual intervention

Activity	Human System (Man Hours)						Computer System (Machine Hours)
	Operations Controller	Order Productions Officer	Duty Officer	UAV Pilot	UAV Commander	Senior Watch Officer	Primary Network
(a) Get flight plan	1				1		2
(b) Fly to final waypoint				4			4
Troubleshooting (b)	0.5		0.5			1	2
(c) Acquire target		1					1
(d) Confirm target			0.5			0.5	0.5
(e) Monitor target				1			1
(f) Return to Base				3			3
Troubleshooting (f)	1					1	2
Total	2.5	1	1	8	1	2.5	15.5 primary system hours 16 man-hours

and an average hourly computer system cost of $100, we incur $625 in system costs. The total cost of completing all of these activities in an ideal state is $1,250. The same total cost is $3,900 in case everything goes wrong (nadir state) and $2,150 under normal circumstances. The total costs of the ideal, nadir and normal states are given in Table 8 along with the total costs for Processes 1 and 2.

We then asked the actors in this case study to estimate the importance weight of the time and cost considerations in the C2 operations.

Table 7. Contested environment with off-course UAV in process 2 - automated intervention

Activity	Human System (Man Hours)						Computer System (Machine Hours)	
	Operations Controller	Order Productions Officer	Duty Officer	UAV Pilot	UAV Commander	Senior Watch Officer	Primary Network	Secondary Network
(a) Get flight plan	1				1		2	
(b) Fly to final waypoint				3.25				3.25
(c) Acquire target		1					1	
(d) Confirm target			0.5			0.5	0.5	
(e) Monitor target				1			1	
(f) Return to Base				3.25				3.25
Total	1	1	0.5	7.5	1	0.5	4.5 primary system hours 6.5 secondary system hours 11.5 man-hours	

Table 8. Resiliency and robustness data for processes 1 and 2

Attribute	Ideal	Nadir	Normal	Process 1		Process 2	
				Manual Recovery	Automated Repair	Manual Recovery	Automated Repair
Man-hours	6.25	20	11	14	11.25	16	11.5
Labor costs	625	2000	1100	1400	1125	1600	1150
Primary system hours	6.25	19	10.5	12.5	7.5	15.5	4.5
Primary System costs	625	1900	1050	1250	750	1550	450
Secondary system hours	0	0	0	0	3.25	0	6.5
Secondary system costs	0	0	0	0	325	0	650
Total Cost	1250	3900	2150	2650	2200	3150	2250

The group agreed that the time consideration is three times more important than the cost consideration. We established a 3 to 1 ratio (or 75% vs. 25%) for the importance weights for the repair-recovery times and repair-recovery costs and found the weighted resiliency and robustness data presented in Table 9.

We then used the normalization procedure prescribed by Equation (1) and computed the normalized resiliency and robustness data for Processes 1 and 2 presented in Table 10.

Next, we used the procedures presented in the proposed framework and found the ideal distance, the nadir distance and the stability

Table 9. Weighted resiliency and robustness data for processes 1 and 2

Attribute	Importance Weight	Ideal	Nadir	Process 1		Process 2	
				Resiliency	Robustness	Resiliency	Robustness
Man-hours	0.75	4.688	15	10.5	8.438	12	8.625
Total Cost	0.25	312.5	975	662.5	550	787.5	562.5

Table 10. Normalized resiliency and robustness data for processes 1 and 2

Attribute	Ideal	Nadir	Process 1		Process 2	
			Resiliency	Robustness	Resiliency	Robustness
Man-hours	0	1	0.564	0.364	0.709	0.382
Total Cost	0	1	0.528	0.358	0.717	0.377
Total Normalized Weighted Score	0	1	1.092	0.722	1.426	0.759
Total Normalized Standardized Weighted Score	0	1	0.546	0.361	0.713	0.380

index of the two processes with Equations (7)-(9). As shown in Table 11, Process 1 is closer to the ideal state and farther away from the nadir state than Process 2. Consequently, the stability index of Process 1 (S_1=0.545) is higher (better) than the stability index of Process 2 (S_2=0.458).

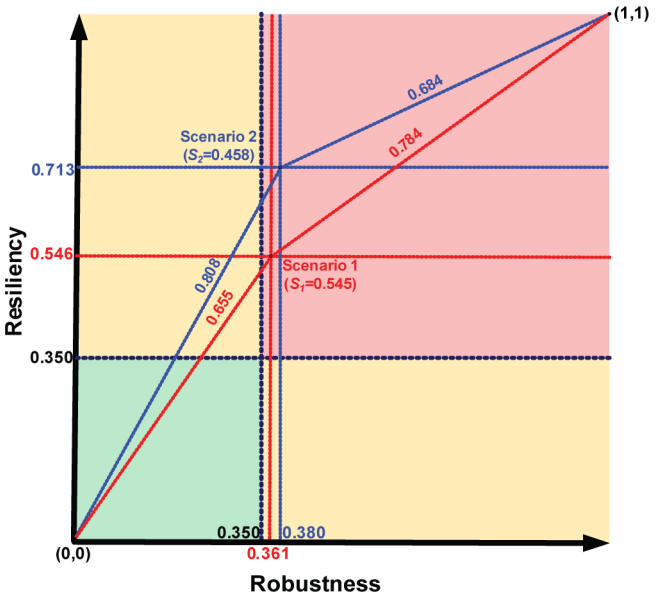
We provide a graphical representation of the two processes in Figure 2. As shown in this figure, the threshold values are set to 0.35 for robustness and 0.35 for resiliency. Process 1 and Process 2 with the robustness scores of 0.361 and 0.380, respectfully, are very similar in terms of their ability to avoid failure. However, Process 1 with a resiliency score of 0.546 is much closer to the ideal state than Process 2 with a resiliency score of 0.713. Therefore, Process 1 is more capable to recover from failure compared with Process 2. As for the Euclidean Distances of the two processes from the ideal and nadir states, Process 1 is closer to the ideal state ($D_1^+ = 0.655$) and farther away from the nadir state ($D_1^- = 0.784$) compared to Process 2 which is farther away from the ideal state ($D_2^+ = 0.808$) and closer to the nadir state ($D_2^- = 0.684$). In addition, the stability index of Process 1 (S_1=0.545) is higher than the stability index for Process 2 (S_2=0.458). Finally, both processes fall into the devastation state indicating that these processes are susceptible to failure, and once they have failed, recovery is difficult.

In addition to Processes 1 and 2, we studies 28 additional randomly simulated processes. The robustness and resiliency scores of

Table 11. Stability index for processes 1 and 2

Attribute	Process 1	Process 2
Ideal Distance	0.655	0.808
Nadir Distance	0.784	0.684
Stability Index	0.545	0.458

Figure 2. The stability index graph for processes 1 and 2



the 30 processes along with their ideal distances, nadir distances and stability indexes are shown in Table 12.

The average robustness and resiliency scores of the 30 processes were 0.5 and 0.3, respectively. In addition, the average stability index of the 30 processes was 0.594. Figure 3 presents a scatter chart of the 30 processes considered in this study along with their robustness and resiliency scores in comparison with the threshold and average values. In general, most processes fall into the restoration state indicating that processes in this quadrant are resilient but not robust. They are not capable of avoiding failure but they are capable of recovering if they fail.

CONCLUSION AND FUTURE RESEARCH DIRECTIONS

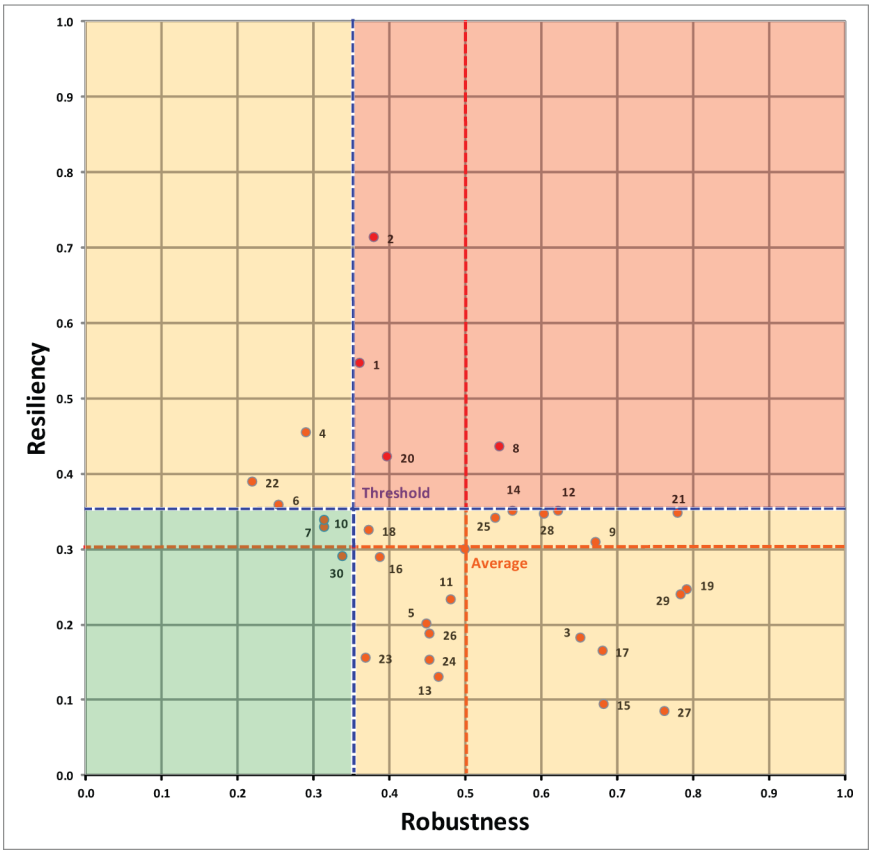
Military organizations use workflow management systems to coordinate their operations, facilitate instant access to accurate and up-to-date data, schedule and synchronize changes and test the effectiveness of their operating procedures and processes. The military C2 systems are subject to higher failure rates because the complex interactions among their components cannot be thoroughly planned, understood, anticipated and guarded against. Several approaches have been suggested in the literature to adequately represent robustness and resiliency in organizations. Despite the importance of developing and maintaining self-protecting and self-healing processes, the simultaneous consideration of robustness and resiliency has received little attention in military C2 systems.

The necessity for readiness and the ability to cope with the possibility and reality of failure in complex systems makes this an important area for future workflow management research. Robustness and resiliency are measured with multiple criteria (i.e. repair-recovery completion times and repair-recovery costs). The cost and time values are measured with crisp and precise numbers. However, the observed cost and time values in real-world military operations are sometimes imprecise or vague. Ideas for future research include:

Table 12. Command and control system performance data for all 30 processes

Process	Robustness	Resiliency	Ideal Distance	Nadir Distance	Stability Index
1	0.361	0.546	0.655	0.784	0.545
2	0.380	0.713	0.808	0.684	0.458
3	0.652	0.182	0.677	0.889	0.568
4	0.290	0.455	0.540	0.895	0.624
5	0.450	0.201	0.493	0.970	0.663
6	0.255	0.359	0.440	0.983	0.691
7	0.314	0.329	0.455	0.960	0.678
8	0.545	0.435	0.698	0.725	0.510
9	0.672	0.309	0.740	0.765	0.508
10	0.314	0.338	0.461	0.953	0.674
11	0.481	0.232	0.534	0.927	0.634
12	0.623	0.350	0.715	0.752	0.513
13	0.465	0.130	0.483	1.022	0.679
14	0.563	0.351	0.663	0.782	0.541
15	0.683	0.094	0.689	0.959	0.582
16	0.388	0.289	0.484	0.938	0.660
17	0.681	0.164	0.701	0.894	0.561
18	0.374	0.325	0.495	0.921	0.650
19	0.793	0.246	0.830	0.782	0.485
20	0.398	0.422	0.580	0.835	0.590
21	0.780	0.347	0.854	0.689	0.446
22	0.220	0.389	0.447	0.991	0.689
23	0.369	0.156	0.401	1.054	0.725
24	0.453	0.153	0.478	1.009	0.678
25	0.540	0.341	0.639	0.804	0.557
26	0.454	0.187	0.491	0.979	0.666
27	0.763	0.085	0.768	0.946	0.552
28	0.604	0.347	0.696	0.764	0.523
29	0.785	0.240	0.821	0.790	0.490
30	0.338	0.290	0.446	0.971	0.685
Average	0.500	0.300	0.606	0.880	0.594
Threshold	0.350	0.350	0.495	0.919	0.650
Ideal	0	0	0.000	1.414	1
Nadir	1	1	1.414	0	0

Figure 3. The stability index graph for all 30 processes



- Capturing the decision makers' subjective judgments by representing inexact cost and time values with fuzzy numbers;
- Incorporating "quality" as a third dimension allowing for an expanded view of monitoring the performance of the C2 system;
- Encompassing a computer implementation of the proposed framework. An automated system will provide the capability for continuous monitoring of the resiliency and robustness in large systems.

In this study, we have built upon the groundwork for the consideration of robustness and resiliency in military C2 systems. We hope that these concepts introduced here will provide inspiration for future research.

ACKNOWLEDGMENT

This research was supported by the U.S. Air Force Research Laboratory grant number FA8750-11-2-0218. The authors would like to thank the anonymous reviewers, the editor, and Alex F. Sisti from the U.S. Air Force Research Laboratory for their insightful comments and suggestions.

REFERENCES

Agostini, A., De Michelis, G., Grasso, M. A., & Patriarca, S. (1994). Re-engineering a business process with an innovative workflow management system: A case study. *Collaborative Computing*, *1*(3), 163–190.

Bae, J. S., Jeong, S. C., Seo, Y., Kim, Y., & Kang, S. (1999). Integration of workflow management and simulation. *Computers & Industrial Engineering*, *37*(1–2), 203–206. doi:10.1016/S0360-8352(99)00055-8.

Casati, F., Ceri, S., Pernici, B., & Pozzi, G. (1995). Conceptual modelling of workflows. In M. Papazoglou (Ed.), *Proceedings of the 14th International Conference on Object-Oriented and Entity-Relationship Modeling* (LNCS 1021, pp. 341-354).

Dragoni, N., Massacci, F., & Saidane, A. (2009). A self-protecting and self-healing framework for negotiating services and trust in automatic communication systems. *Computer Networks*, *53*, 1628–1648. doi:10.1016/j.comnet.2008.07.016.

Gauthier, A., Davis, K., & Schoenbaum, S. (2006). Achieving a high-performance health system: High reliability organizations within a broader agenda. *Health Services Research*, *41*(4), 1710–1720. doi:10.1111/j.1475-6773.2006.00617.x PMID:16898987.

Hollnagel, E., Woods, D., & Levenson, N. (2006). *Resilience engineering: Concepts and precepts*. Hampshire, UK: Hashgate.

Jablonski, S., & Bussler, C. (1996). *Workkfow management: Modeling concepts, architecture and implementation*. London, UK: Thomson Computer Press.

Leveson, N., Dulac, N., & Marais, K. (2009). Moving beyond normal accidents and high reliability organizations: A systems approach to safety in complex systems. *Organization Studies*, *30*(2-3), 227–249. doi:10.1177/0170840608101478.

Liu, D. R., & Shen, M. (2003). Workflow modeling for virtual processes: An order-preserving process-view approach. *Information Systems*, *28*(6), 505–532. doi:10.1016/S0306-4379(02)00028-5.

McCarthy, D., & Sarin, S. (1993). Workflow and transactions in InConcert. *Data Engineering Bulletin*, *16*(2), 53–56.

Nomura, T., Hayashi, K., Hazama, T., & Gudmundson, S. (1998). Interlocus: Workspace configuration mechanisms for activity awareness. In *Proceedings of the Conference on Computer-Supported Cooperative Work*, Seattle, WA (pp. 19-28).

Perrow, C. (1999). *Normal accidents, living with high-risk technologies*. Princeton, NJ: Princeton University Press.

Salimifard, K., & Wright, M. (2001). Petri net-based modelling of workflow systems: An overview. *European Journal of Operational Research*, *134*(3), 664–676. doi:10.1016/S0377-2217(00)00292-7.

Tavana, M., Busch, T. E., & Davis, E. L. (2011a). Modeling operational robustness and resiliency with high-level Petri nets. *International Journal of Knowledge-Based Organizations*, *1*(2), 17–38. doi:10.4018/ijkbo.2011040102.

Tavana, M., Busch, T. E., & Davis, E. L. (2011b). Fuzzy multiple criteria workflow robustness and resiliency modeling with Petri nets. *International Journal of Knowledge-Based Organizations*, *1*(4), 72–90. doi:10.4018/ijkbo.2011100105.

Tsai, C. H., Huang, K. C., Wang, F. J., & Chen, C. H. (2010). A distributed server architecture supporting dynamic resource provisioning for BPM-oriented workflow management systems. *Journal of Systems and Software*, *83*(8), 1538–1552. doi:10.1016/j.jss.2010.04.001.

van der Aalst, W. M. P., van Hee, K. M., & Houben, G. J. (1994). Modelling workflow management systems with high-level Petri nets. In G. De Michelis, C. Ellis, & G. Memmi (Eds.), *Proceedings of the Second Workshop on Computer-Supported Cooperative Work, Petri nets and Related Formalisms* (pp. 31–50).

Weick, K. (2001). *Making sense of the organization*. Oxford, UK: Blackwell.

Weick, K., & Sutcliffe, K. (2001). *Managing the unexpected: Assuring high performance in an age of complexity*. San Francisco, CA: Jossey-Bass.

Winograd, T., & Flores, R. (1987). *Understanding computers and cognition*. Reading, MA: Addison-Wesley.

Madjid Tavana is a Professor of Business Systems and Analytics and the Lindback Distinguished Chair of Information Systems and Decision Sciences at La Salle University where he served as Chairman of the Management Department and Director of the Center for Technology and Management. He has been a Distinguished NASA Research Fellow at Kennedy Space Center, Johnson Space Center, Naval Research Laboratory - Stennis Space Center, and Air Force Research Laboratory. He was recently honored with the prestigious Space Act Award by NASA. He holds an MBA, a PMIS, and a PhD in Management Information Systems and received his post-doctoral diploma in strategic information systems from the Wharton School of the University of Pennsylvania. He is the Editor-in-Chief for Decision Analytics*, the* International Journal of Strategic Decision Sciences*, the* International Journal of Enterprise Information Systems*, and the* International Journal of Applied Decision Sciences*. He has published over one hundred research papers in academic journals such as* Decision Sciences, Information Systems, Interfaces, Annals of Operations Research, Omega, Information and Management, Expert Systems with Applications, European Journal of Operational Research, Journal of the Operational Research Society, Computers and Operations Research, Knowledge Management Research and Practice, Computers and Industrial Engineering, Applied Soft Computing, Journal of Advanced Manufacturing Technology*, and* Advances in Engineering Software*, among others*.

Dawn Trevisani is a Program Manager/Computer Scientist within the Resilient Synchronized Systems Branch at the Air Force Research Laboratory in Rome, New York. She manages modeling and simulation research, experimentation and analysis programs in response to United States Air Force requirements and documented deficiencies. Her focus has been in the area of Integrated Command and Control (C2) Architectures, Operational Level Resiliency, Decision Support Systems and Course of Action Generation and Assessment. She holds a BS in Computer Information Science and an MS in Computer Science from State University of New York - Institute of Technology at Utica/Rome.

Jerry Dussault is the Chief of the Resilient Synchronized Systems Branch at the Air Force Research Laboratory in Rome, New York. He has over 30 years of experience in research, development, and evaluation of Command and Control (C2) Systems, Distributed Fault-Tolerant Computing Technology, Decision Support Software Applications, and Modeling and Simulation. He is a member of the Defense Acquisition Corps, Certified Acquisition Professional SPRDE S&T Manager Level III.