ISBN 978-981-11-7861-0
Proceedings of 2018 the 8th International Workshop on Computer Science and Engineering (WCSE 2018)
Bangkok, 28-30 June, 2018, pp.400-405
doi: 10.18178/wcse.2018.06.070

The Resilience Measure Method to Information Systems

Aimin Luo[+] , YuXiao Kou, Junxian Liu and Tao Chen

[1] Science and Technology on Information systems Engineering Laboratory, National University of Defense Technology, Changsha Hunan 410073, P. R. China

Abstract. Complex information system is always confronted with the various disturbing factors in practical application, and the resilience of the system is one of the important capabilities to deal with the disturbances. The disturbance makes the system capabilities change, and capabilities change reflects the resilience of the system. Through analyzing the response process of the system to the disturbance, a set of resilience evaluation metrics is established based on the change of the system capability. Since the capability is related to the efficiency of the system constitutions, the probability of successfully operation capability under the different condition of constitutions efficiency is taken as the value of the capability. Finally, the quantitative evaluation method of system resilience is provided and verified through case studies.

Keywords: resilience, disruption, capability

1. Introduction

Complex information systems are confronted with various kinds of disturbing factors in actual application, such as the reduction of the reliability of the constitute systems, external interference or attack, environmental influences or change, etc. The disturbances of the system can not be avoided and predicted effectively. These disturbing factors often lead to the reduction of the capability, which severely affect the tasks performed by complex systems. So resilience is an important characteristic of complex systems. When the disturbances occur, resilience systems can detect them in time, and effectively control the influence through self-organization and self-adaptive in configuration.

The concept of resilience is discussed in many papers [1]-[4]. Several different approaches are developed to assess resilience. Han and DeLaurentics proposed a method based on Bayesian networks to evaluate the resilience of SOS design [5]. Pflanz describes a quantitative approach to evaluate the expected resilience of C2 system, and executable properties of Petri Nets are leveraged to support static and dynamic measures of the attributes of resilience [6], [7]. A resilience framework is proposed based on eight generic system functions, i.e. attentiveness, robustness, resistance, re-stabilization, rebuilding, reconfiguration, remembering, and adaptiveness [8]. Reference [9] develops a family of system importance measures (SIMs) that rank the constituent systems based on their impact on the overall SoS performance, and suggests SIMs as one way to analyze resilience with a focus on ranking resilience-critical systems. Zhang introduces an approach to quantify resilience for system described as a network. The resilience-based design optimization is then formulated for both deterministic and stochastic cases of a network system [10].

By analyzing the response process of the disturbed systems, this paper expands the resilience evaluation metrics, and represents a quantitative resilience evaluation method, which can evaluate the resilience of the system from two aspects of time and capability changes.

This paper is organized as follows, Section II mainly analyzes the response process of the system to disturbances, and defines a set of resilience evaluation metrics, and Section III gives a quantitative approach

[+] Corresponding author. Tel.: + 86 13786115986;
E-mail address: amluo@nudt.edu.cn

to measure resilience. In Section IV, the proposed approach is validated by analyzing Maritime Operations Center .Concluding remarks are given in Section V.

2. Key Topics in Considering Resilience

2.1. The Response Process of the System to Disturbances

The International Council on Systems Engineering (INCOSE) defines resilience as "the ability of organizational, hardware and software systems to mitigate the severity and likelihood of failures or losses, to adapt to changing conditions, and to respond appropriately after the fact" [1]. According to the concept of resilience, resilience systems can still maintain required capabilities and accomplish tasks when they are disturbed. Therefore, resilience measure must analyze the system capabilities to perform tasks after being disturbed rather than simply considering the performance of a system.

In general, when a complex system is disturbed, the process of capability change is shown in Figure 1 [5], [6]. The process reflects resilience of complex systems.

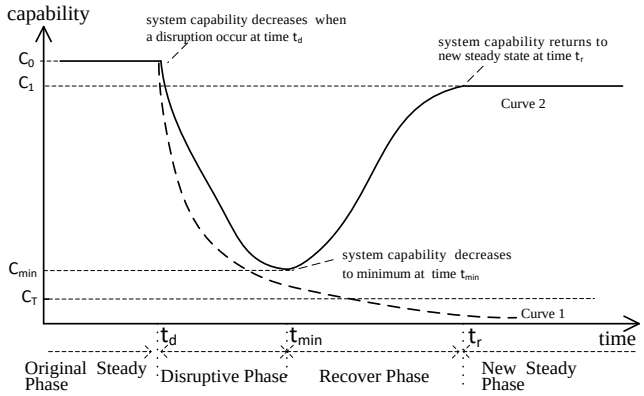

Fig. 1: The response process of system to perturbation.

In Figure.1, the process described by Curve 1 and Curve 2 are typical patterns of change in capability after perturbation. The process described by Curve 1 shows that system capabilities cannot return to the effective level and continue to perform missions of systems. What described by Curve 2 shows that the system capabilities can be restored to a steady state after declining, and continue to support the system to complete tasks. According to the definition of resilience, it is clear that the resilience of systems represented by Curve 1 is worse than that represented by Curve 2. We focus on the process represented by Curve 2 in the paper.

As shown in Figure 1, t_d indicates the moment when the disturbance occurs. t_{min} indicates the moment when system capability descends to the lowest level after disturbance, and t_r represents the moment when system capability returns to new steady state.

The response of the system to disruptions is divided into three phases.

(1)Steady Phase ($t < t_d$)

During the steady phase, complex systems operate at a normal capability level. In Figure. 1, when $t < t_d$, the system is in steady states, the capability value is denoted as C_0, and C_0 is the target value or ideal state value of the capability..

(2) Disruptive Phase ($t_d \leq t \leq t_{min}$)

The second phase is the disruptive phase. In Figure 1, the system is in the second phase when t is between t_d and t_{min}, ie. $t \in (t_d, t_{min})$. The system is usually affected by the internal and external disturbance factors and its capabilities change. When the system is subjected to less disruption, its inherent capacity can be dynamically stabilized. When the disturbance received is greater than the endurance capacity of the system itself, the capability begins to decrease. The level and speed of capability decline are determined by the properties, intensity and duration of the disturbance. The greater the intensity of disturbance, the longer the duration, the greater the degree and the speed of capability decline.

In Figure.1, the system is disturbed at t_d, its capability begins to decrease. After a period of time, the capability drops to the lowest value C_{min} at t_{min}.Let the minimum required capability of a system to complete a task is C_T, below which performance is deemed un-acceptable, or a catastrophic failure could result. When the system is disrupted, if $C_t \leq C_{min}$, the system can still support task completion, otherwise the system may not be able to effectively perform its tasks after being disturbed.

(3)Recovery Phase ($t_{min} \leq t \leq t_r$)

The third phase is the recovery phase, which mainly reflects the capability recovery process after the complex system is disturbed. In Figure 1, the recovery phase is from time t_{min} to t_r. During this phase, the system can restore its capability through backing up, repairing, reorganization, or self-organization. The extent and speed of capability recovery are closely related to system resilience. The resilience is better, and the recovery range is larger and the recovery speed is faster.

During recovery phase, the system capability is continuously increased from the minimum capability and gets to the new steady level C_r at t_r. When $t \geq t_r$, the system maintains the stable operation state, $C_r$and C_d may be the same or different.

2.2. Resilience Measure Metrics

From the process of the system response to disturbances, we can see that the capability change embodies the resilience of the system, so the resilience should be measured according to different stages of the system response to disturbances.

To evaluate system resilience, measure metrics are established as following.

(1)Capability Drop Degree (CDD)

Capability drop degree is described by margin of decrease of capability when the system is disturbed.

Suppose before the system is disturbed the capability value is C_0, after the system is disturbed, the capability drops to the lowest value as C_{min} at t_{min}, capability drop degree ΔC_d is defined as

$$\Delta C_d = C_0 - C_{min} \tag{1}$$

If $C_{min} < C_t$, the system can not meet the task requirements, so the maximum capability drop degree of the system to operate effectively is defined as

$$\Delta Max\_C_d = C_0 - C_t \tag{2}$$

(2)Capability Drop Ratio (CDR)

Capability drop ratio describes the percentage of capability degradation by the influence of disturbances.

Capability drop ratio RC_d is denoted as

$$RC_d = \frac{C_0 - C_{min}}{C_0} \tag{3}$$

The maximum capability drop degree Max_RC_d is expressed as

$$Max\_RC_d = \frac{C_0 - C_t}{C_0} \tag{4}$$

(3)Capability Recovery Degree (CRD)

Capability recovery degree refers to the margin of recovery when capability restores from the lowest level to new dynamic steady state.

Capability recovery degree ΔC_r is defined as

$$\Delta C_r = C_r - C_{min} \tag{5}$$

(4) Capability Recovery Ratio (CRR)

Capability recovery ratio describes the percentage of capability restore after the influence of disturbances.

Capability recovery ratio RC_r is shown as

$$RC_r = \frac{C_r - C_{min}}{C_0 - C_{min}} \tag{6}$$

The measure metrics defined above can identify the impact of disturbances to capabilities, and be used to evaluate the resilience of systems. However, they are not fully sufficient to measure the resilience.

When systems are disturbed, we want the descent speed of the capability as slowly as possible, and the rate of recovery is faster. the better, so that systems have enough time to respond to disturbances by various means and reduce the impact of disturbances.. Time is also an important metric to measure resilience.

(5)Capability Descent Speed (CDS)

Capability descent speed ΔV_d describes the degree of capability to decline within unit time, and is defined as

$$\Delta \mathrm{V}_d = \frac{C_0 - C_{min}}{t_{min} - t_d} \tag{7}$$

(6)Capability Recovery Speed (CRS)

Capability recovery speed ΔV_r represents the degree of capability to be restored within unit time, and is defined as

$$\Delta \mathrm{V}_r = \frac{C_1 - C_{min}}{t_r - t_{min}} \tag{8}$$

(7)Capability Change Ratio (CCR)

Capability change ratio describes the degree of capability change throughout the disturbance. For a disturbance, capability change ratio RC is denoted as

$$\mathrm{RC} = \frac{C_0 - C_1}{C_0} \tag{9}$$

If $C_0 = C_1$, then RC=0, indicating that after being disturbed, the system has no capability to decline through its own resilience, and that is to say, the system is very resilient.

(8)Response Time (RS)

Since the shorter the system disturbed is, the better. We define response time to measure the effectiveness of the system. According to the response process described in Figure 1, the response time is from t_d to t_r,

$$T_{response} = t_r - t_d \tag{10}$$

3. Quantitative Evaluation Method of Resilience

The quantitative capability values are the basis for the resilience assessment. Two methods can be used to quantify capability: the simulation method and the method based on probabilistic analysis. For the simulation method, the capability value of different key points are gathered through simulation models. For example, Ref.[6], the simulation model is established according to the architecture, and the values of the capabilities are obtained by simulation. Since the complexity of simulation modeling, especially for complex system, the second method can be considered in quantifying capability.

3.1. The Quantitative Method of Capability Based on Probability

Information systems consist of various constitutions, and the capabilities of a system are related to the efficiency of these constitutions. Only when the performance and efficiency of constitutions are in normal level, the capabilities of the system can reach the expected level. If the performance and efficiency of constitutions reduced due to the disturbances, the capabilities of the system will reduce naturally.

The disturbances have different impacts on the effectiveness of each constitution. Here we only consider the system is valid or invalid.

Let S denote the set of the constitutions of the systems, $\mathrm{S} = \{s_1, s_2, \cdots, s_N\}$.And capability is denoted as 0 or 1 when it is available or unavailable. Whether the capability is available depends on the effectiveness of each constitution, we define the conditional probability as

$$\mathrm{P}(c = 1) = \sum_{ST_i \in ST} p(c = 1 | ST_i) p(ST_i) \tag{11}$$

where ST is the set of all the possible combinations of constitutions efficiency. For example, if S includes two components, then ST={(0,0),(1,0),(0,1),(1,1)}. $p(c=1|ST_i)$ is the probability of achieving the capability c under the condition ST_i. Here we define the conditional probability P($c=1$) as the value of capability c.

3.2. System Resilience Measure Methods

Complex system can achieve many capabilities, and the disturbances have different effects on each capability. Therefore, the evaluation of system resilience needs to consider a variety of capabilities changes. Let $\overrightarrow{C_t}$ be an N-dimensional vector, $\overrightarrow{C_t}=(p_1^t\ p_2^t\ \cdots\ p_N^t)$, and p_i^t represents the value of capability c_i at moment t. According to equations (11), $0 \le p_i^t \le 1$.

Let $\overrightarrow{C_0}$ denotes the value of capabilities without the disturbances, and $\vec{C}_0$ is unit vector, i.e. $\vec{C}_0 = (1\ 1\ \cdots\ 1)$. In order to measure resilience, set $\vec{C}_{t_d}=\vec{C}_0$.

If the system have N capabilities, the variables C in equations (1) - (9) are replaced by N-dimensional vectors, and the capability difference equals the Euclidean distance between two vectors.

For example, let $\overrightarrow{C^{(t_{min})}}=\left(p_1^{t_{min}}\ p_2^{t_{min}}\cdots p_N^{t_{min}}\right)$ denotes the value of capabilities at time t_{min}, Capability Drop Degree is

$$\Delta C_d=\frac{\left|\vec{C}_{t_d}-\vec{C}_{t_{min}}\right|}{\left|\vec{C}_{t_d}\right|}=\sqrt{\left(1-p_1^{t_{min}}\right)^2+\left(1-p_2^{t_{min}}\right)^2+\cdots+\left(1-p_n^{t_{min}}\right)^2} \quad (12)$$

where $\vec{C}_{t_d}$ is unit vector, $\left|\vec{C}_{t_d}\right|=1$

4. Case Study

The case study is carried out in Maritime Operations Center (MOC) [6]. The MOC is a large, distributed organization at the fleet level, which consists of six major Decision Making (DM) organizations: Assessment (D1), Operational Intelligence (D2), Future Plans (D3), Command (D4), Current Plans (D5) and Current Operations (D6). In order to improve resilience, the MOC also adds additional organizations: Operational Intelligence (D7) and Future Plans (D8). D7 and D8, once required, can be available after a period of response time.

In this case study, the disturbing factor is "loss of situational awareness software". We assess the resilience of the MOC through two capabilities: Generate Mission Orders (c_1) and Target Recognition(c_2). When the situational awareness software fails, the MOC restores some of its capabilities by switching to manual operations and integrating the two additional organizations.

In the case [6], Mission Order Generation Rate is defined as the number of mission orders generated per 24 hours, which represents the value of c_1 and can be obtained by the simulation. According Ref.[6],the situational awareness software fails at time t48, then mission order generation rate falls off dramatically. When t= t_{53}, the value of c_1 drops to the minimum point ($t_{min}=t_{53}$) , the Mission Order Generation Rate is 3. When D7 and D8 have been integrated into command and control process, Generate Mission Orders is partially restored, and Mission Order Generation Rate is 4.01 after $t=t_{72}$

According to Equation (1)-(8), the results of metrics are shown in Table 1.

Table 1: The resilience assessment results of Generate Mission Orders

CDD	CDR	CRD	CRR	CDS	CRS	CCR	RS
2.67	0.46	1.01	0.366	0.534	0.053	0.2	24

We select probability analysis method to measure Target Recognition (c_2). The relevant probabilities are based on expert experience and statistical data.

Assuming that D1 and D2 are related to c_2 , all decision making organizations in original state are valid, so the value of c_2 is

$$P_{20}=p(c_2=1|D1=1,D2=1,D3=1,D4=1,D5=1,D6=1,D7=0,D8=0)=1$$

When the situational awareness software fails, then c_2 decreases the lowest at t_{48}, the value of c_2 at t_{48} is

$$P_{2d} = p(c_2 = 1|D1 = 1, D2 = 0, D3 = 0, D4 = 1, D5 = 1, D6 = 1, D7 = 0, D8 = 0)$$

Suppose $P_{2d} = 0.5$.

In order to restore capabilities, D7 and D8 are integrated into the MOC, the value of c_2 at t_{72} is

$$P_{2r} = p(c_2 = 1|D1 = 1, D2 = 0, D3 = 0, D4 = 1, D5 = 1, D6 = 1, D7 = 1, D8 = 1)$$

Suppose P_{2r}=0.8, the resilience assessment results of c_2 is shown in Table 2.

Table 2: The resilience measure results of Target Recognition

CDD	CDR	CRD	CRR	CDS	CRS	CCR	RS
0.5	0.5	0.3	0.6	0.1	0.015	0.696	24

According to the above results, $\overrightarrow{C_0} = (c_1^0 \ c_2^0) = (1 \ 1)$, $\overrightarrow{C_d} = (c_1^d \ c_2^d) = (0.52 \ \ 0.5)$, $\overrightarrow{C_r} = (c_1^r \ c_2^r) = (0.696 \ \ 0.8)$.According to Equation 12,the resilience measure results of the MOC is shown in Table 3.

Table 3: The resilience measure results of the MOC

CDD	CDR	CRD	CRR	CDS	CRS	CCR	RS
0.693	0.693	0.348	0.348	0.139	0.018	0.364	24

5. Conclusion

A quantitative measure method of system resilience is presented in this paper. This method expands the existing evaluation metrics, and quantify capability based on conditional probability. However the impact between the capabilities is ignored in the paper. For example, in the above case, Target Recognition has a positive impact on Generate Mission Orders in the MOC. Therefore in the future research, the capability value should consider not only the efficiency of systems, but also the impact between capabilities.

6. Acknowledgements

This study is supported by the National Natural Science Foundation of China (No.71571189).

7. References

[1] INCOSE. Resilient Systems Working Group homepage: http://www.incose.org/practice/techactivities/wg/rswg/

[2] D.Henry and J.E.Ramirez-Marquez. Generic metrics and quantitative approaches for sys- tem resilience as a function of time. *Reliab Eng Syst Saf*, 99(2012):114-122.

[3] A. M. Madni and S. Jackson. Towards a Conceptual Framework for Resilience Engineering. *IEEE Systems Journal*, 2009, 3(2):181-191.

[4] D.D. Woods. Four concepts for resilience and the implications for the future of resilience engineering. *Reliab Eng Syst Saf.*, 141(2015):5-9.

[5] S. Y. Han, K .Marais and D. Delaurentis. Evaluating system of system resilience using interdependency analysis. *IEEE* International *Conference on System ,Man,and Cybernetics*,October 14-17,2012,COEX,Seoul Korea:1251-1256

[6] M. Pflanz and A. Levis. An Approach to Evaluating Resilience in Command and Control Architectures. *Procedia Comput. Sci.*, 8(2012):141-146.

[7] M. A. Pflanz. On the Resilience of Command and Control Architectures. Ph.D. Dissertation, George Mason University, United States - Virginia, 2011

[8] S. Hosseini, K. Barker, and J.E.Ramirez-Marquez A review of definitions and measures of system resilience. *Reliab Eng Syst Saf.*,145(2016):47-61

[9] P. Uday and K. B. Marais. Resilience-based System Importance Measures for System-of-Systems, *Procedia Comput. Sci.*, 28(2014) 257-264.

[10] X. Zhang, S. Mahadevan, S. Sankararaman and K.Goebel. Resilience-based Network Design Under Uncertainty, *Reliab Eng Syst Saf.*,169(2018):364-379