Measurement and Analysis of the Key Metrics of Information System Resilience

Wei Jinyi¹, Li Ning¹, Shi Jing² and Xu Luo¹

¹Innovation Center, North China Institute of Computing Technology, Beijing, China
²Center for Peace and Development Studies, Beijing, China

E-mail: 13020077476@163.com;

Abstract. In view of the current situation that the resilience of information systems cannot be accurately assessed, the key metrics that affect the resilience of information systems—the overall system capability, the system's maximum absorptive capacity, the system recovery ability and the system recovery ratio, are established. And the paper shows data calculation model of the key metrics. Finally, the information system resilience analysis method is proposed, and an aerospace simulation system is taken as an example, combined with its dual redundancy and non-redundancy mechanism to test and verify, which provides strong support for the analysis of system resilience ability.

1. Introduction

The information system is the core of the formation of a networked warfare system, and it is the focus of the enemy and the enemy to compete for the dominance of war. Therefore, the information system must be the main target of enemy reconnaissance monitoring and combating damage [1]. At present, the main attacks on information systems include physical attacks, electronic attacks, and cyber-attacks. Any of these attacks may cause damage to information system nodes, degradation, and other risks, not to mention the actual environment. The comprehensive use of attack means makes the information system invincible and faces greater threats. The US Air Force's "Suter" system is a typical example. It uses a variety of attack methods such as electronic warfare, cyber warfare and physical strikes to make the protection more difficult.

In response to the above problems, experts and scholars analyzed a series of complex characteristics such as information system robustness [2], adaptability [3] and invulnerability [4], and found that Resilience is the key attributes of system to deal with risks and damage. So, resilience has received widespread attention in the industry.

The concept of resilience [5] was first proposed by the US military in the Mission-Oriented Resilient Clouds (MRC) project [6], when resilience was the ability to continue to run cloud applications and infrastructure in the event of an attack. The proposed concept of resilience for infrastructure, and then our military proposed a concept of system-oriented resilience, which refers to a capability or quality characteristic that the system presents in response to various disturbances and changes, that is, the system predicts interference from natural or man-made events. The ability to resist, absorb, react, adapt and recover [7]. Therefore, the resilience ability indicates that the information system can be degraded and restored as soon as some nodes fail, collapse, and damage, ensuring the ability to complete critical tasks.
Information systems need resilience, and how to evaluate system resilience becomes a key issue. Testing is an effective means of quantitatively testing system capabilities. However, the current state of the art is that existing testing techniques tend to focus on functional, performance, and reliability testing, and lack of test methods and tools for system resilience.

This paper establishes the key metrics that affect the resilience of information systems, and gives the data calculation model of key metrics. Finally, the information system resilience analysis method is proposed to quantitatively measure the resilience of information systems.

2. Related works
At present, experts and scholars at home and abroad have conducted preliminary research on the resilience of information systems.

In 2014, the Systems Engineering Research Institute with the theme of Resilience Engineering System (ERS) was held in California, USA, reflecting the importance of system resilience. In the same year, Zachary A. Collier et al. proposed the NCO resilience decision-making framework based on network-centric actions. However, it only compares the resilience of different systems from a conceptual perspective [8].

In 2015, resilience received extensive attention. Huy T. Tran et al. used the architecture method to evaluate the resilience of the command and control network, but it only analyzed the structural parameters affecting the network resilience, and did not measure the overall resilience of the system [9]; Lan Yushi et al. proposed resilient command the concept of information system, and its construction mechanism and engineering implementation method are studied, but it lacks the evaluation method of system resilience [10]; Zhao Hongli et al. proposes a network science-based networked allegation information system resilience analysis method. The residual network performance after the failure event is used as the basis of resilience measurement, and a new idea is proposed for the resilience measurement, but it has obvious shortcomings in resilience response, recovery and regeneration [11].

In 2016, Tao Zhigang et al. proposed a C4ISR system resilience research method based on the weighted space exploration. This method provides a direction for the study of system resilience, but lacks research on system resilience measurement [12].

In 2018, a major breakthrough was made in the study of system resilience. Ding Feng et al. proposed a quantitative evaluation method for resilience ability to the mission-oriented command information system, and established a resilience system capability evaluation metrics system and model. However, the evaluation metrics are redundant and difficult to perform digital calculation, and cannot perform a quick analysis to information systems. [13].

The key metrics and resilience analysis methods of information system resilience proposed in this paper can effectively make up for the shortcomings of the above research, which is efficient and fast, and can quantitatively analyze the resilience of resident information systems.

3. The key resilience metrics for information system
According to the method described in the US space system resilience process [14], the information system resilience process can be divided into four states: original state, degradation, recovery and steady state, as shown in Figure 1. The t0-t1 time period is an original state phase, which shows the system capability state of the information system during normal operation. In the normal working process, the information system needs to maintain a relatively stable level F(t1) in order to meet its own simulation test tasks. Of course, due to its complex structural composition, small disturbances are inevitable in the normal working process, but the disturbance is in the range that the resilience can absorb, so the whole is in a dynamic and stable state. The t1-t2 time period is a degradation phase, which shows the state of the system capability of the information system in the event of an attack. When the information system is subject to small disturbances, the system capability is still in a dynamic and stable state due to its resilience ability. When the information system is attacked more seriously, its resilience ability cannot maintain a dynamic stability for the first time, and the system...
capability will decline, enter the degradation phase of system capability, and drop to F(t2). The
degradation rate is related to the system resilience ability and the attack strength suffered. The stronger
the resilience ability, the smaller the attack intensity, the slower the rate of decline, and vice versa. The
t2-t3 time period is the recovery phase, which shows that after the information system is degraded by
the attack system, the resilience plays a role in the recovery of the system capability. The recovery rate
in the recovery phase is closely related to the system resilience ability, but the process of change is
often not well measured, so the relatively stable F(t2) and F(t3) are selected to reflect the recovery
state. The t3-t4 time period is a steady state phase, which shows the capability state of the information
system after the attack system is recovered. After the system is recovered, we hope that the system
capability can be the same as before the attack, but the system is often impossible to implement, only
re-planning and adjustment, constructing a new internal component, enabling itself to adapt to external
attacks and achieving normal working status.

![Information system resilient model](image)

**Figure 1.** Information system resilient model.

By analyzing the resilience process of the information system, we chose to attack the information
system at point t1 and identified four key metrics: the overall system capability, the system's
maximum absorptive capacity, the system recovery ability and the system recovery ratio.

### 3.1. The overall system capability

The overall system capability of the resilience information system refers to the system in which the
system breaks down from the original state, enters to the degradation phase, and then goes to the
recovery level, and then passes through the steady state and finally reaches a relatively stable state.
The overall performance, recorded as P, can be used as the first assessment metric of the resilience of
information systems.

Based on the above analysis, the cumulative normalized value of the system resilience process
integral is used to represent P, namely:

\[
P = F(\text{Original State, All}) = \frac{F(\text{All})}{F(t1)} = \frac{\int_{t0}^{t4} f(t)/(t4-t0)}{\int_{t0}^{t4} f(t)/(t1-t0)}
\]  

(1)

Among them, Original State is the first phase of system capability, all is the whole process of
system capability, and P is the ratio of F(All) to F(t1). It should be noted that in Figure 1, we can
accurately see the values of f(t1), f(t2), f(t3), and f(t4), but in the actual situation, the points of the
original state phase, the degradation phase, the recovery phase, and the steady state phase are difficult
to determine, and the system capacity of the degradation phase and the recovery phase varies greatly.
Therefore, we select the cumulative normalized value of f(t) for a period of time t0-t4 as the value of
F(All). Similarly, the cumulative normalized value of \( f(t) \) for a period of time \( t_0-t_1 \) is selected as the value of \( F(t_1) \), and the ratio of the two represents the overall system capability \( P \) of the evaluation metric.

3.2. The system's maximum absorptive capacity

In the process of networked operations, the resilience information system will break the original state due to the attack and enter the degradation phase. In this process, the system capability drops sharply, and even itself may be affected. The less the degree of decline in the system degradation, the stronger the system's absorption capacity and the stronger the system resilience; the weaker the opposite. In addition, the system degradation rate is also an important parameter of the system's absorption capacity. The longer the system decline time, the stronger the system resilience ability; the weaker the opposite. Eliminating human maintenance and other interferences on the system, the degree of degradation and the rate of decline can be used to reflect the resilience of the information system.

Based on the above analysis, the system's maximum absorptive capacity is represented by the degree of degradation of the system capability in the degradation phase and the negative index of the rate of decline, and is used as the second evaluation metric of the resilience capability of the information system, which is denoted as \( D \), and its relationship is:

\[
D = F(\text{Original State, Degradation}) = e^{-d_1v_1} = e^{\frac{f(t_1)-f(t_2)}{f(t_1)} t_2-t_1} = e^{\frac{f(t_2)-f(t_3)}{f(t_1)} t_3-t_1} \tag{2}
\]

Among them, Original State is the first phase of system capability, Degradation is the second phase of system capability, \( d_1 \) is the degree of system degradation, \( v_1 \) is the system rate of decline, and \( D \) is the negative index of \( d_1v_1 \). The ratio of the difference between \( f(t_1) \) and \( f(t_2) \) to \( f(t_1) \) represents \( d_1 \), and \( v_1 \) is represented by the ratio of the time interval of \( t_1-t_2 \) to the time interval of \( t_1-t_3 \). In addition, it is also necessary to select the cumulative normalized value of \( f(t) \) for a period of time \( t_0-t_1 \) as the value of \( f(t_1) \), and finally use the degradation degree of the system capability of the degradation phase and the negative index of the rate of decline as an evaluation metric.

3.3. The system recovery ability

In the process of networked operations, the resilience information system is attacked to break the original state and enter the degradation phase, and then enter the recovery phase. The system recovery ability is closely related to the system resilience. The more the degree of ascension is when the system is recovered, the stronger the system recovery ability and the stronger the system resilience; the weaker the opposite. Similarly, the system recovery rate is also an important parameter of the system recovery ability. The shorter the system rise time, the stronger the system recovery ability; the weaker the opposite. In addition, human maintenance guarantees have also had an important impact on the recovery of system capability. Therefore, it is necessary to remove the influence of these external factors on the system itself, and use the degree of recovery and the rate of increase to reflect the resilience of the information system.

Based on the above analysis, the system recovery ability is represented by the recovery degree of the system capability in the recovery phase and the negative index of the rising rate, and is regarded as the third evaluation metric of the information system resilience ability, which is denoted as \( R \), and its relationship is:

\[
R = F(\text{Original State, Recovery}) = e^{-d_2v_2} = e^{\frac{f(t_2)-f(t_3)}{f(t_2)} t_3-t_2} = e^{\frac{f(t_2)-f(t_4)}{f(t_2)} t_3-t_2} \tag{3}
\]

Among them, Original State is the first phase of system capability, Recovery is the third phase of system capability, \( d_2 \) is the recovery degree of the system, \( v_2 \) is the rising rate of the system, and \( R \) is the negative index of \( d_2v_2 \). The ratio of the difference between \( f(t_4) \) and \( f(t_2) \) to \( f(t_1) \) represents \( d_2 \), and \( v_2 \) is represented by the ratio of the time interval of \( t_2-t_3 \) to the time interval of \( t_1-t_3 \). In addition, it is also necessary to select the cumulative normalized value of \( f(t) \) for a period of time \( t_0-t_1 \) as the value of \( f(t_1) \), and select the cumulative normalized value of \( f(t) \) for a period of time \( t_3-t_4 \) as the value
of \( f(t4) \). Finally, the recovery degree of the system capacity in the recovery phase and the negative index of the rising rate are taken as an evaluation metric.

### 3.4. The system recovery ratio

In the process of networked warfare, the resilience information system will break the original state due to the attack, enter the degradation phase, and then go to the recovery level, and then go through the steady state phase, and finally reach a relatively stable state. In this process, the system will be damaged, so the first and fourth, two relatively stable states are different. The stronger the resilience of the information system, the smaller the damage it receives, and the stronger the system capability of the stable state after the steady state; the weaker the opposite. Similarly, human maintenance support plays an important role in the system capability to stabilize the information system. In the information system resilience test, the impact of human subjective activities should be removed as much as possible. Therefore, the information system reflects the resilience of the information system in two different relative stable states before and after the attack.

Based on the above analysis, the ratio of the system capability of the steady state phase to the system capability of the original state phase, which is the system recovery ratio, is another evaluation metric of the information system resilience ability, and is expressed as:

\[
\varepsilon = F(\text{Original State}, \text{Steady State}) = \frac{f(t4)}{f(t1)} = \frac{\int_{t3}^{t4} f(t \, dt) / (t4 - t3)}{\int_{t0}^{t1} f(t \, dt) / (t1 - t0)}
\]  

Among them, the Original State is the first phase of the system capability, and the Steady State is the fourth phase of the system capability, which is the ratio of \( F(t4) \) to \( F(t1) \). It should be noted that in Figure 1, we can accurately see the values of \( f(t4) \) and \( f(t1) \), but in the actual situation, the points of the original state phase and the steady state phase are difficult to determine, so we choose the cumulative normalized value of \( f(t) \) for a period of time \( t3-t4 \) is taken as the value of \( f(t4) \), and the cumulative normalized value of \( f(t) \) for a period of time \( t0-t1 \) is also selected as the value of \( f(t1) \). The ratio of the two is used as an evaluation metric.

### 3.5. The key metrics calculation

Information system resilience consists of four states: original state, degradation, recovery and steady state. Therefore, the four metrics of system resilience ability are combined to reflect the resilience of information systems. Set the resilience ability of the information system to \( S \), remember that the overall system capability of the system is \( P \), the system’s maximum absorptive capacity of the system is \( D \), the system recovery ability is \( R \), and the system recovery ratio is \( \varepsilon \), then \( S = P \times D \times R \times \varepsilon \). The specific steps are:

- First, calculate the cumulative normalized value \( F(\text{All}) \) of the \( t0-t4 \) phase, the cumulative normalized value \( F(t1) \) of the \( t0-t1 \) phase, and the cumulative normalized value \( F(t4) \) of the \( t3-t4 \) phase;
- Second, calculate the degree of degradation \( d1 \), the rate of decline \( v1 \), the degree of recovery \( d2 \), and the rate of increase \( v2 \);
- Next, calculate the overall system capability of the system \( P \), the system’s maximum absorptive capacity of the system \( D \), the system recovery ability \( R \), and the system recovery ratio \( \varepsilon \);
- Finally, calculate the resilience ability of the \( t0-t4 \) state information system \( S = P \times D \times R \times \varepsilon \).

### 4. Testing and analysis of information system resilience

Take an aerospace simulation system as the resilience test object, as shown in Figure 2. According to the model established in the paper, the chaotic method [15] is used to simulate electromagnetic interference, network attack, CPU overload, malicious code attack, power failure, physical damage and other faults, resulting in damage to the simulation system, which cannot work properly. After the
The simulation system consists of a signal source, a signal converter, a signal receiver, a signal processor, and a control center. For the composition of the system, the testing process can be designed as: design, battle simulation, attack simulation, intelligence analysis, and resilience assessment. The process is shown in Figure 3.

For the simulation system, the actual combat intelligence short message is sent and received, and the malicious code is used to attack it. Select different attack strengths, and determine the overall system capability, the system's maximum absorptive capacity, the system recovery ability and the system recovery ratio, so as to test and evaluate the system.

Set the attack strength of 10, 20, 30, 40, 50 and 60 Mbit/s of malicious code, and continuously send short messages at 600 pieces per second, which yields 6 curves of the system short message processed ability as shown in Figure 4. It can be seen from Figure 4 that the greater the attack strength suffered by the system, the greater the decline in the processed ability of the short message. When the attack strength reaches 40 Mbit/s, the short message processed ability curve basically coincides, which is mainly caused by the dual redundancy of the system service [16]. At this time, the reference value of the 50 and 60 Mbit/s attack strength curves has decreased. Therefore, we select the 40Mbit/s attack intensity curve data for the analysis and calculation of the key metrics of resilience ability.
The system was modified to test under the condition of non-redundancy [17]. Similarly, in the above basic environment, the 6 curves of the short message processed ability of the system shown in Figure 5 was obtained. It can be seen from the figure that when the system is attacked at 60 Mbit/s, its short message processed ability is once lost and cannot be recovered for a while; when the system is at 50 Mbit/s attack strength, its short message processed ability is slowly maintain a stable level after a while. Therefore, we select the 50Mbit/s attack intensity curve data for the analysis and calculation of the key metrics of resilience ability.

![Figure 5. Non-redundant system's short message processed ability change curves under different attack strengths.](image)

Under the dual redundancy condition of 40 Mbit/s, F(All), F(t1), F(t4), d1, v1, d2, and v2 are calculated by curve fitting, and then

\[
\begin{align*}
P &= 0.73 \\
D &= 0.76 \\
R &= 0.55 \\
\epsilon &= 0.99
\end{align*}
\]

is obtained, and its system resilience ability is:

\[
S = P \cdot D \cdot R \cdot \epsilon \approx 0.30.
\]

Under the non-redundancy condition of 50 Mbit/s, F(All), F(t1), F(t4), d1, v1, d2, and v2 are calculated by curve fitting, and then

\[
\begin{align*}
P &= 0.68 \\
D &= 0.69 \\
R &= 0.56 \\
\epsilon &= 0.99
\end{align*}
\]

is obtained, and its system resilience ability is:

\[
S = P \cdot D \cdot R \cdot \epsilon \approx 0.26.
\]

Since the calculation of data is based on the premise of minimizing the impact of redundancy on the system, the system recovery ability R and the system recovery ratio \(\epsilon\) of the dual redundant and single redundant systems are basically equal; in addition, the dual redundant system is greater than non-redundant system int the overall system capability P and the system's maximum absorptive capacity D, so dual redundant system has better resilience than non-redundant systems.

The analysis results can intuitively determine the resilience of the information system. At the same time, the system's dual redundancy mechanism greatly enhances its system resilience, which also proves the practicability of our information system's dual redundancy and even multiple redundancy mechanisms.

5. Conclusion

This paper analyzes the system resilience processing, proposes the key metrics and resilience analysis methods of information system, and uses the actual system as an example to verify the effectiveness of the key metrics of information system resilience and the practicability of the system's dual redundancy mechanism.

Acknowledgments

Funded by the “13th Five-Year” Pre-research Project of the Ministry of Equipment Development (9140A15050208DZ25). Wei Jinyi is the corresponding author.
References

[1] Cui Qiong, Li Jianhua. Elastic Measurement Method of Networked Command Information System[J]. Military Planning and Systems Engineering, 2016, 30(4): 18-24

[2] Zhang Jieyong, Yi Wei, Wang Wei. Dynamic Robustness Measurement Method for C4ISR System Structure Considering Cascading Failure[J]. Systems Engineering and Electronics, 2016, 38(9): 2072-2079

[3] WANG Jie, ZHANG Lin-lin, ZHAO Wei et al. Adaptation Measurement Method of Aspect Oriented Software Architecture[J]. Microelectronics & Computer, 2015(6): 41-45

[4] Yi Yi, Wang Wei, Mao Shaojie et al. Optimization Method of Network C4ISR System Structure Destruction Ability[J]. Command Information Systems & Technology, 2015, 6(3): 9-15

[5] HOLLING C S. Resilience and stability of ecological systems [J]. Annual Review of Ecology and Systematics, 1973, 4(4): 1-23

[6] DARPA-BAA 11-55. Mission-oriented Resilient (MRC) [R]. Information Innovation Office, 2011: 12

[7] GOERGER S R, MADNI A M, ESLINGER O J. Engineered resilient systems: a DoD perspective [J]. Procedia Computer Science, 2014, 28: 865-872

[8] ZACHARY A COLLIER, LGOR LINKOW. Decision making for resilience within the context of network centric operations [C] // 18thICCRTS, 2014

[9] TRAN H T, DOMERCANT J C, MAVRIS D N. A SoS approach for assessing the resilience of reconfigurable command and control networks [R]. American Institute of Aeronautics and Astronautics SciTech, Kissimmee, Florida, 2015: 1-14

[10] Lan Yushi, Zhou Guangxia, Wang Wei et al. Research on the Construction Mechanism and Implementation of Resilience Command Information System[J]. Journal of Command and Control, 2015, 1(3): 284-286

[11] Zhao Hongli, Yang Haitao, Fu Wei. Research on Elastic Analysis Method of Networked Allegation Information System[J]. Journal of Command and Control, 2015, 1(1): 14-19

[12] Tao Zhigang, Xu Hao, Yi Wei et al. Research on the resilience of C4ISR system based on the analysis of trade-off space [C] // Proceedings of the 4th China Command and Control Conference. Beijing: Publishing House of Electronics Industry, 2016: 110-113

[13] Ding Feng, Zhou Fang, Cheng Wendi et al. Quantitative Evaluation of Resilience of Command Information System for Task Support[J]. Journal of Command and Control, 2018, 9(6): 13-18

[14] BURCH R. Measures of resilience for space systems [EB/OL]. (2013-08-14) [2017-02-20].http://www.ndia.org/Divisions/Divisions/Space/Documents/Space_forum-Boeing-NDIA-Resilience-Forum-081413-RevA.pdf

[15] PRINCIPLES OF CHAOS ENGINEERING. [2018-05]. http://principlesofchaos.org/

[16] Ding Jin, Xu Guoqiang. Design and Implementation of Automatic Switching Test Module for Dual Redundant Network Interfaces[J]. Ship Electronic Countermeasure, 2017, 40(3)

[17] Yu Meijie. Research on MMC-STATCOM control system with fault tolerance; [D]. Harbin University of Science and Technology, 2018