MODELING THE EFFECTS OF THE TWO STOCHASTIC-PROCESSES ON THE RELIABILITY AND MAINTENANCE OF *k*-OUT-OF-*n* SURVEILLANCE SYSTEMS

By YAO ZHANG

A Dissertation submitted to the

Graduate School-New Brunswick

Rutgers, The State University of New Jersey

In partial fulfillment of the requirements

For the degree of

Doctor of Philosophy

Graduate Program in Industrial and Systems Engineering

Written under the direction of

Dr. Hoang Pham

And approved by

_____

_____

_____

_____

New Brunswick, New Jersey

MAY, 2014

ABSTRACT OF THE DISSERTATION

Modeling the Effects of the Two Stochastic-Processes on the Reliability and Maintenance of *k*-out-of-*n* Surveillance Systems

By YAO ZHANG

Dissertation Director:

Dr. Hoang Pham

Surveillance systems, including security cameras, have been widely used to monitor some critical processes and enhance the safety-security level of high-risk large-scale security systems. The failure of these systems should be analyzed and associated with the intrusion/incident arrival process in order to achieve a comprehensive representation of the system outcomes. This thesis aims to model the effects of the two stochastic processes on the reliability modeling of the surveillance systems. The two processes are: (1) the traditional system failure process (first process) and (2) the intrusion/incident arrival process or the demand process (second process).

In this research we develop reliability models with considerations of the two stochastic-processes for the *k*-out-of-*n* surveillance systems. The first model considers the undetectable failures of each subsystem along with the random environmental factors, the skill factor of the intruders to avoid detection, and a periodic inspection maintenance aspect. The second model includes both the detectable and undetectable failure modes for

the subsystems. The reliability of the system is derived with a consideration of an opportunistic maintenance policy. Numerical examples are given to demonstrate the validity of the modeling and the sensitivity of various model parameters.

We also develop a cost model with considerations of both the detectable and undetectable failure modes for the subsystems. We then obtain the opportunistic maintenance policy that minimizes the total system cost based on the second model. We also extend the second reliability model by considering the fail-safe error for each subsystem in the two-process modeling of the k-out-of-n surveillance systems. Numerical examples are discussed to illustrate the model developments and results.

ACKNOWLEDGEMENT

I would like to thank my research advisor, my committee members, colleagues and my family for the help and support during the research.

Firstly, I would like to express my deep gratitude to my advisor, Dr. Hoang Pham, for his priceless advices, patience, support and encouragement not only on my research topics but also on being a better person.

I would also like to express my appreciation to the committee members, Dr. W. Art Chaovalitwongse, Dr. Elsayed A. Elsayed and Dr. Myong K. Jeong, for their valuable suggestions on my research.

Special thanks go to the staff and colleagues of the department of Industrial and Systems Engineering for creating and maintaining a harmonious and positive working environment.

Finally, I wish to thank my family for their undivided support and encouragement.

DEDICATION

To my beloved wife Yi Xu, my parents Xu Zhang and Ming Yao.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

Chapter 1

Introduction

The application of surveillance systems is a great enhancement of security level to the monitored area by providing important reference for the security teams to make prompt actions against threats or incidents. The US government spent billions of dollars on installation of surveillance cameras to protect citizens from crime [1]. The widespread implementation of the surveillance cameras significantly deters criminal behavior and reduces vandalism to agency property. With the rapid progress in automated control, image processing and high performance computing, the surveillance system become more and more capable of providing comprehensive information on the protected area [2]. Since the wide implementation of the surveillance systems and the fact that either failure or deterioration in performance of the system may result in severe damage to the protected facility, the reliability estimation of the system and inspection or maintenance scheduling is worth receiving serious attention [3]. Two incidents are discussed briefly here just to emphasize the importance of modeling and scheduling for the surveillance systems. On January 3rd, 2010, the Newark Liberty International Airport had a security breach that one man reached the secure sterile area through a checkpoint exit without being screened by airport security [4]. Due to the breakdown of the surveillance recording system, the airport authority failed to identify the inadvertent intruder until they got the footage from the redundant cameras two hours later. The incident caused hours of delay in flights and thousands of passengers to be rescreened before boarding. The second example is the incident occurred on August 13, 2012. A man ran out of gas of his jet ski at Jamaica Bay in New York. He climbed the 8-foot-high perimeter fence and

walked across the two runways seeking for help, without being detected by the perimeter intrusion detection system (PIDS), which should be given out series of warnings under the circumstance [5]. Those lessons raise the questions about how reliable of such security detection systems and the requirements of comprehensive model for assessing the reliability of those critical systems in general. To design reliability model and maintenance schedules for the surveillance systems subject to environmental factors, several aspects such as the intrusion/incident process and multiple subsystem failure modes are critical to be considered in the modeling.

1.1 Consideration of Multi-Unit Multi-State Systems

Adding redundancy is one of the most widely used approaches to enhance the reliability of the system. The application of k-out-of-n systems receives a lot of attention in the literature for its generality and simplicity to evaluate the reliability. Hence it is selected in the modeling of the surveillance systems. The subsystems in the system usually have certain type of mechanism to examine the performance of the unit so that a portion of the failures can be detected. Thus both detectable and undetectable failures are possible for the unit of the system. Automatic scene classification has been developed for years in order to use computer to extract information from surveillance videos to detect potential threats [6]. Since the pattern recognition technique is never perfect, each subsystem can either fail to detect an upcoming threat or falsely report a threat that does not exist. In summary, considering the units with multiple failure mechanism is necessary for a realistic surveillance system modeling.

1.2 Consideration of Multi-Process Models

For most reliability modeling, only the system operating process is taken into consideration. However, for the surveillance redundant system, its goal is to monitor and record actions of incidents or attacks. Ideally, the system is only required to be available at the time point when the attack occurred and perhaps can fail for some other time. Although it is not possible for the ideal case because of the random nature of the arrival of attacks, consider the following scenario: the system may have already failed; however, it reaches maintenance point without encountering any incident. This case may still be considered as "soft-failure" since no incident has taken the chance of the surveillance system failure to produce real damage to the area. If ignoring the intrusion/incident arrival process, it will result in more frequent maintenance action than necessary, which is always associate with increment of system down time and restore cost.

1.3 Consideration of Appropriate Maintenance Schedules for Multi-Unit Systems

For multi-unit systems, it is typical that there exists dependency between subsystems, such as economic dependence, failure dependence and structural dependence [7]. The maintenance strategy defers from the ones for single unit systems, as that the failure of one subsystem provides the opportunity to maintenance other subsystems in the system as well. On the one hand, if the failure status of the individual unit is not available, the only possible rule that can be applied is the periodic inspection. The policy requires that the system to be repeatedly inspected in scheduled checking time points. Once the failures are detected, they are fixed right after the successful inspection. On the other hand, if the failure status of the individual unit is available, some failures in the system can be held

until the pre-determined number of failures has been accumulated in the system to perform the maintenance. For both cases, the preventive maintenance on the working subsystems can also be carried out at the same time to further enhance the performance of the entire system.

1.4 Consideration of Maintenance Optimization

The maintenance policy for multi-unit systems aims to reduce the cost by grouping the maintenance action of multiple units together instead of determining the optimal time point for each individual unit for service. It will sacrifice with higher risks in the system by leaving failures in the system, in order to achieve overall economic benefits. Once the costs of different system outcome are determined, the optimal maintenance parameters can be achieved by balancing the system requirements and resources available in hand.

1.5 Overview of the Thesis

The thesis is organized as the following. In Chapter 1, a general introduction on the needs of the reliability modeling and maintenance schedule of the surveillance systems is given. In Chapter 2, the literature review on different aspects that is considered in the modeling is presented, including multi-unit, multi-state and multi-process system reliability modeling, along with the maintenance schedule for system with multi-units and undetectable failure mechanism. In Chapter 3, the objectives of the research and the logics between different developed models are discussed. In Chapter 4, a reliability model considering both the unit failure and intrusion/attack process is first introduced, with relatively simple assumption of two-state units and periodic perfect maintenance

rule. In Chapter 5, the modeling extends to the system with components that have both detectable and undetectable failure modes. In Chapter 6, the cost model to obtain the optimal maintenance parameters based on the system model in Chapter 5 are developed. In Chapter 7, the full model that includes all 4 types of failure modes for each sensor for the surveillance system is derived. Comparisons between all purposed models are given to demonstrate that the models in Chapter 4 and 5 are special cases of the model in Chapter 7. Chapter 8 presents the conclusion of this research and discusses potential future research problems.

Chapter 2

Literature Review

In this thesis work, several reliability models and the maintenance scheduling for the surveillance systems have been developed. The models have considered k-out-of-n system structure with sensors having multiple states, especially the undetectable failure mode. Since the surveillance systems are used to monitor some critical areas and environments, the demand process that describes the arrival of intrusion to the protected area is also taken into consideration. Finally, for multi-unit systems, the economic and failure dependence between components in maintenance is addressed in the modeling because it is a more realistic assumption. In summary, the modeling of the surveillance systems considers the following three aspects: multi-unit multi-state system configuration, two dependent processes and the opportunistic maintenance policies. The first section of the literature review focuses on the existed works on surveillance system modeling, including the topics on sensor placement, intelligent surveillance system design and attack-defense models. The second part summarizes the traditional reliability modeling, including multi-unit multi-state systems and maintenance scheduling. The last section discusses the reliability models considering multiple dependent processes, which is the main topic directly linked to this research.

2.1 Surveillance System Design and Modeling

The modeling of the surveillance systems receives wide attention by multiple areas of researchers over the years. Many efforts are dedicated in searching ways to build functional, cost-effective, automated surveillance systems with consideration of

interactions between the systems and their adversaries (either making effort to avoid detection or sabotage the system units). Three distinguish categories are discussed in this section. They are sensor placement and coverage models, intelligent video surveillance systems and attack-defense models.

2.1.1 Sensor Placement and Coverage Models

One of the designs of surveillance system problems that receive the most attention from the research communities is the sensor deployment problem. Given the geometric layout of the facility that needs surveillance coverage, a designer of the system needs to determine the types, number of sensors required and the locations of the sensors to meet the safety specification. This sub-section reviews selected works discussing about ways to quantify the performance of the surveillance system and models for the sensor deployment problem. Generally these models are computationally complex to solve. Many approximation models and heuristic search algorithms are developed to solve the optimal deployment problem more efficiently.

Bai *et al.* [8] design a surveillance system detecting intruders of an empty area using two types of sensors to enhance the performance. The first type of sensor applied is the ultrasonic sensor detects a moving object when the signal of the ultrasonic from the transmitter to the receiver is cut off. The second type of sensor is the Pyroelectric Infrared sensor that is used to detect the environment temperature change. A majority voting algorithm is used to interpret the conflict signals between multiple sensors.

Zhao *et al.* [9] propose a general visibility model as a flexible sensor planning framework. The designed model takes the self and mutual occlusion of the objects in the surveillance

area into consideration. It can be used to search optimal sensor placement in an arbitrary-shape 3-D structure. The optimizer in the model tries to maximize the system performance and minimize the cost of the system at the same time using a greedy search via binary integer programming.

The above proposed binary integer programming model has a high computational complexity. Zhao extends the research in his dissertation [10] by comparing multiple approximation algorithms such as simulated annealing and semi-definite program to simplify the sensor planning model. The author further investigates the geometric fusion of the object information observed from different sensors in the surveillance network in order to improve the human body segmentation accuracy in the surveillance scene and generate better views of the object with the collected information in real time.

Dhillon and Chakrabarty [11] propose a probabilistic optimization framework for sensor placement under the constraint of sufficient coverage. The optimizer minimizes the number of sensors deployed while maintaining desired coverage level of the monitored area. To reduce the number of sensors in the network also indicates the reduction of the transmission of data and power consumptions, along with low initial investment of the system. The model considers the nature of the terrain, such as the obstacles blocking the sight of the cameras and the preferential coverage of different locations. It also considers the imprecise detection of each sensor and different sensor capabilities.

Wang *et al.* [12] present a wireless sensor network configuration model that is flexible to provide different degrees of coverage options based on system requirements. The applicable system of the model should have high node density so that many sensors can be scheduled with sleep intervals and are not required to work continuously to conserve

energy. For wireless sensor network, connectivity means that all the sensors are able to communicate with every other sensor in the network. In other words, the graph of the working nodes should not be broken into isolated pieces. The model needs to maintain the connectivity of the network in addition to satisfying the coverage requirements when deciding which sensors are selected to provide continuous service.

Zou and Chakrabarty [13] develop a virtual force metric to describe the geometric relationship between multiple sensors. The metric is applied to aim the deployment adjustment to enhance coverage after initial random deployment of multiple sensors that is practical in military applications (throwing the sensors in the field). The virtual force metric defines an attractive force if the distance between the two sensors is longer than twice the radius of the sensor coverage. A repulsive force is defined by contraries. The total force on each sensor provides the adjustment direction and distance. Hence the final deployment is more uniform and provides better coverage compared to the initial random scattering.

Krishnamachari and Iyengar [14] develop two distributed Bayesian algorithms to distinguish false alarms from real event detection for a wireless sensor network. Intuitively, if a real event occurs in a region, the sensor detections are likely to have agreements with neighbours. On the contrary, a false alarm appears more randomly. The designed approaches use randomized decision scheme and threshold decision scheme of the Bayesian algorithms to determine the correlation between event detection of the sensors.

Gupta *et al.* [15] present three algorithms that select a subset of sensors to execute a given query in a large-scale sensor network. The centralized approximation algorithm

provides the most near-optimal solution of the minimal set of censors providing the desired coverage level. The two distributed algorithms saves communication data transfer between sensors so that they extend the service life of the battery driven sensors. As a trade-off, the performance of the solutions by the distributed algorithms is degraded compared to the centralized one.

Ram *et al.* [16] develop a metric calculating average probability of target discovery to evaluate the performance of a surveillance system consisted of video cameras and motion sensors. When s desired performance level is given, the model is able to find the optimal solution with information of the locations of the cameras, minimal number of motion sensor required, and the minimal field of view of the camera. The field of vision represents an important characteristic of the camera such that the wider field of vision requirement often indicates a more sophisticated type of camera thus significantly increase the total cost to set up the entire system.

Yao *et al.* [17] propose a sensor positioning algorithm for persistent surveillance considering the handoff safety margin between adjacent cameras. The handoff of the target between cameras can be achieved smoothly only if the two cameras have sufficient overlap of effective coverage range, as shown in Figure 2.1. In addition, the excessiveness of the overlap is considered as a waste of resource. The authors define an observation metric as the combination of camera resolution and the distance to edge of the field of view. A max coverage and min cost problem is formulated to balance the overall coverage, appropriate level of overlap margins and total cost of the system by optimizing the deployment of the sensors. Experimental results on a real-world implementation is carried out and compared with the work proposed by Erdem and

Sclaroff [18]. With a minimal sacrifice of the overall coverage, the handoff successful rate of the target increases dramatically for the proposed model.

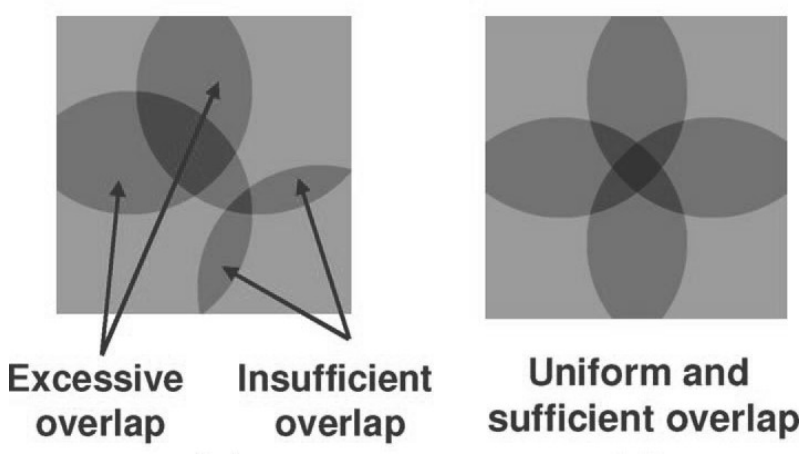

Figure 2.1 Graphical demonstration of the overlap concept introduced in [17]

Herrera *et al.* [19] develop a coverage strength model that takes many camera intrinsic parameters into consideration when evaluating the coverage performance of the sensors. The intrinsic parameters considered in this work include camera visibility, pixel resolution, depth of field and angle of view. An example that only involves one camera with one laser line projector is studied to demonstrate the use of the proposed model.

Liu *et al.* [20] propose a localization-oriented coverage (L-coverage) model based on Bayesian estimation to measure the overall performance of random deployment sensor networks. The random deployment is modeled as a two-dimension stationary Poisson point process. At any discretized point in the monitored field, it is defined to be L-covered if at least k cameras are able to estimate the target location at that point within an acceptable estimation error range. Then the total L-coverage probability is calculated by the ratio of L-covered points over all points in the field. The relationship between the L-coverage probability and the random deployment intensity parameter λ is further

investigated so that one can find the minimum Poisson intensity of the random deployment for a desired level of L-coverage probability.

Nam and Hong [21] present an agent space trajectory model to simulate the trajectories of people traveled in an arbitrary-shaped monitoring field. Within the simulation one can estimate the different weight of the importance for each spot in the field and develop the camera placement algorithm in order to cover the most significant spots. Thus the optimizer can be understood as a min-cost max-weighted-coverage probabilistic model. In the experiments, the authors demonstrate the selection between three different types of cameras and their optimal deployment plan (optimal number of cameras and layouts) under different budget constraints.

Rashmi and latha [22] develop a surveillance network using IP cameras that can transmit signals via network. The operator can directly control the camera network via his smart phone devices remotely to realize facial recognition, object identification and other tasks. The development enhances the mobility and ease of access to the surveillance system control. However, the security issues such as hackers to the remote control system are also raised by the development.

Liu *et al.* [23] proposed a trans-dimensional simulated annealing algorithm to efficiently search near optimal solutions to camera placement problem subject to different system design requirements. Four different constraints have been discussed for the camera placement model. The first constraint is the common 100% floor coverage. The second one is the 100% floor coverage with important targets covered by multiple cameras (critical coverage redundancy). The third constraint is to guarantee 100% facial recognition success rate. The last one is to re-planning the existing camera network so

that the total number of cameras is given. The placement plan to satisfy the floor coverage is compared with some existed algorithms to show its effectiveness.

Wang [24] discusses the classification of the sensor network coverage problem based on different types of coverage model assumptions. The first type is the point coverage problems, in which the area under surveillance are discretized into individual points or there only exists a finite number of targets to be monitored in the field. The second type is the area coverage problem, in which the whole surveillance area is treated equally and the percentage of the coverage is studied to estimate the effectiveness of the deployment. The last type is noted as the barrier coverage problem, where the goal of designing certain type of surveillance system is to form a protection barrier so that the intruder cannot find any uncovered path between possible entrances to the targeted locations. The author reviews many existing works with the focus on the computational complexity of the models and the different optimizing techniques that applied to solve the coverage problems.

Mavrinac and Chen [25] separate the coverage models by distinguishing their coverage geometry, coverage overlap and transition topology. A geometric coverage model may be further deferred by the dimension of the monitored field, camera's field of view, resolution, focus and angle, treatment of the occlusion (not considered, static or dynamic). A coverage overlap model describes the physical topology of the camera system, while a transition model covers more functional topology of the system. For example, a non-overlap deployed surveillance system can perform a prediction tracking of the intruder. When the target leaves the view of one camera, the system will predict the possible

movement of the target and coordinating the other cameras to increase the possibility to recapture the target. This can be considered as a typical example of the transition model.

2.1.2 Intelligent Video Surveillance Systems

The performance of the human operators is a limitation of the surveillance systems, as it is hard to conduct consistent and focused monitoring to the screens. Many incidents and events that captured by the optimally deployed surveillance cameras may be missed due to the lack of awareness of the officers. With the rapid progress of vision processing and data mining techniques, the new generation of intelligent surveillance systems can automate many detection tasks to improve the performance of the system.

Marcenaro *et al.* [26] propose a decomposition model of surveillance functionalities, including video tracking, object classification and behavior understanding, etc. The decomposed logical tasks are then optimally allocated to the physical distributed nodes subject to available bandwidth, processing power and the dynamic loads of the logical task. Through demonstration examples, the authors show the convenience to concentrate the processing power to the central office when the system is composed of a small number of cameras. If the bandwidth cost is high, allocating the intelligence tasks to distributed processing unit is preferred to the centralized processing.

Marchesotti *et al.* [27] present a semi-automatic alarm generation technique applied to a parking lot surveillance to draw the operator's attention by sending blink icons on screen and generating sound signals when detecting events such as car parking in non-parking zones, pedestrian detection in car limited zones and erratic trajectories inside the lot. The

application also compares the accuracy of the auto-alarm under different environment conditions such as bad weather or night illumination scenarios.

Trivedi *et al.* [28] develop the distributed interactive video array (DIVA) system to track and identify vehicles and people, monitoring facilities and interpreting activities. The authors demonstrate the vehicle tracking and identification in bridge and roadway surveillance via overlap of camera view coordination and car feature extraction (color, size, speed, etc.) techniques. In a long-term room watch example, the system successfully records and identifies 9 different people entering the room multiple times. In some cases, two people are presented under the surveillance the same time.

Saini *et al.* [29] propose a queuing model consisted of four levels of components: sensor, co-located processing elements (CoPE), aggregate processing element (APE) and the network. Each of the components for every level has a finite processing rate hence the incidents are possible to be missed due to the resource limitation or unexpected delay of the system. The missing probability and response time are studied under different combinations of the surveillance system parameters.

Doblander *et al.* [30] propose a multi-objective optimization algorithm to balance service availability, quality of service and energy consumption of the intelligent video surveillance system. The reported system runs several video analysis algorithms on a network processor to enhance the surveillance performance. These algorithms consume a lot of calculating power if all running at full quality at the same time. The proposed algorithm determines which algorithm could be run at lower quality mode and how the algorithms are distributed on different processors in the network to minimize the energy consumption while maximizing the quality of service and system availability.

Malik *et al.* [31] present a surveillance system design and implementation programming language Systemj. The program simulates the surveillance system in a highly abstract manner to evaluate the system performance based on the sensor distribution, sensor type selection, communication between sensor, controller, operating unit and storage units. Then Systemj can also generate executable codes for computers serving as different roles in the system (camera controller, SystemJ control box, operating unit and storage servers, etc.) as shown in Figure 2.2 in the deployment stage.

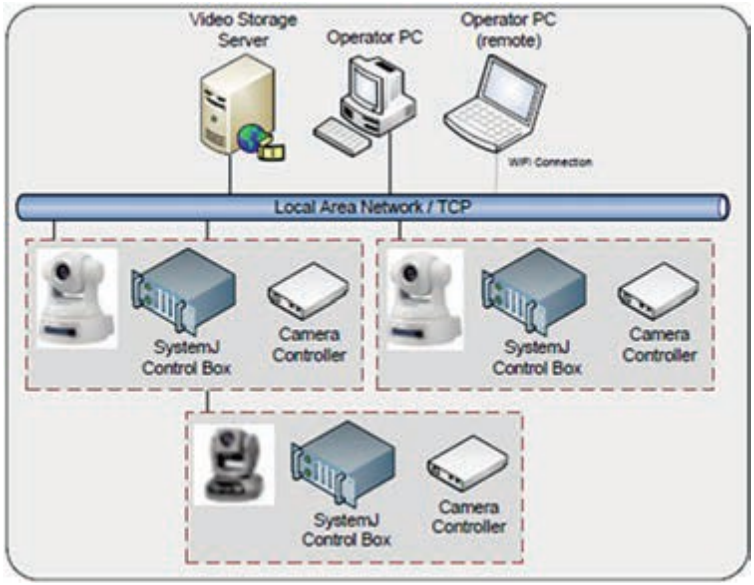

Figure 2.2 The smart distributed surveillance system physical implementation from Malik *et al.* [31]

Riveiro *et al.* [32] develop a maritime anomaly detection surveillance system that can interact with operators. The anomaly detection module applies Gaussian mixture model and self organizing map to realize the detection of the anomaly behavior of the vessel movement. The system notifies the operator with each detection then waits for feedback. If the detection is indeed an anomaly, it is then added to the training model. If the

observation is considered false, the operator can adjust the weight vector in the model to prevent the false alarm in the future. Thus the system updates itself with the human experience until the performance reaches satisfaction.

Stauffer and Grimson [33] present a background tracking model by treating each pixel of the camera image as a mixture of Gaussians. The mixture of Gaussians for the whole image is then analyzed to identify the range of the background. The model is robust to deal with shadows, specularities and swaying branches and can be applied to different types of cameras, lightening conditions and different objects being studied.

Szczodrak *et al.* [34] borrow the idea of the three metrics introduced in [35] to evaluate the performance of video object tracking algorithms applied to 4 pieces of video recordings. The three metrics are known as fragmentation, average object area recall and average detected box area precision, where these metrics are designed to evaluate the precision and processing speed of each object tracking algorithm.

Atrey *et al.* [36] propose a human-centric approach to provide adaptive schedule of the best views of cameras for better observation of events. Based on the findings in [37], the human operator can typically monitor 4 screens effectively at a time. Thus the model applies adaptive Gaussian type event detection and an operator eye tracking feedback method to select the 4 best views of camera screens when an incident occurs in the monitored area.

Anwar *et al.* [38] present an anomaly event detection algorithm by monitoring the sequential pattern of a frequently occurred series of events. This method is effective in detecting unknown anomalous events that are not likely to follow a pattern of a frequent series of events. Various experiments are carried out to test the computational

complexities of the proposed algorithm subject to variations of model parameters such as the number of input event and duration of the sequence of events.

Clapes *et al.* [39] propose a facial identification and object recognition module for an intelligent surveillance system. The model estimates the environment and applies background subtraction to extract objects in the camera image. Then the extracted object is compared with a skeletal model in order to identify if a person is detected. Then facial recognition is conducted on the human tracking result. The extraction is updated online to realize robustness against partial occlusions and camera 3-D rotation.

2.1.3 Attack Defense Models of Surveillance Systems

Many existing models related to surveillance reliability are the attack-defense models where game theory is often applied for consideration of both intelligent attackers and defenders. Hausken and Levitin [40] develop a table which categorizes the literature according to system structure, defense measures, attack tactics and circumstances. System structure is further divided into single element, series systems, parallel systems, series-parallel systems, networks, multiple elements, interdependent systems, and other types of systems. Defense measures are divided into separation of system elements, redundancy, protection, multi-level defense, false targets deployment and preventive strike. Attack tactics and circumstances are divided into attack against single element, attack against multiple elements, consecutive attacks, random attack, combination of intentional and unintentional impacts, incomplete information and variable resources. The classification is intended to give an overview of the field and implicitly suggest future research trajectories, false targets, separation, redundancy and number of attacks.

Guikema [41] points out three classical critiques of applying game theory on the intelligent actors in reliability analysis: assumption of instrumental rationality, common knowledge of rationality and knowledge of the game rules. One should treat these assumptions carefully when modeling with game theory since the nature of uncertainty of the attackers. Thorough discussion of robustness of the parameters and even violation of assumptions would be useful to enhance the effectiveness and generalization of the modeling.

Most of the attack-defense models, if not all, consider protection on the potential targets. Protection is defined as the type of actions carried out by the defenders to reduce the probability of target destruction by attackers. Golany, *et al.* [42] compare optimal resource allocation plans under two types of risks, random and strategic attack. Under the probabilistic risk assumption, the optimal allocation plan tends to fully protect the states that have the largest population but remains some low population states unprotected. The optimal plan under strategic attack balances the risk and achieves an average expected loss for every state despite of the population size. Paté-Cornell and Guikema [43] present a probabilistic model for determining priorities among different types of threats attempted by different terrorist groups. This model considers multiple scenarios, the objectives of both the attackers and the defenders and the dependency between them. The model can help achieving a rational balance between enhancing the defense on previously occurred types of attacks and over-investment on prevention of repeated attacks. It can also help the decision makers to avoid inaccurate intuition on priorities of threats. Dighe, *et al.* [44] state that the secrecy in the allocation plan can be beneficial to the defender. They study a two-node system by enumerating all possible attack-defense strategy

combinations to support the statement. Both centralized and decentralized defending structures are considered. Siqueira and Sandler [45] analyze the allocation of agents by general terrorist organizations based on different types of governments and local terrorist supporters. The findings further provide information to the government on how to effectively alter the positive attitude to terrorists of the local supporters. Against the intuition, the higher cost of investment for government actions may not reduce terrorism. Bandyopadhyay and Sandler [46] compare the preemptive and defensive measures. The preemptive actions weaken terrorist assets or ability to attack, while the defensive actions reduce the damage after an attack occurred. The proposed model analyzes the interaction between the preemptive and defensive actions by the nation, considering the dependency between the two types of actions (the effective preemptive action is likely to reduce the need of the defensive action) and the interaction between the decision makers for different nations. The allocation of resources are also related to the terrorist preference of attack and both domestic and oversea assets. Hausken and Levitin [47] present a model that both actors can invest in offensive and defensive resources. Each actor can either maximize its own survivability or minimize the other's. The result includes the optimal solutions on how to allocate the resources on offensive and defensive actions for all four combinations of the possible actors' objectives. Nikoofal and Zhuang [48] derive a model including extreme bounds of the estimation of attacker's target valuation in the decision of optimal defensive resource allocation. Azaiez and Bier [49] propose an optimal resource allocation algorithm for a general series-parallel system configuration. When under a constraint budget, the defender tends to protect the most attractive component, but can also consider some less attractive components if the cost of enhancing the

security level on these components is minor. The algorithm is under the assumption of perfect knowledge for the attackers that they fully aware the improvement the defender can make to the system prior to the attack. Thus the result of expected attack cost is a lower bound since it is more realistic that the attacker can only achieve imperfect information on the defensive plan. Hausken *et al.* [50] develop a defense model including both terrorism and natural disaster threat. The defender has the options to invest in protection against both threats simultaneously, or in protection against either threat separately. In the modeling, three different scenarios of two-step games are considered: both attacker and defender move simultaneously, the attacker moves first and the defender moves first. It shows that the player that has the lower cost per unit tends to make the first move. The selection of the defensive policy depends on the relationship of the costs for different plans (either joint protection or separate protection). Hausken [51] proposes a two-period game model with consideration of a multi-state two-unit system. In each period, both actors make one investment decision on each non-failed components. Detailed discussions have been made for various parameter selections. Levitin and Hausken [52] consider a situation that the attacker can make repeat attempts of attack to ensure destruction of the target The attacker has an imperfect observation of the attack outcomes with a probability to falsely identify a destroyed target as undestroyed and vise versa. The error rates of the wrong outcome observation by the attacker have a great impact on the strategy of the attacker. For example, it is suggested for the attacker to alter the favor from multiple attacks to single attack when the false probability to identify an undestroyed target as destroyed rises above a threshold.

Besides the protection on individual units, some action can benefit to multiple or all targets at the same time, as the consideration of dependency between units. Golalikhani and Zhuang [53] develop an attack-defense model with consideration of joint protection based on similarities of the threats or the protected targets. For example, the chemical and biological threats can be both monitored through the public-health surveillance program, but not the explosion threats. The investment on the arbitrary layer protection is compared with individual target protection and traditional boarder hardening which is a technique to enhance the security of all targets together (on the contrary of the arbitrary cluster of protected targets). Haphuriwat and Bier [54] compare the protection effect of target hardening and overarching protection where hardening represents the enhancement of the security level of individual targets and overarching stands for the protection over all targets available. The result shows that when the total number of the significant valuable targets is small, hardening of individual dominates the protective action, vise versa.

As alternatives to protection, other defensive actions are available for the defenders to form a more complex defense strategy to compete against the attackers. Creating false targets also receives some attention in the literature. Levitin and Hausken [55] study the effectiveness of deploying false target comparing with investment in protection of the genuine target The assumptions include that the attacker is not able to distinguish the real target from the false distraction. The model also requires that both the attacker and the defender are rational players for the game. The optimal solution of that how many false targets the defender decides to create and how many targets the attacker decides to attack is obtained for the cases that the Nash equilibrium of the described game existed. The

conclusion shows that the optimal solution relies on the resources both players have, the cost of each false target and the intensity of the contest. Levitin and Hausken [56] also study the effect of the random and strategic attacks on the defense planning mentioned in Golany, *et al.* [42]. Moreover, the different attacks can be mixed in the modeling. Both redundancy and protection (resources to put on the unit to reduce the risk of successful attacks) are considered in the defensive strategy. In Levitin and Hausken [56], they expand the comparison of defensive strategies to three types: redundancy, protection and false elements. Redundancy requires genuine units placed in the system more than needed, while false units cannot provide the function of genuine units. It is only replaced to confuse the attackers for selecting the correct targets thus normally is cheaper than distribution of a genuine unit. With a limited resource, the optimal allocation is dependent on the total resources (defensive and attacking), attacking intensity and the relative cost for each type of defensive strategies. Levitin and Hausken [57] further extend the non-cooperative game to a more generalized model, in which the defender considers all possible actions of protection, redundancy and false targets to enhance the survival rate of the protected system. To be specific, the attacker and defender compete in an intelligence contest prior to the attack-defense game. If the attacker wins the intelligence contest, he can identify all the false targets and take down all genuine targets unprotected with minimal effort. Then he can further attack the protected real targets with the resources left from the intelligence contest. If the defender wins the intelligence contest, the attacker has to attack all targets (both real and false ones) randomly with the left resource. Peng *et al.* [58] propose an attack-defense model considering imperfect false targets that have some probability to be identified by the attacker. In the modeling,

it is first considered of the identical imperfect false targets with the same probability of being detected. Then the model is further extended to one that the probability of being detected is a decision variable that the defender can choose, along with the number of false targets he wants to create. The numerical examples show that the flexibility of choosing different types of false targets with different probability of being detected for the defender is beneficial especially when the contest intensity in uncertain.

Many of the above examples on attack-defense model are based on general system models, while others are directly related to real life applications (networks, power system, transportation, etc). Lin, *et al.* [59] derive a mixed nonlinear integer programming model to study the allocation of resources to protect the network. The objective of the defender is to either maximize the total cost of the attacker or minimize the probability of the core node under attack. Li *et al.* [60] discuss a dynamic voting system of networks, in which all the available units can either be selected as redundancy or used to create false targets. This is special compared to the false targets discussed earlier since all the false targets created in this work are capable to function as a working unit. They are simply not selected in the voting cluster. In this way the defender can focus the resource on protecting the small set of voting clusters, meanwhile distracting the attackers with hard-to-detect false targets. This is proven in the paper effective especially when the defender is limited with sparse resource. Singh and Kankanhalli [61] address the concern of the adversary in the surveillance scheme. They propose a zero-sum game for an ATM lobby defense scenario and a nonzero-sum game for a traffic control surveillance scenario. A generic treatment for enhancing the surveillance performance against rational adversary is provided with discussion on how to change the factors such as spatial, temporal and

external, etc. Bier, *et al.* [62] propose an algorithm of interdiction strategies for a transmission system. The power systems are highly interconnected systems. One of the advantages is that the spare can be shared over the grid to enhance the capacity against shock loads such as a failure of a single generating site. However, if the shock is strong enough, the chain reaction of one site failing down after the other will cause wide-area black outs. Terrorist attacks can be one of the reasons to cause certain shocks. In the paper, an algorithm is developed to identify the critical transmission lines for interdiction. The algorithm is two-staged that it first chooses candidate lines then has them strengthened. The process is repeated until the desired resources run out. Bier and Haphuriwat [63] discuss a model of determining the number of containers for inspection at the US ports to protect against terrorist attacks. The optimal portion that requires inspection should minimize the loss of the defender while the attackers are trying to maximize their rewards. It is found out that it is easier to deter an attack risk when the terrorists invest high attack costs. Thus lowering down the portion to be inspected will increase the chance of small threats (assault rifles) but not likely to impact the risk of huge threat much (nuclear). The model also considers the effect of retaliation on deterring terrorist attacks. K., et al. [64] study the safety of transportation networks against random incidents and terrorist attacks by using an attacker-defender model proposed by Bell [65]. The model can help identify the critical routs in the network and shows the advantages of applying mixed route strategies. Visible, invisible and announced but not specified protections are compared as possible defensive measures.

2.2 Traditional Reliability Modeling

With all the discussion of the coverage optimization model and the new technologies to automate the event/threat/intrusion detection, there are little attention on the reliability and maintenance of the surveillance system. How much a failure of component will affect the overall performance of the surveillance system? Is redundancy required to enhance the system reliability? How soon the first failure is expected and how often the maintenance action should be carried out? Without the proper answers to these questions, the designed system may perform well at the beginning but soon deteriorates to fail the safety requirements of the protected area. Although there are only few papers directly address the reliability and maintenance issues of surveillance systems, many traditional reliability models can be borrowed according to the characteristics of the surveillance systems. Three categories of reliability modeling will be discussed in this section.

2.2.1 Model for Multi-Unit Multi-State Systems

Adding redundancy is one of the most effective techniques to improve the system reliability level through the use of replicated units [66]. Among all possible structures of the system configuration, k-out-of-n system receives a lot of attention in the reliability modeling. The parameter k represents the minimal set of components to maintain a functional state of the system. Once there are $(n-k+1)$ components down in total, the system is considered as failure. The reliability of such a system configuration is easy to estimate as in [67]:

$$R(t) = \sum_{i=k}^{n} \binom{n}{i} R_0(t)^i \left(1 - R_0(t)\right)^{n-i} \tag{2.1}$$

where $R_0(t)$ is the reliability function of the individual component.

In the literature, models are developed with more complexity than the k-out-of-n system with identical units. Mathur [68] presents an N-modular redundancy (NMR) system operated in simplex mode with spares as a majority voting system. The system uses $N = 2n+1$ modules to form a majority voting system such that if at least $(n+1)$ units make the correct decision, the system outcome will be correct. It equivalents to the system with $(n+1)$-out-of-$(2n+1)$ configuration plus S spare units. The simplex mode is worked as that the failure in $(2n+1)$ modules is simply replaced when spares are available. If no more spare units left, the further failure in the $(2n+1)$ modules is discarded, along with a good unit so that the system reduces to $(2n-1)$ units. This process repeats until a single working unit is left in the system. The reliability function of such a system with triple modules and S spares is developed in the paper. Mathur and de Sousa [69] modify this model with multi-state units. The units are used to identify binary input thus they are functional if they can read 1 when the input is 1 and 0 otherwise. Traditionally the failure is only considered as stuck-at-x, which means the failed module randomly gives value despite the input. Two more failure modes, stuck-at-0 and stuck-at-1, are considered in the modeling. For the voting system, when a pair of stuck-at-0 and stuck-at-1 failures occurred, they compensate each other so that the system outcome is not affected. The reliability model for NMR system considering this type of compensation is developed for comparison with the NMR simplex model to determine if discarding of good units along with failures are beneficial to the system reliability. Mathur and de Sousa [70] further generalize the model to k-out-of-n configuration (k can be any value between 1 and n) with S spares, in which each unit still has 3 failure

modes (stuck-at-a, a = 0, 1, x). They show in the work that with careful selection of parameters, many existed models can be summarized as special cases of the general modular redundant system.

Pham [71] applies the similar idea of the multi-unit voting system with 2 failure mode (stuck-at-0, stuck-at-1) for each unit. Instead of majority voting, the model uses a variable threshold k to determine the output of the system. When less than k units transmit signal 1, the system has output 0. When at least k units transmit signal 1, the system decides to transmit 1. The majority voting is a special case of this model with odd number of n and $k = (n+1)/2$. Selection of k to maximize the system reliability is also discussed in the paper. Nordmann and Pham [72] implement the model in decision making of human organizations where the probability of stuck-at-a (a = 0, 1) differs from individual decision makers. The outcome of each voter is further weighted to represent more realistic modeling. A recursion algorithm to simplify the evaluation of the reliability of the weighted voting system is reported in [73] by constraining the weight parameters for only integers and the threshold k as a rational number. Pham [74] also explores the effect of varying the total number of units in the system on the reliability function of the system with three failure modes.

The above models on multi-unit multi-state systems have the following limitations. Firstly, the probability of each failure mode for individual component was considered time invariant. Secondly, although multiple failure modes for each component are taken into account, on the system level, there is either functional or failure state existed. Take a deeper look at the voting systems that is majorly focused in the above works. Based on the voters' observation, the system can either misread an input "1" as "0", or the opposite.

It is acceptable to consider both types of failures as the same when making decisions of whether accepting or rejecting a project, or either transmitting a "1" or "0" bit in the computer. But for a safety-related system, the outcome of misreporting a threat that does not exist is essentially different from one of misdetection of a real threat. A safety-related system is the type of system that the failure of which will result in significant increment of risk to human lives and/or the environment [75]. Knight [76] discusses the definition, types, challenges of development and made prognosis on the technology and applications of the future safety-critical systems. Bukowski [77] develops a Markov based reliability model for a 1-out-of-2 safety-shutdown controller. On the component level, each unit has 5 possible states: working; fail-safe recognized; fail-safe unrecognized; fail-danger recognized; fail danger unrecognized. Fail-safe mode for each component means that the component falsely shuts down a process that is operating properly. Thus for a 2-unit system there are in total of 25 combined elementary states, which can be further combined to system level states for reliability and mean time to failure (MTTF) estimations. Zhang, *et al.* [78] repeats the work with similar assumptions on the component (5 states) and system structure (1-out-of-2). The development of the Markov model for MTTF calculation is revised from the previous study. Both of the examples were only considered system with 2 units. As pointed out in Guo and Yang [79], the complexity of the model grows exponentially with the increment of the number of units considered for the system structure. They develop a framework of automatic generation of Markov model for k-out-of-n structured safety-instrumented system. The model also includes the common cause failure into consideration, which can cause two or more failure occurred at the same time. As a demonstration of the proposed framework, a

numerical estimation of the reliability for a 2-out-of-3 architecture is given at the end of the work. Bukowski and van Beurden [80] further take proof test completeness and correctness into the loop. If the undetectable failures are failed to be identified by the inspection point (the proof test is not 100% complete and/or cannot correct all the errors), they will remain as undetectable failures and degrade the performance of the safety-instrumented system. The new assumption adds more possible states on the system level. Torres-Echeverría, *et al.* [81] add a testing reconfiguration that if a component is under test, the system is downgraded to the state that the tested item is treated as known failure, hence further extends the complexity of the system level outcomes. Levitin, *et al.* [82] apply the same 5-level component assumption on a series-parallel structure of a fuel supply system. A recursive method is derived to obtain the system state distribution.

Another significant portion of the research on modeling of multi-state components is the competing risk model where the component can have failures due to either degradation or fatal shocks. The competing risk model also involves the modeling with multiple processes, thus will be discussed in the next section.

2.2.2 Maintenance Model for Multi-Unit System

Let us take a brief look at the maintenance schedules for single-unit system first. As summarized in Wang [7], hundreds of papers and models are published on the maintenance schedule for single-unit systems. In our opinion, the categories of the maintenance schedule can be determined when the maintenance is carried out and how complete the maintenance has been performed. To be specific, if the maintenance is only conducted upon failure then it is a corrective maintenance; if the maintenance is

scheduled before failure occurred to the unit from time to time, it is preventive maintenance. Judging by the completeness, if the maintenance restores the unit to "as good as new", it is a perfect maintenance; if it only recovers partially of a unit to a state somewhere between "as good as new" and "as bad as old", it is imperfect maintenance; if the maintenance intentionally to restore the system to a stage with the same failure rate before it fails, it is called minimal repair. Imperfect preventive maintenance, possible with combinations of the minimal repair for early period of operation, receives the most attention in the literature, as that the modeling assumptions are more realistic and the models are more complicated in the forms. Renewal theory is a common choice for application of optimal maintenance policy, as there is often a time point that the system deteriorates significantly and has to be repaired fully back to state "as good as new", which is clearly a renewal point. The optimal policy is obtained by either maximizing the availability of the system or minimizing the cost per unit time to operate the system, which is evaluated by

$$Cost\ per\ unit\ time = \frac{\mathrm{E}[\text{total cost in one renewal cycle}]}{\mathrm{E}[\text{renewal cycle length}]} \tag{2.2}$$

For multi-unit systems, if there is no dependency between components, the development of the maintenance schedule is similar to the ones for single-unit systems. However, it is typical that there exists dependency between components, such as economic dependence, failure dependence and structural dependence [83]. The maintenance strategy then defers from the ones for single unit systems, as that the failure of one component provides the opportunity to maintenance other components in the system as well. Wang and Pham [84] highlight two main categories of the maintenance schedule for multi-unit systems in their survey. The first type is group maintenance that the maintenance actions are always

carried out for multiple units at the same time, either upon each failure and preventively maintaining a group of other working components, or holding some failures and performing corrective maintenance until accumulation of some pre-determined number of failures. The other type is opportunistic maintenance that the group maintenance is only carried out when some criteria has been met in the system. To our understanding, the only difference between these two types of policies for multi-unit systems is that whether it is possible that the maintenance action on single units is performed. For group maintenance, maintenance actions are never carried out along for a single unit. One can argue that the opportunistic maintenance is a generalization of the group maintenance. Examples of these works can be found in [85-107].

2.3 Multi-Process Modeling

For a single process modeling, the reliability function $R(t)$ is defined as the probability that the process is in working status by the time t. As the modeling becoming more complicated, events in one process often represent trigger of consequences in other processes. Thus the reliability estimation has to consider the dependencies between multiple processes. Two categories of multi-process modeling are discussed in this section, along with a summary of the application of non-homogeneous Poisson process (NHPP) to model the incident arrival process.

2.3.1 Modeling of the Standby Systems

Standby redundancy has been widely applied in industry such as computer fault-tolerant systems [70], power plants [108] and space exploration systems [109]. From the relationship between the failure rate of the standby units and the active units, the standby systems can be categorized into 3 groups. The first type is that the standby units have the same failure rate as the active units, referred to as the hot-standby systems, or the active-standby systems. If the switching mechanism is perfect, this type of system can be easily modeled as the k-out-of-n system. In the second type of the standby systems, the standby units have 0 failure rate until being switched into use. This type of the systems is referred to as the cold-standby systems. The third category lies in between the first two types that the failure rate of the standby units is less than the active ones, but not 0. When modeling the reliability of the standby systems, the moment of the process that modeling the active units working status altering from success to failure triggers the working status of the standby process, if there are still spare units available at the time. The key of modeling the reliability of the system is the analysis of the sequence of events in the time line. Coit [110] proposes the reliability estimation of a cold standby system with one primary unit and $(n-1)$ cold standby units.

$$R(t) = r(t) + \int_0^t Pr[T_2 > t-u]\, f(u)du + \int_0^t Pr[T_3 > t-u]\, f_{S_2}(u)du + \cdots + \int_0^t Pr[T_n > t-u]\, f_{S_{n-1}}(u)du \tag{2.3}$$

where components in the system are identical with reliability function $r(t)$ and failure density $f(t)$. $f_{Si}(t)$ is the density function of the failure time of the sum of the total i components.

Many other researches on standby systems can be found considering different system scenarios. She and Pecht [111] derive a reliability model to study a k-out-of-n warm-standby system. In the modeling, k units are in active status and the other $(n-k)$ units are spares thus have a lower failure rate than the active ones. Once a working component fails, one spare item is being activated and starts to fail at the active failure rate. This procedure repeats until no more spare unit is available. The system fails at the time point that the $(n-k+1)^{th}$ failure occurred. Levitin and Amari [112] estimated the reliability with the similar system assumptions, but using a universal generating function approach. In the numerical example, it is demonstrated that the reliability distribution for each component in this modeling has not to be identical. The example also shows that the sequence of activating the spares has an impact on the system reliability, given that the failure rates of the spare units vary from one to another. Yun and Cha [113] develop a two-unit hybrid model that the standby component first serves as cold standby then shift to warm standby after some time of the successful operation of the active unit. If the active unit failure before the standby unit switches to warm mode, the system fails. Otherwise the warm standby unit can be activated immediately to replace the failed one. Given the failure densities of both components, and the switching mechanism (either perfect switch or imperfect), there exists an optimal switching time, which is carefully studied with several numerical cases. Amari [114] presents a k-out-of-n cold-standby system with components following Erlang distribution. Amari, *et al.* [115] explore the

effects of changing the number of spares on the reliability improvement factor. Adding more redundant units to the system will always improve the reliability of the system, but the improvement is not linear. They find out that with the number of spares increases from 0, the reliability improvement first increases and then decreases. Moreover, the reliability improvement factor follows the probability mass function of the negative binomial distribution. These findings can be considered as factors to determine the optimal number of spares for k-out-of-n warm standby systems.

2.3.2 Competing Risk Models

The reliability of the components in the complex system is usually estimated using life testing techniques [116]. For some cases, it is not necessary to complete the test until failure of the tested component. Instead, there are some measurements that can provide enough information on how fast the unit wears out. Those types of measurements can be used to model the degradation path of each component. Compared to the reliability function estimation, the degradation analysis is more related to the physical representation of the failure mechanism. Both the reliability and degradation analysis are used to describe the normal wear process of a component. In reality, the components not only endure normal usage, but also suffer random shocks from the environment. Some of the shocks are strong enough to be fatal to the component. The competing risk model takes both degradation analysis and shock model under consideration. The processes for degradation and random shocks are competing with each other. The earlier arrival of failure in either process will cause failure of the component. Thus the competing risk models are also categorized as multi-process modeling. If one achieves the cumulative

distributions of both the degradation $F_d(t)$ and the shock $F_s(t)$ separately (without the consideration of the influence of the other), then the competing risk of one hazard arrives earlier than the other can be calculated as

$$F_{T_s}(t) = \int_0^t \big(1 - F_d(u)\big) dF_s(u) \tag{2.4}$$

$$F_{T_d}(t) = \int_0^t \big(1 - F_s(u)\big) dF_d(u) \tag{2.5}$$

where $F_{Ts}(t)$ represents the cumulative distribution that the shock causes the system to failure earlier than the degradation, vice versa for $F_{Td}(t)$.

Wang and Pham [83] give a comprehensive structural review on dependent competing risk models with degradation and random shocks. The shock models can be categorized into cumulative shock model [117], extreme shock model [118] and δ-shock model [119]. The degradation model includes general path model [120], stochastic model [121], parametric [122] and nonparametric statistical model [123]. The combination of the two risk models can be either independent with simpler representation [124], or dependent that is more realistic and complex [125]. In this type of modeling, both the degradation and shock model are not limited to 1 process only, where examples can be found in Wang and Coit [126]. Some summaries on additional literature of the competing risk models are provided as a supplement to the review. Li and Pham [127] present a multiple competing risk model considering two degradation processes and one cumulative random shock process. There is no interaction between these processes in the modeling. On the system level, the states are combination of states for individual process. The probability function of each system outcome is developed but no maintenance model based on the probability

analysis is performed. Wang and Zhang [128] consider a model that two types of failures can be generated by the shock process. One denotes for the type caused by short interval between arrivals of consecutive shocks and the other stands for the type caused by the magnitude of the shock strength. Since the two types of failures are due to the same shock process, there exists some dependency between the failure modes. Cui and Li [129] apply the shock model on a multi-unit system that each shock has the same damage cumulated for different components of the system so that their failure rates become dependent. They further derive an opportunistic maintenance schedule to lower down the maintenance cost based on the dependency between components. Liu, *et al.* [130] bring both degradation and shock process into the modeling of a series-parallel system. Peng, *et al.* [131] consider the dependency by assuming that the shocks contribute as a step increment in the degradation process, if they are not strong enough to fail the component. Jiang, *et al.* [132] push the dependency in the model one step further by considering not only the raising of degradation by the shocks, but also the dependency of thresholds by the shocks. To be more specific, each shock may lower the threshold for other processes and drive the system faster to failures than the case without the shock, besides the accumulation in the degradation process. Wang and Pham [83, 133-135] develop several competing risk models considering dependency between processes. In Wang and Pham [133], they develop an imperfect maintenance scheduling for a system with only one degradation process and one shock process. They modified this model in Wang and Pham [134] by considering hidden failures that the system status is only available by each inspection point. The optimal scheduling is achieved by multi-objective optimization instead of optimization on the single cost per unit function. In Wang and Pham [135],

they derive a model with multiple dependent degradation processes and multiple shock processes using Copulas, a statistical method to estimate the joint distribution based on marginal distributions.

2.3.3 Modeling of the Surveillance System Considering the Demand Process

The orientation of this research is from Pham and Xie [136] where they propose a two-process model to determine the unfavorable ratings of airplane repair stations. The agents from Federal Aviation Administration have had inspection records for different repair stations. Due to the resource limitation, they have to wait for a certain period of time between paying each visit to a selected station for inspection. Hence it is important to choose the station with the worst favorable rating based on the historical service record in order to maximize the overall performance of all the repair stations. The two processes under consideration in the model are the frequency of inspection to each station and the occurrence of unfavorable rating of each station. Both processes are modeled using NHPP with parametric time dependent models, which can also be found in [137, 138]. The inspection process determines the time point that the individual repair station restores to favorable status, while the performance of the station affects the frequency of the inspection. Thus the two processes are dependent and have impacts on each other. In the modeling, the arrival rate of surveillance (the first process) at station k is represented as

$$\lambda_I^{(k)}(t) = \lambda_0 e^{G^{(k)}(t,\boldsymbol{\gamma})} \tag{2.6}$$

where λ_0 is a baseline visit rate and $G^{(k)}(t, \boldsymbol{\gamma})$ contains all the factors (such as time from last inspection and the number of unfavorable inspections over a period of time) that

influence the surveillance rate to station k, weighted by scalar vector $\boldsymbol{\gamma}$. The intensity of the occurrence of the unfavorable rating at a station k (the second process) is modeled as

$$\lambda_Z^{(k)}(t) = \alpha r_k^{i-1} t^{\beta-1} e^{\boldsymbol{b}\boldsymbol{x}^{(k)}} \tag{2.7}$$

where α, β are global parameters (same for every station) and r_k is a scalar for individual station k. $\boldsymbol{x}^{(k)}$ includes all the information of each individual station to affect the performance, such as number of different types of employees. $\boldsymbol{b}$ is the corresponding coefficient vector of $\boldsymbol{x}^{(k)}$.

Recently some research focus on the safety related and defense-attack modeling considering the two processes modeling with demand. Xu, *et al.* [139] purpose a model for a multi-unit multi-state safety-related system. The system is used to monitor the status of the production line and to shut down the production system to reduce damage when dangerous situation occurs. Thus if the production system is safe but only the safety-related system fails, the damage is much smaller than the situation that the safety-related system fails to respond to a failure in the production line. A universal generating function approach [140] is applied to obtain the probability outcomes of the system. Although multiple components are considered for the safety-related system, maintenance actions can only be applied on the whole system (either replace the whole system or do nothing). The component status is not available to the maintenance team also. For the surveillance system, it is possible to conduct different types of maintenance on individual subsystems. Each subsystem constantly transmits video for the central officer thus the interruption of working status has the chance to be discovered during operation. These assumptions are not compatible with the modeling in [139] thus a lot of modifications are needed for a more realistic surveillance modeling.

Deferred from the existing research, our proposed models on surveillance systems consider not only the component failure process but also the process that describes the discrete arrival of random intrusions or incidents.

Chapter 3

Objectives of the Study

Our objective of this research is to develop a generalization of reliability modeling framework for the surveillance systems considering two stochastic-processes. The first process is the traditional system status process. The second process is defined as the demand process, or the intrusion/incident arrival process. The hard damage by the failure of the surveillance system requires two things to happen in sequence. Firstly the surveillance system has to fail due to the loss of enough subsystems. Then, the intrusion/incident arrival during the downtime of the surveillance system is considered as the real failure. Since the arrival of incident is discrete and sparse, it is valuable to take the second process into consideration for a more comprehensive evaluation of the system reliability. The reliability framework should also include the following aspects to keep the model realistic: multi-unit multi-state system configuration and the group maintenance policies for dependency between subsystems. The possible component level failure states are combinations of detectable or undetectable failures and fail-safe or fail-dangerous modes. Optimal maintenance policies that minimize the expected system cost rate are obtained based on the developed two-process reliability modeling. More specifically, the following sequences of sub-objectives are aimed for the research:

1) Develop the two-process model for predicting the reliability of surveillance systems consisting of multi-units with only undetectable failures and periodic inspection.
2) Develop the two-process model of surveillance systems consisting of multi-units with subsystems that have both detectable and undetectable failure modes. Since a portion of the component status is available in this case, more choices of system

outcomes have to be considered when developing the mathematical representations of the outcome probability. An opportunistic maintenance policy is considered to address the economical dependency between subsystems.

3) Derive the cost optimization model that depends on the expected failure number of possible system outcomes based on the proposed system reliability model in objective 2 above. Develop an algorithm to obtain the optimal solutions for an opportunistic maintenance policy to minimize the total cost per unit time.
4) Further extend the reliability model in objective 2 with the assumption that the subsystems have both fail-safe and fail-dangerous modes. Thus for this extended reliability model of the k-out-of-n system, each subsystem includes five possible states such as: working, fail-dangerous detectable, fail-dangerous undetectable, fail-safe detectable and fail-safe undetectable. The surveillance system may be stopped prior to failure due to the accumulation of both the fail-dangerous detectable and fail-safe detectable failures. Compare the 3 reliability models for the surveillance systems are and demonstrate that the model described in objective 1) and 20 are special cases of the model described in objective 4).

Chapter 4

A Two-Stochastic Process Reliability Model with Considerations of the Incident Arrivals and the Operating Environments

4.1 Introduction

Surveillance system is widely used today to enhance the security level of the protected area. Reliability of the entire surveillance system is a critical issue since the breakdown of such system would leave the monitoring area unobserved and encountered much higher risk under the attacks. In this chapter we present a dual stochastic-process model for predicting the reliability of surveillance systems consisting of many subsystems (units) with considerations of the environmental factors, skill of intruder to avoid detection, the intrusion/incident arrival process and subsystem failure process. Several numerical examples are presented to illustrate the proposed model.

When discussing the system structure configuration, normally the assumption of independent component lifetimes is implied. However, if the components of the system are sharing in a common operating environment which is differ from the laboratory test environment, a type of induced dependency is introduced between the components, which is well discussed in Currit and Singpurwalla [141]. In the work, the authors presented the expression of the reliability model for a two-component system sharing a common uncertain environment following a Gamma distribution. They also discussed the effect of ignoring the environmental factor and applying the independence assumption between components that would first overestimate then underestimate the reliability of the system. Pham [142] presented a systemability model in which he also derived the expression of systemability for series, parallel and k-out-of-n system configurations.

This work is further applied to model an automatic packaging machine and a motorcycle drive system where real data sets are available for parameter estimation [143].

In this chapter, we present a framework to model the reliability of the surveillance systems with considerations of the environmental factors, skill of intruder to avoid detection, the intrusion/incident process and the subsystem failure process [144]. The surveillance system often has complex structure, thus multi-unit system configuration should be taken into consideration instead of single unit system. Since the subsystems, i.e., cameras and the motion sensors, likely will be placed outdoor and stay close to each other, the uncertainty of common environment is worth to consider in the modeling that reflects the reality of reliability prediction. It is also worth to note that a careful analysis of the intrusion/incident arrival rate can provide useful information and, therefore, our proposed framework is worth the effort to study.

4.2 Description of the Surveillance System Framework

Consider a traditional reliability modeling where only the unit failure process is being considered. This type of modeling is suitable for the products or systems processing demands continuously. Once the system fails, it can no longer provide any service to the customer to meet their persistent need. Applications for systems with continuous work load include car engines, power plant, and production lines.

For the non-continuous work load of systems such as alarm-detection units, nuclear power plants, airbag car system, medical monitoring control units, that require frequent surveillance by certified personnel who must identify potential problem through inspections, there is a chance that even though the system has already failed, but no

incident or attack arrives since the failure until the system is being inspected and repaired to functional status. Because of the characteristic of this type of system that we discussed here, the reliability of the system responding to sparse discrete demand should be revised as to properly function when a pulse demand takes place. In other words, the reliability discussed in this chapter which consists of two parts: the first is the reliability with respect to the unit failure process subject to environmental factors, and the other is the system has actually failed but no incident arrives between the failure and the next inspection point after the failure.

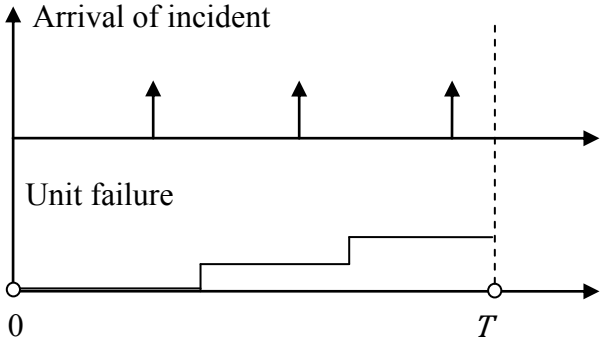

Figure 4.1 Two processes surveillance system scheme within single inspection period

To realize the estimation of the extended reliability, a two stochastic processes model is proposed with the application of the surveillance camera systems. The first process is a non-homogeneous Poisson process (NHPP) for the incident arrival. The second is a two-stage stochastic process indicating the status of the system (failure or functioning). The hidden failure that is not aware of by the certified personnel (or central stations) is the main focus in the modeling of this study and is considered as an innovation modeling approach. This type of failure can only be detected and fixed by periodic inspection. If

the occurring failure raises the attention of the central stations, then immediately a maintenance action will be provided and the time to repair on-line is ignored. All the subsystems are periodically inspected for hidden failure and the failed subsystems are perfectly repaired [99]. Figure 4.1 illustrates a possible series of events of the two processes within an inspection cycle. With the assumption of perfect maintenance, we only need to consider a single inspection cycle in this work. A future research can be extended to consider the multiple inspection cycles subject to imperfect maintenance etc.

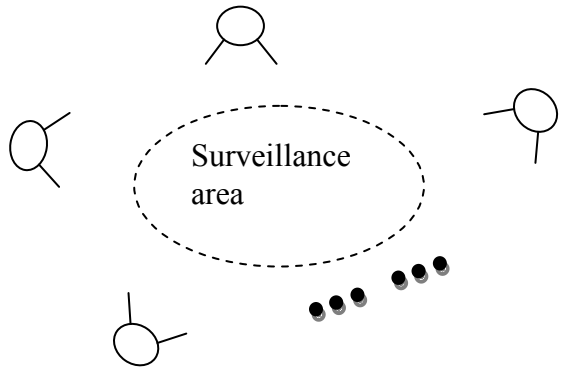

Figure 4.2 Sketch of redundant surveillance system

As shown in Figure 4.2, there are n identical subsystems (i.e. cameras) are installed to enhance the system performance. For the k-out-of-n surveillance system to work, there are at least k subsystems must work. We assume that each of the working subsystem has the probability $p(\omega_i)$ of detecting an incident. This probability reflects the fact that there is a chance, although the subsystem is properly functioning, the subsystem cannot detect the attacker's action which is $(1-p(\omega_i))$. All subsystems are considered to work under a common random environment, which adds the dependency between the life-time of each subsystem.

Based on the assumption of the two processes model, the proposed surveillance system may result in three different states by the next inspection point as follows:

- *Working state*: The system still works (i.e., at least k subsystems are working);
- *Soft-failure state*: There are at least $(n-k+1)$ subsystems have failed during the inspection interval, but no incident has arrived till time T. In this case the surveillance system is down, but we are lucky to reach the maintenance point without serious damage. This outcome is referred to as the soft-failure;
- *Hard-failure state*: Undetected incident occurred during the surveillance system failure period.

Based on the reliability modeling, the inspection period T is determined to meet the system performance requirement. The extended reliability of the system is defined as the sum of the probabilities of the first two outcomes (working state and soft-failure state).

4.3 Mathematical Modeling

Consider a model consisting of two mutually dependent stochastic processes.

One is a NHPP for the incident arrival process; and the other is a two-stage stochastic process of the system failure process.

A. *NHPP Incident Arrival Process*

We assume that the arrival of the incident follows a NHPP with intensity function $\lambda_I(t)$ which has the following form:

$$\lambda_I(t) = \lambda_0 e^{A(t,\theta)} \tag{4.1}$$

where λ_0 is the baseline and $A(t,\ \theta)$ is a function that incorporates the environmental effects on the intensity function. This type of parametric arrival rate estimation can be found in [136, 137]. Those factors considered in this work include:

- Time from the last incident, T_s;
- Number of incidents have occurred in the past T_p units of time prior to time t, $N_p = N(t \in T_p)$;

The larger value of T_s or the more number of incidents in the past would likely result to the higher intensity rate of the incident arrival. We define the function $A(t,\ \theta)$ as follows

$$A(t, \theta) = \gamma_1(t - T_s) + \gamma_2 N_p \tag{4.2}$$

B. *Two-stage System Failure Process*:

Here we consider a random variable η that represents the uncertainty of comment environments of each subsystem using the concept of systemability addressing the uncertainty of operating. The detail development of the systemability can be found in Pham [142].

The mathematical formulation of the systemability is defined as:

$$R_s(t) = \int_{\eta} e^{-\eta \int_0^t h(s)ds} dG(\eta) \tag{4.3}$$

where $h(t)$ is the hazard rate function of the subsystem and $G(\eta)$ represents the distribution of the operating environment of random variable η.

Let us assume that the subsystem lifetime follows a Weibull distribution, that is $R_i(t) = e^{-\lambda_i t^{\gamma_i}}$ or $R_i(t) = e^{-\lambda t^{\gamma}}$ for identical subsystems. As in Pham [142], we also considered

the Gamma distribution for the random operating environment η, that is $\eta \sim$ Gamma(α, β) where the probability density function (pdf) of η is given by

$$f_\eta(x) = \frac{\beta^\alpha x^{\alpha-1} e^{-\beta x}}{\Gamma(\alpha)} \tag{4.4}$$

The reliability function of each subsystem under the uncertainty of operating environments is defined as

$$R_i(t|\eta) = e^{-\eta\lambda t^\gamma} \tag{4.5}$$

Assuming that the incident detection probability is constant, i.e., $p(\omega_i) = p$. In this chapter, we assume that for the subsystem to function, it has to satisfy that the subsystem does not fail by time t and has successfully detected the incident. Thus the subsystem reliability can be expressed as

$$R_{pi}(t|\eta) = pR_i(t|\eta) \tag{4.6}$$

Thus the reliability of the entire k-out-of-n surveillance system in terms of the uncertainty common operating environment can be formulated as

$$\begin{aligned} R_c(t|\eta) &= \sum_{j=k}^{n} \binom{n}{j} R_{pi}(t|\eta)^j \left(1 - R_{pi}(t|\eta)\right)^{n-j} \\ &= \sum_{j=k}^{n} \binom{n}{j} \left(pe^{-\eta\lambda t^\gamma}\right)^j \left(1 - pe^{-\eta\lambda t^\gamma}\right)^{n-j} \end{aligned} \tag{4.7}$$

Hence the reliability of k-out-of-n surveillance system with respect to the operating environments is given by:

$$R_c(t) = \int_{\eta} R_c(t|\eta) dG(\eta)$$
$$= \int_{\eta} \sum_{j=k}^{n} \binom{n}{j} p^j e^{-j\eta\lambda t^\gamma} \left(1 - pe^{-\eta\lambda t^\gamma}\right)^{n-j} dG(\eta) \tag{4.8}$$

Since η follows a Gamma distribution, a close-form function of equation (4.8) can be obtained using the Laplace transform [142]. The failure distribution function of k-out-of-n systems under the common operating environment is given by

$$F_c(t) = 1 - R_c(t) \tag{4.9}$$

System Probability States

a. *Working state*: The probability that the system is working by time t which is defined as in (4.8):

$$R_c(t) = \int_{\eta} R_c(t|\eta) dG(\eta)$$

b. *Soft-failure state* (fail-safe mode): The probability that the system will be in soft-failure state. That is

$$R_{sf}(t) = \int_0^t Pr[N(t) - N(\tau) = 0]\, dF_c(\tau) \tag{4.10}$$

By definition, the soft-failure requires that the system fails between two consecutive inspections. Assuming that the failure happens to be at the moment time τ where $0 \leq \tau \leq t$ and in the remaining time interval $[\tau, t]$. The probability that there will be no incident arrival during this period and is given by

$$Pr[N(t) - N(\tau) = 0] = e^{-\int_\tau^t \lambda_I(x)dx} \tag{4.11}$$

Then equation (4.10) yields

$$R_{sf}(t) = \int_0^t e^{-\int_\tau^t \lambda_I(x)dx} dF_c(\tau) \tag{4.12}$$

c. *Hard-failure state*: The probability of an incident occurs during the period of surveillance system failure which is defined as

$$F_{hf}(t) = 1 - R_C(t) - R_{sf}(t) \tag{4.13}$$

By definition, $F_{hf}(t)$ is the probability that the system encounters an incident and the surveillance system has already failed before the next inspection takes place.

In the modeling, we define that the extended reliability of the surveillance system by time *t* is given by

$$R(t) = R_C(t) + R_{sf}(t) = 1 - F_{hf}(t) \tag{4.14}$$

Once the inspection interval T is scheduled based on the system requirement, one can simply replace t with T in order to calculate the outcome probability at selected inspection interval.

4.4 Numerical Example

Let us consider a 2-out-of-3 surveillance system structure to illustrate the proposed model.

A list of all the parameters is given as follows for numerical example:

For the NHPP arrival rate: $\lambda_0 = 0.01$, $\gamma_1 = 0.005$, $T_s = 500$, $\gamma_2 = 0.002$. $N_p = 5$.

For the subsystem life time Weibull distribution: $\lambda = 0.0001$, $\gamma = 1.5$.

For the Gamma distribution of random variable η: $\alpha = 2$, $\beta = 3$.

The incident detection probability: $p = 0.9$.

Then, from equations (4.1), (4.7), (4.8) and (4.12), we have:

$$\lambda_I(t) = 0.01e^{0.005(t+500)+0.01}$$

$$R_c(t|\eta) = 3[(0.9)e^{-\eta 0.0001t^{1.5}}]^2 - 2[(0.9)e^{-\eta 0.0001t^{1.5}}]^3$$

$$R_c(t) = 3(0.9)^2[\frac{3}{3+2(0.0001)t^{1.5}}]^2 - 2(0.9)^3[\frac{3}{3+3(0.0001)t^{1.5}}]^2$$

$$R_{sf}(t) = \int_0^t e^{-\frac{0.01}{0.005}e^{0.005(t+500)+0.01}+\frac{0.01}{0.005}e^{0.005(\tau+500)+0.01}} dF_c(\tau)$$

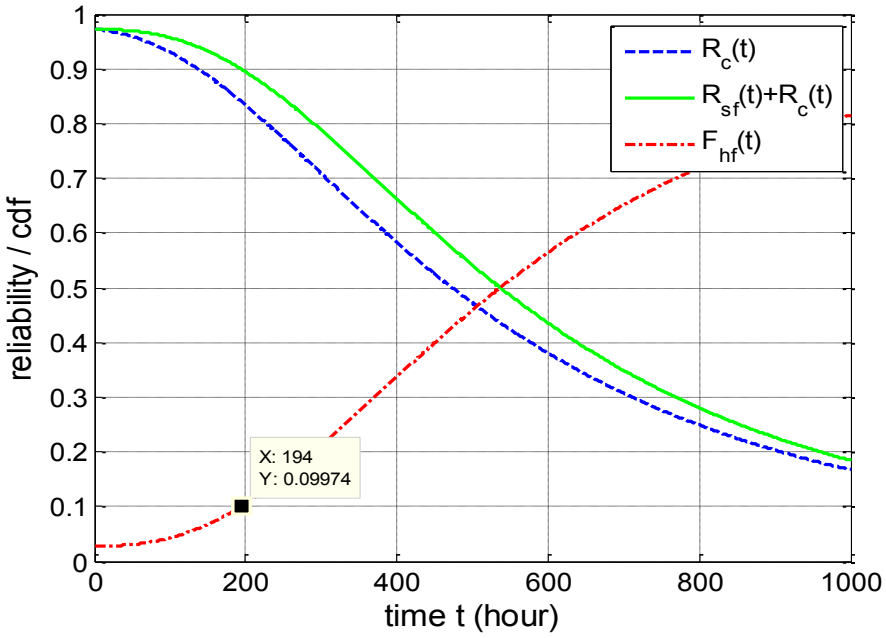

Figure 4.3 Probability of system states plot within one inspection cycle

The probability of the surveillance system ending in each state, i.e., working, soft-failure, and hard-failure, by the next inspection time point is plotted in Figure 4.3, with the variation of different inspection interval lengths. The dash line represents the reliability, $R_c(t)$, or probability of observing the system in working status by the end of the inspection period. The solid line represents the extended reliability of the entire surveillance system by adding both the traditional reliability of k-out-of-n system and the probability of having soft-failure by the end of the inspection period using equation

(4.14). The das-dotted line represents the hard-failure probability by the end of the period, $F_{hf}(T)$. For example, we wish to determine the inspection interval time T where the probability that the system encountering hard-failure must be less than 0.1, i.e. $F_{hf}(T) < 0.1$. Then from Figure 4.3 and equation (4.13), the result of the inspection interval time T that satisfies the system failure requirement would be $T = 194$ hours in this case.

4.5 Sensitivity Analysis

The proposed model includes several parameters. For the sensitivity analysis, we vary various parameters in the following manner so that each case corresponds to a physical modification of the surveillance system framework. The system performance can be evaluated by the maximum inspection interval length that keeps the hard-failure probability less than 0.1. The longer interval length indicates the better performance of the surveillance system. In Figure 4.4, we modify the incident arrival rate $\lambda_I(t)$ by increasing the baseline rate λ_0 from 0.01 to 0.05 which corresponds to the higher rate of attack in reality. As a result, the probability of system having a soft-failure by the next inspection decreases, represented by the gap between the dash and solid lines. In Figure 4.5, we increase the incident detection rate parameter p from 0.9 to 0.98. This change indicates that the subsystem is likely to detect the incident when it is functioning. Similarly, the reliability of the entire surveillance system as well as subsystem obviously increase as the failure rate of subsystem in the Weibull distribution decreases by half (i.e., from $\lambda = 0.0001$ to $\lambda = 0.00005$) as shown in Figure 4.6. The reliability of the surveillance system for various values of β is shown in Figure 4.7. As for Figure 4.8, we present the reliability measures of the 2-out-of-4 surveillance system configuration. By

adding one redundant subsystem from 2-out-of-3 (see Figure 4.3) to 2-out-of-4 (Figure 4.8), obviously the entire system performs better in terms of reliability measure. Thus to enhance the reliability of the surveillance system in general, the following actions can be considered: reduce the incident arrival rate; use a reliable subsystem (i.e., camera, sensors) in the field; reduce the probability of having the subsystem working under harsh environments; and add more redundancy to the surveillance system.

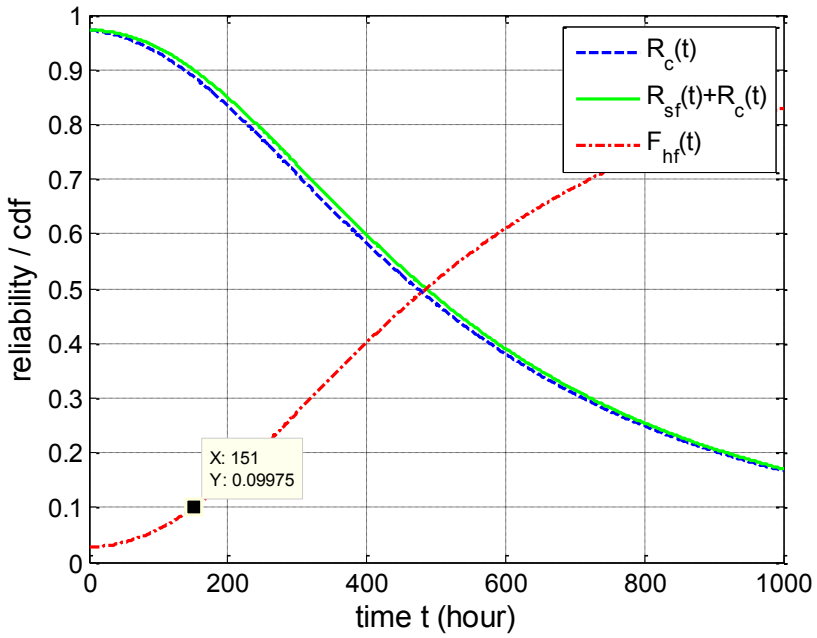

Figure 4.4 Reliability plot with change in $\lambda_I(t)$: $\lambda_O = 0.01 \rightarrow \lambda_O = 0.05$

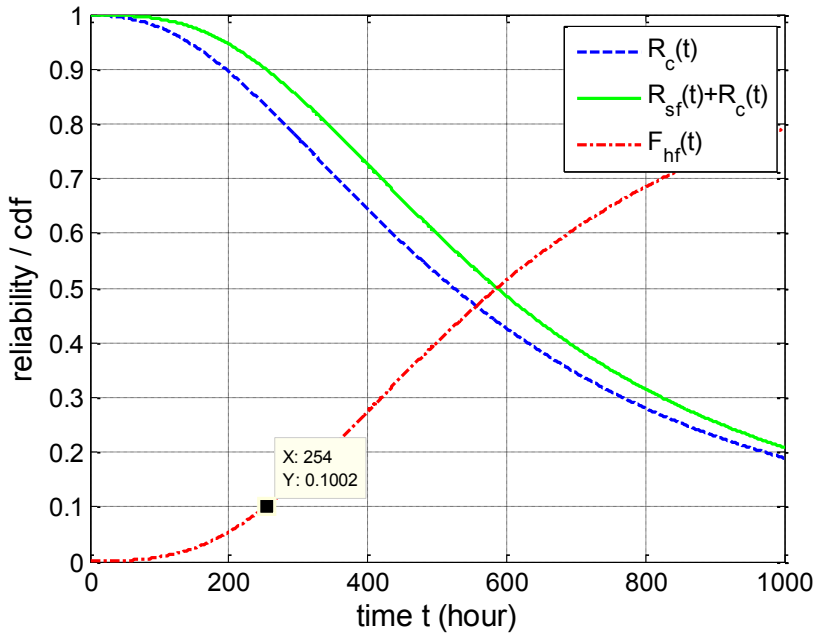

Figure 4.5 Reliability plot with change in p: $p = 0.9 \rightarrow p = 0.98$

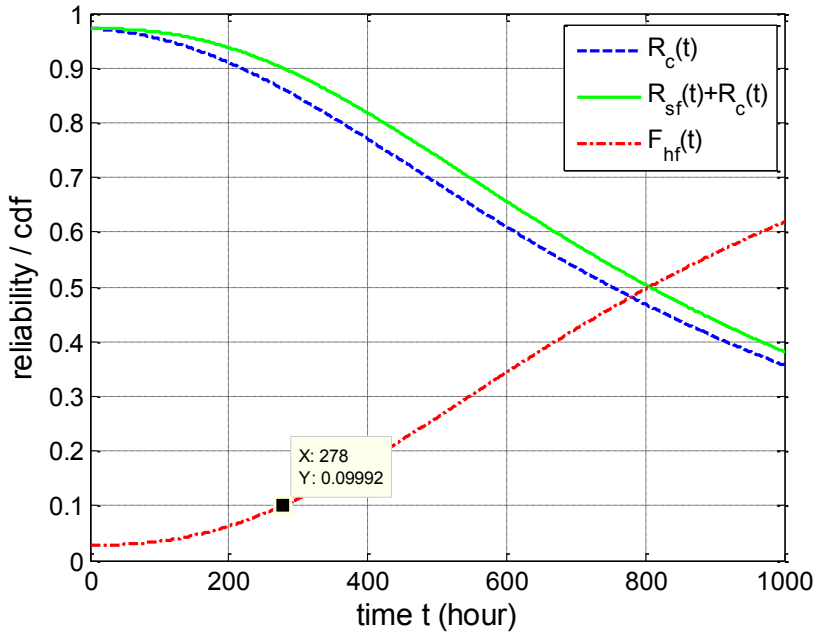

Figure 4.6 Reliability plot with change in $R_i(t)$: $\lambda = 0.0001 \rightarrow \lambda = 0.00005$

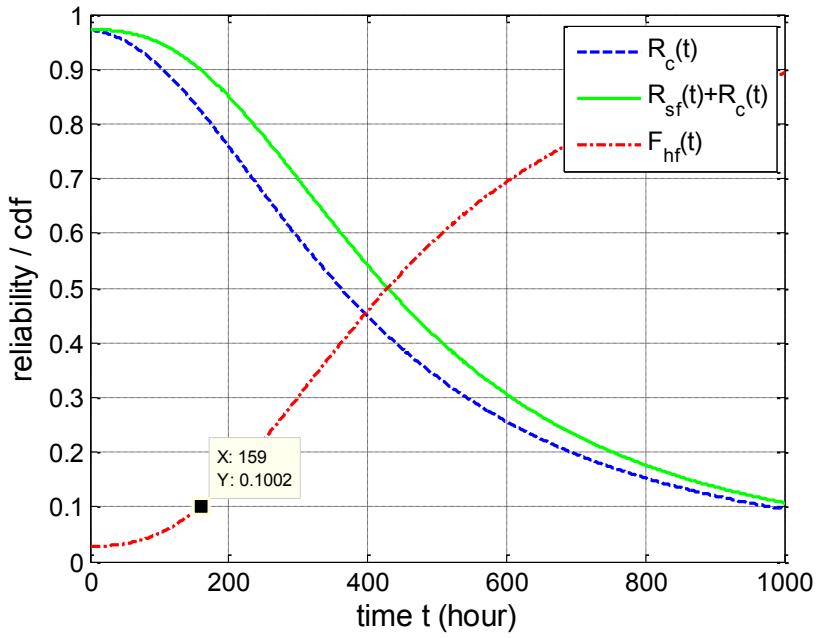

Figure 4.7 Reliability plot with change in $G(\eta)$: $\beta = 3 \rightarrow \beta = 2$

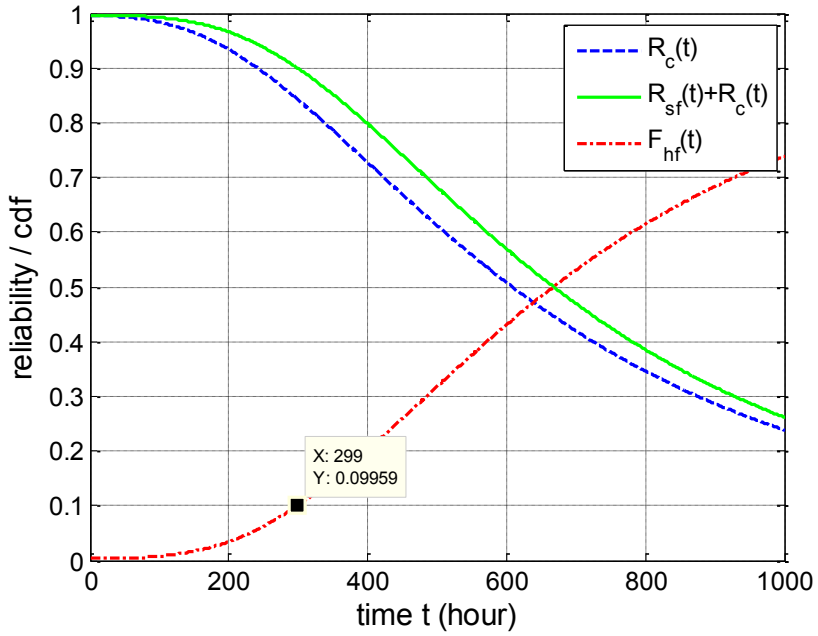

Figure 4.8 Reliability plot with change in configuration: 2-out-of-3 → 2-out-of-4

4.6 Conclusion

In this chapter, a surveillance system reliability model is presented with consideration of a dual stochastic-dependent process: incident arrival process and system failure process. The framework of the surveillance systems can be applied to other applications as modification can be easily conducted following the mathematical modeling in Section 3. One can adopt different system configurations, consider different environmental effects based on the collected data and evaluate intruder's effort to avoid being detected using different mechanisms. The quantitative evaluation of the reliability and soft-failure and hard-failure probabilities with the variation of the inspection interval length is derived and illustrated with numerical examples and several sensitivity analyses. Possible actions to enhance the reliability of the surveillance system are also discussed.

Chapter 5

Modeling the Effects of Two Stochastic-Process on the Reliability of k-out-of-n Surveillance Systems with Two Competing Failure Modes

5.1 Introduction

Surveillance systems, along with safety instrumented devices have critical functions in preventing massive damage to human life and property. The failure of these systems should be analyzed associated with the incident arrival process to achieve a comprehensive representation of the system outcomes. A k-out-of-n surveillance system is defined with subsystems having two competing failure modes: detectable and undetectable. The reliability of the system is derived with the consideration of the intrusion process and a (m, T) opportunistic maintenance policy. Several numerical examples are given to demonstrate the validity of the modeling and the sensitivity of important parameters.

In this chapter, a k-out-of-n system is defined as the surveillance redundant system with subsystems that have two types of failure modes: detectable and undetectable [145]. An opportunistic maintenance policy is applied to the system. The intrusion process is taken into consideration after the system softly failed (number of failed units is more than ($n-k$)).

Besides the surveillance camera system, the model can be easily adopted for various types of systems where the two process relationship existed. For example, many safety critical systems (nuclear, chemical processing plants, high speed railways, etc.) [78] use safety instrumented devices to protect the system from hazard failures or minimize its consequences [80]. These devices are usually consisted of electronic voting units and

have specific functional requirements [75]. The subsystem often has both self-announced and hidden type of failures [76, 77, 79]. The occurrence of the hazard to the safety critical system can be treated as the second process. Thus our proposed model is a direct match for reliability analysis of the safety instrumented devices.

5.2 Description of the Surveillance Systems with (m, T) Maintenance Policy

Consider a k-out-of-n surveillance system consisting of n subsystems (i.e., cameras) to monitor a certain area for security. The typical distributions and the coordination of multiple cameras surveillance system are being elaborately designed to form some redundancy in the system. For the k-out-of-n surveillance system to work, it requires at least k subsystems must work.

Each camera unit (i.e. subsystem) in the system transmitted live view of the monitored area to the central office. On the unit level, all subsystems are possible to go through two different failure modes. The first type of failure is the noticeable failure, or referred to as the type of failure that "announces" itself in [77]. For example, any type of camera failure that causes the transmitted view feed interrupted will raise immediate notice by the officer. The alternative failure mode for each unit does not raise awareness of the officer, noted as unnoticeable failure. Such type of failure may include a view stuck, that is the camera still transmits some figure (or picture) on the monitor of the central office, but it may be stuck frames from earlier time and no longer being a live view. Hence the total number of the failed subsystems is always larger than the number of failures noticed by the central officer. Thus, it is important to obtain the reliability and design ways to determine the maintenance schedule of such complex surveillance systems.

On the system level, we consider a two stochastic-processes model for the reliability modeling [19]. The first process is the traditional counting process of the failed subsystems. The second process addresses the intrusion/incident arrival rate. This second process can be also considered as the demand process. For many applications such as generators in the power station and the pressure controller in a furnace, the demand is dense or even continuous. Once the system fails, the loss of capacity processing the demand is instantaneous. Thus in the traditional reliability approach, the demand process can be ignored. For the surveillance system, it is designed to monitor dangerous actions of the protected area. Strictly speaking, it is only required to be working once an intrusion/incident occurred in the area. In other words, if there is no suspicious action in the protected area, it is still considered safe that the surveillance system is down for a while which is obviously a risk during this period and being repaired in time. This is because that the demand (intrusion/incident) process for the surveillance system is sparse and discrete. Thus the modeling of the reliability of the surveillance system should be different from the traditional reliability analysis and taking into consideration of the second process. From the description above, the real failure of the surveillance system requires two things to happen in sequence. Firstly, the surveillance system has to fail due to more than $(n-k)$ subsystem failures. Secondly, after the loss of the surveillance system, an intrusion/incident arrives before the system being repaired. In summary, the intrusion/incident arrival after the failure of the surveillance system would cause a huge loss of the protected area. In this chapter, we assume that if an intrusion arrives prior to the system failure, the area is considered "safe" and there is no damage caused by the intrusion as the functioning surveillance system carries out its duty to discover the attack.

All the damage should be attributed to the unresponsive action to the attack, not the surveillance system. On the contrary, if the surveillance system fails due to more than $(n-k)$ subsystem failures, but no incident arrives until one maintenance action carried out, the protected area is still considered "safe", as no real damage is resulted by the system failure. For the ease of expression, we define the soft-failure as the surveillance system fails due to more than $(n-k)$ subsystem failures. The hard-failure is defined as an intrusion/incident arrival given the soft-failure already occurred to the system.

If there is economic or reliability dependency between the subsystems, the maintenance decision is often based on the states of all the subsystems, which is known as the opportunistic maintenance [146]. For instance, a company with the installation of the multi-camera surveillance system is not likely to request for the visit of the maintenance team from the purchasing company every time they discovered that failure occurred to a single camera. Usually after accumulating several problems, given that the entire system is still working, the maintenance team is brought in to fix all the failures at once. This maintenance policy is referred to as $(m,\ T)$ rule in our proposed model. To elaborate, this maintenance rule is to stop the process for maintenance after m noticeable failures discovered in the system or after time T passed from the last maintenance. Here m is chosen to be less than $(n-k)$ in order to maintain a reasonable probability for the system to be in working condition by maintenance point. However since the existence of the undetectable failures of the subsystem, the system may still fail without awareness of the central office with the $(m,\ T)$ maintenance rule. Besides the maintenance rule, maintenance is also required immediately after any hard-failure occurred during the operation. The system is restored to the state "as good as new" after each maintenance

action by replacing all the failed subsystems and performing preventive maintenance for all the working subsystems.

The assumptions of the proposed model of a k-out-of-n surveillance system are as follows:

1. The k-out-of-n system is composed of n subsystems subject to two competing failure modes.
2. There are two types of failure modes for each subsystem such as detectable (failure mode 1) and undetectable (failure mode 2) failures where the failures are competing and nontransferable. That means if either failure occurred to one of the subsystems, it will remain that failure mode until maintenance is performed to the system.
3. A two stochastic-process model subject to two types of failures on the system level: soft-failure and hard-failure, is studied. The *first process* is the traditional counting process of the failed subsystems. The *second process* addresses the frequency of intruder's arrival.
4. *Soft-failure* is defined as the time when the system reaches $(n-k+1)$ total failures; *Hard-failure* is defined as the time when the first intrusion occurred after the soft-failure of the system.
5. The optimistic maintenance (m, T) rule is applied to the system.

Based on these assumptions, the outcomes of the two processes at the end of each maintenance period can be described as a two-level structure shown in Figure 5.1 and summarized as follows:

A. The system reaches the maintenance point after time T from the last maintenance without going through the soft-failure mode (stopped by T).

B. The system reaches the maintenance point by observing m noticeable failures of subsystems without going through the soft-failure mode (stopped by m).

C. Soft-failure occurred before any maintenance action. The outcome is further divided into three cases:

   a. The system reaches the maintenance point by rule T (noted as $sf\text{-}T$).

   b. The system reaches the maintenance point by rule m (noted as $sf\text{-}m$).

   c. The system reaches the maintenance point by having a hard-failure (noted as $sf\text{-}H$).

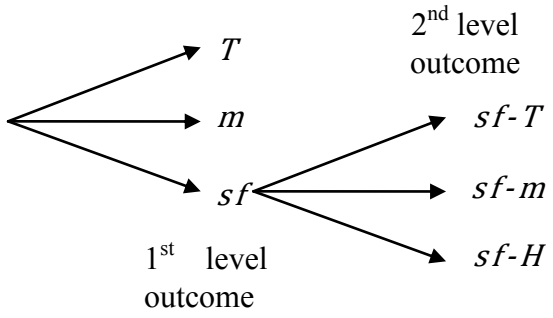

Figure 5.1 Diagram of the two levels of maintenance action

In the next section, the mathematical expressions of the probabilities of all the outcomes are derived. The combination of the outcomes can then be used to define the reliability of the surveillance systems.

5.3 Surveillance System Reliability Modeling

Consider the k-out-of-n surveillance system where subsystems are subjected two competing failure modes. Each subsystem can be in working status, detectable failure mode (noted as failure mode 1) or undetectable failure mode (failure mode 2). It is assumed that the time to failure of each subsystem is distributed exponential with constant rate λ_1 for failure mode 1 (detectable failures) and λ_2 for mode 2 (undetectable failures). It should be noted that one can extend this work by considering other distributions such as Weibull etc. without loss of generality. To simplify our proposed modeling and mathematical derivation, in this chapter we only consider the exponential density function for each subsystem. First we analyze the two failure mechanisms separately. Then the reliability and cdf of each subsystem under each failure mode are given by

$$R_{si}(t) = e^{-\lambda_i t} \tag{5.1}$$

$$F_{si}(t) = 1 - e^{-\lambda_i t} \tag{5.2}$$

where $i = 1, 2$ represents failure mode index.

Now consider the dependency between the two failure modes. Since the two failures are competing and non transferable (see system assumption B in section 5.2), the incident that a subsystem failed noticeably by time t requires the mode 1 failure happened and the second failure mode did not happen by time t. The probability that failure mode 1 occurs prior to failure mode 2 by time t of each subsystem is given by

$$F_{u1}(t) = \int_0^t R_{s2}(\tau) dF_{s1}(\tau)$$

$$= \int_0^t e^{-\lambda_2 \tau} d\left(1 - e^{-\lambda_1 \tau}\right) \tag{5.3}$$

$$= \frac{\lambda_1}{\lambda_1 + \lambda_2}\left(1 - e^{-(\lambda_1 + \lambda_2)t}\right)$$

In the similar manner, the probability that failure mode 2 occurs prior to failure mode 1 by time t for each subsystem is as follows

$$F_{u2}(t) = \frac{\lambda_2}{\lambda_1 + \lambda_2}\left(1 - e^{-(\lambda_1 + \lambda_2)t}\right) \tag{5.4}$$

Thus the reliability for each subsystem subject to competing failure modes is

$$R_u(t) = 1 - F_{u1}(t) - F_{u2}(t) = e^{-(\lambda_1 + \lambda_2)t} \tag{5.5}$$

On the system level, the status of the surveillance system by time t is defined as $(I(t), J(t))$ where row $I(t)$ represents the number of subsystems with undetected failures, and column $J(t)$ represents the number of subsystems with detectable failures by time t. The possible state distribution for a k-out-of-n configured system is sketched in Figure 5.2.

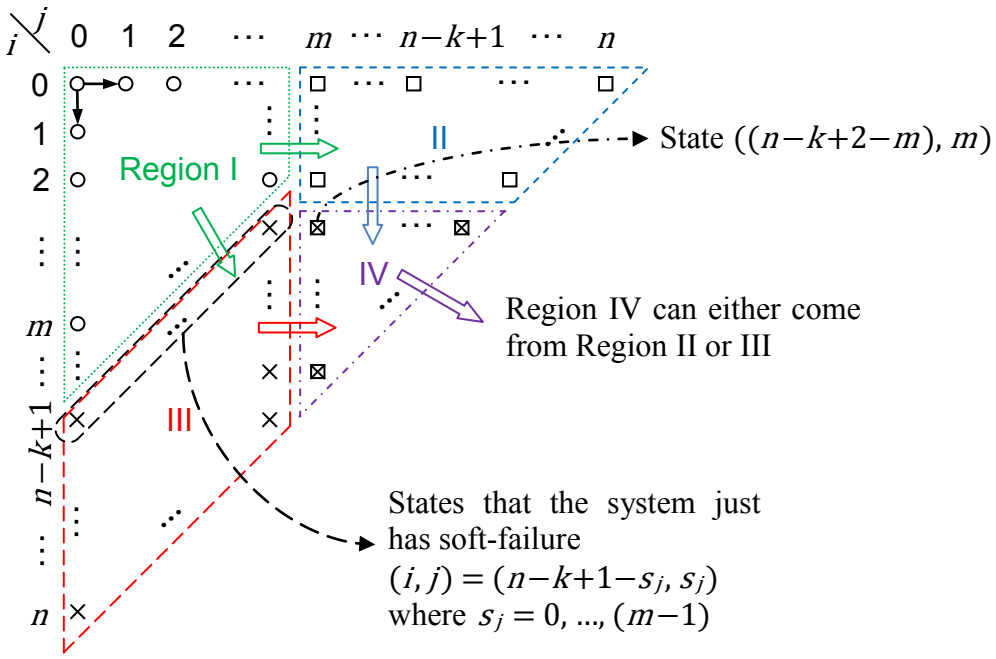

Figure 5.2 Distribution of system states and region of outcomes

Our assumption of the system indicates that all subsystems can be restored to 100% healthy ("as good as new") after each maintenance action. Thus the system is always renewed at state (0, 0) for each cycle at $t_0 = 0$. The probability to observe state $(I(t), J(t)) = (i, j)$ by time t in Figure 5.2 follows the multinomial distribution and is given by

$$P_{ij}(t) = \binom{n}{i,j} F_{u1}(t)^j F_{u2}(t)^i R_u(t)^{n-i-j} \tag{5.6}$$

where $\binom{n}{i,j} = \frac{n!}{i!j!(n-i-j)!}$, $\binom{n}{i,j}$ is the trinomial coefficient. $i, j = 0, 1, 2...$ and $i+j \leq n$. Each state (i, j) has rate $(n-i-j)\lambda_1$ to move to state $(i, j+1)$ and rate $(n-i-j)\lambda_2$ to enter state $(i+1, j)$. The transitions of states are only in one-way direction, which means that back step is not allowed in the model. The states where $i+j = n$ are absorbing states.

In Figure 5.2, there are 3 lined-up sets of states that separate the total states into 4 different regions as follows:

- The first set is the vertical line set that include the states with $j = m$. Once those states are reached, the process will be stopped by rule m. Thus the states on the right hand side of the first set of states with $j = m$ are not reachable during the real process. They are all absorbed by the states with $j = m$. Thus when counting the probability of that process is stopped by m, we are not only summing up the probabilities of the vertical line states but also the probabilities of the right hand side states as shown in Figure 5.2.
- The second set is the tilted line set with those states satisfied $i+j = n-k+1$ and $j < m$. This set of states combined with the first vertical line set is used to separate region I and III.
- The third set is the horizontal line of states satisfied $j > m$ and $i = n-k+1-m$. This is the boarder of region II and IV, with itself belongs to region II.

When a state in region I is observed, the system neither has m noticeable failures nor $(n-k+1)$ total failures. Thus the process has not been stopped by rule m or there is no soft-failure occurred for the system. The boundaries of region I include $0 \leq j < m$ and $0 \leq i < (n-k-j)$. The probability to observe a state in region I by time t is given by

$$\begin{aligned} P_I(t) &= \sum_{j=0}^{m-1} \sum_{i=0}^{n-k-j} P_{ij}(t) \\ &= \sum_{j=0}^{m-1} \sum_{i=0}^{n-k-j} \binom{n}{i,j} F_{u1}(t)^j F_{u2}(t)^i R_u(t)^{n-i-j} \end{aligned} \tag{5.7}$$

If a state is in region II, it means that the system has been stopped for maintenance by criterion m without soft-failures. The boundaries of region II include $0 \leq i \leq (n-k+1-m)$ and $m \leq j \leq (n-i)$. The probability to observe a state in region II by time t can be obtained as follows

$$P_{II}(t) = \sum_{i=0}^{n-k+1-m} \sum_{j=m}^{n-i} P_{ij}(t)$$

$$= \sum_{i=0}^{n-k+1-m} \sum_{j=m}^{n-i} \binom{n}{i,j} F_{u1}(t)^j F_{u2}(t)^i R_u(t)^{n-i-j} \tag{5.8}$$

$$= \sum_{i=0}^{n-k+1-m} \sum_{j=m}^{n-i} \binom{n}{i,j} F_{u1}(t)^j F_{u2}(t)^i R_u(t)^{n-i-j}$$

The states in region III stand for the ones that the soft-failure has occurred to the system. After the soft-failure of the surveillance system, which means $(n-k+1)$ total failure number of subsystems, the monitored area/facility is at risk and the intrusion process has been taken into account. The system is still up running in this case so that it can keep accumulating both types of subsystem failures. In region III, the process is terminated by either the following 3 cases: (i) stopped by m at the moment jumped into region IV; (ii) stopped by T; or (iii) stopped by an intrusion activity. The boundaries of region III include $0 \leq j < m$ and $(n-k+1-j) \leq i \leq (n-j)$. The probability of observing a state in region III has the following expression

$$P_{III}(t) = \sum_{j=0}^{m-1} \sum_{i=n-k+1-j}^{n-j} P_{ij}(t)$$
$$= \sum_{j=0}^{m-1} \sum_{i=n-k+1-j}^{n-j} \binom{n}{i,j} F_{u1}(t)^j F_{u2}(t)^i R_u(t)^{n-i-j} \quad (5.9)$$

States in region IV is more complicated than the other 3 regions. It satisfies both criteria of having at least m detectable failures and $(n-k+1)$ total failures. That means when a state in region IV is observed, the process can be either terminated by rule m already without having the soft-failure or having the soft-failure at first then be stopped by rule m. Thus the route from state $(0,\ 0)$ to reach the state in region IV is required to determine which outcome is corresponded. $P_{IVm}(t)$ stands for the probability of observing a state in region IV that is coming through region II, while $P_{IVs}(t)$ stands for the probability of observing a region IV state that is coming through region III. The boundaries of region IV include $m \leq j < (m+k-2)$ and $(n-k+2-m) \leq i \leq (n-j)$. From the boundary condition we can also get the condition for existence in region IV is $k \geq 2$, that is, as long as the system is not a parallel configuration, region IV will exist.

$$P_{IVm}(t) = \sum_{j=m}^{m+k-2} \sum_{i=n-k+2-m}^{n-j} P_{ij}(t) q_{ijm}$$
$$= \sum_{j=m}^{m+k-2} \sum_{i=n-k+2-m}^{n-j} \binom{n}{i,j} F_{u1}(t)^j F_{u2}(t)^i R_u(t)^{n-i-j} q_{ijm} \quad (5.10)$$

$$P_{IVs}(t) = \sum_{j=m}^{m+k-2} \sum_{i=n-k+2-m}^{n-j} P_{ij}(t) q_{ijs}$$
$$= \sum_{j=m}^{m+k-2} \sum_{i=n-k+2-m}^{n-j} \binom{n}{i,j} F_{u1}(t)^j F_{u2}(t)^i R_u(t)^{n-i-j} q_{ijs} \quad (5.11)$$

where q_{ijm} stands for the probability that state $(i,\ j)$ in region IV comes across region II, while q_{ijs} represents the probability that state (i, j) comes across region III.

$$q_{ijm} = \left[\sum_{l=m}^{\substack{m+\min(j-m,\\ n-k+1-m)}} \binom{n-k+1}{l} \binom{i+j-(n-k+1)}{j-l} \right] \Big/ \binom{i+j}{i} \quad (5.12)$$

$$q_{ijs} = 1 - q_{ijm} \quad (5.13)$$

where (i, j) belongs to region IV.

With the development of the probability of regions, the probability of the first level process outcomes are as follows:

A. Probability that the process does not stop by rule m or having soft-failures by time t. If we choose $T = t$ in the equation, then $P_T(T)$ stands for the probability that the process is stopped by reaching the predetermined age T without having soft-failure:

$$P_T(t) = P_I(t) \quad (5.14)$$

B. Probability that the process has stopped by m is given by:

$$P_m(t) = P_{II}(t) + P_{IVm}(t) \quad (5.15)$$

C. Probability that the process has had a soft-failure by time t:

$$F_{sf}(t) = P_{III}(t) + P_{IVs}(t) \quad (5.16)$$

Since the three probabilities above cover all the possibility outcomes of the process, we have

$$P_T(t) + P_m(t) + F_{sf}(t) = 1 \tag{5.17}$$

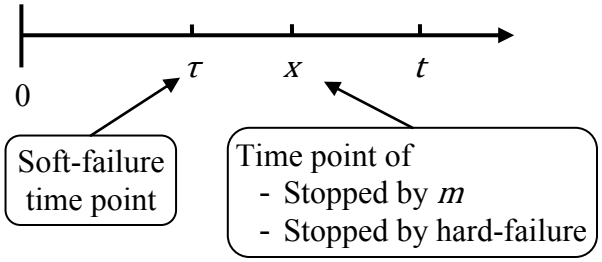

Figure 5.3 Time sequences of possible system outcomes

To further develop the probabilities of the second level outcomes after the soft-failure occurred to the system (outcome C.a $P_{sf\text{-}T}(t)$, C.b $P_{sf\text{-}m}(t)$ and C.c $P_{sf\text{-}H}(t)$), the time sequences can be summarized as shown in Figure 5.3. At time $\tau \in [0, t)$, the soft-failure happened first. Then if at time $x \in [\tau, t)$, the process had stopped by rule m before any intrusion took place, it was considered as the outcome $P_{sf\text{-}m}(t)$. Similarly, if at time $x \in [\tau, t)$, the process had stopped by arrival of intrusion, it was considered as the outcome $P_{sf\text{-}H}(t)$. Finally, during the time interval $[\tau, t)$, the process was neither stopped by rule m nor interrupted by intrusion arrival, it is considered as $P_{sf\text{-}T}(t)$. The representation of each is developed as follows:

$$P_{sf-m}(t) = \sum_{s_j=0}^{m-1} \int_0^t \int_\tau^t R_{H|sf}(x|\tau)\, dF_{m|sf}(x|\tau, s_j) dF_{sf}(\tau, s_j) \tag{5.18}$$

$$P_{sf-H}(t) = \sum_{s_j=0}^{m-1} \int_0^t \int_\tau^t R_{m|sf}(x|\tau, s_j)\, dF_{H|sf}(x|\tau) dF_{sf}(\tau, s_j) \tag{5.19}$$

$$P_{sf-T}(t) = \sum_{s_j=0}^{m-1} \int_0^t R_{m|sf}(x|\tau, s_j) R_{H|sf}(x|\tau)\, dF_{sf}(\tau, s_j) \tag{5.20}$$

where the entering state to region III $(n-k+1-s_j, s_j)$ is considered separately.

$$\begin{aligned} F_{sf}(t, s_j) &= P_{III}(t, s_j) + P_{IVs}(t, s_j) \\ &= \sum_{j=0}^{m-1} \sum_{i=n-k+1-j}^{n-j} P_{ij}(t) q_{ijs_j} + \sum_{j=m}^{m+k-2} \sum_{i=n-k+2-m}^{n-j} P_{ij}(t)\, q_{ijs_j} \end{aligned} \tag{5.21}$$

where q_{ijsj} is the probability that state $(i,\ j)$ in region III or IV is entering region III from state $(n-k+1-s_j, s_j)$

$$q_{ijs_j} = \left[\binom{n-k+1}{s_j}\binom{i+j-(n-k+1)}{j-s_j}\right] \Big/ \binom{i+j}{j} \tag{5.22}$$

To obtain $F_{m|sf}(x|\tau,\ s_j)$, a revised triangular state distribution from Figure 5.2 is needed with the starting state at $(n-k+1-s_j,\ s_j)$ and $t_0 = \tau$. Thus $F_{m|sf}(x|\tau,\ s_j)$ is the probability of observing any state in the right hand small triangular in Figure 5.4.

$$\begin{aligned} &F_{m|sf}(x|\tau, s_j) \\ &= \sum_{j=m-s_j}^{k-1} \sum_{i=0}^{k-1-j} \binom{k-1}{i,j} F_{u1}(x-\tau)^j F_{u2}(x-\tau)^i R_u(x-\tau)^{k-1-i-j} \end{aligned} \tag{5.23}$$

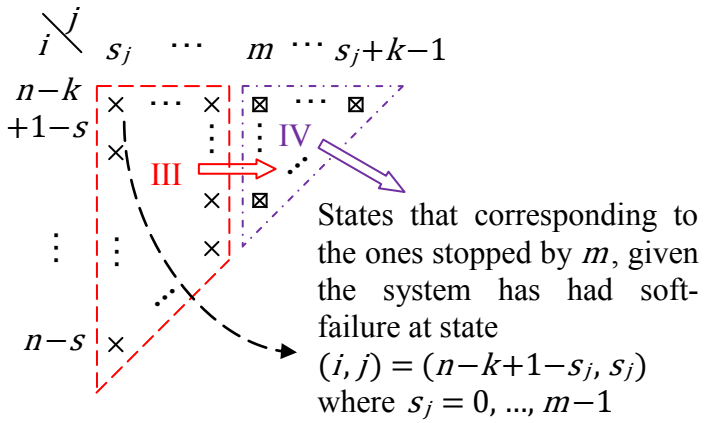

Figure 5.4 Distribution of system states for calculation of $F_{m|sf}(x|\tau, s_j)$ given that the system has had soft-failure at state $(n-k+1-s_j, s_j)$

Note that to guarantee the existence of the right hand small triangular in Figure 5.4, this inequality $(m-s_j) > (k-1)$ must hold. Otherwise $F_{m|sf}(x|T_s = \tau, S_j = s_j) \equiv 0$.

$$R_{m|sf}(x|T_s = \tau, S_j = s_j) = 1 - F_{m|sf}(x|T_s = \tau, S_j = s_j) \tag{5.24}$$

The intrusion process (second process) is defined as arriving at rate μ right after the system reaches soft-failure state. Thus

$$R_{H|sf}(x|T_s = \tau) = e^{-\mu(x-\tau)} \tag{5.25}$$

$$F_{H|sf}(x|T_s = \tau) = 1 - R_{H|sf}(x|T_s = \tau) = 1 - e^{-\mu(x-\tau)} \tag{5.26}$$

Since the 2nd level outcome probabilities are separated from $F_{sf}(t)$, we have

$$F_{sf}(t) = P_{sf-m}(t) + P_{sf-H}(t) + P_{sf-T}(t) \tag{5.27}$$

where $P_{sf\text{-}m}(t)$, $P_{sf\text{-}H}(t)$ and $P_{sf\text{-}T}(t)$ are given in equation (5.18), (5.19) and (5.20), respectively. Depending on the design requirement of the system, the following two reliability functions can be defined:

Reliability function 1, $R_1(t)$: If the system is less strict and can afford some portion of time in the soft-failure state as it is our main focus in this study for the surveillance systems, then the *failure of the system* can be defined only for the *hard- failure* part. In this case, the reliability function of the system can be expressed as

$$R_1(t) = P_T(t) + P_m(t) + P_{sf-m}(t) + P_{sf-T}(t) = 1 - P_{sf-H}(t) \qquad (5.28)$$

Reliability function 2, $R_2(t)$: If the system is only considered the soft-failure aspect that is the traditional k-out-of-n system reliability modeling where at least k-out-of-n subsystems must work for the system to work, then the reliability of the system can be defined as follows

$$R_2(t) = P_T(t) + P_m(t) = 1 - F_{sf}(t) \qquad (5.29)$$

5.4 Numerical Examples

We now illustrate the proposed model through several numerical examples using equations (5.14) – (5.16), (5.18) – (5.20), and (5.28) – (5.29). Each model is focused on the effect of variation of one parameter to the probability outcomes of the system.

Case 1: Given $n = 5$ and $k = 3$. The number of detectable failures to stop the process for maintenance m was varying for all possible values from 1 to $(n-k)$. In this case $n-k = 2$. The model parameters are also given as follows:

The detectable failure rate $\lambda_1 = 0.005$.

The undetectable failure rate $\lambda_2 = 0.001$.

The failure rate of the intrusion process ("second process") $\mu = 0.01$.

In this case, it is much easier to move to the right than to move down in the state distribution diagram, which is shown in Figure 5.4. The probabilities of the two-level

outcomes of the process for $m = 1$ and $m = 2$ are shown in Figure 5.5 and 5.6, respectively.

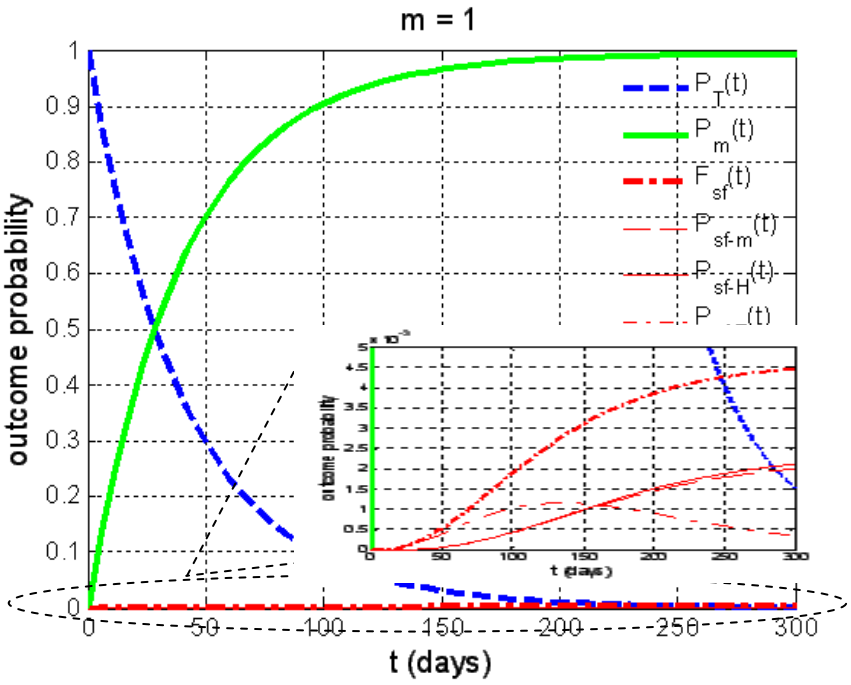

Figure 5.5 Probabilities of the two-level outcomes with stopping criterion $m = 1$

We can observe that as time increases the probability that the system is going to stop by the time T (called rule T) quickly decreases. On the contrary, all the functions $P_m(t)$, $F_{sf}(t)$, $P_{sf\text{-}m}(t)$ and $P_{sf\text{-}H}(t)$ each first increases significant then slightly increase as the time increases. It can be easily explained that by holding a constant m and only increasing t, the process is more likely to be stopped by rule m (either with or without soft-failure happened first) or the hard-failure.

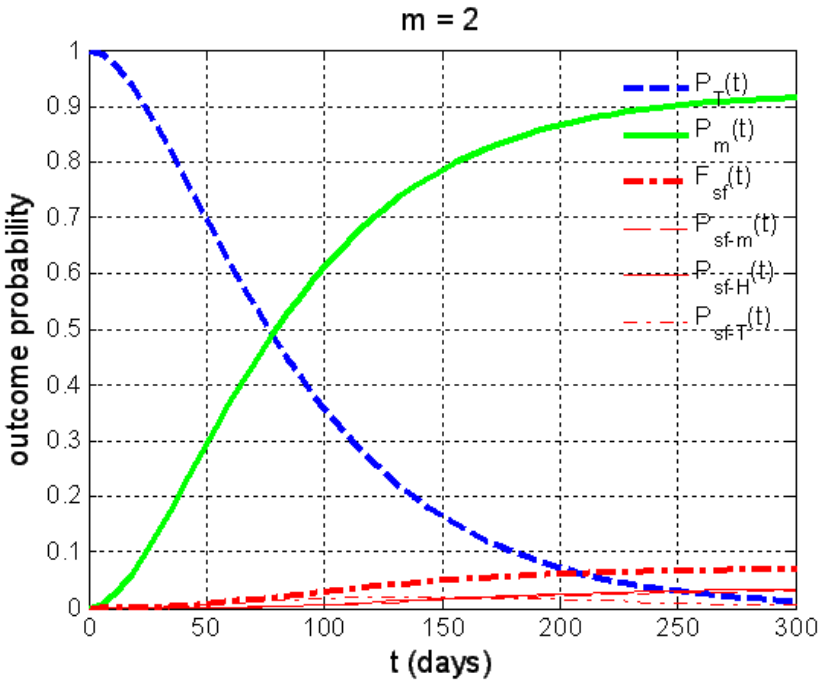

Figure 5.6 Probabilities of the two-level outcomes with stopping criterion $m = 2$

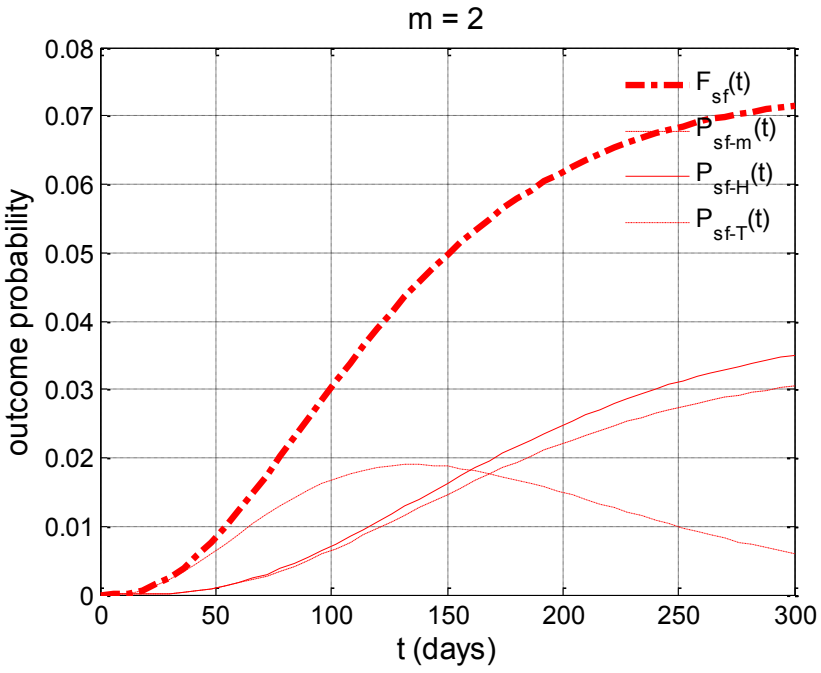

Figure 5.7 Zoomed plot of the second level outcome of the system with $m = 2$

As shown in Figure 5.7, it is interesting to observe that $P_{sf\text{-}T}(T)$ first increases then decreases as t increases. There is a trade-off pair of effects on by an increment of time. When t is small, increasing t will result in higher probability of having soft-failure. Thus the probability that the process survives some time after the soft-failure also increases accordingly. This effect contributes to the rising portion of $P_{sf\text{-}T}(t)$, When t is not so small, the probability of having a soft-failure becomes more stable and barely increases with t. Then to keep the process for longer running time would only make the process more likely to be stopped either by rule m or hard-failure. Thus the probability that the process survives until time after having soft-failure drops when t increases. Hence the combination of the two effects gives the rise-then-drop profile for $P_{sf\text{-}T}(t)$. As m increases from 1 to 2 (see Figure 5.8), the process has less probability to be stopped by rule m because the absorbing boundary has shifted one step to the right. Accordingly, it is easier to have soft-failure thus also leads to increment of the hard-failure probability. Hence the reliability function $R_1(t)$ drops as shown in Figure 5.8. The plot of the variation of type 2 reliability function $R_2(t)$ is similar to the plot of $R_1(t)$, only with different scales. Thus the plot is omitted. Since $R_1(t)$ only excludes $P_{sf\text{-}H}(t)$, while $R_2(t)$ subtracts the whole probability of having soft-failure $F_{sf}(t)$ from 1, therefore, $R_1(t)$ is always greater than or equal to $R_2(t)$ as shown in Figure 5.9.

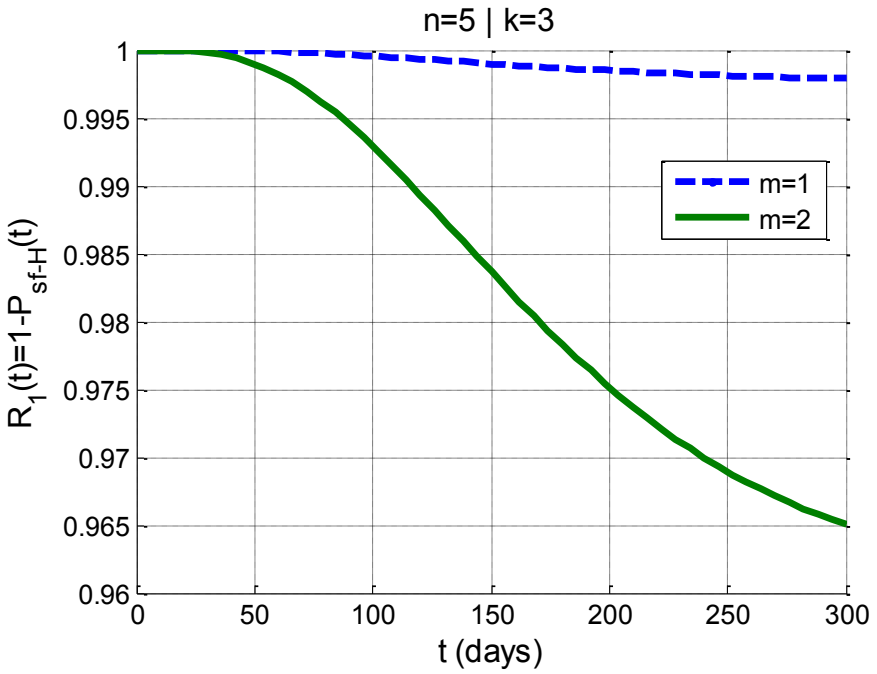

Figure 5.8 Type 1 reliability (equation (5.28)) comparison with change of m

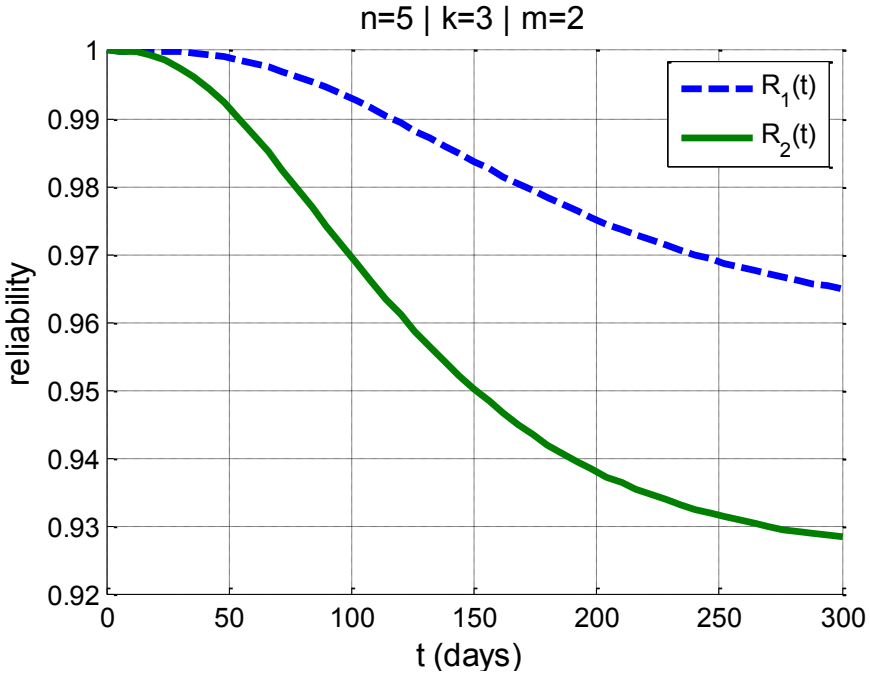

Figure 5.9 Comparison of $R_1(t)$ and $R_2(t)$ with $m = 2$

Case 2: Model parameters λ_1, λ_2 and μ are the same as Case 1 above but we fixed $k = (n+1)/2$ and $m = 3$. Figure 5.10 shows the reliability function for values of n vary from 7 to 15 with a step of 2. Fixing k at $(n+1)/2$ is a standard configuration to represent majority voting systems [73]. From Figure 5.10, the reliability function increases as n increases. This is because that the safety gap $(n-k+1-m)$ increased with n, resulting in less probability of failures of the system.

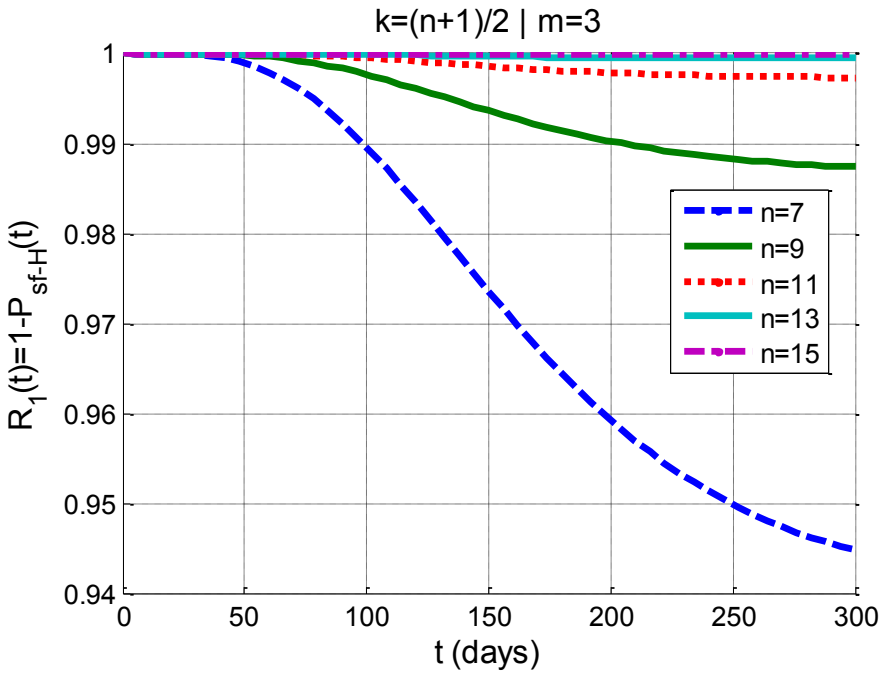

Figure 5.10 Type 1 reliability comparison with change of n; $m = 3$

Case 3: Here we define $m = n-k-1$ and $k = (n+1)/2$. In this manner, we always had a safety gap of 2. As in Figure 5.11, the reliability function drop with the increment of n. The reliability function values are highly related to the portion of region III in the whole triangular area, as in the triangular state distribution diagram. If the safety gap value $(n-k+1-m)$ is maintained, increasing n results in increasing of percentage of area of region III over the total thus increases the failure probability. Hence the reliability

function decreases as n increases. This example demonstrates that with certain configuration of the system parameters, it is not always beneficial in terms of reliability to increase the number of subsystems in the entire system.

5.5 Conclusion

In this chapter, a k-out-of-n surveillance system subject to two competing failure modes -- detectable and undetectable -- is discussed. The two stochastic-process reliability of the surveillance system is derived with the consideration of the intrusion process and a (m, T) opportunistic maintenance policy. Several numerical examples are given to demonstrate the validity of the modeling and the sensitivity of several important parameters. For the future works, with the development of all the probability outcomes, cost can be associated with different scenarios to stop the process for maintenance and optimal maintenance schedule (m^*, T^*) can be developed by minimizing the total surveillance system cost per unit time.

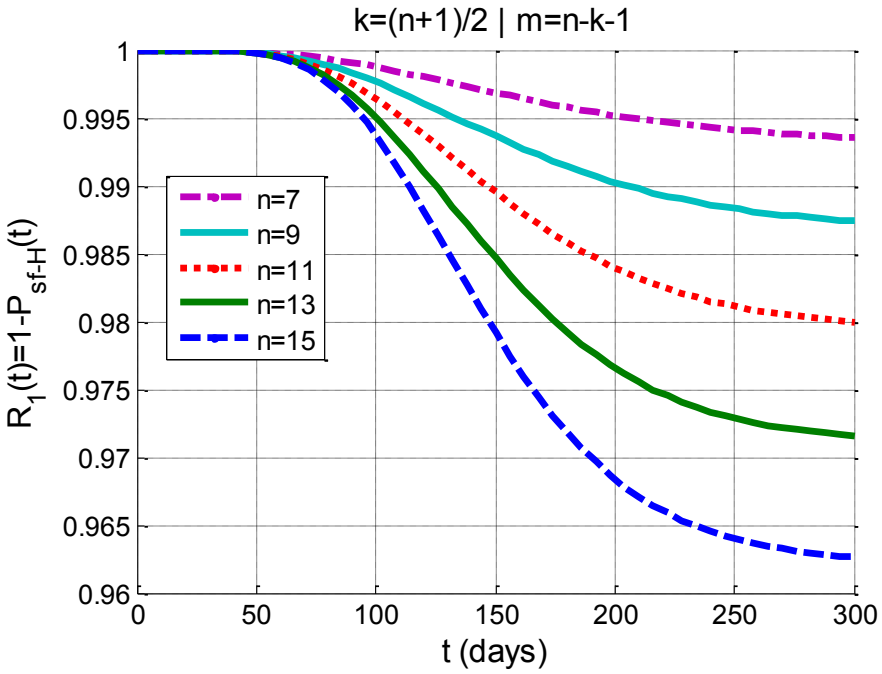

Figure 5.11 Type 1 reliability comparison with various values of n where

$$m = n-k-1$$

Chapter 6

A Cost Model of an Opportunistic Maintenance Policy on *k*-out-of-*n* Surveillance Systems Considering Two Stochastic-Processes

6.1 Introduction

The surveillance system has been widely applied to enhance the security level of the protected area. US government invests billions of dollars each year on installation of surveillance cameras to monitor crime activities. The reliability of the surveillance systems is critical since failure of such systems may result in severe damage to the protected facilities. Two typical methods are widely applied to enhance the system reliability: adding redundancy and scheduling preventive maintenance to restore the system to younger states. For multi-unit systems, the maintenance policy often takes the dependency between components into consideration. One of the applications is the opportunistic maintenance, where in each maintenance action, several units are being serviced together to save resource [7, 85, 129, 147].

For most reliability modeling, only the system operating process is taken into consideration. However, for the surveillance redundant systems, its goal is to monitor and record all the actions and activities when the incidents or attacks occurred. In other words, if the system has many failed components and are not functioning properly, but it reaches maintenance point without encountering any incident. This case may still be considered as “fail-safe” or “soft-failure” since no incident has yet occurred, and thus no real damage to the area. If ignoring the incident arrival process, or intrusion process, it will result in more frequent maintenance action than necessary. Note that this is not always been good since the maintenance usually associate with system down time and restore cost. In

Chapter 5, a two-process model on reliability modeling of the surveillance system with both noticeable and hidden failures is proposed considering an (m, T) opportunistic maintenance policy. However, the optimal design of the policy is left out in the modeling. The cost model is frequently applied to determine the optimal maintenance policy by unifying the measurement of the maintenance consumption and the system risk with prices. Many related works can be found in [84, 92, 93, 106, 127, 134, 139, 148, 149]. Pham and Zhang [150] propose a model on optimal software releasing time by addressing different functions to different phases of the software development or marketing. Teng and Pham [151] present a cost model on a software gain model with consideration of the random environment. Wang and Pham [134] proposed a cost model on optimal preventive maintenance of system with dependent competing risks and hidden failures.

In this chapter, we develop a cost model to determine the optimal maintenance policy of the (m, T) rule for the two-process reliability modeling of the k-out-of-n surveillance systems developed in Chapter 5. The cost model addresses the expected number of failures for each outcome of the multi-unit system and penalties for soft and hard-failures of the surveillance system. A search algorithm is proposed to obtain the optimal solution of the cost model. Several numerical examples are given to demonstrate the proposed models.

6.2 Cost Model

6.2.1 Description of the Surveillance Systems with (m, T) Maintenance Policy

The surveillance system model considered in this work is presented in Chapter 5. The system structure is a k-out-of-n system with subsystems that have two failure modes:

detectable and undetectable. Both types of failures are countable to determine the system status. Once $(n-k+1)$ total failure are accumulated, the surveillance system is considered as in "soft-failure" mode. Because of the existence of the undetectable failures in the subsystems, the soft-failure is not self announced. When enough subsystems are working, the monitored area is considered protected. Any arrivals of attacks will be discovered and responded accordingly. From the time point of the soft-failure, any additional arrival of the attack will strike the surveillance area and cause severe damage. Thus the first arrival of attack after the soft-failure is defined as hard-failure. Since we gain partial information from the system status from the detectable failures, the following opportunistic maintenance policy is adapted to enhance the system performance, noted as $(m,\ T)$ rule. In the policy the whole system is renewed at one of the following events, whichever occurred first:

(1) The system has accumulated m noticeable failures

(2) The system has survived time T from last maintenance action

(3) Then system has had a hard-failure

The maintenance action is considered perfect, that is, to replace the failed subsystem and fully restore all the working subsystems to their "as good as new" states. Parameter m here is considered as a hazard indication and is applied for early termination of one renewal cycle to prevent hard-failure. Thus it should be selected smaller than $(n-k+1)$, which is the number of total failures for the lost of the surveillance system in order to leave some safety gap for the undetectable subsystem failures. Thus the range for m is $[1, n-k]$.

Based on the description of the system and the maintenance rules, the possible system outcome is summarized as the following and shown in Figure 6.1.

A. The system stops for maintenance after time T from the last maintenance without soft-failure (stopped by T).

B. The system stops for maintenance by observing m noticeable failures of subsystems without soft-failure (stopped by m).

C. Soft-failure occurred before any maintenance action. Notice that there is no way to discover the soft-failure immediately and terminate the system. Three possible outcomes can occur after the soft-failure:

   a. The system reaches the maintenance point by rule T (noted as $sf\text{-}T$).

   b. The system reaches the maintenance point by rule m (noted as $sf\text{-}m$).

   c. The system reaches the maintenance point by having a hard-failure ($sf\text{-}H$).

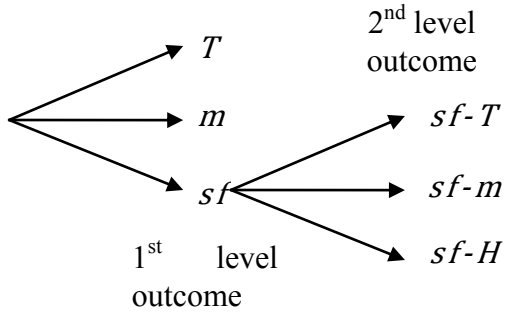

Figure 6.1 Diagram of the two levels of maintenance action

The mathematical expressions of the outcome probability are developed in Chapter 5. The first part $P_1(t)$ is the probability that the process is neither stopped by rule m nor having soft-failures by time t:

$$P_T(t) = \sum_{j=0}^{m-1} \sum_{i=0}^{n-k-j} P_{ij}(t) \tag{6.1}$$

The probability that the process has stopped by m directly and has no soft-failure in the cycle is given by:

$$P_m(t) = \sum_{i=0}^{n-k+1-m} \sum_{j=m}^{n-i} P_{ij}(t) + \sum_{j=m}^{m+k-2} \sum_{i=n-k+2-m}^{n-j} P_{ij}(t) q_{ijm} \tag{6.2}$$

The probability that the process has had a soft-failure by time t:

$$F_{sf}(t) = \sum_{j=0}^{m-1} \sum_{i=n-k+1-j}^{n-j} P_{ij}(t) + \sum_{j=m}^{m+k-2} \sum_{i=n-k+2-m}^{n-j} P_{ij}(t) q_{ijs} \tag{6.3}$$

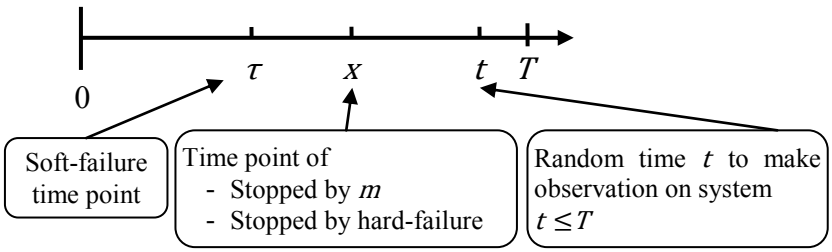

Figure 6.2 Time sequences of possible system outcomes

The probabilities of the second level outcomes after the soft-failure are listed as the following:

$$P_{sf-m}(t) = \sum_{s_j=0}^{m-1} \int_0^t \int_\tau^t R_{H|sf}(x|\tau) dF_{m|sf}(x|\tau, s_j) dF_{sf}(\tau, s_j) \tag{6.4}$$

$$P_{sf-H}(t) = \sum_{s_j=0}^{m-1} \int_0^t \int_\tau^t R_{m|sf}(x|\tau, s_j) dF_{H|sf}(x|\tau) dF_{sf}(\tau, s_j) \tag{6.5}$$

$$P_{sf-T}(t) = \sum_{s_j=0}^{m-1} \int_0^t R_{m|sf}(x|\tau, s_j) R_{H|sf}(x|\tau) dF_{sf}(\tau, s_j) \tag{6.6}$$

For the detailed development of the probability outcomes, please refer to Chapter 5.

6.2.2 Cost Model Description

The performance of the surveillance system is highly determined on the maintenance schedule. For the opportunistic maintenance (m, T) policy chosen in Chapter 5, the selection of the two parameters has dependent interference on the system cost per unit time. On the one hand, if either parameter is too small, the maintenance actions will be carried out too frequently so that the cost to restore the system to perfect state increases. The risk of having failures (both soft-failures and hard-failures) will be low in this case. On the other hand, if both the parameters are set at large values, the intervals between two maintenance actions will be too long so that the system is under too much risk, although some cost of the maintenance is saved. Thus we can clearly see the trade-off of the high maintenance cost vs. the system risk. With the development of the system probability outcomes in Chapter 5 and the cost model in this work, the optimal maintenance schedule can be obtained to achieve the lowest cost per unit time while remaining the system risk at a reasonable level. The assumptions of the cost model are given as the following:

1) There is a set-up cost to initiate every maintenance action. This is corresponding to the economic dependency of the subsystems.
2) For each maintenance action, the system is restored to “as good as new”, which means that all the failed subsystems have to be fixed and all the survived

subsystem have to be serviced so that every subsystem is in perfect state after a maintenance. One can expect a higher cost for renewing a failed unit than servicing a working unit in the cost model.

3) Whenever a maintenance action is initiated by a hard-failure, a very large cost is addressed in the model, as an intrusion/incident arrival when the surveillance is down often resulting in massive damage to the protected area. The hard-failure is the most important thing we are trying to avoid by having the maintenance policy.
4) When a soft-failure occurs, there is a penalty addressed from the time of the soft-failure to the next maintenance action. The penalty cost per unit time represents the risk of losing the protection of the surveillance system, although the hard-failure may or may not strike the area after the soft-failure.

The expected maintenance cost per cycle includes the following parts:

i. A constant set-up cost c_0.
ii. Cost for restoring the system $C_R(m,\ T)$. This part of the cost is related to the expected number of failed subsystems $E_{Si}[N_F|m,\ T]$.
iii. Penalty cost for hard-failure $C_H(m,\ T)$. The cost represents the massive damage due to the success attack under no protection of the surveillance system.
iv. Penalty cost for the time lost of protection with the surveillance system $C_S(m,\ T)$.

Each of the cost components can be determined as the following:

A. Cost for restoring the system $C_R(m,\ T)$.

$$C_R(m,T) = \sum_{s_i \in S} \left[c_f E_{S_i}[N_F|m,T] + c_s\left(n - E_{S_i}[N_F|m,T]\right)\right] P_{s_i}(m,T) \qquad (6.7)$$

where set S includes all possible outcomes in each maintenance cycle. The elements can be found in Table 6.1. $P_{S1}(m,\ T)$ to $P_{S5}(m,\ T)$ can be calculated from equation (6.1), (6.2), (6.4) – (6.6), respectively.

Table 6.1 Label representation of the possible outcomes

s_i	Corresponding outcome
s_1	stopped by T (without soft-failure)
s_2	stopped by m (without soft-failure)
s_3	stopped by T after soft-failure
s_4	stopped by m after soft-failure
s_5	stopped by hard-failure after soft-failure

where the expected number of different outcomes are represented as the following respectively.

$$E_{S_1}[N_F|m,T] = \sum_{j=0}^{m-1}\sum_{i=0}^{n-k-j}(i+j)P_{ij}(T) \tag{6.8}$$

$$\begin{aligned} E_{S_2}[N_F|m,T] = &\sum_{i=0}^{n-k+1-m}\sum_{j=m}^{n-i}(i+m)P_{ij}(T) \\ &+\sum_{j=m}^{m+k-2}\sum_{i=n-k+2-m}^{n-j}(n-k+1)P_{ij}(T)q_{ijm} \end{aligned} \tag{6.9}$$

$$E_{S_3}[N_F|m,T] = \sum_{j=0}^{m-1}\sum_{i=n-k+1-j}^{n-j}(i+j)P_{ij}(T) \tag{6.10}$$

$$E_{S_4}[N_F|m,T] = \sum_{j=m}^{m+k-2} \sum_{i=n-k+2-m}^{n-j} (i+m) P_{ij}(T) q_{ijs} \tag{6.11}$$

$$E_{S_5}[N_F|m,T] = \sum_{j=0}^{m-1} \sum_{i=n-k+1-j}^{n-j} (i+j) P_{ij}(T) \tag{6.12}$$

B. Penalty cost for hard-failure $C_H(m,\ T)$.

This is a onetime cost for hard-failure. It represents the massive damage due to the success attack under no protection of the surveillance system. It is the major risk we are trying to reduce with the maintenance policy.

$$C_H(m,T) = c_H P_{S_5}(m,T) \tag{6.13}$$

C. Penalty cost for the time lost of protection with the surveillance system $C_S(m,\ T)$.

This part of cost is proportion to the expected time length from one soft-failure to the time point T_{end} to carry out the next maintenance action. The separate cases for outcome s_3, s_4 and s_5 have to be discussed.

$$E\left[T_{S_3} - \tau\right] = \sum_{s_j=0}^{m-1} \int_0^T (T-\tau) R_{m|sf}\left(x|\tau, s_j\right) R_{H|sf}(x|\tau) dF_{sf}\left(\tau, s_j\right) \tag{6.14}$$

$$E\left[T_{S_4} - \tau\right] = \sum_{s_j=0}^{m-1} \int_0^T \int_\tau^T (x-\tau) R_{H|sf}(x|\tau) dF_{m|sf}\left(x|\tau, s_j\right) dF_{sf}\left(\tau, s_j\right) \tag{6.15}$$

$$E\left[T_{S_5} - \tau\right] = \sum_{s_j=0}^{m-1} \int_0^T \int_\tau^T (x-\tau) R_{m|sf}\left(x|\tau, s_j\right) dF_{H|sf}(x|\tau) dF_{sf}\left(\tau, s_j\right) \tag{6.16}$$

$$E[T_{end} - \tau] = E\left[T_{S_3} - \tau\right] + E\left[T_{S_4} - \tau\right] + E\left[T_{S_5} - \tau\right] \tag{6.17}$$

$$C_S(m,T) = c_p\, E[T_{end} - \tau] \tag{6.18}$$

The total expected cost per renewal cycle $C(m,\ T)$ thus is expressed as

$$C(m,T) = c_0 + C_R(m,T) + C_H(m,T) + C_S(m,T) \tag{6.19}$$

The expected time length of each interval between two consecutive maintenance actions is estimated by summing up the expected time for each outcome.

$$E\left[T_{cycle}|m,T\right] = \sum_{s_i \in S} E\left[T_{s_i}|m,T\right] \text{ for all } i = 1, 2, ..., 5 \tag{6.20}$$

where

$$E\left[T_{s_1}|m,T\right] = TP_T(T) \tag{6.21}$$

$$E\left[T_{s_2}|m,T\right] = \int_0^T t dP_m(t) \tag{6.22}$$

$$E\left[T_{s_3}|m,T\right] = TP_{sf-T}(T) \tag{6.23}$$

$$E\left[T_{s_4}|m,T\right] = \sum_{s_j=0}^{m-1} \int_0^T \int_\tau^T x R_{H|sf}(x|\tau) dF_{m|sf}\left(x|\tau, s_j\right) dF_{sf}\left(\tau, s_j\right) \tag{6.24}$$

$$E\left[T_{s_5}|m,T\right] = \sum_{s_j=0}^{m-1} \int_0^T \int_\tau^T x R_{m|sf}\left(x|\tau, s_j\right) dF_{H|sf}(x|\tau) dF_{sf}\left(\tau, s_j\right) \tag{6.25}$$

With the above development, the expected cost per unit time of the designed maintenance policy can be defined as

$$EC_L(m,T) = \frac{C(m,T)}{E\left[T_{cycle}|m,T\right]} = \frac{c_0 + C_R(m,T) + C_H(m,T) + C_S(m,T)}{\sum_{s_i \in S} E\left[T_{s_i}|m,T\right]} \tag{6.26}$$

We wish to find the optimal maintenance parameters m^* and T^* that minimizes the expected total system cost in equation (6.26). Mathematically, the optimization cost model is as follows

$$\begin{aligned} \min_{m,T} \quad & EC_L(m,T) = \frac{c_0 + C_R(m,T) + C_H(m,T) + C_S(m,T)}{\sum_{s_i \in S} E\left[T_{s_i}|m,T\right]} \\ \text{s.t.} \quad & m \in [1, n-k], T > 0 \end{aligned} \tag{6.27}$$

where $C_R(m,\ T)$, $C_H(m,\ T)$, $C_S(m,\ T)$ and $E[T_{si}|m,\ T]$ are given in equation (6.7), (6.13), (6.18) and (6.21) to (6.25), respectively.

6.3 Numerical Optimal Maintenance Policy

There is a trade-off between high maintenance cost and high risk of the system. On the one hand, when the maintenance interval is too short, much money will be wasted on the maintenance actions thus the total system cost per unit time will be high. On the other hand, when the interval is large, the system is going under too much risk to have failures that the expected penalty is too high. The parameter m must be integers and restricted in the range $[1,\ n-k]$. Hence there is only a small set of candidates for possible m so that we can enumerate all possibilities instead of using some integer programming techniques. However, both the numerator $C(m,\ T)$ and the denominator $E[T_{cycle}|m,\ T]$ of $EC_L(m,\ T)$ have too many terms and it is tedious to use equation (6.27) to achieve the optimal solution. Based on several observations from the numerical calculations, although we won't be able to prove it in theory, we are confident to conclude that there is only one local minima (unimodel) for $EC_L(m,\ T)$ for every given m. The observations are shown in Figure 6.3 to Figure 6.9. These observations are also the plots for the numerical examples provided in Section 6.4.

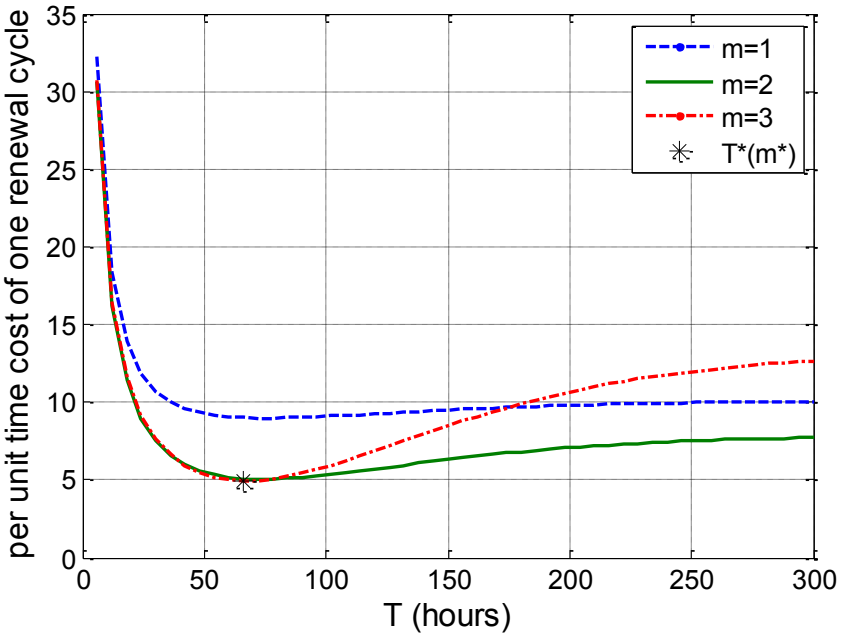

Figure 6.3 Expected cost per unit time of Case 1

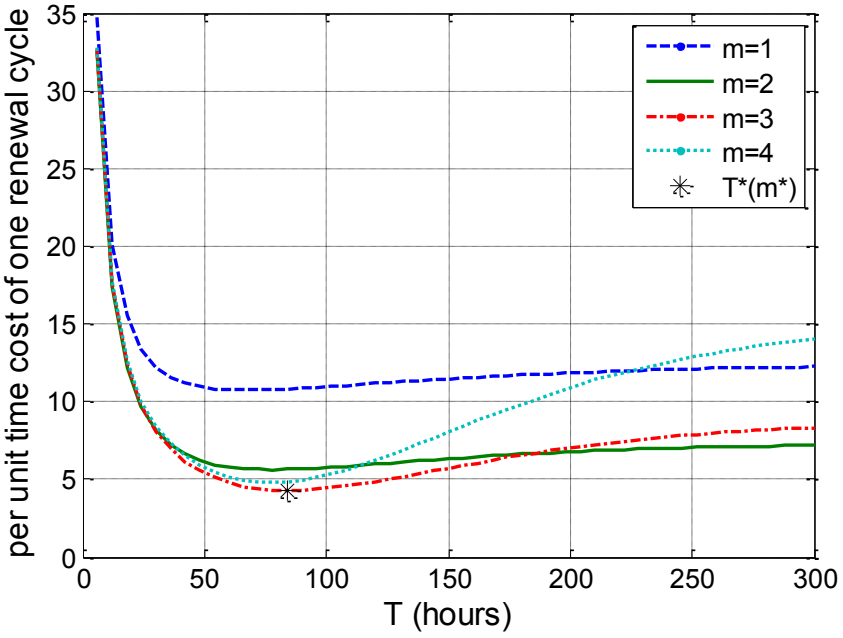

Figure 6.4 Expected cost per unit time of Case 2.1

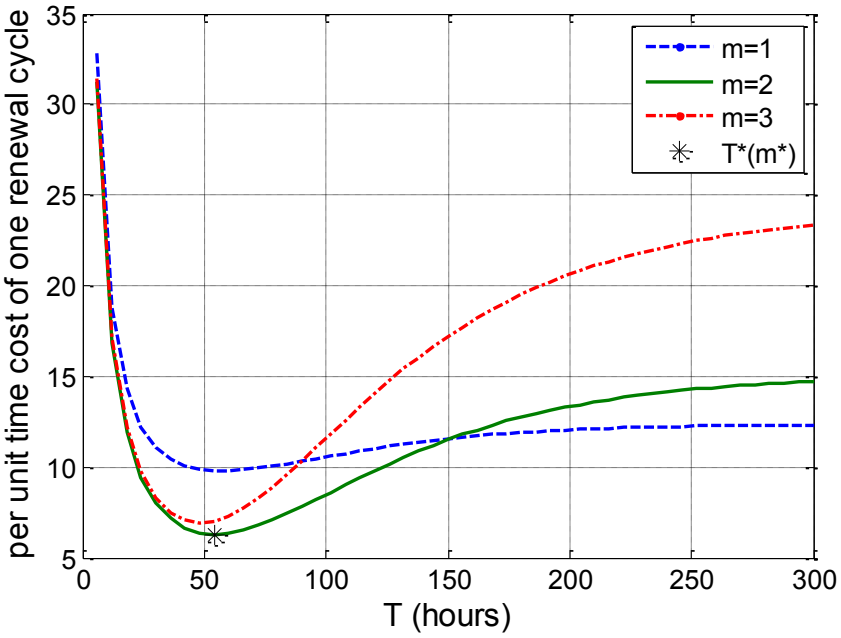

Figure 6.5 Expected cost per unit time of Case 3

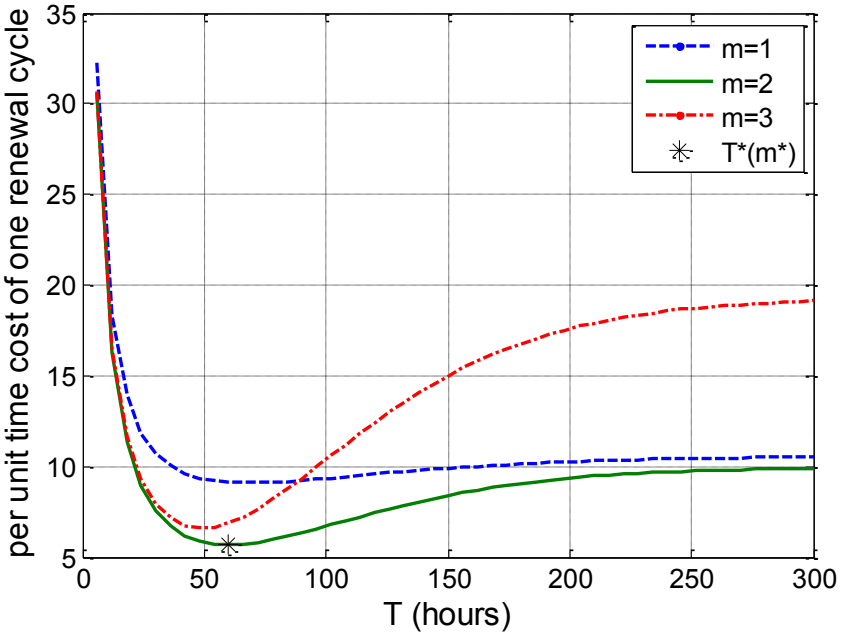

Figure 6.6 Expected cost per unit time of Case 4

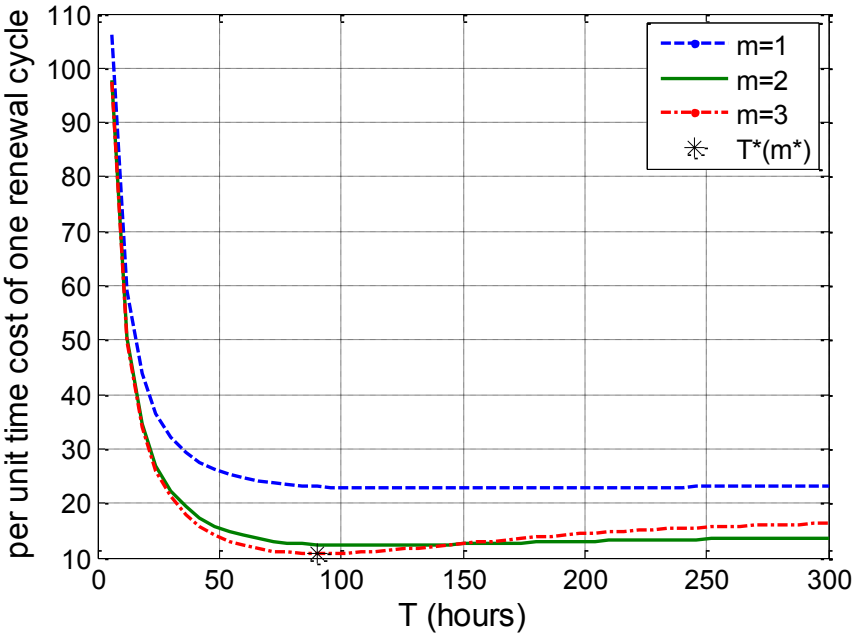

Figure 6.7 Expected cost per unit time of Case 5

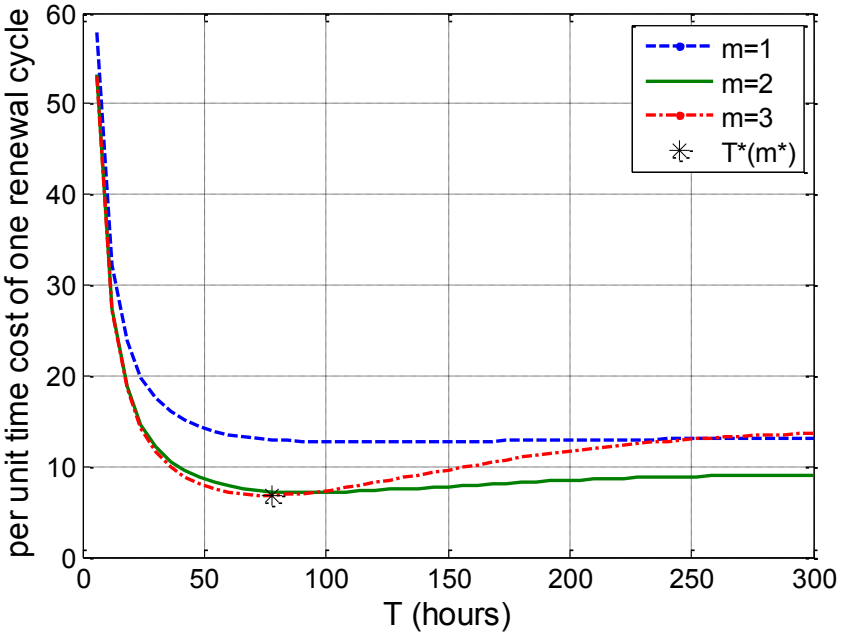

Figure 6.8 Expected cost per unit time of Case 6

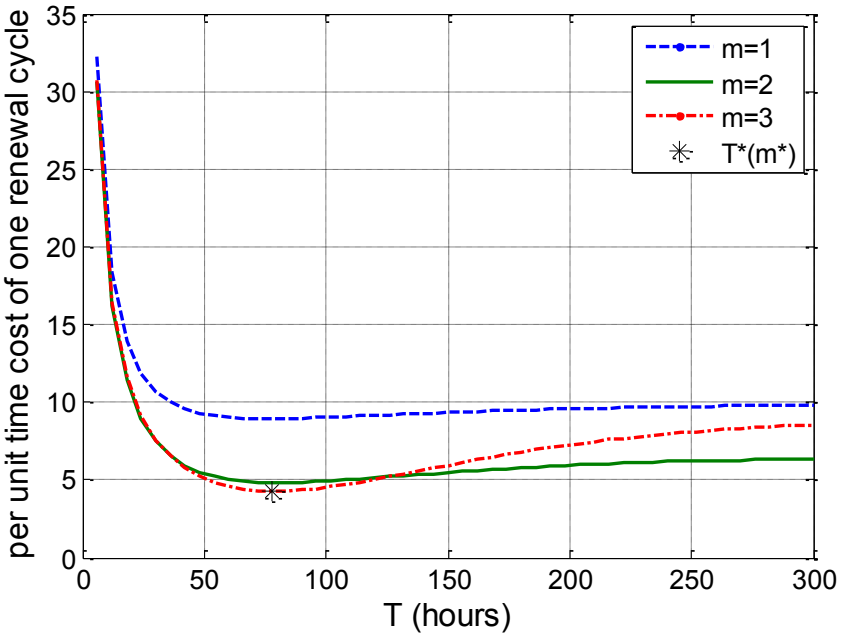

Figure 6.9 Expected cost per unit time of Case 7

After many numerical calculations and investigation, we can assume that the expected total cost function $EC_L(m,\ T)$ behaves as a unimodel. We now discuss a numerical algorithm in order to obtain the optimal solution for m and T for given parameters k, n, λ_1, λ_2, μ, c_0, c_f, c_s, c_H, and c_p.

Firstly an initial point to start the search algorithm is generated. The mean time to failure (MTTF) for the traditional k-out-of-n surveillance system without the consideration of the second process is calculated to generate a starting point of the search algorithm for the optimal maintenance predetermined age T. It is expressed as

$$MTTF = \int_0^\infty R_{k,n}(t)dt = \int_0^\infty \sum_{l=k}^{n} \binom{n}{l} e^{-l(\lambda_1+\lambda_2)t}(1-e^{-(\lambda_1+\lambda_2)t})^{n-l}\,dt \quad (6.28)$$

Since the maintenance policy is designed to remain some safe margin to prevent the surveillance system from failure, thus the initial point of the predetermined age is selected smaller than the traditional MTTF, as the following:

$$T_0 = \alpha MTTF \quad \text{for } 0<\alpha<1 \tag{6.29}$$

The search algorithm will enumerate all possible m values from 1 to $(n-k)$ and find a $T^*(m)$ for each m. Then $(m^*,\ T^*)$ is selected from all the candidate $(m,\ T^*(m))$ pairs with the smallest $EC_L(m,\ T)$.

Algorithm:

1) $\alpha = 2/3$, $m = 1$, $T = T_0$, calculate $EC_L(m,\ T)$.
2) if $EC_L(m,\ T) \le EC_L(m,\ T+\Delta T)$

$$T^*(m) = \inf\{T: EC_L(m,T) \ge EC_L(m,T-\Delta T)\}, \Delta T > 0$$

else

$$T^*(m) = \sup\{T: EC_L(m,T) \ge EC_L(m,T+\Delta T)\}, \Delta T > 0$$

3) $m = m+1$, $T = T_0$, until $m = n-k$, calculate $EC_L(m,\ T)$. Go to 2)
4) Obtain $(m^*,\ T^*)$ by selecting the candidate $(m,\ T^*(m))$ pair with the minimal $EC_L(m,\ T)$.

6.4 Numerical Example

To demonstrate the proposed cost model and algorithm to obtain the optimal maintenance policy, several cases with different parameter settings are studied. The results are posted in Table 6.2.

Table 6.2 Optimal maintenance policies under different conditions

Case #	Conditions	(m^*, T^*)	min $EC_L(m, T)$
Case 1	$k = 4, n = 7, \lambda_1 = 0.005, \lambda_2 = 0.002, \mu = 0.01$ $c_0 = 100, c_f = 60, c_s = 10, c_H = 5000, c_p = 10$	(3, 67)	4.9439
Case 2.1	$n = 8$	(3, 84)	4.2975
Case 2.2	$n = 9$	(4, 96)	4.0939
Case 2.3	$n = 10$	(4, 104)	4.0388
Case 3	$\lambda_2 = 0.004$	(2, 54)	6.2985
Case 4	$\mu = 0.05$	(2, 60)	5.6675
Case 5	$c_0 = 500$	(3, 91)	10.7764
Case 6	$c_s = 30$	(3, 75)	6.818
Case 7	$c_H = 2000$	(3, 79)	4.2661

Note: the coefficients not listed in Case 2–7 are the same as in Case 1.

6.4.1 The Impact of the System Structure

From case 2.2 to 2.4, the total number of the subsystems has been increased with all the other parameters unchanged. We can find out that with the minimal number of subsystem remaining at $k = 4$, increasing n decreases the optimal per unit time cost of the system $EC_L(m^*, T^*)$. It is not hard to understand the effect since increasing redundancy of the system will lower down the risk of the system. A consequence of this change is the trend of the increment of optimal (m^*, T^*), as that it is rational to carry out the maintenance action less often for system with lower failure rate.

6.4.2 The Impact of the Failure Rates

In case 3 and 4, the undetectable failure rate of each subsystem and the arrival rate of intrusion/incident are changed respectively. The undetectable failure rate increases from 0.002 to 0.004 that is more close to the detectable failure rate. Thus the system is expected to have more hidden failure units during operation. The optimal maintenance policy suggests to set $m = 2$ instead of 3 to leave a larger safe margin to failure. The predetermined age to renew the system also has been shortened from 67 hours to 54 hours. The subsystem has higher rate to experience the undetectable failure thus the optimal per unit time cost increases. If the arrival rate of the second process enlarges 5 times, the system is more vulnerable to the hard-failure. Thus the optimal maintenance policy also suggests smaller m and shorter T compared to case 1 in order to reduce the risk of the system. As no surprise, the expected cost per unit time increases in μ.

6.4.3 The Impact of the Cost Coefficient

Each cost coefficient is varied from case 5 to 7. As mentioned before, the set-up cost represents the economic dependency between maintenance of subsystems. The higher this cost is, the more units each maintenance action is trying to group. Thus T^* increases from 67 to 91, leaving the system under more risk trying to pack more units to maintain at once. The expected cost increases as a result in case 5. In case 6, the cost to service a working unit increases from 10 to 30. Thus it is less beneficial to renew the system early with fewer failures. The cost of each maintenance action should also increase due to this change. Hence T^* and $EC_L(m^*, T^*)$ increases. In case 7, the penalty for the hard-failure

reduces from 5000 to 2000. Thus T^* increases for less often renewal, and $EC_L(m^*, T^*)$ drops as there is less penalty.

6.5 Conclusion

In this chapter, a cost model on the opportunistic maintenance policy of a k-out-of-n surveillance system with consideration of the two stochastic processes is developed. The model includes maintenance cost dependent on the expected number of failed subsystems and penalty terms due to both soft-failure and hard-failure of the system. A numerical search algorithm to obtain the optimal maintenance policy is provided. Several numerical examples are given to demonstrate the validity of the modeling and the sensitivity of different parameters. For the future works, we will focus on the reliability modeling of the surveillance system with the two processes considering the false alarm failure mode on both the sensor and system level.

Chapter 7

Reliability Analysis of k-out-of-n Surveillance Systems Subject to Dual Stochastic Process and (m, d, T) Opportunistic Maintenance Policy

7.1 Introduction

Surveillance systems have been widely used in areas that need monitoring such as airports, railroads, banks, shopping malls, hospitals, schools, etc. The failure of these systems should be analyzed associated with the intrusion/incident arrival process (called intrusion process) in order to achieve a comprehensive representation of the system outcomes. In this chapter, we develop a generalized dual-stochastic-process reliability model of k-out-of-n surveillance systems with complete four failure modes on the subsystem level, noted as fail-dangerous detectable, fail-dangerous undetectable, fail-safe detectable and fail-safe undetectable modes. The reliability of the system is derived with considerations of the intrusion process and a (m, d, T) opportunistic maintenance policy. The closed-form reliability function of a triple-modular redundancy (TMR) system is obtained. Numerical examples are given to demonstrate the validity of the modeling.

7.2 Description of the Surveillance Systems with (m, d, T) Opportunistic Maintenance Policy

The defined surveillance system is used to monitor the safety of a critical area. The conditions of the protected area are defined as normal and abnormal. Depending on the conditions of the area, each sensor may operate in the following status:

1) Report normal when the area is normal.
2) Report abnormal when the area is abnormal.

3) Report normal when the area is abnormal.

4) Report abnormal when the area is normal.

Note that the first two states are considered as working states for an individual sensor. State 3) above is defined as the fail-dangerous type of sensor failure since the sensor is no longer capable to detect any abnormal condition of the protected area. State 4) is defined as the fail-safe type of sensor failure, since the sensor reports dangerous actions even when the area is under normal condition. The failure will most likely to cause a false alarm for the surveillance area, but no dangerous actions will be ignored by this type of failure.

The states of the sensors are tested by some imperfect monitoring techniques such as an indicating LED light in the central control room for each of the sensor. Thus when either the fail-safe or fail-dangerous type of failure occurs to one of the sensors, it has some probability to "announce" itself in order to notify the central officer that the system is operating under a degraded condition. If a sensor failure is announced, it is defined as detectable, otherwise undetectable. Thus consider all the combinations, there are in total 4 types of failure at the sensor level: fail-dangerous detectable, fail-dangerous undetectable, fail-safe detectable and fail-safe undetectable. Such failure modes assumption can be found in [77, 139] and is very typical on the reliability modeling of the safety instrumental system, a sensor system that is used to monitor the status of other safety critical processes. It is also suitable to define surveillance systems as the surveillance sensor can also fail to detect an incident (corresponding to fail-dangerous) or report a suspicious action while there is nothing abnormal going on (corresponding to fail-safe) in the protected area.

The general surveillance system model considered in this work is a k-out-of-n system. Assume that each sensor in the system is capable to observe the entire surveillance area. The system uses n identical sensors to enhance the performance. On the system level, it requires at least k sensors reporting incident detection in the area to trigger the alarm. At any time, if less than k sensors report incident detection, those reports are considered as false detections and will be discarded. Hence, if k or more sensors fall into the fail-safe mode, the surveillance system is considered as fail-safe, as the system has enough votes to trigger the alarm when there is no incident in the surveillance area. On the contrary, if $(n-k+1)$ or more sensors fall into the fail-dangerous mode, the surveillance system will no longer be capable to detect the incident in the area. Even if all the remaining sensors are working properly and detect the real incident, they will be discarded by the system since the valid report number is guaranteed to be less than k (too many sensors in the fail-dangerous mode). To summarize the fail-safe and fail-dangerous mode on the system level, we have

1) System fail-safe mode: at least k sensors in fail-safe mode (either detectable or undetectable). This system mode is noticeable immediately since a false-alarm will be triggered.
2) System fail-dangerous mode: at least $(n-k+1)$ sensors in fail-dangerous mode (either detectable or undetectable). When the system enters the fail-dangerous mode, it loses the ability to detect any incident occurred in the field. It may not be detectable since some of the sensor failures are undetectable and there is no alarm triggered when entering the mode.

Because the partial states information is available to the central officer, the system may be scheduled for maintenance before a false-alarm is triggered or the surveillance area is hit by an incident/attack. When the fail-safe detectable and fail-dangerous detectable failures are cumulated to certain numbers prior to the actual system failure numbers, the maintenance action should be carried out to prevent the high risk of failure for a degraded system. To be specific, when $m \in [1, n-k]$ fail-dangerous detectable failures are cumulated, or when $d \in [1, k-1]$ fail-safe detectable failures are cumulated, or when the system has survived time T from the last maintenance action, a maintenance action should be performed to the surveillance system. The described maintenance schedule is noted as (m, d, T) maintenance policy.

In this chapter, we assume that the maintenance action is considered to be perfect. In other word, each maintenance action will restore the whole surveillance system to "as good as new". The surveillance system under the (m, d, T) maintenance policy may experience the following possible outcomes to be stopped for a new maintenance action, as shown in Figure 7.1:

a) Stopped directly by rule T: the system survives for time T from last maintenance action, without entering the fail-dangerous mode.
b) Stopped directly by rule m: the system accumulates m fail-dangerous detectable failures, without entering the fail-dangerous mode.
c) Stopped directly by rule d: the system accumulates d fail-safe detectable failures, without entering the fail-dangerous mode.
d) Stopped by fail-safe alarm: the system has encountered a false alarm.

e) Entered the fail-dangerous mode: the system enters the fail-dangerous mode and continue to operate, it will reach:

e1) Stopped by rule T: the system survives for time T after fail-dangerous mode

e2) Stopped by rule m: the system accumulates m fail-dangerous detectable failures after fail-dangerous mode

e3) Stopped by rule d: the system accumulates d fail-safe detectable failures after fail-dangerous mode

e4) Stopped by H: the system encounters an incident/attack after fail-dangerous mode. This is treated as the hard-failure of the system that will cause the most damage.

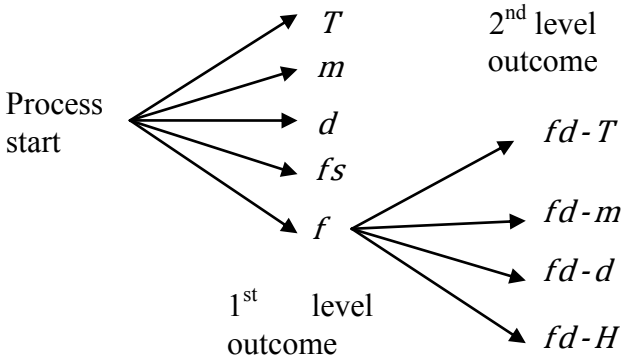

Figure 7.1 Diagram of the two levels of maintenance action

7.3 Surveillance System Reliability Modeling

7.3.1 A Generalized k-out-of-n System

Consider the k-out-of-n systems discussed in section 7.2 with sensors of having 4 possible failure modes. The probability to observe failure mode f by time t can be represented by

$$P_{uf}(t) = p_f\left(1 - e^{-\lambda t}\right) \tag{7.1}$$

where the index $f = 1d,\ 1u,\ 0d,\ 0u$ corresponding to fail-dangerous detectable, fail-dangerous undetectable, fail-safe detectable and fail-safe undetectable modes respectively, and p_f is the probability that the failure is a mode f failure when a failure is occurred.

The reliability function for each sensor by time t is

$$R_u(t) = e^{-\lambda t} \tag{7.2}$$

Note that the exponential life time function can be substitute with any type of reliability functions. Here the exponential function is used for simplicity of equation developments, without the loss of generality. Firstly the detectability of the sensor failures is collapsed. Only two dimensions of fail-safe number and fail-dangerous number are taken into consideration. Thus on the system level, the status of the surveillance system by time t can be defined as $(I(t),\ J(t))$ where row $I(t)$ represents the number of sensors with fail-safe failures, and column $J(t)$ represents the number of subsystems with fail-dangerous failures by time t. When combining the detectable and undetectable types of failures, the probability to observe a fail-dangerous or a fail-safe type of failure can be defined as

$$p_1 = p_{1d} + p_{1u} \tag{7.3}$$

$$p_0 = p_{0d} + p_{0u} \tag{7.4}$$

The possible state distribution for the *k*-out-of-*n* surveillance system is represented in Figure 7.2.

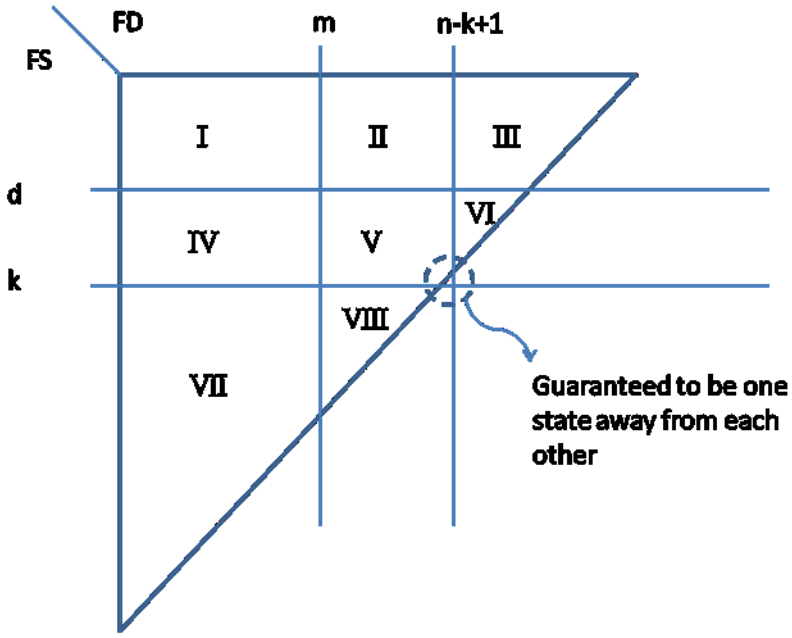

Figure 7.2 Virtual distribution of system states and region of outcomes

The assumption of the system indicates that all subsystems can be restored to 100% healthy ("as good as new") after each maintenance action. Thus the system is always renewed at state $(0,\ 0)$ for each cycle at $t_0 = 0$. The probability to observe state $(I(t), J(t)) = (i, j)$ by time t in Figure 7.2 follows the trinomial distribution and is given by

$$P_{ij}(t) = \binom{n}{i,j}\left(p_1\left(1-e^{-\lambda t}\right)\right)^i\left(p_0\left(1-e^{-\lambda t}\right)\right)^j\left(e^{-\lambda t}\right)^{n-i-j} \qquad (7.5)$$

where $\binom{n}{i,j} = \frac{n!}{i!j!(n-i-j)!}$, $i,\ j = 0,\ 1,\ 2\ldots$ and $i+j \le n$. Each state $(i,\ j)$ has rate $(n-i-j)p_1\lambda$ to move to state $(i,\ j+1)$ and rate $(n-i-j)\ p_0\lambda$ to enter state $(i+1,\ j)$. The transitions of states are only in one-way direction, which means that back step is not allowed in the model. Notice that many states in Figure 7.2 are considered as virtual states meaning that they do not actually exist in reality. For example, all the states in Region VII except the ones on the horizontal line k do not exist in reality, since that the

system is stopped for maintenance when k fail-safe failures are cumulated. In other words, the probabilities to observe the states in Region VII are absorbed by the ones on the horizontal line k.

In Figure 7.2, there are 4 lines of states that separate the total area into 8 different regions as follows:

- $i = d$ and $i = k$ as horizontal lines
- $j = m$ and $j = n-k+1$ as vertical lines

Region I represents the states that the surveillance system is functioning properly. The probability to observe a state in Region I can be found with

$$P_I(t) = \sum_{i=0}^{d-1} \sum_{j=0}^{m-1} P_{ij}(t) \tag{7.6}$$

States in Region II can be either the working states or the ones that stopped by rule m, depending on the number of detectable fail-dangerous failures it has in the system. Similar situations are for Region IV, V and VII where two to three outcomes are possible depending on the numbers of detectable failures of certain type.

$$P_{II\,T}(t) = \sum_{i=0}^{d-1} \sum_{j=m}^{n-k} P_{ij}(t) \sum_{j_d=0}^{m-1} p_{mj} \tag{7.7}$$

$$P_{II\,m}(t) = \sum_{i=0}^{d-1} \sum_{j=m}^{n-k} P_{ij}(t) \sum_{j_d=m}^{j} p_{mj} \tag{7.8}$$

where

$$p_{mj} = \binom{j}{j_d} \left(\frac{p_{1d}}{p_1}\right)^{j_d} \left(\frac{p_{1u}}{p_1}\right)^{j-j_d} \tag{7.9}$$

Similarly, the results of Region IV can be obtained:

$$P_{IV\,T}(t) = \sum_{i=d}^{k-1} \sum_{j=0}^{m-1} P_{ij}(t) \sum_{i_d=0}^{d-1} p_{di} \tag{7.10}$$

$$P_{IV\,d}(t) = \sum_{i=d}^{k-1} \sum_{j=0}^{m-1} P_{ij}(t) \sum_{i_d=d}^{i} p_{di} \tag{7.11}$$

where

$$p_{di} = \binom{i}{i_d} \left(\frac{p_{0d}}{p_0}\right)^{i} \left(\frac{p_{0u}}{p_0}\right)^{i-i_d} \tag{7.12}$$

For Region V and VII,

$$P_{V\,T}(t) = \sum_{i=d}^{k-1} \sum_{j=m}^{n-k} P_{ij}(t) \sum_{i_d=0}^{d-1} p_{di} \sum_{j_d=0}^{m-1} p_{mj} \tag{7.13}$$

$$P_{V\,m}(t) = \sum_{i=d}^{k-1} \sum_{j=m}^{n-k} P_{ij}(t) \sum_{i_d=0}^{d-1} p_{di} \sum_{j_d=m}^{j} p_{mj} \tag{7.14}$$

$$P_{V\,d}(t) = \sum_{i=d}^{k-1} \sum_{j=m}^{n-k} P_{ij}(t) \sum_{i_d=d}^{i} p_{di} \sum_{j_d=0}^{m-1} p_{mj} \tag{7.15}$$

$$P_{VII\,fs}(t) = \sum_{j=0}^{m-1} \sum_{i=k}^{n-j} P_{ij}(t) \sum_{i_d=0}^{d-1} p_{di} \tag{7.16}$$

$$P_{VII\,d}(t) = \sum_{j=0}^{m-1} \sum_{i=k}^{n-j} P_{ij}(t) \sum_{i_d=i-k+d+1}^{i} p_{di} \tag{7.17}$$

These outcomes can be developed by conditioning on the number of detectable type of failures. For the outcomes of Region VIII though, only conditioning on the detectable failure is not enough. The paths to reach the states in Region VIII also matter. The same as the outcomes in Region III and VI where the second layer outcomes become possible.

The separation of outcomes for the three regions can only be represented in the general form

$$P_{VIII}(t) = P_{VIII\ m}(t) + P_{VIII\ d}(t) + P_{VIII\ fs}(t) \tag{7.18}$$

$$P_{III+VI}(t) = P_{III+VI\ m}(t) + P_{III+VI\ d}(t) + P_{III+VI\ fd}(t) \tag{7.19}$$

The first layer outcomes for the general k-out-of-n surveillance system are

$$P_T(t) = P_{I\ T}(t) + P_{II\ T}(t) + P_{V\ T}(t) \tag{7.20}$$

$$P_d(t) = P_{IV\ d}(t) + P_{V\ d}(t) + P_{VII\ d}(t) + P_{VIII\ d}(t) + P_{III+VI\ d}(t) \tag{7.21}$$

$$P_m(t) = P_{II\ m}(t) + P_{V\ m}(t) + P_{VIII\ m}(t) + P_{III+VI\ m}(t) \tag{7.22}$$

$$P_{fs}(t) = P_{VII\ fs}(t) + P_{VIII\ fs}(t) \tag{7.23}$$

$$P_{fd}(t) = P_{III+VI\ fd}(t) \tag{7.24}$$

7.3.2 A Representation for a special case: TMR (2-out-of-3) Model

The states in Region VIII become tricky with possible outcomes as stopped by m, d or fail-safe. A single state in Region VIII may belong to different outcomes for different paths to reach that state. Things become even more complicated for Region III and VI when the second layer outcomes become possible. It is problematic to get the analytic solution for the general k-out-of-n system with arbitrary (m, d, T) maintenance parameters.

The triple-modular redundancy (TMR), as one of the simplest forms of the k-out-of-n configuration, can dramatically simplify the complexity of the problem and make the analytical solution of the probability outcomes for the surveillance system possible as we now discuss in this subsection. The only possible maintenance parameters in this case are $m = d = 1$.

For Region VIII, only one possible state exists with 1 fail-dangerous and 2 fail-safe failures. Further considering all the combinations of the detectable and undetectable types can be obtained as shown in Table 7.1. In column 1, Table 7.1, a 4-digit format is used to represent the state with the numbers of the fail-dangerous detectable, fail-dangerous undetectable, fail-safe detectable and fail-safe undetectable in order. The following three columns define the probabilities of the outcomes (either stopped by m, by d or by fail-safe) when observing a state in region VIII. For the possible outcomes information, please refer to Figure 7.1.

Table 7.1 Probability of outcomes for states in Region VIII

State: (*jd, ju, id, iu*)	Stopped by m	Stopped by d	Stopped by *fs*
(0102)	0	0	1
(1002)	2/3	0	1/3
(0111)	0	1	0
(1011)	3/6	3/6	0
(0120)	0	1	0
(1020)	1/3	2/3	0

The probabilities in the table are obtained by counting the fraction of the possible routes from state (0000) to the desired state following each criterion.

Thus for Region VIII, we have:

$$P_{VIII\,m}(t) = \frac{2}{3}P_{1002}(t) + \frac{1}{2}P_{1011}(t) + \frac{1}{3}P_{1020}(t) \qquad (7.25)$$

$$P_{VIII\ d}(t) = P_{0111}(t) + \frac{1}{2}P_{1011}(t) + P_{0120}(t) + \frac{2}{3}P_{1020}(t) \quad (7.26)$$

$$P_{VIII\ fs}(t) = P_{0102}(t) + \frac{1}{3}P_{1002}(t) \quad (7.27)$$

For Region III and VI, the following steps are required in order to calculate the probabilities of the two-level outcomes:

A. Discuss the probability of outcome for each state that belongs to Region III and VI. There are 6 categories possible. Taking the entering point (0200) as an example.

   a. States that have entered the fail-dangerous mode only

(0200)	(0300)

   b. States that either stopped by d directly or have $fd\text{-}d$

State	d directly	$fd\text{-}d$
(0210)	2/3	1/3

   c. States with m or $fd\text{-}m$

State	m directly	$fd\text{-}m$
(1200)	2/3	1/3

   d. States that only stopped by m directly

(2000)	(3000)
(1100)	(2100)

e. States that either stopped by m directly or d directly

States	m directly	d directly
(2010)	2/3	1/3
(1110)	3/6	3/6

f. States that may be corresponding to the outcome m, d, $fd\text{-}m$ or $fd\text{-}d$. Only applicable to higher order of problems, e.g., a 3-out-of-5 system will need to consider states in category f).

B. Calculate fail-dangerous probability by conditioning on the entering points (0200) and (0201)

C. Evaluate the conditioned probabilities of the second layer outcomes without the second process: $P_{m|fd}(x|\tau, s_j)$, $P_{d|fd}(x|\ \tau, s_j)$ and $P_{T|fd}(x|\ \tau, s_j)$, $P_{H|fd}(x|\ \tau)$

D. Calculate the probabilities of the second layer outcomes

In summary, the system probability outcomes for the TMR (2-out-of-3) surveillance system considering all 4 types of failures and the incident/attack process can be calculated from equation (7.20) – (7.24) with the detailed terms defined as

$$P_{III+VI\ m}(t) = \frac{2}{3}P_{1200}(t) + P_{2000}(t) + P_{3000}(t) + P_{1100}(t) + P_{2100}(t) + P_{2001}(t) + P_{1101}(t) + \frac{2}{3}P_{2010}(t) + \frac{1}{2}P_{1110}(t) \tag{7.28}$$

$$P_{III+VI\ d}(t) = \frac{2}{3}P_{0210}(t) + \frac{1}{3}P_{2010}(t) + \frac{1}{2}P_{1110}(t) \tag{7.29}$$

$$P_{III+VI\ fd}(t) = \sum_{j=n-k+1}^{n}\sum_{i=0}^{n-j} P_{ij}(t) - P_{III+VI\ m}(t) - P_{III+VI\ d}(t) \tag{7.30}$$

The second layer outcomes are estimated as

$$P_{fd-m}(t) = \sum_{s_j} \int_0^t \int_\tau^t \bar{P}_{H|fd}(x|\tau) dP_{m|fd}(x|\tau, s_j) dP_{fd}(\tau, s_j) \tag{7.31}$$

$$P_{fd-d}(t) = \sum_{s_j} \int_0^t \int_\tau^t \bar{P}_{H|fd}(x|\tau) dP_{d|fd}(x|\tau, s_j) dP_{fd}(\tau, s_j) \tag{7.32}$$

$$P_{fd-H}(t) = \sum_{s_j} \int_0^t \int_\tau^t P_{T|fd}(x|\tau, s_j) dP_{H|fd}(x|\tau) dP_{fd}(\tau, s_j) \tag{7.33}$$

$$P_{fd-T}(t) = \sum_{s_j} \int_0^t P_{T|fd}(x|\tau, s_j) \bar{P}_{H|fd}(x|\tau) dP_{fd}(\tau, s_j) \tag{7.34}$$

where

$$P_{H|fd}(x|\tau) = 1 - e^{-\mu(x-\tau)} \tag{7.35}$$

$$\bar{P}_{H|fd}(x|\tau) = e^{-\mu(x-\tau)} \tag{7.36}$$

The entering state to the second layer outcomes (after fail-dangerous occurred to the system) s_j = 0200 and 0201. At state 0200, there is one working sensor left. It can reach the fail-dangerous detectable state, which will lead to the outcome $fd\text{-}m$.

$$P_{m|fd}(x|\tau, s_{0200}) = p_{0d}\left(1 - e^{-\lambda(x-\tau)}\right) \tag{7.37}$$

It can reach the fail-safe detectable state, which will lead to the outcome $fd\text{-}d$.

$$P_{d|fd}(x|\tau, s_{0200}) = p_{1d}\left(1 - e^{-\lambda(x-\tau)}\right) \tag{7.38}$$

The sensor can also remain as working, enter fail-dangerous undetectable or fail-safe undetectable, which will lead to the outcome $fd\text{-}T$.

$$P_{T|fd}(x|\tau, s_{0200}) = e^{-\lambda(x-\tau)} + p_{0u}\left(1 - e^{-\lambda(x-\tau)}\right) + p_{1u}\left(1 - e^{-\lambda(x-\tau)}\right) \tag{7.39}$$

At state 0201, all sensors are failed in undetectable modes. The state will remain until time T, if not interrupted by hard-failure H.

$$P_{m|fd}(x|\tau, s_{0201}) = 0 \tag{7.40}$$

$$P_{d|fd}(x|\tau, s_{0201}) = 0 \tag{7.41}$$

$$P_{T|fd}(x|\tau, s_{0201}) = 1 \tag{7.42}$$

7.4 Numerical Examples

In this section, we discuss a numerical result based on the TMR system to illustrate our proposed reliability analysis with the following parameters:

The total failure rate $\lambda = 0.005$.

The arrival rate of the intrusion process ("second process") $\mu = 0.01$.

The probability of having each failure type is listed in Table 7.2.

Table 7.2 Probability of each failure type

Failure type	Probability
Fail-dangerous detectable (jd)	0.6
Fail-dangerous undetectable (ju)	0.2
Fail-safe detectable (id)	0.1
Fail-safe undetectable (iu)	0.1

The first layer probability outcomes are plotted in Figure 7.3, where the outputs are calculated from equation (7.28) to (7.32). As we can see that the case of stopped by reaching life time T to carry out maintenance is a transient state, while all the other stopping criteria for maintenance actions are absorbing states. In the TMR model, the outcomes of stopped by m and stopped by d require only one step from the original

perfect state. The outcomes of having the fail-safe alarm and reaching the fail-dangerous mode require two steps. Thus the probabilities to observe the first two outcomes are significantly higher than the latter two. Within the same steps, it is easier to have fail-dangerous type of sensor failure than the fail-safe type by parameter setup in Table 7.2. It is consistent with the plot showing that $P_m(t) > P_d(t)$ and $P_{fd}(t) > P_{fs}(t)$.

After reaching the fail-dangerous mode, the system keeps operating until one of the stopping criteria is reached. Thus the purple line of the total probability of the fail-dangerous outcome in Figure 7.3 can be further divided into the second-layer outcomes, as shown in Figure 7.4. The outcomes are calculated from equation (7.36) to (7.39). $P_{fd}(t)$ is the total probability in this case. It is divided into $P_{fd\text{-}m}(t)$, $P_{fd\text{-}d}(t)$, $P_{fd\text{-}T}(t)$ and $P_{fd\text{-}H}(t)$. Again only the outcome of survival to time T is transient. Hence in the long run, the probability drops and approaches zero. However, in the beginning of the process, the total probability to observe a fail-dangerous mode is low and rising rapidly afterwards until stable. That is why $P_{fd\text{-}T}(t)$ has the rising trend at first then drops down with t increasing. After entering the fail-dangerous mode, the arrival rate of the second process (incident/attack process) is high. Thus a significant portion after the fail-dangerous mode belongs to the hard-failure of the system.

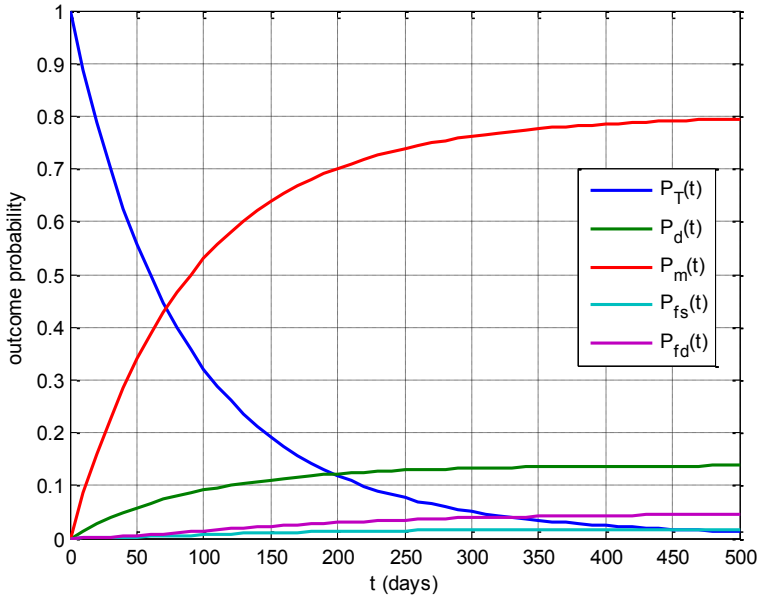

Figure 7.3 Probability plot of first level outcomes for the numerical 2-out-of-3 system

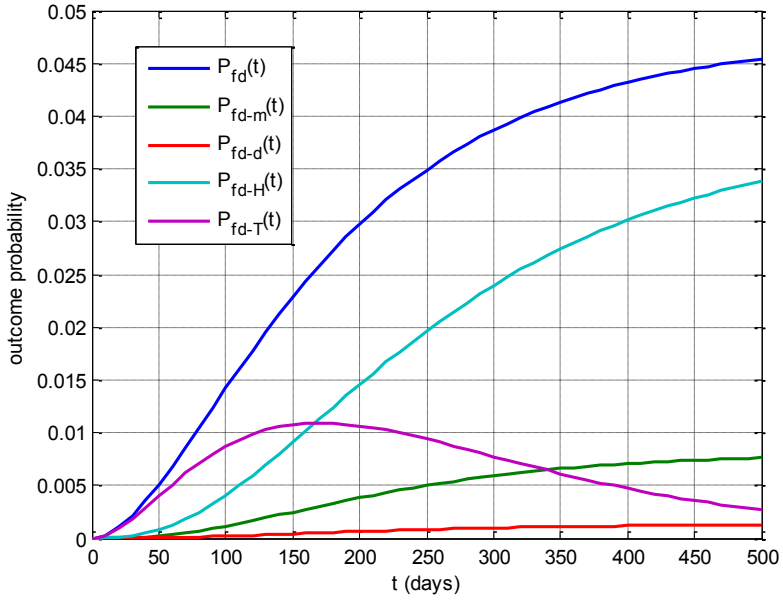

Figure 7.4 Probability plot of second level outcomes for the numerical 2-out-of-3 system

7.5 Comparison between models

The reliability models developed in Chapter 4, 5 and 7 all consider the effect of the two stochastic-processes on the system probability outcomes. The first model developed in Chapter 4 only considers the fail-dangerous undetectable type of failures. The second model considers fail-dangerous detectable and undetectable failures. The full model developed in this chapter includes all 4 types of failures. By carefully setting up the parameters, the first two models can be covered by the model presented in this chapter. We demonstrate that the first two models are special cases for the third model with a 3-out-of-5 system as an example.

The model one considers the effect of the random environment, the imperfect detection rate and the time dependent second process arrival rate, other than the two process effect that we are focusing on comparing the models here. Thus firstly we have to ignore all these factors and rewrite the system outcomes as

$$R_C(t) = \sum_{j=3}^{5} \binom{5}{j} \left(e^{-\lambda t}\right)^j \left(1 - e^{-\lambda t}\right)^{5-j} \tag{7.43}$$

$$F_C(t) = 1 - R_C(t) = 1 - \sum_{j=3}^{5} \binom{5}{j} \left(e^{-\lambda t}\right)^j \left(1 - e^{-\lambda t}\right)^{5-j} \tag{7.44}$$

$$R_{sf}(t) = \int_0^t e^{-\mu(t-\tau)} dF_C(\tau) \tag{7.45}$$

$$F_{hf}(t) = \int_0^t R_C(\tau) \mu e^{-\mu\tau} d\tau \tag{7.46}$$

Select $\lambda = 0.005$ and $\mu = 0.002$ for model 1. To achieve the equivalent model for model 2 and 3, the parameters are selected as follows. For model 2, $\lambda_1 = 0$, $\lambda_2 = 0.005$, $\mu =$

0.002. For model 3, $\lambda = 0.005$, $\mu = 0.002$, $p_{1u} = 1$, $p_{1d} = p_{0d} = p_{0u} = 0$. The plots are shown in Figure 7.5.

If only comparing model 2 and 3, both fail-dangerous detectable and fail-dangerous undetectable types of failures can be present. For model 2, let $\lambda_1 = 0.003$, $\lambda_2 = 0.002$, $\mu = 0.002$ and $m = 2$. To have an equivalent model from model 3, the following relationships have to be satisfied besides selecting $\mu = 0.002$ and $m = 2$:

$$\lambda = \lambda_1 + \lambda_2 = 0.005$$

$$p_{1d} = \frac{\lambda_1}{\lambda} = 0.6$$

$$p_{1u} = \frac{\lambda_2}{\lambda} = 0.4$$

$$p_{0d} = p_{0u} = 0$$

The plots have been shown in Figure 7.6 and Figure 7.7. From the results we can clearly see that setting the non-existing failure mode probabilities to zero, model 3 can be used to represent model 1 and model 2. The comparison is another angle to validate the models developed with different assumptions. On the one hand, the complex model covers a wider range of problems. On the other hand, the simple model is easier to be combined with other considerations of the modeling (model 1) and saves computation resources. It certainly depends on the characteristics of the problem to determine which model is the most suitable one.

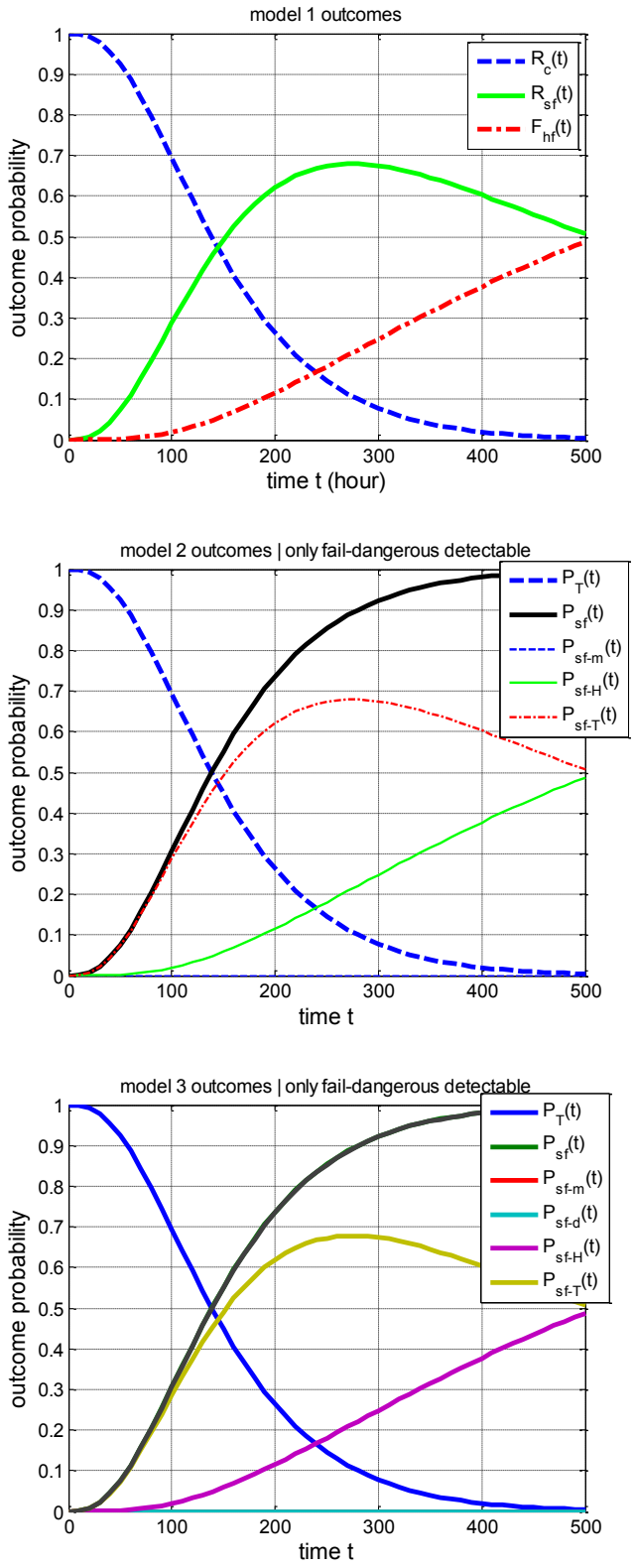

Figure 7.5 Probability plot of 3 models with only fail-dangerous undetectable

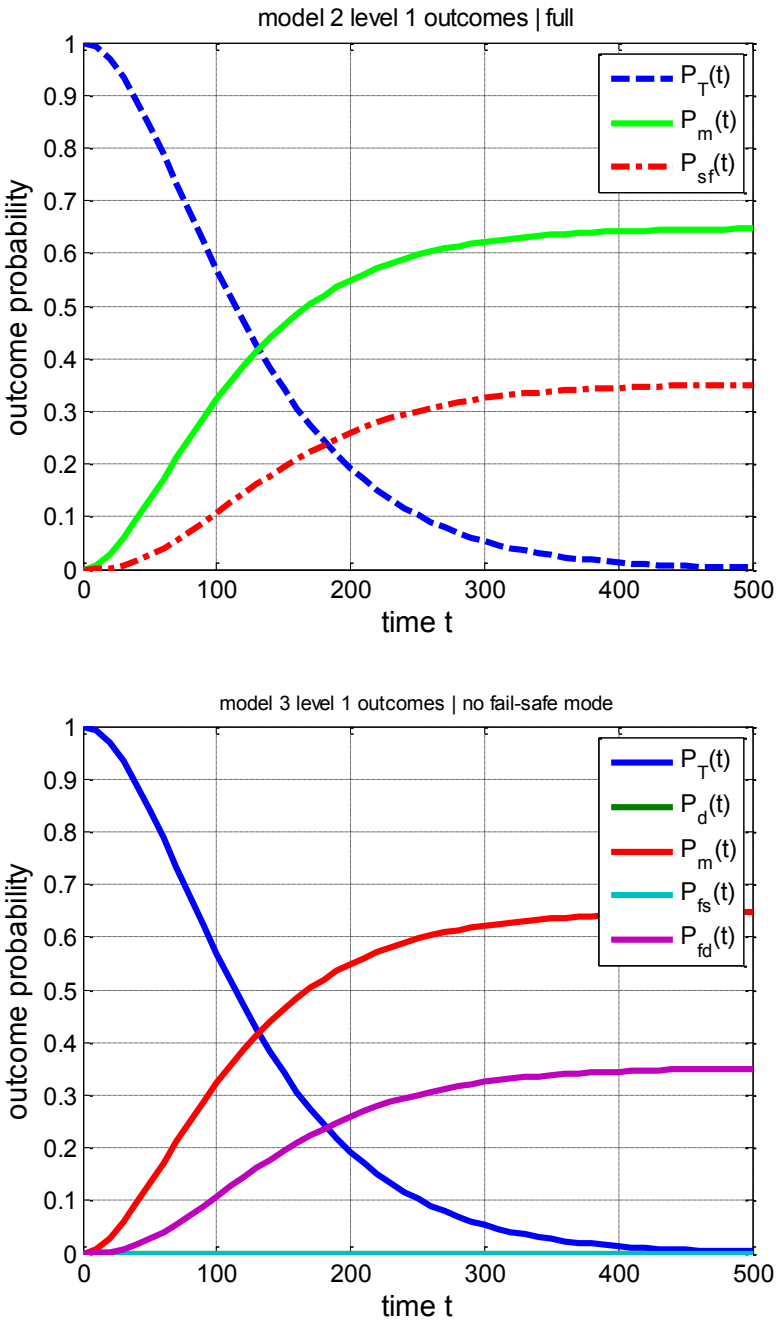

Figure 7.6 Probability plot of level 1 for model 2 and 3

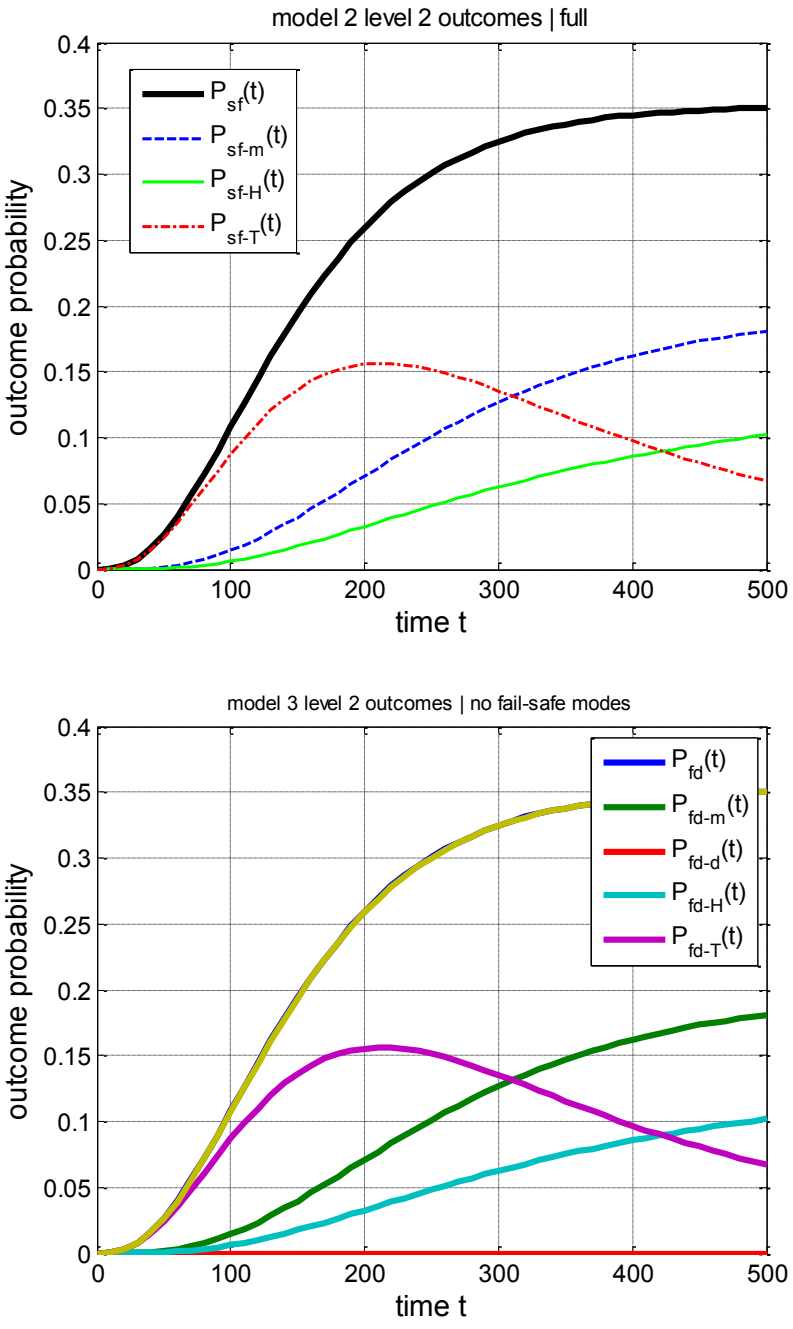

Figure 7.7 Probability plot of level 2 for model 2 and 3

7.6 Conclusion

In this chapter, a k-out-of-n surveillance system subject to complete four failure modes on the subsystem level, such as fail-dangerous detectable, fail-dangerous undetectable, fail-safe detectable and fail-safe undetectable mode, is discussed. The probability outcomes of the surveillance system are derived with the consideration of the intrusion process (as "second process") and a (m, d, T) opportunistic maintenance policy. Numerical example on the TMR system is given as a special case to demonstrate the validity of the modeling. Comparison between models developed in Chapter 4, 5 and 7 are made to demonstrate that the former two models are the special cases of the model presented in this chapter.

Chapter 8

Conclusion and Future Research

8.1 Conclusion

In the previous chapters, three dual-process reliability models for the surveillance systems have been developed. The two dependent processes are the system failure process and the intrusion arrival process where the system failure in the first process is the trigger of the start for the second process taking into account. All systems are considered the k-out-of-n system structure. For maintenance policies, periodic maintenance and group maintenance policies are selected in the modeling respectively.

In Chapter 4, a surveillance system reliability model is presented with consideration of a dual stochastic-dependent process: incident arrival process and system failure process. The framework of the surveillance systems can be applied to other applications as modification can be easily conducted following the mathematical modeling. One can adopt different system configurations by considering different environmental effects based on the collected data and evaluate intruder's effort to avoid being detected using different mechanisms. The quantitative evaluation of the reliability and soft-failure and hard-failure probabilities with the variation of the inspection interval length is derived and illustrated with numerical examples and several sensitivity analyses. Possible actions to enhance the reliability of the surveillance system are also discussed.

In Chapter 5, a k-out-of-n surveillance system model with the two processes is presented with subsystems having two competing failure modes: detectable and undetectable. With the partial information of the subsystem status, a pre-selected number for the accumulation of the detectable failures in the surveillance system is determined. When

the number is reached or the pre-determined age is reached, the surveillance process is terminated for maintenance to protect the system from large loss of the higher risk. The reliability of the system is derived with the consideration of the above opportunistic maintenance policy. Several numerical examples are given to demonstrate the validity of the modeling and the sensitivity of various model parameters.

In Chapter 6, a cost model based on the surveillance model from Chapter 5 is derived in order to minimize the total system cost per unit time of the optimal $(m,\ T)$ opportunistic maintenance policy. The developed model considers the expected number of failed subsystems for each possible system outcome. It also considers the penalty for the duration of time that the surveillance area loses protection of the surveillance system and the cost due to the hard-failure. A numerical search algorithm is presented to obtain the optimal maintenance parameters (m, T).

In Chapter 7, the full model that considers all possible 4 failure modes for each sensor of the surveillance system is developed. The 4 failure modes are fail-dangerous detectable, fail-dangerous undetectable, fail-safe detectable and fail-safe undetectable. On the system level, the surveillance system is possible to send out false alarm while the surveillance are is safe in reality. Thus the accumulation of detectable fail-safe type of failures can also result in pre-termination of the system for maintenance to prevent false alarms. The probability outcomes of the system is developed and demonstrated with a TMR numerical example. The relationships between the models developed in Chapter 4, 5 and 7 are also discussed. A 3-out-of-5 numerical example is used to demonstrate that the models in Chapter 4 and 5 are special cases of the model in Chapter 7.

8.2 Future Research

Based on the developed surveillance models with the two stochastic-processes and the maintenance policies, several directions can be further investigated to extend this research. Firstly, the second process can be used to describe much more complicated behaviors of the incident arrivals, such as the arrivals of a cluster of attacks, or the rational attack that is capable to adjust behavior based on the health status of the surveillance systems. Secondly, the maintenance is only considered for one interval in this research, since the repair and restore actions are all perfect by assumption. To involve imperfect maintenance for multiple cycles, such as partially restoring the subsystem life or decision making of whether to carry out a maintenance action or not at a break point, will certainly describe a more realistic system behavior, but also need to face the challenge of increment of complexity of the modeling.

References

[1] D. Schorn. (2009, We're Watching. Available: http://www.cbsnews.com/2100-500923_162-1968121.html?pageNum=1&tag=page

[2] V. Singh, P. Atrey, and M. Kankanhalli, "Coopetitive Multi-Camera Surveillance Using Model Predictive Control," *Machine Vision and Applications,* vol. 19, pp. 375-393, Oct 2008.

[3] E. Zio, "Reliability Engineering: Old Problems and New Challenges," *Reliability Engineering & System Safety,* vol. 94, pp. 125–141, 2009.

[4] A. Katersky. (2010, Newark Airport's Security Cameras Were Broken. Available: http://abcnews.go.com/Travel/newark-airports-security-cameras-broken-slowed-tsa-security/story?id=9484216#.UG8li5jYHoF

[5] N. Ibarra. (2012, Security System Fails to Detect Man on Runway at NY's Kennedy Airport. Available: http://articles.cnn.com/2012-08-13/travel/travel_airport-intrusion_1_security-system-perimeter-intrusion-detection-system-raytheon

[6] K. Huang, D. Tao, Y. Yuan, X. Li, and T. Tan, "Biologically Inspired Features for Scene Classification in Video Surveillance," *IEEE Transactions on Systems, Man, and Cybernetics, Part B: Cybernetics,* vol. 41, pp. 307–313, 2011.

[7] H. Wang, "A Survey of Maintenance Policies of Deteriorating Systems," *European Journal of Operational Research,* vol. 139, pp. 469–489, 2002.

[8] Y. Bai, Z. Li, and Z. Xie, "Use of Multi-Frequency Ultrasonic Censors with PIR Sensors to Enhance the Sensing Probability of an Embedded Surveillance System," *2010 International Symposium on Communications and Information Technologies (ISCIT),* pp. 170–175, Oct 2010.

[9] J. Zhao, S. Cheung, and T. Nguyen, "Optimal Visual Sensor Network Configuration," *Multi-Camera Networks: Principles and Applications,* pp. 139–162, 2009.

[10] J. Zhao, "Camera Planning and Fusion in a Heterogeneous Camera Network," Ph. D. Doctoral Dissertation, 2011.

[11] S. Dhillon and K. Chakrabarty, "Sensor Placement for Effective Coverage and Surveillance in Distributed Sensor Networks," *IEEE Wireless Communications and Networking,* vol. 3, pp. 1609–1614, March 2003.

[12] X. Wang, G. Xing, Y. Zhang, C. Lu, R. Pless, and C. Gill, "Integrated Coverage and Connectivity Configuration in Wireless Sensor Networks," *Proceedings of the 1st International Conference on Embedded Networked Sensor Systems,* pp. 28–39, 2003.

[13] Y. Zou and K. Chakrabarty, "Sensor Deployment and Target Localization Based on Virtual Forces," *22nd Annual Joint Conference of the IEEE Computer and Communications,* vol. 2, pp. 1293–1303, 2003.

[14] B. Krishnamachari and S. Iyengar, "Distributed Bayesian Algorithms for Fault-Tolerant Event Region Detection in Wireless Sensor Networks," *IEEE Transactions on Computers,* vol. 53, pp. 241–250, 2004.

[15] H. Gupta, Z. Zongheng, S. Das, and Q. Gu, "Connected Sensor Cover: Self-Organization of Sensor Networks for Efficient Query Execution," *IEEE/ACM Transactions on Networking,* vol. 14, pp. 55–67, 2006.

[16] S. R., K. Ramakrishnan, P. Atrey, V. Singh, and M. Kankanhalli, "A Design Methodology for Selection and Placement of Sensors in Multimedia Surveillance Systems," *Proceedings of the 4th ACM International Workshop on Video Surveillance and Sensor Networks,* pp. 121–130, 2006.

[17] Y. Yao, C. Chen, B. Abidi, D. Page, A. Koschan, and M. Abidi, "Can You See Me Now? Sensor Positioning for Automated and Persistent Surveillance," *IEEE Transactions on Systems, Man, and Cybernetics, Part B: Cybernetics,* vol. 40, pp. 101–115, 2010.

[18] U. Erdem and S. Sclaroff, "Automated Camera Layout to Satisfy Task-Specific and Floor Plan-Specific Coverage Requirements," *Computer Vision and Image Understanding,* vol. 103, pp. 156–169, 2006.

[19] J. Herrera, A. Mavrinac, and X. Chen, "Sensor Planning for Range Cameras via a Coverage Strength Model," *2011 IEEE/ASME International Conference on Advanced Intelligent Mechatronics (AIM),* pp. 838–843, Jul 2011.

[20] L. Liu, X. Zhang, and H. Ma, "Localization-Oriented Coverage in Wireless Camera Sensor Networks," *IEEE Transactions on Wireless Communications,* vol. 10, pp. 484–494, 2011.

[21] Y. Nam and S. Hong, "Optimal Placement of Multiple Visual Sensors Considering Space Coverage and Cost Constraints," *Multimedia Tools and Applications,* pp. 1–22, Nov 2012.

[22] R. Rashmi and B. Latha, "Video Surveillance System and Facility to Access Pc from Remote Areas Using Smart Phone," *2013 International Conference on Information Communication and Embedded Systems (ICICES),* pp. 491–495, Feb 2013.

[23] J. Liu, S. Sridharan, C. Fookes, and T. Wark, "Optimal Camera Planning Under Versatile User Constraints in Multi-Camera Image Processing Systems," *IEEE Transactions on Image Processing,* vol. 23, pp. 171–184, 2014.

[24] B. Wang, "Coverage Problems in Sensor Networks: A Survey," *ACM Computing Surveys,* vol. 43, pp. 1–53, 2011.

[25] A. Mavrinac and X. Chen, "Modeling Coverage in Camera Networks: A Survey," *International Journal of Computer Vision,* vol. 101, pp. 205–226, Jan 2013.

[26] L. Marcenaro, F. Oberti, G. Foresti, and C. Regazzoni, "Distributed Architectures and Logical-Task Decomposition in Multimedia Surveillance Systems," *Proceedings of the IEEE,* vol. 89, pp. 1419–1440, 2001.

[27] L. Marchesotti, L. Marcenaro, and C. Regazzoni, "A Video Surveillance Architecture for Alarm Generation and Video Sequences Retrieval," *Proceedings of International Conference on Image Processing,* vol. 1, pp. 892–895, 2002.

[28] M. Trivedi, T. Gandhi, and K. Huang, "Distributed Interactive Video Arrays for Event Capture and Enhanced Situational Awareness," *IEEE Intelligent Systems,* vol. 20, pp. 58–66, 2005.

[29] M. Saini, Y. Natraj, and M. Kankanhalli, "Performance Modeling of Multimedia Surveillance Systems," *11th IEEE International Symposium on Multimedia,* pp. 179–186, Dec 2009.

[30] A. Doblander, A. Maier, B. Rinner, and H. Schwabach, "Improving Fault-Tolerance in Intelligent Video Surveillance by Monitoring, Diagnosis and

Dynamic Reconfiguration," *Third International Workshop on Intelligent Solutions in Embedded Systems,* pp. 194–201, 2005.

[31] A. Malik, Z. Salcic, C. Chong, and S. Javed, "System-Level Approach to the Design of a Smart Distributed Surveillance System Using Systemj," *ACM Transactions on Embedded Computing Systems (TECS),* vol. 11, pp. 1–24, 2013.

[32] M. Riveiro, G. Falkman, and T. Ziemke, "Improving Maritime Anomaly Detection and Situation Awareness through Interactive Visualization," *11th International Conference on Information Fusion* pp. 1–8, 2008.

[33] C. Stauffer and W. Grimson, "Adaptive Background Mixture Models for Real-Time Tracking," *IEEE Computer Society Conference on Computer Vision and Pattern Recognition,* vol. 2, pp. 246–252, 1999.

[34] M. Szczodrak, P. Dalka, and A. Czyzewski, "Performance Evaluation of Video Object Tracking Algorithm in Autonomous Surveillance System," *2010 2nd International Conference on Information Technology (ICIT),* pp. 31–34, Jun 2010.

[35] V. Mariano, J. Min, J. Park, R. Kasturi, D. Mihalcik, H. Li, D. Doermann, and T. Drayer, "Performance Evaluation of Object Detection Algorithms," *Proceedings of16th International Conference on Pattern Recognition,* vol. 3, pp. 965–969, 2002.

[36] P. Atrey, A. El Saddik, and M. Kankanhalli, "Effective Multimedia Surveillance Using a Human-Centric Approach," *Multimedia Tools and Applications,* vol. 51, pp. 697–721, 2011.

[37] E. Wallace and C. Diffley, "CCTV Control Room Ergonomics," *Published by Police Scientific Development Branch of the Home Office, Publication,* 1988.

[38] F. Anwar, I. Petrounias, T. Morris, and V. Kodogiannis, "Mining Anomalous Events Against Frequent Sequences in Surveillance Videos from Commercial Environments," *Expert Systems with Applications,* vol. 39, pp. 4511–4531, 2012.

[39] A. Clapés, M. Reyes, and S. Escalera, "Multi-Modal User Identification and Object Recognition Surveillance System," *Pattern Recognition Letters,* vol. 34, pp. 799–808, 2013.

[40] K. Hausken and G. Levitin, "Review of Systems Defense and Attack Models," *International Journal of Performability Engineering,* vol. 8, pp. 355–366, 2012.

[41] S. Guikema, "Game Theory Models of Intelligent Actors in Reliability Analysis: An Overview of the State of the Art," in *Game Theoretic Risk Analysis of Security Threats*, ed: Springer, 2009, pp. 1–19.

[42] B. Golany, E. Kaplan, A. Marmur, and U. Rothblum, "Nature Plays with Dice–Terrorists Do Not: Allocating Resources to Counter Strategic Versus Probabilistic Risks," *European Journal of Operational Research,* vol. 192, pp. 198–208, 2007.

[43] E. Paté-Cornell and S. Guikema, "Probabilistic Modeling of Terrorist Threats: A Systems Analysis Approach to Setting Priorities Among Countermeasures," *Military Operations Research,* vol. 7, pp. 5–20, 2002.

[44] N. Dighe, J. Zhuang, and V. Bier, "Secrecy in Defensive Allocations as a Strategy for Achieving More Cost-Effective Attacker Detterrence," *International Journal of Performability Engineering,* 2009.

[45] K. Siqueira and T. Sandler, "Terrorist Networks, Support, and Delegation," *Public Choice,* vol. 142, pp. 237–253, 2010.

[46] S. Bandyopadhyay and T. Sandler, "The Interplay Between Preemptive and Defensive Counterterrorism Measures: A Two-stage Game," *Economica,* vol. 78, pp. 546–564, 2011.

[47] K. Hausken and G. Levitin, "Shield versus Sword Resource Distribution in K-round Duels," *Central European Journal of Operations Research,* vol. 19, pp. 589–603, 2011.

[48] M. Nikoofal and J. Zhuang, "Robust Allocation of a Defensive Budget Considering an Attacker's Private Information," *Risk Analysis,* vol. 32, pp. 930–943, 2012.

[49] M. Azaiez and V. Bier, "Optimal Resource Allocation for Security in Reliability Systems," *European Journal of Operational Research,* vol. 181, pp. 773–786, 2007.

[50] K. Hausken, V. Bier, and J. Zhuang, "Defending Against Terrorism, Natural Disaster, and All Hazards," *Game Theoretic Risk Analysis of Security Threats, Springer, New York,* pp. 65–97, 2009.

[51] K. Hausken, "Game Theoretic Analysis Of Two-Period-Dependent Degraded Multistate Reliability Systems," *International Game Theory Review,* vol. 13, pp. 247–267, 2011.

[52] G. Levitin and K. Hausken, "Resource Distribution in Multiple Attacks with Imperfect Detection of the Attack Outcome," *Risk Analysis,* vol. 32, pp. 304–318, 2012.

[53] M. Golalikhani and J. Zhuang, "Modeling Arbitrary Layers of Continuous-Level Defenses in Facing with Strategic Attackers," *Risk Analysis,* vol. 31, pp. 533–547, 2011.

[54] N. Haphuriwat and V. Bier, "Trade-offs between Target Hardening and Overarching Protection," *European Journal of Operational Research,* vol. 213, pp. 320–328, 2011.

[55] G. Levitin and K. Hausken, "False Targets Efficiency in Defense Strategy," *European Journal of Operational Research,* vol. 194, pp. 155–162, 2009.

[56] G. Levitin and K. Hausken, "Redundancy vs. Protection vs. False Targets for Systems Under Attack," *IEEE Transactions on Reliability,* vol. 58, pp. 58–68, 2009.

[57] G. Levitin and K. Hausken, "Intelligence and Impact Contests in Systems with Redundancy, False Targets, and Partial Protection," *Reliability Engineering & System Safety,* vol. 94, pp. 1927–1941, 2009.

[58] R. Peng, G. Levitin, M. Xie, and S. Ng, "Optimal Defence of Single Object with Imperfect False Targets," *Journal of the Operational Research Society,* vol. 62, pp. 134–141, 2010.

[59] F. Lin, P. Tsang, and Y. Lin, "Near Optimal Protection Strategies Against Targeted Attacks on the Core Node of a Network," *The Second International Conference on Availability, Reliability and Security,* pp. 213–222, 2007.

[60] L. Wang, S. Ren, B. Korel, K. A. Kwiat, and E. Salerno, "Improving System Reliability Against Rational Attacks Under Given Resources," *IEEE Transactions on Systems, Man, and Cybernetics: Systems,* vol. PP, pp. 446–456, 2013.

[61] V. Singh and M. Kankanhalli, "Adversary Aware Surveillance Systems," *IEEE Transactions on Information Forensics and Security,* vol. 4, pp. 552–563, 2009.

[62] V. Bier, E. Gratz, N. Haphuriwat, W. Magua, and K. Wierzbicki, "Methodology for Identifying Near-Optimal Interdiction Strategies for a Power Transmission System," *Reliability Engineering & System Safety,* vol. 92, pp. 1155–1161, 2007.

[63] V. Bier and N. Haphuriwat, "Analytical Method to Identify the Number of Containers to Inspect at U.S. Ports to Deter Terrorist Attacks," *Annals of Operations Research,* vol. 187, pp. 137–158, Jul 2011.

[64] U. K., J.-D. S., A. F., and M. G., "Improving Reliability through Multi-Path Routing and Link Defence: An Application of Game Theory to Transport," in *Game Theoretic Risk Analysis of Security Threats*, ed: Springer, 2009, pp. 1–29.

[65] M. Bell, "A Game Theory Approach to Measuring the Performance Reliability of Transport Networks," *Transportation Research Part B: Methodological,* vol. 34, pp. 533–545, 2000.

[66] K. Kobbacy and D. Murthy, *Complex System Maintenance Handbook*: Springer, 2008.

[67] H. Pham, "On the Estimation of Reliability of k-out-of-n Systems," *International Journal of Systems Assurance Engineering and Management,* vol. 1, pp. 32–35, 2010.

[68] F. Mathur, "On Reliability Modeling and Analysis of Ultrareliable Fault-Tolerant Digital Systems," *IEEE Transactions on Computers,* vol. C–20, pp. 1376–1382, 1971.

[69] F. Mathur and P. de Sousa, "Reliability Models of NMR Systems," *IEEE Transactions on Reliability,* vol. R–24, pp. 108–113, 1975.

[70] F. Mathur and P. de Sousa, "Reliability Modeling and Analysis of General Modular Redundant Systems," *IEEE Transactions on Reliability,* vol. R–24, pp. 296–299, 1975.

[71] H. Pham, "Reliability Analysis of Digital Communication Systems with Imperfect Voters," *Mathematical and Computer Modelling,* vol. 26, pp. 103–112, 1997.

[72] L. Nordmann and H. Pham, "Reliability of Decision Making in Human-organizations," *IEEE Transactions on Systems, Man and Cybernetics, Part A: Systems and Humans,* vol. 27, pp. 543–549, 1997.

[73] L. Nordmann and H. Pham, "Weighted Voting Systems," *IEEE Transactions on Reliability,* vol. 48, pp. 42–49, 1999.

[74] H. Pham, "Reliability Analysis for Dynamic Configurations of Systems with Three Failure Modes," *Reliability Engineering & System Safety,* vol. 63, pp. 13–23, 1999.

[75] I. 61508, "Functional Safety of Electric/Electronic/Programmable Electronic Safety-Related Systems," vol. 61508, ed, 2010.

[76] J. Knight, "Safety Critical Systems: Challenges and Directions," *Proceedings of the 24rd International Conference on Software Engineering,* pp. 547–550, 2002.

[77] J. Bukowski, "Modeling and Analyzing the Affects of Periodic Inspection on the Performance of Safety-Critical Systems," *IEEE Transactions on Reliability,* vol. 50, pp. 321–329, Sep 2001.

[78] T. Zhang, Y. Wang, and M. Xie, "Analysis of The Performance of Safety-Critical Systems with Diagnosis and Periodic Inspection," *Reliability and Maintainability Symposium,* pp. 143–148, 2008.

[79] H. Guo and X. Yang, "Automatic Creation of Markov Models for Reliability Assessment of Safety Instrumented Systems," *Reliability Engineering & System Safety,* vol. 93, pp. 829–837, 2008.

[80] J. Bukowski and I. van Beurden, "Impact of Proof Test Effectiveness on Safety Instrumented System Performance," *Reliability and Maintainability Symposium,* pp. 157–163, 2009.

[81] A. Torres-Echeverría, S. Martorell, and H. Thompson, "Modeling Safety Instrumented Systems with MooN Voting Architectures Addressing System Reconfiguration for Testing," *Reliability Engineering & System Safety,* vol. 96, pp. 545–563, 2011.

[82] G. Levitin, T. Zhang, and M. Xie, "State Probability of a Series-Parallel Repairable System with Two-Types of Failure States," *International Journal of Systems Science,* vol. 37, pp. 1011–1020, 2006.

[83] Y. Wang and H. Pham, "Dependent Competing-Risk Degradation Systems," in *Safety and Risk Modeling and Its Applications*, H. Pham, Ed., ed: Springer London, 2011, pp. 197–218.

[84] H. Wang and H. Pham, *Reliability and Optimal Maintenance*: Springer-Verlag, 2006.

[85] S. Sheu and J. Jhang, "A Generalized Group Maintenance Policy," *European Journal of Operational Research,* vol. 96, pp. 232–247, 1997.

[86] A. Barros, A. Grall, and C. Berenguer, "Maintenance Policies for a Two-Units System: A Comparative Study," *International Journal of Reliability, Quality and Safety Engineering,* vol. 9, pp. 127–149, 2002.

[87] Y. Tsai, K. Wang, and L. Tsai, "A Study of Availability-Centered Preventive Maintenance for Multi-Component Systems," *Reliability Engineering & System Safety,* vol. 84, pp. 261–270, 2004.

[88] W. J. Li and H. Pham, "An inspection-maintenance model for systems with multiple competing processes," *Ieee Transactions on Reliability,* vol. 54, pp. 318-327, Jun 2005.

[89] T. Vaughan, "Failure Replacement and Preventive Maintenance Spare Parts Ordering Policy," *European Journal of Operational Research,* vol. 161, pp. 183–190, 2005.

[90] K. de Smidt-Destombes, M. van der Heijden, and A. van Harten, "On the Interaction between Maintenance, Spare Part Inventories and Repair Capacity for a k-out-of-n System with Wear-out," *European Journal of Operational Research,* vol. 174, pp. 182–200, 2006.

[91] H. Wang and H. Pham, "Availability and Maintenance of Series Systems Subject to Imperfect Repair and Correlated Failure and Repair," *European Journal of Operational Research,* vol. 174, pp. 1706–1722, 2006.

[92] R. Nicolai and R. Dekker, "Optimal Maintenance of Multi-component Systems: A Review," in *Complex System Maintenance Handbook*, ed: Springer London, 2008, pp. 263–286.

[93] B. Sung and D. Schrage, "Optimal maintenance of a multi-unit system under dependencies," *Reliability and Maintainability Symposium,* pp. 118–123, 2009.

[94] T. Nowakowski and S. Werbińka, "On Problems of Multicomponent System Maintenance Modelling," *International Journal of Automation and Computing,* vol. 6, pp. 364–378, 2009.

[95] Y. Liu and H. Huang, "Optimal Replacement Policy for Multi-State System Under Imperfect Maintenance," *IEEE Transactions on Reliability,* vol. 59, pp. 483–495, 2010.

[96] M. Park and H. Pham, "A Generalized Block Replacement Policy for a k-out-of-n System With Respect to Threshold Number of Failed Components and Risk Costs," *IEEE Transactions on Systems, Man and Cybernetics, Part A: Systems and Humans,* vol. 42, pp. 453–463, 2012.

[97] T. Almgren, N. Andréasson, M. Palmgren, M. Patriksson, A. Strömberg, A. Wojciechowski, and M. Önnheim, "Optimization Models for Improving Periodic Maintenance Schedules by Utilizing Opportunities," *Proceedings of 4th Production and Operations Management World Conference,* 2012.

[98] Z. Cheng, Z. Yang, and B. Guo, "Opportunistic Maintenance Optimization of a Two-Unit System with Different Unit Failure Patterns," *International Conference on Quality, Reliability, Risk, Maintenance, and Safety Engineering,* pp. 409–413, Jun 2012.

[99] H. Golmakani and H. Moakedi, "Periodic Inspection Optimization Model for a Two-Component Repairable System with Failure Interaction," *Computers & Industrial Engineering,* vol. 63, pp. 540–545, 2012.

[100] W. Hou and Z. Jiang, "An Optimization Opportunistic Maintenance Policy of Multi-Unit Series Production System," *Advanced Materials Research,* vol. 421, pp. 617–624, 2012.

[101] J. Koochaki, J. Bokhorst, H. Wortmann, and W. Klingenberg, "Condition Based Maintenance in the Context of Opportunistic Maintenance," *International Journal of Production Research,* vol. 50, pp. 6918–6929, 2012.

[102] G. Liu, "Three m-Failure Group Maintenance Models for M/M/N Unreliable Queuing Service Systems," *Computers & Industrial Engineering,* vol. 62, pp. 1011–1024, 2012.

[103] M. Patriksson, A. Strömberg, and A. Wojciechowski, "The Stochastic Opportunistic Replacement Problem, Part II: A Two-Stage Solution Approach," *Annals of Operations Research,* pp. 1–25, 2012.

[104] A. Sarkara, D. Beherab, and S. Kumarc, "Maintenance Policies of Single and Multi-Unit Systems in the Past and Present," *Asian Review of Mechnical Engineering,* pp. 196–205, 2012.

[105] H. Vu, P. Van, A. Barros, and C. Bérenguer, "Maintenance Activities Planning and Grouping for Complex Structure Systems," *Annual Conference of the European Safety and Reliability Association,* 2012.

[106] X. Zhou, Z. Lu, and L. Xi, "Preventive Maintenance Optimization for a Multi-Component System under Changing Job Shop Schedule," *Reliability Engineering & System Safety,* vol. 101, pp. 14–20, 2012.

[107] S. Martorell, A. Sanchez, and V. Serradell, "Age-Dependent Reliability Model Considering Effects of Maintenance and Working Conditions," *Reliability Engineering & System Safety,* vol. 64, pp. 19–31, 1999.

[108] C. Singh and J. Mitra, "Reliability Analysis of Emergency and Standby Power Systems," *Industry Applications Magazine, IEEE,* vol. 3, pp. 41–47, 1997.
[109] G. Sinaki, "Ultra-Reliable Fault-Tolerant Inertial Reference Unit for Spacecraft," *Advances in the Astronautical Sciences,* vol. 86, 1994.
[110] D. Coit, "Cold-Standby Redundancy Optimization for Nonrepairable Systems," *IIE Transactions,* vol. 33, pp. 471–478, 2001.
[111] J. She and M. Pecht, "Reliability of a k-out-of-n Warm-Standby System," *IEEE Transactions on Reliability,* vol. 41, pp. 72–75, 1992.
[112] G. Levitin and S. Amari, "Approximation Algorithm for Evaluating Time-to-Failure Distribution of k-out-of-n System with Shared Standby Elements," *Reliability Engineering & System Safety,* vol. 95, pp. 396–401, 2010.
[113] W. Yun and J. Cha, "Optimal Design of a General Warm Standby System," *Reliability Engineering & System Safety,* vol. 95, pp. 880–886, 2010.
[114] S. Amari, "Reliability Analysis of k-out-of-n Cold Standby Systems with Erlang Distributions," *International Journal of Performability Engineering,* vol. 8, pp. 417–425, 2012.
[115] S. Amari, H. Pham, and R. Misra, "Reliability Characteristics of k-out-of-n Warm Standby Systems," *IEEE Transactions on Reliability,* vol. 61, pp. 1007–1018, Dec 2012.
[116] E. A. Elsayed, *Reliability Engineering*: Prentice Hall, 1996.
[117] C. Qian, S. Nakamura, and T. Nakagawa, "Replacement and Minimal Repair Policies for a Cumulative Damage Model with Maintenance," *Computers & Mathematics with Applications,* vol. 46, pp. 1111–1118, 2003.
[118] J. Chen and Z. Li, "An Extended Extreme Shock Maintenance Model for a Deteriorating System," *Reliability Engineering & System Safety,* vol. 93, pp. 1123–1129, 2008.
[119] A. Rangan and A. Tansu, "A New Shock Model for System Subject to Random Threshold Failure," *Proceedings of World Academy of Science, Engineering and Technology,* vol. 30, pp. 1065–1070, 2008.
[120] X. Yuan and M. Pandey, "A Nonlinear Mixed-Effects Model for Degradation Data Obtained from in-Service Inspections," *Reliability Engineering & System Safety,* vol. 94, pp. 509–519, 2009.
[121] J. Kharoufeh and S. Cox, "Stochastic Models for Degradation-Based Reliability," *IIE Transactions,* vol. 37, pp. 533–542, 2005.
[122] S. Bae and P. Kvam, "A Nonlinear Random-Coefficients Model for Degradation Testing," *Technometrics,* vol. 46, pp. 460–469, 2004.
[123] M. Zuo, R. Jiang, and R. Yam, "Approaches for Reliability Modeling of Continuous-State Devices," *IEEE Transactions on Reliability,* vol. 48, pp. 9–18, 1999.
[124] J. Chiang and J. Yuan, "Optimal Maintenance Policy for a Markovian System Under Periodic Inspection," *Reliability Engineering & System Safety,* vol. 71, pp. 165–172, 2001.
[125] J. Fan, S. Ghurye, and R. Levine, "Multicomponent Lifetime Distributions in the Presence of Ageing," *Journal of Applied Probability,* vol. 37, pp. 521–533, 2000.

[126] P. Wang and D. Coit, "Reliability Prediction Based on Degradation Modeling for Systems with Multiple Degradation Measures," *Reliability and Maintainability Symposium,* pp. 302–307, 2004.
[127] W. Li and H. Pham, "Reliability Modeling of Multi-State Degraded Systems with Multi-Competing Failures and Random Shocks," *IEEE Transactions on Reliability,* vol. 54, pp. 297–303, 2005.
[128] G. Wang and Y. Zhang, "A Shock Model with Two-Type Failures and Optimal Replacement Policy," *International Journal of Systems Science,* vol. 36, pp. 209–214, 2005.
[129] L. Cui and H. Li, "Opportunistic Maintenance for Multi-component Shock Models," *Mathematical Methods of Operations Research,* vol. 63, pp. 493–511, 2006.
[130] Y. Liu, H. Huang, and H. Pham, "Reliability Evaluation of Systems with Degradation and Random Shocks," *Reliability and Maintainability Symposium,* pp. 328–333, 2008.
[131] H. Peng, Q. Feng, and D. Coit, "Reliability and Maintenance Modeling for Systems Subject to Multiple Dependent Competing Failure Processes," *IIE Transactions,* vol. 43, pp. 12–22, 2010.
[132] L. Jiang, Q. Feng, and D. Coit, "Reliability Analysis for Dependent Failure Processes and Dependent Failure Threshold," *International Conference on Quality, Reliability, Risk, Maintenance, and Safety Engineering,* pp. 30–34, 2011.
[133] Y. Wang and H. Pham, "Imperfect Preventive Maintenance Policies for Two-Process Cumulative Damage Model of Degradation and Random Shocks," *International Journal of System Assurance Engineering and Management,* vol. 2, pp. 66–77, 2011.
[134] Y. Wang and H. Pham, "A Multi-Objective Optimization of Imperfect Preventive Maintenance Policy for Dependent Competing Risk Systems With Hidden Failure," *IEEE Transactions on Reliability,* vol. 60, pp. 770–781, Dec 2011.
[135] Y. Wang and H. Pham, "Modeling the Dependent Competing Risks With Multiple Degradation Processes and Random Shock Using Time-Varying Copulas," *IEEE Transactions on Reliability,* vol. 61, pp. 13–22, 2012.
[136] H. Pham and M. Xie, "A Generalized Surveillance Model with Applications to Systems Safety," *IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews,* vol. 32, pp. 485–492, 2002.
[137] P. Lewis and G. Shedler, "Statistical Analysis of Non-stationary Series of Events in a Data Base System," *IBM Journal of Research and Development,* vol. 20, pp. 465–482, 1976.
[138] K. Muralidharan, "A Review of Repairable Systems and Point Process Models," *ProbStat Forum,* vol. 1, pp. 26–49, 2008.
[139] M. Xu, T. Chen, and X. Yang, "Optimal Replacement Policy for Safety-Related Multi-Component Multi-State Systems," *Reliability Engineering & System Safety,* vol. 99, pp. 87–95, 2012.
[140] I. Ushakov, "Universal Generating Function," *Soviet Journal of Computer and System Sciences,* vol. 24, pp. 37–49, 1986.

[141] A. Currit and N. Singpurwalla, "On the Reliability Function of a System of Components Sharing a Common Environment," *Journal of Applied Probability,* vol. 25, pp. 763–771, Dec 1988.
[142] H. Pham, "A New Generalized Systemability Model," *International Journal of Performability Engineering,* vol. 1, pp. 145–155, Oct 2005.
[143] A. Persona, F. Sgarbossa, and H. Pham, "Systemability Function to Optimization Reliability in Random Environment," *International Journal of Mathematics in Operational Research,* vol. 1, pp. 397–417, 2009.
[144] Y. Zhang and H. Pham, "A Dual-Stochastic Process Model for Surveillance Systems with the Uncertainty of Operating Environments Subject to the Incident Arrival and System Failure Processes," *International Journal of Performability Engineering,* 2013.
[145] Y. Zhang and H. Pham, "Modeling the Effects of Two Stochastic-Process on the Reliability of k-out-of-n Surveillance Systems with Two Competing Failure Modes," *Submitted to IEEE Transactions on Reliability,* 2014.
[146] H. Pham and H. Wang, "Optimal (τ, T) opportunistic maintenance of a k-out-of-n:G system with imperfect PM and partial failure," *Naval Research Logistics (NRL),* vol. 47, pp. 223-239, 2000.
[147] H. Pham and H. Wang, "Optimal (τ, T) Opportunistic Maintenance of a k-out-of-n : G System with Imperfect PM and Partial Failure," *Naval Research Logistics,* vol. 47, pp. 223–239, Apr 2000.
[148] W. Li and H. Pham, "An Inspection-Maintenance Model for Systems with Multiple Competing Processes," *IEEE Transactions on Reliability,* vol. 54, pp. 318–327, 2005.
[149] F. Sgarbossa and H. Pham, "A Cost Analysis of Systems Subject to Random Field Environments and Reliability," *IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews,* vol. 40, pp. 429–437, 2010.
[150] H. Pham and X. Zhang, "A Software Cost Model with Warranty and Risk Costs," *IEEE Transactions on Computers,* vol. 48, pp. 71–75, Jan 1999.
[151] X. Teng and H. Pham, "Software Cost Model for Quantifying the Gain with Considerations of Random Field Environments," *IEEE Transactions on Computers,* vol. 53, pp. 380–384, 2004.