


# A Fault Management Oriented Resilience Model for Networking Systems

Carlo Vitucci 


*Technology Management*  
Ericsson AB  
Stockholm, Sweden  
carlo.vitucci@ericsson.com

Daniel Sundmark 

*Computer Science and Software Engineering*  
Mälardalen University  
Västerås, Sweden  
daniel.sundmark@mdu.se

Marcus Jägemar 

*Sys Compute Dimensioning*  
Ericsson AB  
Stockholm, Sweden  
marcus.jagemar@ericsson.com

Thomas Nolte 

*Division of Networked and Embedded System*  
Mälardalen University  
Västerås, Sweden  
thomas.nolte@mdu.se

**Abstract**—The ability of a system to maintain the availability of its services for the end user is a crucial indicator of performance, both in terms of infrastructure and serviceability. In other words, the service’s availability depends on the system’s resilience, which is its ability to handle disruptions in the deployed service. Fault management is crucial to increasing system resilience because it aims to control and recover error conditions. However, the efficiency of the fault management implementation depends on the infrastructure design: hardware-assisted fault management allows the quickest recovery action and a better fault isolation. From what we have written above, we can understand why an efficient infrastructure design and practical implementation of fault management can lead to high system resilience. How can we evaluate the efficiency of fault management and infrastructure design relative to system resilience? This paper proposes a new model for measuring system resilience that considers the different fault management aspects contributing to resilience.

**Index Terms**—Modelling, Resilience Triangle, Resilience System, Fault Management, Run Time Fault Recovering

## I. INTRODUCTION

In previous work [1], we underlined how the growing complexity of networking systems has increased the attention to the role of fault management. The value of the network has increasingly shifted from simply providing connectivity to encompassing availability questions, like end user service usability and resilience. Services with a low availability rate and poor performance immediately impact the provider’s business. Therefore, systems need a reliable network infrastructure in terms of performance and its ability to supervise the available resources to detect, locate, and resolve adverse events. The system function capable of carrying out all the actions described above is, by definition, fault management. A network needs an optimal fault management implementation to be reliable. Since the final aim of the fault management function is to recover as best as possible from a fault condition before it becomes a failure [2], we can conclude that the efficient implementation of the fault management function is how we allow the system

to be resilient [3]. The relationship between fault management and resilience is explicitly in their definition: Resilience is the system’s ability to react to an internal or external disruptive event and return to the equilibrium in the shortest time possible, mitigating the probability of failure and losses [4], while fault management aims to detect, locate and recover from a disruptive event. Therefore, if resilience is the system’s ability to manage fault conditions, fault management is the function to achieve it.

Resilient systems engineering has been an area of growing interest in recent years, mainly to manage and maintain increasingly complex technologies. The objective is to ensure network operators maintain their service at an acceptable level: in other words, the sustainability of their business.

It is worth noting the relationship between complexity and resilience of a system. We hypothesise that more complex systems require more significant fault management investment to maintain a high level of system resilience. It is a hypothesis that can be readily accepted but would require a specific study to understand the ratio between the cost of fault management and maintenance function. Only through that ratio it is possible to quantify the impacts on the operators’ business due to the lack of system resilience.

Having established what the resilience of a system is and its link with fault management, it remains to understand why its quantification is necessary. Watson et al. [5] have excellently summarized the reasons for the measurability of resilience in the following points:

- it allows for improvement of the design of interwork mechanisms between system components, measuring their impact on the stability of the service.
- it allows you to optimize the deployment of the system infrastructure, improving its economic sustainability and energy consumption.

- it allows you to identify the relationship between resilience and the design of existing systems to identify the areas of improvement (the critical areas of the system for the stability of the service).

**Paper Contribution:** This paper introduces a fault management oriented revised resilience model that is considering the capacity of the system to *absorb* and *recover* faulty hardware conditions. The paper shows the correlations existing between the system resilience and the fault management strategies, supporting decision making during fault management design.

**Outline:** Section II analyzes available works on resilience metrics. Section III describes the research method. Section IV introduces our model. Section V describes an empirical application of the proposed model. Section VI discusses the results and possible future work.

## II. RELATED WORKS

The research in resilient systems has developed primarily over the past twenty years. It is no coincidence that the concept of the resilience triangle was introduced only in 2003 by Bruneau et al. [6]. We can identify four domains of interest in which to group resilience studies:

*Studies about the Resilience as a System Function:* This category encompasses works that consider the engineering of resilient systems to define models, quantify, and define metrics. The work of Buchanan et al. [7] belongs to this group and proposes an interesting measurement of system resilience as a vector function of the system's input, states, and output. It's an intriguing approach but keeps resilience measurement at a theoretical and ideal level, which seems difficult to measure. The *Resilience as a System Function* category is the most interesting for our research because it offers various frameworks and working methods. Watson et al. [5], for example, use a resilience measurement method that allows for comparison between complex systems, an exciting approach for identifying criticality in the components and understanding where to invest if you want to increase the system's resilience, though using an ideal condition for the resilience model might be a limitation of their work. Ren et al. [8] use a more realistic model of the resilience triangle. The paper focuses on optimizing the design of complex systems to improve their resilience, resulting in a resilience metric based on the system's technical characteristics. The drawback of their approach is that it may take time to understand the effect of a fault condition. Zobel et al. [9] developed a new method for measuring resilience by introducing resilience curves. It is an approach that highlights the link between implementing resilience as a system function and the disturbance impacts. They used the resilience triangle model for an ideal condition, which doesn't help understanding the resiliency robustness, function-oriented, and recovery implementation contributions to the system's resilience.

*Survey of resilience studies:* This category includes analysis and review of resilience systems studies. They provide an excellent contribution to defining concepts and indicating the methodologies most followed. As a survey, Hosseini et al. [10]

is a noteworthy one, which first classifies the research as quantitative and qualitative. Their paper identifies differences, challenges yet to be resolved, and possible further studies. As visualized in Figure 1, the works of Bruneau by first and Hosseini by second constitute the backbone of research in system resilience.

Aldea et al. [4] specifically focus on the metrics of a resilience system, identifying those most commonly used but without utilizing a model to quantify system resilience.

*Studies about Resilience Metrics:* This category includes works that measure the resilience of more or less complex systems. The main merit of these works is the revisiting of resilience metrics and the definition of different frameworks for measurement. Notably, this class includes the already-mentioned work of Bruneau et al. [6]. Only sometimes, papers in the group consider an exhaustive resilience contribution subset. Bevilacqua et al. [11], for example, offer an exciting definition of resilience as a vector of input functions, system states, and outputs with a valid holistic vision. Still, its practical measurement needs to be comprehended. Lu et al. [12] and Niu et al. [13] propose quantification methodologies that lack some components of resilience (such as robustness or the functional-oriented contribution), that, instead, add value to resilience study [14]–[17]. The functional-oriented component is instead central in the work of Ravulakollu et al. [18], but too specific to the considered domain, that is the limits of Singh et al. [19] and Song et al. [20] propose quantitative evaluation methods as well.

*Investigation of Resilience in specific domain: Case studies type:* Chen et al. [21] case study is the resilience analysis of urban rail transport. The domain is the Chengdu metro network. The paper proposes a performance indicator for the network structure and passenger demand. It also introduces a node centrality metric to evaluate the importance of stations in

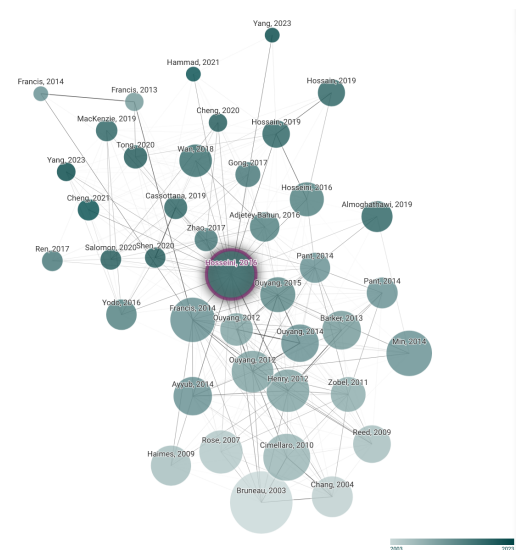


Fig. 1: The connected paper for Hosseini [10] survey (created via [www.comparedpapers.com](http://www.comparedpapers.com))

actual travel paths. Those parameters drive the modification of the resilience triangle. It is interesting that, as part of future work, the paper proposes the modification of the resilience triangle by considering three different phases: disturb, reaction, and recovery. Dong et al. [22] case study is the resilience analysis of road transport networks during extreme events. The domain is Harris County, Texas, during the Harvey hurricane. The paper introduces the concept of connection reliability using network reliability scaling and network stability indexes. The paper suggests that the method applies to any network, like telecommunication or electricity, to evaluate the network's resiliency to extreme events. Kanno et al. [23] case study is the resilience analysis of a service system during a disaster. The domain is the dialysis treatment service. The paper presents a method that considers service activities and critical infrastructure recovery. The paper finds that strengthening service and infrastructure recovery is fundamental to improving resilience. The model is relatively simple and requires considering additional complexity. However, understanding and predicting all aspects in a detailed assessment of service resilience in a disaster is challenging. Wang et al. [24] case study is the resilience analysis of naval transport systems. The domain is the Deepwater channel of the Yangtze estuary. The paper proposes a discrete event-based simulation model to quantify the resilience of shipping transport systems based on ship loading, ship delay and recovery cost. The proposed decomposition of the resilience triangle event-based is interesting. Disruptive, action, end of reaction, and recovered event, though it is complex to think of other domains for the paper findings. Yin et al. [25] case study is the resilience analysis of an urban rail transport system. The domain is the Beijing subway network. The paper addresses erratic driving, signalling systems and extreme weather conditions. The paper uses knowledge and data for quantitative resilience analysis based on the Bayesian Networks model. It is worth mentioning the usage of deep learning, even if the paper does not consider the traditional resilience triangle concept.

### III. RESEARCH OBJECTIVE

The paper is a quantitative engineering study [26] that aims to design a resilience triangle model that best lends itself to analyzing the different components of a system's resilience for a realistic and non-ideal case of a failure event.

To achieve our objective, we structure the study in several phases:

- We analyze existing research for metrics and resilience measures, focusing mainly on research that defines resilience as a system function.
- We need to rethink the resilience triangle model proposed by Bruneau to incorporate the differences in the components design of a resilient system that enhances resilience. This reassessment establishes a direct relationship between fault management components and resilience elements.

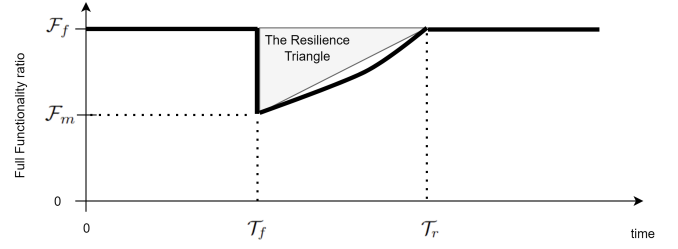


Fig. 2: The Bruneau model [6] for the Resilience triangle

- Using the updated resilience triangle model, we quantify the contribution of each component to resilience based on the impacts of error events on the system.

Research on system resilience finds application across various disciplines, including ecology, sociology, psychology, economics, industry, and transportation. This paper explicitly revisits the resilience triangle model, focusing specifically on embedded systems and networking, wherein every component contributes significantly to the system's resilience.

### IV. MODEL DESCRIPTION

The resilience triangle, introduced by Bruneau in 2003 [6] (see Figure 2), is a quantitative conceptual model of resilience and expresses the ability of a system to react to an internal or external disturbance that affects its full functionality. If

$$\Delta_f = F_f - F_m, \text{ where } 0 < \Delta_f < 1$$

represents the loss of system functionality at time  $T_f$  of the disturbance event, and

$$\Delta_t = T_r - T_f$$

represents the time interval between the disturbance at time  $T_f$  and the full functional recovery event at the time  $T_r$ , then the area of the triangle

$$\mathcal{A}_R = \frac{1}{2} \Delta_f \Delta_t \quad (1)$$

measures the impact of the disturbance on the system, and

$$\mathcal{R} = \Delta_t \left( 1 - \frac{\Delta_f}{2} \right) \quad (2)$$

measures the resilience of the system.

It follows that to improve the resilience of a system, one must minimize the area of the resilience triangle, by reducing the ratio of functionality lost at the time of the disturbance, and the time taken by the system to return to the equilibrium state.

If we denote by  $\mathcal{F}(t)$  the curve describing the functionality ratio of the system over time (*with*  $0 < \mathcal{F}(t) < 1$ ), then the measure of resilience is given by the following formula:

$$\mathcal{R} = \int_{T_f}^{T_r} \mathcal{F}(t) dt \quad (3)$$

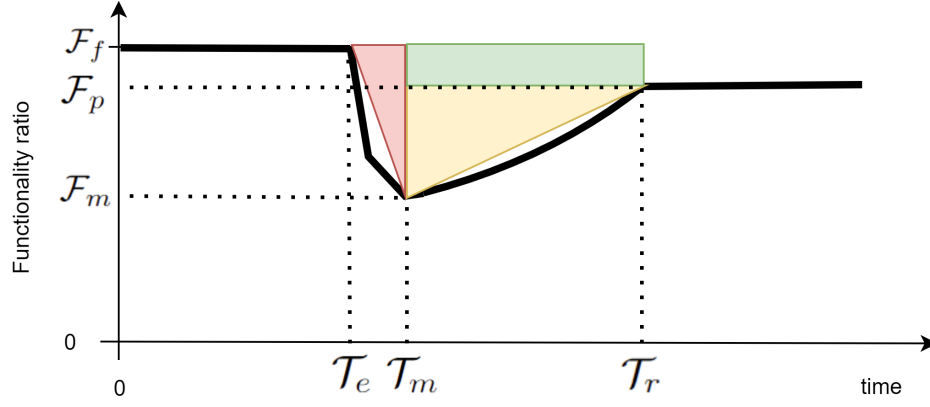


Fig. 3: The proposed model for the Resilience triangle

In this section, we want to do a hardware fault management-oriented review of the resilience triangle, i.e., when a hardware error condition causes the problem. The resilience triangle, as shown in Figure 2, is a conceptual representation of the system's ability to recover from the effects caused by a faulty event (fault tolerance). Still, it does not allow a complete classification of the system's resilience in a real case: the system takes a while to detect a fault condition; the system takes a while to start recovering actions; the functional ratio level after the recovering action could be limited, depending on the system's capability to cope with a failure status, for example, thanks to the redundancy solution or a reallocation of available resources to continue working under a degraded function condition. How quickly the system reacts to a fault condition depends on efficiently implementing fault management, such as fault reporting. How much a disturbance affects the functional drop depends on the fault isolation, that is, the ability to avoid fault propagation in other devices or system components. It does not consider the system's ability to continue to work even in the presence of a fault condition thanks to fault masking or the system's ability to quickly detect a fault condition thanks to fault coverage. Revisiting the "ideal" resilience triangle must consider these resilience components.

Figure 3 represents an advancement in our understanding of system resilience, offering a new model that addresses the limitations of the previous one. The red triangle represents the system's ability to recognize a failure condition and its drawback to functionality. We identify this area as the *Robustness* resilience characteristic: the system design must guarantee that the fault coverage is the maximum possible and consider a proper set of redundancy techniques to mask a faulty event. It is also crucial that the system design can report fault detection with the highest possible granularity to facilitate fault condition isolation (for example, recognizing a single memory row rather than the entire device memory in fault condition). The yellow triangle represents the system's ability to recover from a failure condition. We identify this area as the *Recovering* resilience characteristic: it is fault tolerance

in the most coherent meaning of the term. The green area is the impact on the resilience metric due to the inability of the system to recover up to full functionality. We identify this area as the *Functional-oriented* resilience characteristic: it is a cost in terms of resilience but a characteristic of the system to continue working, even if in a condition of degraded function. Even for the revised version of the resilience triangle, increasing the system's resilience means minimizing the areas of the described three regions.

If:

- $\mathcal{F}_f$  is the full functionality ratio (1) at  $\mathcal{T}_e$  disturb event time
- $\mathcal{F}_p$  is the partial functionality ratio (degraded-function) at  $\mathcal{T}_r$  recovery event time
- $\mathcal{F}_m$  is the minimum functionality ratio caused by a faulty condition at  $\mathcal{T}_m$  time

then the area of the revised resilience triangle is:

$$\begin{aligned} \mathcal{A}_{\text{Resilience}_{new}} &= \mathcal{A}_{\mathcal{R}_{new}} = \\ &= \mathcal{A}_{red} + \mathcal{A}_{yellow} + \mathcal{A}_{green} = \\ &= \frac{1}{2}(\mathcal{T}_m - \mathcal{T}_e)(1 - \mathcal{F}_m) + \frac{1}{2}(\mathcal{T}_r - \mathcal{T}_m)(\mathcal{F}_p - \mathcal{F}_m) + (\mathcal{T}_r - \mathcal{T}_m)(\mathcal{F}_f - \mathcal{F}_p) \end{aligned} \quad (4)$$

Equation 4 is the measure of the impact of the faulty condition on the system. As a consequence, equation 3 approximation is:

$$\begin{aligned} \mathcal{R}_{new} &= (\Delta t \cdot H) - \mathcal{A}_{\text{triangle}} = \\ &= (\mathcal{T}_r - \mathcal{T}_e)(\mathcal{F}_f - 0) - \mathcal{A}_{\mathcal{R}_{new}} = \\ &= (\mathcal{T}_r - \mathcal{T}_e) - \mathcal{A}_{\mathcal{R}_{new}} \end{aligned} \quad (5)$$

where:

$H$  is the amplitude of the maximum ratio of the function (1),  $\Delta t$  is the interval of the phenomenon, and  $\mathcal{A}_{\text{triangle}}$  is the area of the resilience triangle.

$\mathcal{R}_{new}$  measures the resilience of the system.

Consider how formally the proposed model for the resilience triangle coincides with the ideal triangle in the scenario of a



system exhibiting immediate response to events and capable of fully restoring its functionality.

$$\lim_{\mathcal{T}_m \rightarrow \mathcal{T}_e, \mathcal{F}_p \rightarrow \mathcal{F}_f} \mathcal{R}_{new} = \mathcal{R} \quad (6)$$

Equation 3 remains applicable (supposing  $\mathcal{F}(t)$  is a continuous function).

Section I states that effective fault management is crucial for system reliability and robustness. Fault management encompasses various strategies aimed at detecting, isolating, recovering from, and even avoiding faults within a system. These strategies ensure system resilience and uninterrupted functionality, particularly in complex and mission-critical environments. Therefore, a quick recall of crucial fault management concepts is valid, while more details are available in [1].

- **Fault Masking** Fault masking describes the phenomenon where a system can maintain full functionality despite a fault, thanks to implementing appropriate redundancy mechanisms (data, physical, or execution). In essence, fault masking ensures that faults do not disrupt system operations, enhancing system reliability and performance.
- **Fault Reporting** Fault reporting involves the timely and accurate identification and communication of faults within a system. It encompasses the process of signaling when a fault occurs, enabling subsequent actions such as fault isolation and recovery. Clear and concise fault reporting mechanisms facilitate swift troubleshooting and remediation efforts.
- **Fault Coverage** Fault coverage measures the extent to which a system's design or testing processes can detect and address faults. It quantifies the comprehensiveness of fault detection mechanisms and the system's ability to identify potential points of failure. High fault coverage indicates a thorough approach to fault management, reducing the likelihood of critical faults going unnoticed.
- **Fault Tolerance** Fault tolerance refers to a system's ability to maintain acceptable performance in the presence of faults or failures. It involves designing redundancy, error detection, and recovery mechanisms to ensure uninterrupted operation, even when faults occur. Systems can reliably work despite adverse conditions by implementing fault-tolerant architectures and techniques.
- **Fault Avoidance** Fault avoidance strategies aim to preemptively identify and mitigate potential faults before they manifest into critical failures. This proactive approach involves rigorous design, testing, and validation processes to minimize the likelihood of faults occurring during system operation. Fault avoidance measures complement other fault management techniques, enhancing system robustness and reliability.

Fault management is essential for safeguarding the reliability and resilience of complex systems. Figure 4 depicts the logical correlation between the area of the New resilience triangle

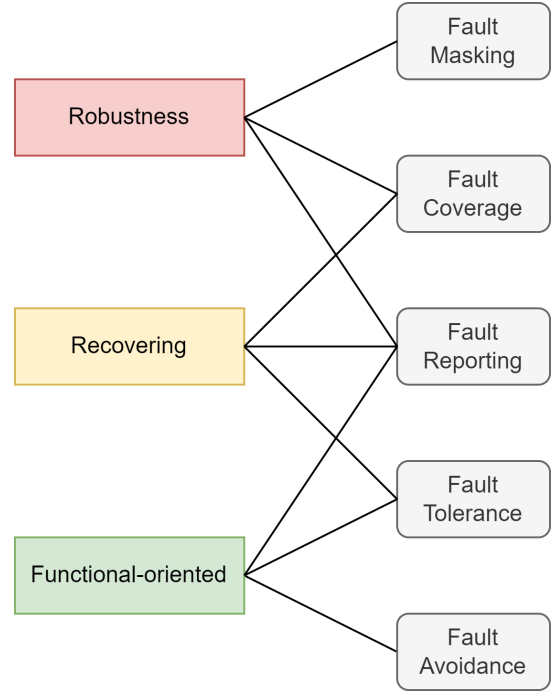


Fig. 4: The correlation between fault management concepts and the revised resilience triangle

model and the five areas of fault management, showing the fault management-oriented revisitation nature of the proposal.

## V. AN EMPIRICAL EXAMPLE: FAULTY CORE

In this section, we utilize a practical case within an embedded networking system to demonstrate the application of the new triangular model of resistance and its correlations with fault management: handling a CPU core in a faulty condition (① in Figure 5).

As previously mentioned, the hardware design phase reduces the robustness resilience component area: *fault coverage*, in this context, corresponds to the system's ability to recognize a CPU core in error condition (② in Figure 5). *Fault reporting* corresponds to the system's ability to react to the error through error notification immediately (③ in Figure 5), e.g., a system interrupt, and *fault masking* corresponds to the ability to provide error information with the necessary granularity for targeted recovery action, indicating the number of core or core ID of the one faulty condition and avoiding fault propagation based on the fault information (④ in Figure 5).

### A. Effects of Missing or Inadequate Design Fault Management for Robustness

- Lack of fault reporting → Increase in the time required to undertake recovery action due to a lack of restricted "location" or delay in fault signaling (⑥ in Figure 5).
- Lack of fault masking → Increased loss of functional ratio due to error propagation in the system (⑦ in Figure 5).

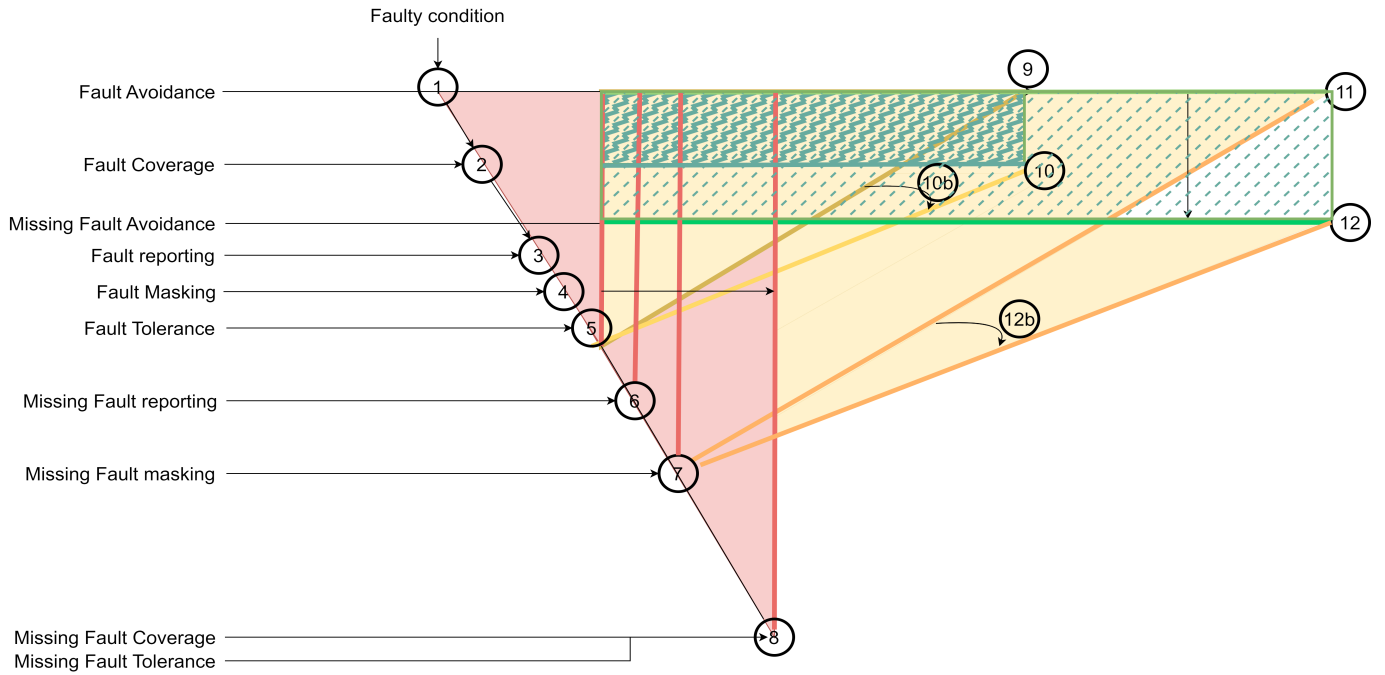


Fig. 5: The effect of fault management in the resilience triangle for a faulty core handling case

- Lack of fault coverage → Inability to detect a fault condition, increased robustness area due to the inability to directly detect functionality loss and lack of a trigger for the error condition (⑧ in Figure 5).

The fault recovery action depends on the system's fault management characteristics. *Fault coverage* is the system's ability to undertake recovery action, the core recovery mechanism in the section. *Fault tolerance*, conversely, determines the most efficient recovery action to undertake: CPU core self-test and recovery (from ⑤ in Figure 5), CPU restart (from ⑥ in Figure 5), board restart (from ⑦ in Figure 5), or power-off due to an unknown condition (at ⑧ in Figure 5). Actions that, by definition, strongly depend on *fault reporting* implementation.

#### B. Effects of Missing or Inadequate Design Fault Management on Recovery

- Lack of fault coverage → Inability to measure the functional level achieved within the recovery time (from ⑧ in Figure 5).
- Lack of fault tolerance → Inability to initiate a recovery action or ineffective recovery policy resulting in a much longer recovery time (from ⑧ in Figure 5).
- Lack of fault reporting → Increase in recovery time from an error condition due to the need for corrective and verification measures over broader system areas (core, chipset, board) (⑪ and ⑫ in Figure 5).

The recovery action's turnaround point is a function of fault management features dedicated to functional-oriented resilience components. Proper *fault reporting* identifies the *minimum functional slice* involved in the error. Allocating hardware resources into *functional slices* is a policy with which it is

possible to implement minimal-impact *fault tolerance*: fault impacts remain restricted to the *functional slice*, which means that the non-involved *functional slices* remain working at the same performance level. For the core example under discussion, the *functional slice* is the virtual core, namely the computing capacity assigned to a service instance. Resource allocation as *functional slices* also defines the redundancy cost, which is the purpose of *fault avoidance*: the system's capability to count on a spare number of redundant cores. The *fault tolerance* action could be a service migration to a spare functional slice (⑨ or ⑪ in Figure 5) or the need to review the system's resource availability to continue to work in a degraded function condition (⑩ or ⑫ in Figure 5).

#### C. Effects of Missing or Inadequate Design Fault Management on Functional-Oriented Resilience

- Lack of fault reporting → Identifying a core, rather than a cluster, or the entire processor impacts the level of function that can continue to perform even in degraded function conditions.
- Lack of fault tolerance → Without a missed function assignment for functional slices (e.g., software threads or containers for dedicated cores), the recovery action cannot be limited and tends to involve increasingly significant parts of the entire system. As a consequence, recovery times become very long (⑪ or ⑫ in Figure 5).
- Lack of fault avoidance → Directly impacts the system's ability to recover to maximum capacity. Having a certain number of redundant cores means planning activity migration to them (⑨ or ⑪ in Figure 5). The number and management of redundant cores define the breadth of the

functional ratio lost during the recovery action (from (10b) or (12b) in Figure 5).

## VI. CONCLUSIONS AND FUTURE WORK

In this paper, by defining resilience as the system's ability to withstand and recover from disruptions. We have underscored the significance of efficient fault management practices in achieving resilience. Our proposed model for measuring system resilience offers an approach that considers various aspects of fault management design, including fault management-oriented hardware design, recovery-oriented policy, and degraded function condition. By revisiting and extending the original model, we aimed to provide a more comprehensive framework that accounts for various aspects of system behavior in response to disturbances. The proposed model incorporates three key system resilience characteristics: i) Robustness, representing the system's ability to isolate and mask faults; ii) Recovery, capturing the system's ability to recover from faults and restore functionality; iii) Functional-oriented, quantifying the impact of degraded function conditions on system resilience.

Considering these aspects, our model clearly correlates system resilience and fault management strategies. Furthermore, we derived mathematical formulations to quantify the impact of faults on system resilience, providing a basis for objective evaluation and comparison of different fault management approaches. Integrating fault management concepts within the resilience model highlights the importance of effective fault detection, isolation, reporting, recovery, and avoidance strategies in enhancing system reliability and robustness.

Since the proposed model can support quantifying the fault management impacts in enhancing system resilience, as a consequence, possible future work could be: a) Conduct more empirical studies and validation experiments using real-world systems to assess the applicability and effectiveness of the proposed resilience model. b) Investigate if the resilience model applies to dynamic and evolving environments like cloud and edge computing systems. c) Explore integrating the resilience model with decision support systems to assist engineers in evaluating fault management strategies.

## ACKNOWLEDGEMENT

The work presented in this paper is sponsored by Ericsson, Mälardalen University and the Swedish Knowledge Foundation (KKS), via the industrial PhD School ARRAY.

## REFERENCES

- [1] C. Vitucci, D. Sundmark, M. Jägemar, J. Danielsson, A. Larsson, and T. Nolte, "Fault management impacts on the networking systems hardware design." Annual Conference of the IEEE Industrial Electronics Society, IECON, 2023, pp. 1–8.
- [2] —, "A reliability-oriented faults taxonomy and a recovery-oriented methodological approach for systems resilience," *Proceeding IEEE 46th Annual Computers, Software, and Applications Conference (COMPSAC)*, pp. 48–55, 6 2022.
- [3] C. Vitucci, D. Sundmark, J. Danielsson, M. Jägemar, A. Larsson, and T. Nolte, "Run time memory error recovery process in networking system." International Conference on System Reliability and Safety, ICSRS, 2023, pp. 590–597.
- [4] A. Aldea, E. Vaicekauskaitė, M. Daneva, and J. P. S. Piest, "Assessing resilience in enterprise architecture: A systematic review," 2020.
- [5] B. C. Watson, M. J. Weissburg, and B. Bras, "Sosrm: A new metric to standardize system-of system resilience evaluation," 2020.
- [6] M. Bruneau, S. E. Chang, R. T. Eguchi, G. C. Lee, T. D. O'Rourke, A. M. Reinhorn, M. Shinozuka, K. J. Tierney, W. A. Wallace, and D. von Winterfeldt, "A framework to quantitatively assess and enhance the seismic resilience of communities," *Earthquake Spectra*, vol. 19, pp. 733 – 752, 2003. [Online]. Available: <https://api.semanticscholar.org/CorpusID:1763825>
- [7] R. K. Buchanan, S. R. Goerger, C. H. Rinaudo, G. Parnell, A. Ross, and V. Sitterle, "Resilience in engineered resilient systems," *Journal of Defense Modeling and Simulation*, vol. 17, 2020.
- [8] F. Ren, T. Zhao, J. Jiao, and Y. Hu, "Resilience optimization for complex engineered systems based on the multi-dimensional resilience concept," *IEEE Access*, vol. 5, pp. 19 352–19 362, 9 2017.
- [9] C. W. Zobel, "Comparative visualization of predicted disaster resilience." Information Systems for Crisis Response and Management, ISCRAM, 2010.
- [10] S. Hosseini, K. Barker, and J. E. Ramirez-Marquez, "A review of definitions and measures of system resilience," *Reliability Engineering and System Safety*, vol. 145, 2016.
- [11] M. Bevilacqua, F. E. Ciarapica, and G. Marcucci, "Supply chain resilience triangle: The study and development of a framework," *International Journal of Economics and Management Engineering*, vol. 11, pp. 2046–2053, 2017.
- [12] Q. C. Lu, "Modeling network resilience of rail transit under operational incidents," *Transportation Research Part A: Policy and Practice*, vol. 117, 2018.
- [13] C. Niu, T. Zhang, D. J. Nair, V. Dixit, and P. Murray-Tuite, "Link-level resilience analysis for real-world networks using crowd-sourced data," *International Journal of Disaster Risk Reduction*, vol. 73, 4 2022.
- [14] K. Govindan, S. G. Azevedo, H. Carvalho, and V. Cruz-Machado, "Lean, green and resilient practices influence on supply chain performance: interpretive structural modeling approach," *International Journal of Environmental Science and Technology*, vol. 12, 2015.
- [15] A. Luo, Y. X. Kou, J. Liu, and T. Chen, "The resilience measure method to information systems," 2018.
- [16] R. Freeman, C. McMahon, and P. Godfrey, "Design of an integrated assessment of re-distributed manufacturing for the sustainable, resilient city," vol. 52, 2016.
- [17] D. Wei and K. Ji, "Resilient industrial control system (rics): Concepts, formulation, metrics, and insights," 2010.
- [18] A. K. Ravulakollu, L. Urciuoli, B. Rukanova, Y. H. Tan, and R. A. Hakvoort, "Risk based framework for assessing resilience in a complex multi-actor supply chain domain," *Supply Chain Forum*, vol. 19, pp. 266–281, 10 2018.
- [19] P. Singh, A. Amekudzi-Kennedy, B. Ashuri, M. Chester, S. Labi, and T. A. Wall, "Developing adaptive resilience in infrastructure systems: an approach to quantify long-term benefits," *Sustainable and Resilient Infrastructure*, vol. 8, 2023.
- [20] K. Song, S. You, and J. Chon, "Simulation modeling for a resilience improvement plan for natural disasters in a coastal area," *Environmental Pollution*, vol. 242, 2018.
- [21] J. Chen, J. Liu, Q. Peng, and Y. Yin, "Resilience assessment of an urban rail transit network: A case study of chengdu subway," *Physica A: Statistical Mechanics and its Applications*, vol. 586, 1 2022.
- [22] S. Dong, X. Gao, A. Mostafavi, J. Gao, and U. Gangwal, "Characterizing resilience of flood-disrupted dynamic transportation network through the lens of link reliability and stability," *Reliability Engineering and System Safety*, vol. 232, 2023.
- [23] T. Kanno, T. Fujii, R. Watari, and K. Furuta, *Modeling And Simulation Of A Service System In A Disaster To Assess Its Resilience*. Presses des Mines, 10 2016, pp. 128–134.
- [24] N. Wang and K. F. Yuen, "Resilience assessment of waterway transportation systems: Combining system performance and recovery cost," *Reliability Engineering and System Safety*, vol. 226, 2022.
- [25] J. Yin, X. Ren, R. Liu, T. Tang, and S. Su, "Quantitative analysis for resilience-based urban rail systems: A hybrid knowledge-based and data-driven approach," *Reliability Engineering and System Safety*, vol. 219, 2022.
- [26] D. Escudero-Mancebo, N. Fernández-Villalobos, Óscar Martín-Llorente, and A. Martínez-Monés, "Research methods in engineering design: a synthesis of recent studies using a systematic literature review," *Research in Engineering Design*, 2023.