Analysis of Shipboard Survivable Fire Main Systems

Albert Ortiz[1], Don Dalessandro[1], Dong Qing[1], Li Bai[2] and Saroj Biswas[2]

1. Department of the Navy, Naval Surface Warfare Center, Carderock Division, Philadelphia, USA
2. Department of Electrical and Computer Engineering, Temple University, Philadelphia, USA

ABSTRACT

This paper presents a study for the shipboard fire main systems using a new probabilistic approach to analyze the survivability of a system. Similarities and differences between survivability and reliability analysis are compared. In a reliability model, one can describe a k-out-of-n:G system (k <= n), in which the component system is valid only if any k or more components function. The system can also be configured into an initial k-out-of-n:G model with m backup components (0 <= m <= n). If the system cannot perform its intended function, the m backup components will be reconfigured with the remaining working components into a new form to sustain system function. Academia refers to such studies to calculate the system successful probabilities as the survivability analysis. In this paper, we focus on the survivability analysis of a shipboard fire main piping system. This study could potentially be used to analyze the survivability of power network systems, dependable secure computing systems, military reconfigurable information systems, and other large reconfigurable network systems.

Keywords – survivability, reliability, k-out-of-n:G system, reconfiguration.

1. INTRODUCTION

In shipboard applications, many systems are built with reconfiguration capabilities that the systems can still perform its intended operations when the initial configuration cannot sustain its original functions due to break down of certain components or sub-components. In the theory of evolution, Charles Darwin addressed the issue of reconfiguration capability as a way to survive through species' adaptation due to environment changes. He referred natural selection or survival of the fittest as a direct result from variations. To complement the theory of reliability defined for redundancy systems, Bai et. al. [1] proposed a probabilistic definition of survivability and developed a survivability framework for redundancy systems which are capable of reconfiguring themselves at the event of failure. Since the system can have different configurations, situation assessment becomes a direct extension of the theory because the system has to correctly identify the direction of threat.

Papanikolaou and Boulougouris [2] also addressed design aspects of survivability for surface naval and merchant ships. They offered a mathematical formula showing how to compute survivability. According to their definition, the survivability P_s is calculated as

$$P_s = 1 - P_k = 1 - P_{su}P_v ,$$

where P_k is the killability, P_{su} is the susceptibility and P_v is the vulnerability. This formulation is very intuitive and a top-down approach. Since large integrated system often consists of many subsystems such as power modules, communication modules, or computation modules, etc, they are not only susceptible for failure in the direction of threats, also are affected by cascade failures from other interconnected subsystems. To calculate system's survivability, the system can first be divided into these smaller subsystems in terms of probability of susceptibility. The vulnerability of the system is directly dependent on the reliability of subsystems. As a result, the survivability formulation for a reconfigurable system becomes complex and difficult to be evaluated. Varshney et al. [3] explained the difference between reliability and survivability in the context of mean time between failures (MTBF). Likewise, the definition did not consider the system reconfiguration.

In this paper, we review the theory of survivability proposed by Bai et. al. [1] using a simple reconfigurable piping system and investigate the survivability of the fire main systems. The rest of the paper is organized as follows. The main survivability ideas are reviewed and presented in section II. Section III is given to show how the survivability is calculated for the fire main systems. We conclude the paper in section IV.

2. REVIEW OF SURVIVABILITY

To better understand the reliability and survivability analysis, we describe briefly several key reliability models.

2.1 Reliability Models

Typically, a reliable system has redundant components to sustain system function if a few components fail. For example, there are various studies on *k*-out-of-*n*:G or *k*-out-of-*n*:F systems. Kuo and Zuo [4] classified:

i. The *k*-out-of-*n*:G system works (well) when at least k components work among all n components.
ii. The *k*-out-of-*n*:F system fails when at least k components can not function among all n components.

These two systems are equivalent where a *k*-out-of-*n*:G system is the same as a (*n*−*k*+1)-out-of-*n*:F system. The reliability of a *k*-out-of-*n*:G system is to compute the successful probability of the system. For example, we can calculate the reliability of a *k*-out-of-*n*:G with *n* identical components whose successful probabilities are *p* as,

$$R = \sum_{i=k}^{n} \binom{n}{i} p^i (1-p)^{n-i} ,$$

where $\binom{n}{i}$ is the combination for *n* choose *i*. Also, the reliability model considers the uniform threat from all directions. In other words, a specific threat direction does not have any influence on the successful probability of the components in the reliability model, or the reliability stays the same regardless of where the threat is from.

2.2 Survivability Models

A survivable system is a reliable system with reconfiguration capability. To precisely define survivability, the initial form (or original configuration) is an important factor which is also directly related to where the threat direction is from. The system can perform its functions by varying into a new form when it cannot survive in its original form. We define the survivability of a reconfigurable system as

$$S = R(f_0) + \sum_{i \neq 0} Q(f_0 \rightarrow f_i) A(f_i) R(f_i, c_i) \qquad (1)$$

where $R(f_0)$ is the reliability of an initial configuration f_0 and $A(f_i)$ is probability of successful adaptation into a new configuration f_i. Since a system has to be fault tolerant, the configuration f_0 requires several redundant components in order to provide sufficient reliability. When threats come from different directions, we can compute reliability of each component by using total probability theorem as,

$$p(c) = \sum_j p(c \mid T_j) p(T_j)$$

where T_j is the direction of a threat, p(T_j) is a-prior probability of the threat, and $p(c|T_j$) is conditional reliability of component based on a particular threat T_j . The component reliability can further be classified as a *k*-out-of-*n*:G (good) system reliability metric shown as $R(f_0)$ and $R(f_i, c_i)$. This formulation includes the idea of susceptibility, reliability as well as adaptability for possible reconfiguration solutions. As shown in the formulation, there is a term $Q(f_0 \rightarrow f_i)$ that implies the system requires modification from its initial form. Since the modification can occur under different circumstances, it can result in the following two types of survivability analysis: i) adaptation and ii) mutation.

i. Adaptation survivability refers to a system that reconfigures itself only when its initial form fails to work.

ii. Mutation survivability refers to a system that can reconfigure itself even when its initial form is still performing its tasks.

In our engineering analysis of survivability, we simply investigate the adaptation survivability of a system because many survivable engineering applications require a new configuration to sustain operations only when the initial form fails to work. During reconfiguration states, engineers and technicians can be dispatched to repair the failed components in their initial form. It is apparent that adaptation survivability is a more applicable analysis for engineering survivable systems.

2.3 A Simple Survivable System

First, we consider a simple survivable system shown in Figure 1 where the system has two pumps and only one can be operated due to a limited power supply or pipe pressure. The pump supplies enough water to three sprinkler pipes in the middle segment of the system at any given time. We refer to the middle segment as the survivable space. As we can see, the main threat is from the right hand-side of the system and we can assume that $p_1 < p_2$ where p_i is the successful probability of the pump *i*. However, a reliable model will not consider the two pumps as being different because the system is unaware of where the threat is coming from. Rather, an initial form can be chosen to either operate pump 1 or operate pump 2.

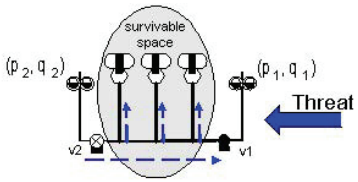


Fig. 1. Two Pumps Shipboard Firemain System

After the initial form is chosen to operate pump 1, the reliability is

$$R = p_1,$$

or the reliability can become p_2 if pump 2 is operated in its initial form.

The values of p_1 and p_2 are highly dependant on where the threat is coming from. If a reliable and reconfigurable system can identify where the threat is coming from and reconfigure itself accordingly, the system becomes survivable. A better way is to operate the pump with the lower threat. In other words, the appropriate survivable system is to operate pump 2 and reconfigure itself to operate pump 1 when pump 2 fails. Here we have a survivable model with an initial form of operating a 1-out-of-1:G system for pump 2 with pump 1 as a backup. If pump 2 fails, there are four reconfiguration possibilities to open or close valve 1 and valve 2. Among them, two

possibilities enable pump 1 to supply water flow to the sprinkler pipes as shown in Figure 2:

i. valve 1 is on and valve 2 is on,
ii. valve 1 is on and valve 2 is off.

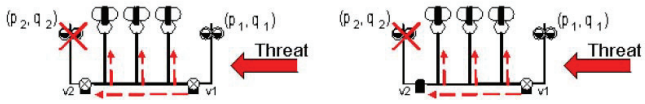


Fig. 2. Pumps Reconfiguration Choices

Consequently, the system survivability is computed by using (1) as

$$S = R(f_0) + \sum_{i=1}^{2} Q(f_0 \rightarrow f_i) A(f_i) R(f_i, P^{(1)})$$

$$= p_2 + q_2 \frac{2}{4} p_1 = p_2 + \frac{1}{2} q_2 p_1,$$

where q_2 is the failure probability of pump 2. Conversely, we can define the non-survivability as

$$\overline{S} = \sum Q(f_0 \rightarrow f_i)(A(f_i) Q(f_i, c_i) + \overline{A}(f_i)) \qquad (2)$$

where $A(f_i)$ is the probability of successfully adaptation, $\overline{A}(f_i)$ is the probability of failed adaptation, and $Q(f_i, c_i)$ is the failure probability of newly added components c_i in the newly reconfigured form f_i. The definition is relatively easy to understand that

i. The term $Q(f_0 \rightarrow f_i)$ indicates the probability that a new form f_i will be reconfigured.
ii. The term $A(f_i)Q(f_i, c_i)$ indicates that newly components c_i fails to work in the new form f_i.
iii. The third term $\overline{A}(f_i)$ indicates that the system cannot be updated into a new form f_i.

These conditions all produce a system without survivable options. We can use the same idea to compute the non-survivability of the current system when pump 2 fails to work. There are two situations:

i. valve 1 is on but pump 1 fails, and
ii. valve 1 cannot be turned on.

In both conditions, we can use (2) to calculate the non-survivability as,

$$\overline{S} = q_2 \left(\frac{1}{2} q_1 + \frac{1}{2} \right)$$

Interesting enough, we can also verify that the sum of the survivability and non-survivability is unity, or

$$S + \overline{S} = p_2 + \frac{1}{2} q_2 p_1 + q_2 \left(\frac{1}{2} q_1 + \frac{1}{2} \right) = 1.$$

In the current system, we can easily see that S > R. It implies that a survivable system can have a higher successful probability than a reliable system. The survivable system is capable of configuring an initial form depending on where the threat is coming from, and it can reconfigure itself to avoid failures. If the system cannot identify where the threat is coming from, its survivability will be degraded. For the same system shown in Figure 1, the survivability of the system when it can identify the threat correctly is

$$S = p_2 + \frac{1}{2} q_2 p_1.$$

We can compare it with another system that identifies the threat as coming from the wrong direction, or the system operates pump 1 in its initial form. The survivability of such a system is

$$\widetilde{S} = p_1 + \frac{1}{2} q_1 p_2.$$

Clearly, we can calculate

$$S - \widetilde{S} = \left(p_2 + \frac{1}{2} q_2 p_1 \right) - \left(p_1 + \frac{1}{2} q_1 p_2 \right) = \frac{3}{2} (p_2 - p_1) \geq 0.$$

More precisely, we prove that $S \geq \widetilde{S}$. This result suggests that a reconfigurable system is more survivable if its initial form is determined by avoiding the threat. In other words, a threat aware and reconfigurable system has a clear advantage in terms of better survivability. We can prove this concept in the following theorem.

Theorem 1: Survival of the Fittest – *A threat aware and reconfigurable system is more capable of surviving.*

Proof For a more general system, suppose we have two different initial forms, $f_0^{(1)}$ and $f_0^{(2)}$. If the form $f_0^{(1)}$ is configured with threat awareness capability, we have $R(f_0^{(1)}) > R(f_0^{(2)})$. Since both initial forms have the same number of components and backup components. We have same number of survivable forms available for the survivable options, or

$$R(f_0^{(1)}) + \sum_{i \neq 0} Q(f_0^{(1)} \rightarrow f_i) = 1,$$

$$R(f_0^{(2)}) + \sum_{i \neq 0} Q(f_0^{(2)} \rightarrow f_i) = 1.$$

Since $R(f_0^{(1)}) > R(f_0^{(2)})$, it implies that

$$\sum_{i \neq 0} Q(f_0^{(1)} \rightarrow f_i) < \sum_{i \neq 0} Q(f_0^{(2)} \rightarrow f_i), \text{ or}$$

$$\sum_{i \neq 0} Q(f_0^{(1)} \rightarrow f_i) - \sum_{i \neq 0} Q(f_0^{(2)} \rightarrow f_i) < 0..$$

Also, since $A(f_i) \geq 0$ and $Q(f_i, c_i) \geq 0$, we know $A(f_i)Q(f_i, c_i) + \overline{A}(f_i) \geq 0$. It suggests that

$$\sum_{i \neq 0} Q(f_0^{(1)} \rightarrow f_i)\left(A(f_i)Q(f_i, c_i) + \overline{A}(f_i)\right) - \sum_{i \neq 0} Q(f_0^{(2)} \rightarrow f_i)\left(A(f_i)Q(f_i, c_i) + \overline{A}(f_i)\right) < 0.$$

It implies that $\overline{S}^{(1)} - \overline{S}^{(2)} < 0$. We know that $S = 1 - \overline{S}$, it means that $S^{(1)} > S^{(2)}$. ■

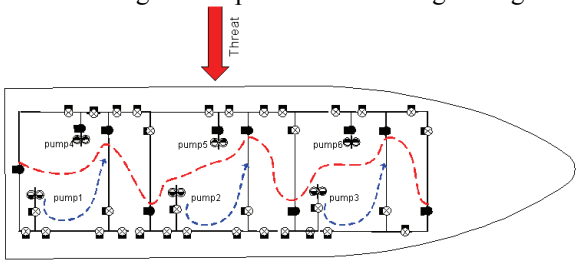
From Theorem 1, we validate the concept that a reconfigurable system has better survivability if the system has threat awareness capability. Nonetheless, we

demonstrate the difference between the survivability and reliability analysis.

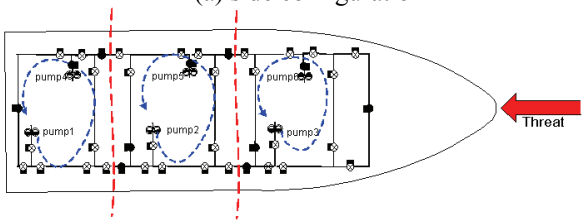
3. SURVIVABILITY OF SHIPBOARD FIRE MAIN SYSTEM

In a simplistic view of the shipboard fire main system, there are six pumps, and each pump can supply water flow into the sprinkler pipes. There are two types of threats that can result with two initial configurations as shown in Figures 3(a) and 3(b).

In either configuration for the complete shipboard survivability, maximum three pumps are allowed to operate in the same time, say that pumps 1-3 are in operation to supply the water flow into the sprinkler pipes so that water pressure will be provided to extinguish fires. Generally, at least one pump per compartment or two pumps per three compartments have be operated so that there is enough water pressures for extinguishing fire.



(a) side configuration



(b) zone configuration

Consequentially, system design allows the following two initial configurations:

- side configuration (shown in Figure 3(a)) has an initial 2-out-of-3:G system (two pumps per three compartment). When any two pumps fail, the system will reconfigure and sustain the survivable mission.
- zonal configuration (shown in Figure 3(b)) has three initial 1-out-of-1:G systems (one pumps per compartment). When a pump in any subsections fails, other pump will be in operation to sustain the survivable mission.

Here, we denote $p^{(i)}$ as successful probability and $q^{(i)}$ as failure probability of the i-th pump respectively. Then, we can determine the survivability two shipboard fire main system configurations.

3.1 Survivability of Side Configuration

As shown in the Figure 3(a), the threat comes from the opposite side of pumps 1-3. Therefore, we can assume

$$p^{(1)} = p^{(2)} = p^{(3)},\ p^{(4)} = p^{(5)} = p^{(6)},$$
$$q^{(1)} = q^{(2)} = q^{(3)},\ \text{and}\ q^{(4)} = q^{(5)} = q^{(6)}.$$

For simplicity, we denote

$$p^{(1)} = p^{(2)} = p^{(3)} = p1,$$
$$p^{(4)} = p^{(5)} = p^{(6)} = p2,$$
$$q^{(1)} = q^{(2)} = q^{(3)} = q1,$$
$$q^{(4)} = q^{(5)} = q^{(6)} = q2.$$

Also, $p1+q1 = 1$ and $p2+q2 = 1$. Since the threat is from the side of pumps 4-6, we know that $p1 > p2$. The initial configuration is to allow pumps 1-3 to operate in a 2-out-of-3:G system because the system can provide at least two pumps' water pressure to three compartments. Therefore, the reliability of the initial system configuration is

$$R(f_0) = p_1^3 + \binom{3}{2} p_1^2 q_1$$

There are two conditions that the system must be reconfigured.

1. When any two pumps among pumps 1-3 fail, any one or two pumps among pumps 4-6 are switched open to continue operating with the pumps remain working.
2. When all three pumps among pumps 1-3 fail, the section of the pumps are close. Any two or three pumps among pumps 4-6 have to be switched open.

Therefore, the probability that the first condition will occur with either one or two pumps and corresponding valve opening correctly as

$$\binom{3}{1}\frac{1}{8} p_2 + \binom{3}{2}\frac{1}{4} p_2^2,$$

Similarly, the probability is the second condition is

$$\binom{3}{2}\frac{1}{4} p_2^2 + \binom{3}{3}\frac{1}{8} p_2^3,$$

The system survivability is

$$S_{side} = R(f_0) + \sum_{i \neq 0} Q(f_0 \rightarrow f_i) A(f_i) R(f_i, c_i)$$

$$= p_1^3 + \binom{3}{2} p_1^2 q_1 + \binom{3}{2} q_1^2 p_1 \left[\binom{3}{1}\frac{1}{8} p_2 + \binom{3}{2}\frac{1}{4} p_2^2 \right] +$$

$$\binom{3}{3} q_1^3 \left[\binom{3}{2}\frac{1}{4} p_2^2 + \binom{3}{3}\frac{1}{8} p_2^3 \right]$$

3.2 Survivability of Zonal Configuration

As shown in the zone configuration in Figure 3(b), the successful and failure probabilities of pumps are different than that in the side configuration because the threat is in the front of the ship. The probabilities are:

$$p^{(1)} = p^{(4)},\ p^{(2)} = p^{(5)},\ p^{(3)} = p^{(6)},$$
$$q^{(1)} = q^{(4)},\ q^{(2)} = q^{(5)},\ \text{and}\ q^{(3)} = q^{(6)}.$$

Also, we denote

$$p^{(1)} = p^{(4)} = p1,$$
$$p^{(2)} = p^{(5)} = p2,$$

$$p^{(3)} = p^{(6)} = p3,$$
$$q^{(1)} = p^{(4)} = q1,$$
$$q^{(2)} = p^{(5)} = q2,$$
$$q^{(3)} = p^{(6)} = q3.$$

Also, $p1+q1 = 1$, $p2+q2 = 1$, and $p3+q3 = 1$. Since the threat is coming from in the front of the ship, we know that $p1 > p2 > p3$. The initial configuration is to allow pumps 1-3 to operate in a 1-out-of-1:G system because the system can provide at least two pumps' water pressure to three compartments.

There are many possibilities that different zone can survive from the attack and each compartment has the exact same survivability, we can compute the non-survivability of one zone before we calculate whole shipboard survivability.

To compute the non-survivability of the compartment with pumps 1 and 4, there are two possibilities that the subsection can fail completely:

1. When pump 1 fails, pump 4 is not operable even the pump valve is switched open, and
2. When pump valve cannot be opened despite whether pump 4 is operable.

Therefore, the non-survivability of the subsection can be calculated as

$$\bar{S}_1 = Q(f_0 \to f_1)\left(\frac{1}{2}q_1 + \frac{1}{2}\right) = \frac{1}{2}q_1(q_1+1).$$

Consequentially, the whole shipboard system survivability is the product of three subsections' survivability

$$S_{zone} = \prod_{i=1}^{3}(1-\bar{S}_i) = \prod_{i=1}^{3}\left(1-\frac{1}{2}q_i(q_i-1)\right).$$

3.3 Wrong Fire Main Configuration

Intuitively, zonal configuration is suitable for the threat is coming from in the front of ship; and side configurable is better for the threat is from the side of the ship. Here we demonstrate how to use the survivability metric why the zonal configurable cannot be used when the threat is coming from the side of the ship as shown in Figure 4.

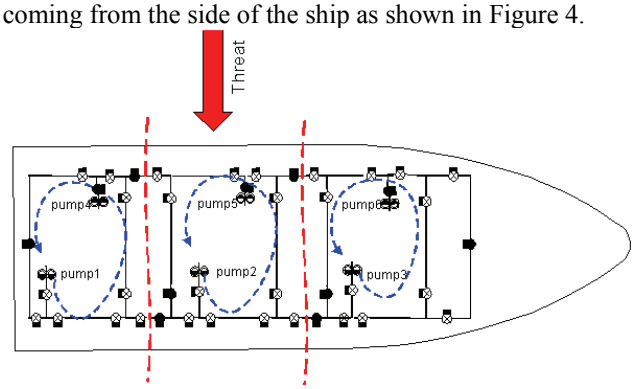


Figure 4. Wrong Fire Main Configuration

As shown in the Figure 4, the threat comes from the opposite side of pumps 1-3. We know that

$$p^{(1)} = p^{(2)} = p^{(3)},\ p^{(4)} = p^{(5)} = p^{(6)},$$
$$q^{(1)} = q^{(2)} = q^{(3)},\ \text{and}\ q^{(4)} = q^{(5)} = q^{(6)}.$$

We denote

$$p^{(1)} = p^{(2)} = p^{(3)} = p1,$$
$$p^{(4)} = p^{(5)} = p^{(6)} = p2,$$
$$q^{(1)} = q^{(2)} = q^{(3)} = q1,$$
$$q^{(4)} = q^{(5)} = q^{(6)} = q2.$$

Also, $p1+q1 = 1$ and $p2+q2 = 1$. Since the threat is from the side of pumps 4-6, we know that $p1 > p2$. However, the initial configuration is to allow pumps 1-3 to operate in a 1-out-of-1:G system because it is in the zonal configuration.

Using the same analysis from the zonal configuration, we can find the whole shipboard survivability as

$$S_{wrong} = \prod_{i=1}^{3}(1-\bar{S}_{wrong}) = \left(1-\frac{1}{2}q_1(q_2+1)\right)^3$$
$$= \left(p_1 + \frac{1}{2}q_1p_2\right)^3.$$

One can easily validate that $S_{side} > S_{wrong}$. It implies that the side configuration should be used when the threat is coming in the side of the ship. The similar result can be obtained if we use side configuration for the threat which is coming the front of the ship. Consequentially, situation awareness is important for the survivability of the shipboard fire main system.

4. CONCLUSION

In this paper, we present a theory for analyzing survivability, and show how it is different from reliability analysis. We are able to use the theory to compute the survivability of shipboard fire main systems. Furthermore, we can mathematically describe how effective a configuration can be measured to survive threat.

REFERENCES

[1] Li Bai, Saroj Biswas, Albert Ortiz, Frank Ferrese, Don Dalessandro and Qing Dong, "Survivability Analysis of Reconfigurable Systems", the International Conference on Industrial Engineering and Engineering Management (IEEM) 2007, Singapore.

[2] Papanikolaou, A., Boulougouris, E. "Design aspects of survivability of surface naval and merchant ships", in Proceedings of International Conference on Naval Technology, Piraeus, Greece (1998)

[3] Varshney, U., Snow, A.P., Malloy, A.D. "Measuring the reliability and survivability of infrastructure-oriented

wireless networks" in The 26th Annual IEEE Conference on Local Computer Networks, 2001. Proceedings. LCN 2001, IEEE (2001) pp. 611 – 618

[4] Kuo, W., Zuo, M.J. "Optimal Reliability Modeling: Principles and Applications". John Wiley & Sons, Inc. (2002), chapter 7, pp. 231–280.