NTNU – Trondheim
Norwegian University of
Science and Technology

Reliability Analysis of Wireless Safety-Instrumented Systems

Soheil Sobhani

Reliability, Availability, Maintainability and Safety (RAMS)
Submission date: June 2015
Supervisor: Yiliu Liu, IPK

Norwegian University of Science and Technology
Department of Production and Quality Engineering

RAMS
Reliability, Availability,
Maintainability, and Safety

Reliability Analysis of Wireless Safety-Instrumented Systems

Soheil Sobhani

Winter-Spring 2015

PROJECT THESIS

Department of Production and Quality Engineering
Norwegian University of Science and Technology

Supervisor: Associated professor Yiliu Liu

Co-supervisor: Stig Petersen

Preface

This report has been carried out as a task of my master thesis at the department of production and quality engineering at the Norwegian University of Science and Technology, NTNU, during spring semester 2015. This project is the final step in my master program in RAMS engineering.

This report is written for the audience who has the knowledge in field of reliability and safety. It is therefore expected that readers have knowledge of probability theory, engineering statistics and concept of risk and reliability to some extent.

Soheil Sobhani

Trondheim, 2015-06-02

Soheil Sobhani

Acknowledgment

I would like to thank to my academic supervisor, Professor Yiliu Liu, NTNU, for all valuable comments and input during this project. All of the advices and guidances I have gotten, are reflected in this report.

Gratitude is also expressed to my co-supervisor Stig Petersen, SINTEF for his meaningful discussions and valuable inputs on this master thesis.

I would also like to express my gratitude to Professor Mary Ann Lundteigen for her guidance and assistance in this project.

S.S.

Summary and Conclusions

Progressive development of wireless technology in recent years has enabled it to span its application to a wide verity of systems. Simple house hold monitoring and monitoring of a patient in a hospital gives two diverse examples of these systems. Recently *wireless sensor networks* (WSN) are suggested as an alternative for safety monitoring subsystem in *safety instrumented systems* (SISs). SISs have an important role in safety barriers management where each SIS is assigned to one or more *safety integrity functions* (SIFs). The added wireless feature to the SISs may create uncertainties concerning their field performance. It is therefore necessary to develop methods to assess the reliability and *safety integrity level* (SIL) of SIFs in an adequate, sufficiently accurate and practical way.

To identify and analyze the failures of wireless SIS, *failure modes, effects and criticality analysis* (FMECA) method is suggested. FMECA can reveal changes in underlying failure causes of the system by comparing the wired and wireless sensors in a table. It is observed that the main reason behind the failure of WSNs is due to the packet-loss. It is therefore reasonable to focus on the packet-loss rate and the unavailability of SIS for the reliability assessment purpose. Packet loss between two nodes can occur due to two main failure categories: (i) hardware failure such as battery, memory. (ii) environmental factors such as channel occupation, interference.

Since a WSN functions in different operational modes, it can be modeled as a multi-state system i.e. the system with multiple possible states rather than being limited only to working and fail states. Different states in the system are because of different *quality of service* (QoS) over time. The data packet-loss rate and time latency are the relevant indicators for the network performance as they are dynamic over time and monitor different levels of QoS in the system. Accordingly, in this study, it is suggested to apply Markov method for WSN modeling. By doing so, we aim at utilizing the Markov method's potential in modeling dynamic and multi-state systems. The suggested model considers the whole group of sensors as a single block with different states.

WSNs are by nature complex structures but the proposed model is required to be simple in order to be practical. Therefore, this study first simplifies the WSN and then proposes the model for the simplified structure. On the other hand, the complexity of the model and modeling should be understandable and feasible such that the verification of the SIS performance become straightforward and sufficiently accurate for safety applications.

Contents

Chapter 1

Introduction

1.1 Background

Progressive development of wireless technology in recent years has enabled it to span its application to a wide verity of systems. Simple house hold monitoring and monitoring of a patient in a hospital gives two diverse examples of these systems (Yick et al., 2008). Recently *wireless sensor networks* (WSN) are suggested as an alternative for safety monitoring of *safety instrumented systems* (SIS) . However, the performance for such systems needs to be analyzed before implementing WSNs for critical applications. Due to the change in the communication medium for sensors, it is important to provide a practical and accurate method which can assess the reliability of wireless safety systems according to standards and requirements.

SIS has an important role in management of safety barriers where each SIS is assigned to one or more *safety integrity functions* (SIFs). Those functions are designed in order to mitigate the consequences of events and put equipment under control into a safe state. Recently by advancement in technology, SISs are developed to be more reliable and cost effective. These systems may have complexities and new technical features which can create uncertainties concerning their field performance. It is therefore necessary to develop methods to assess the reliability and *safety integrity level* (SIL) of SIS in an adequate, sufficiently accurate and practical way (Brissaud et al., 2010).

As the new trend in utilizing wireless technology has grown significantly in the last years, SINTEF has also started investigating different applications of this technology. Accordingly, the foundation of this thesis is based on a project by SINTEF which studies the application of wireless technology in safety monitoring. This thesis is a continuation and completion of my summer project at SINTEF. My summer project report was a part of the on-going PDS Petromaks project at SINTEF and contributed to fulfill the objective of the third task; i.e. evaluate how the effect of new technology may influence barrier management, and the availability/reliability of the safety barriers in particular.

1.2 Objectives

The main objectives of this Master's project are;

1. Identifying the unique features in the wireless safety-instrumented systems
2. Investigating different failure modes
3. Determining failures of the interest in the reliability analysis
4. Determining relevant measures for reliability analysis
5. Present a method which is able to calculate the probability of failure and provide the performance level
6. Model a case to exemplify the presented method

1.3 Limitation

The main goal of this project is to provide a methodology for reliability analysis of wireless SISs. However, time and resource constrains confined the scope of this research. Following items list the main limitations of the current study:

- The main focus point of this study is limited to the WSN sub-system of the wireless SIS and other subsystems are not considered.
- (Norsok S-001, 2008) combined with customer regulation is chosen as the required safety specification and other regulations is not investigated.

- for modeling and qualitative analysis of the system the scope is confined to Markov and FMECA while other methods are skipped in this study.
- Markov modeling is executed in GRIF-Markov module and results of steady-state probabilities are obtained by analytic computation engine Albizia-Markov. However, the results are not verified with other methods in order to calculate the uncertainty.
- The wireless SISs are installed as an experimental safety systems. Thus, in the absence of sufficient field data, results from SINTEF investigations are used for modeling inputs.

1.4 Structure of The Report

Generally, this thesis provide a guideline for performance analysis of a SIS consisting of a new technology and in particular the availability/reliability analysis of the wireless SIS is investigated. In the Section 2, wireless SIS is presented with its specifications where the importance of analysis about WSN is demonstrated. In the section 3 a qualitative analysis about WSN has been done by FMECA method which focuses on new added failures. The modeling and quantitative analysis according to FMECA results is presented in section 4. In this section, Markov method is suggested as an alternative approach for modeling and analysis of the system. In order to exemplify the analysis method, a case study is done in the section 5 according to the proposed method in section 4. At last the conclusion of the report and further research directions are presented in section 6.

Chapter 2

Wireless Safety Instrumented Systems Properties

According to IEC61508 (2010) a *safety instrumented system* (SIS) is an instrument, which implement one or more *safety instrumented functions* (SIF). A safety function is usually implemented to protect against a specific undesired event that can cause harm. The system that is protected by the safety-critical system is called *equipment under control* (EUC). A SIS may include software or human action as a part of the SIFs. Each SIS is composed of any combination of sensors, logic solver, or final elements. Sensors also refer to as an input element that detects the risk of the undesired event for EUC and sends the signal to the logic solver (Rausand and Høyland, 2004). The communication medium for a group of sensors can be wired or wireless. A group of sensors that communicate through the wireless channel is named a *wireless sensor network* (WSN). Similarly, WSN can also be defined as a collection of distributed, autonomous sensor devices which collaborate in monitoring physical or environmental phenomena such as temperature, pressure, vibration, noise, gas and smoke. The constant monitoring of a phenomenon by sensors results in measuring and displaying the deviation from predefined indicators. The deviation can be defined as an initiating event, which accordingly might lead to the undesired event (Rausand, 2011). In the following chapter a brief history about the development of wireless protocols and standards is presented then WSN and its properties are introduced and finally the specification regulations and challenges of wireless safety system are explained.

2.1 Wireless SIS Specifications

Each SIS is composed of any combination of sensors, logic solver, or final elements (Rausand, 2014a). Traditionally, sensors are powered via a cable and similarly the detected signal is transferred using the same cable. Therefore every sensor is connected to the logic solver through a wire. As a possible simplifying solution, the data from many sensors can be multiplexed in a Junction-box and sent to the logic solver via a single wire. Figure 2.1 shows the two type of sensors.

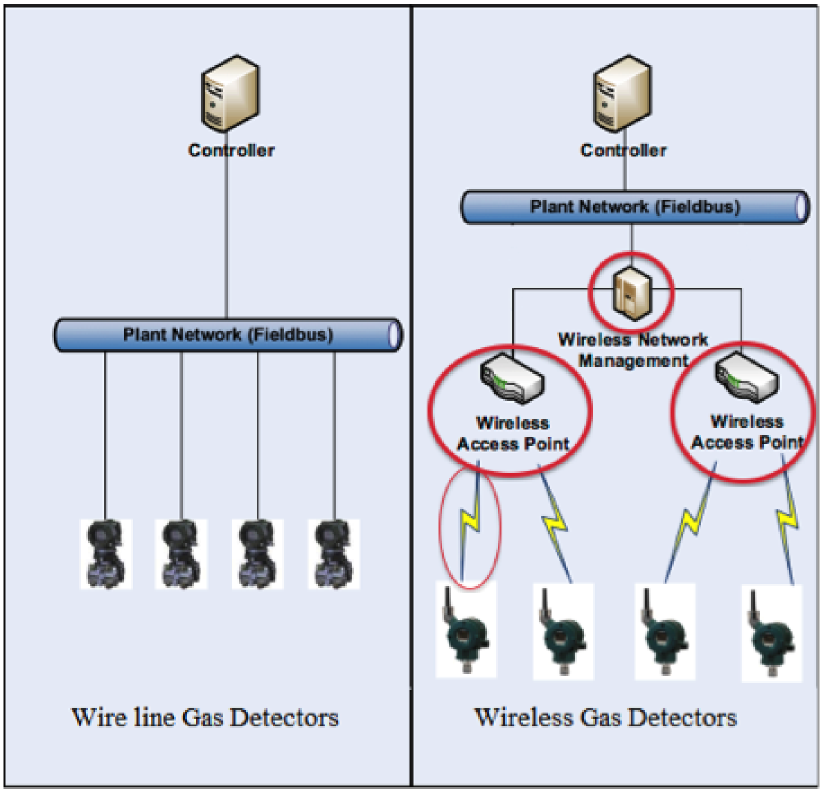

Figure 2.1: Wried and Wireless Sensors From SINTEF-ICT

In the new design, wireless technology is applied as an alternative to hard-wiring in order to save installation costs. However, a wireless detector device consists of several elements, some parts remain the same as traditional detectors, some new components are added and some components are redesigned. A sensors network consists of a group of sensors that has wireless communication to access point . An access point is a send/receive device which receives the signal from sensors by means of wireless and transmits them to the logic solver via a wired connection. Similar procedure is executed in the reverse channel from the logic solver to the sensors (Yick et al., 2008).

For the wireless sensors, the controller (logic solver) and the sensors operate as questioner and respondents such that the controller asks about the exposure status of sensors and then the sensors respond. This request and respond procedure would be done in predefined time intervals which are called diagnostic test intervals. From the safety controllers perspective, there is no difference between a wireless and a wired sensor. The controller sends a request to a sensor (regardless of connection type), and upon receiving the corresponding response, it will immediately send a new request. If the controller does not receive any response within 60 seconds from a specific sensor it assumes the sensor dead (Ikram et al., 2013) (Petersen and Carlsen, 2014).

A wired sensor will send an immediate response upon reception of a request, as it has a high capacity wired communication link, and unlimited power. The wireless sensor, on the other hand, will take advantage of the "60 second timeout limit", and hold on to the request for some time (approx. 18 sec) (Petersen et al., 2007). Figure 2.2 shows the principle of the communication procedure.

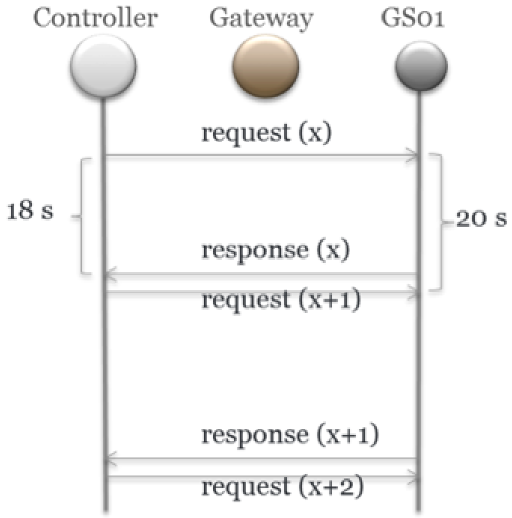

Figure 2.2: Wireless Communication Intervals

2.2 Wireless Sensor Network

A number of wireless sensor nodes (a few ten to thousands) with minimum infrastructure constitute a WSN in order to monitor phenomena in a region. The WSN can be categorized into two different types of structured and unstructured . The difference is highlighted in location and deployment of the sensors. The unstructured WSNs has random deployment of sensor nodes while the structured networks has predetermined sensor nodes placement . The network maintenance, managing the connectivity of sensors and detecting the failures are challenging for unstructured WSN, which is not well suited for a SIS.

The structured WSN is applied for a SIS such that the sensors are placed at specific locations to provide coverage. This is an advantage since fewer nodes are deployed with lower network maintenance and management cost (Yick et al., 2008).

2.2.1 WSN History

In 1980s, *defense advanced research project agency* (DARPA) of the US department of defense developed the *distributed sensor networks* (DSNs) program as a conceptual model and was not ready to apply in a great scale. In order to apply DSN, the size and the cost of sensors must be reduced to make them practically applicable. During 1990s, DARPA initiated a research to develop knowledge about ad-hoc networking, dynamic querying and tasking, reprogramming and multi-tasking. This research program was carried out in parallel with IEEE research on the different application of WSN. The research revealed some issues in WSN e.g. information security is considered one of the main challenges in such networks. The first full standard that was released based on the IEEE was the ZigBee in 2004. The ZigBee specification was initially designed to address applications within home automation and consumer electronics (Radmand et al., 2010).

The *HART communication foundation* (HCF) presented the HART field communication protocol specification in 2007, which was specifically designed for process automation applications and named as WirelessHART. In 2010 WirelesHart was approved by IEC62591 as an international standard for wireless communication in process automation (Falmmini and Sisinni, 2014).

Along with HCF, the *international society of automation* (ISA) conducted a family of standards for wireless systems in industrial automation applications and ratified the ISA100.11a standard in 2009. This standard has provided a secure and reliable wireless communication for non-critical monitoring and control applications in the process automation industries similar to WirelessHART (Petersen and Carlsen, 2014).

ISA100

The standards committee of ISA has lined up a set of standards adjusted for industrial automation. The first release introduced in 2009 and updated 2011, which is named ISA100.11a. The standard is specified a secure and reliable wireless communication for non-critical monitoring and control applications while the specification for critical monitoring are due to be published in future versions (Petersen and Carlsen, 2014) .

IEEE Std. 802.15.4 *physical layer* (PHY) and *medium access control* (MAC) are the main idea behind ISA100.11a. The definition for MAC in IEEE Std. 802.15.4 has designated frequency hopping and extended security mechanisms while ISA100.11a only allows operating in 2.4 GHz band (Petersen and Carlsen, 2014)(Steiner et al., 2014). *time division multiple access* (TDMA) with frequency hopping is used as the channel access mechanism in ISA100.11a. In addition the standard supports both routing and non-routing devices, so network topology can be either star, star-mesh or full mesh depending on the configuration and capabilities of the devices in the network (Petersen and Carlsen, 2011).

According to ISA100.11a, a device can be as the visualization of the behaviors, configuration settings, or capabilities in order to supply the essentials of implementation and operation of a network. The function of a device is defined as roles where they must handle at least one. The below is the list of roles and their functions according to (Petersen and Carlsen, 2014):

Input/output(I/O) device provides data to and/or utilizes data from other devices, that is, field sensors and/or actuators. There is no routing capacity or message forwarding ability for an I/O device and has the minimum specification required in ISA100.11a-compliant network.

Router device is capable of forwarding and routing messages from other devices in the network, which has a clock propagation capability which behaves as a proxy

Provisioning device is able to provision other devices to join the network.

Backbone router A backbone router is capable of routing messages via the backbone network.

Gateway device provides an interface between the wireless instrumentation network and the plant network.

System manager is responsible for governing the network, devices, and communications.

Security manager is a function that works together with the system manager to enable secure system operation.

System time source is the master time source for the system. The common sense of time is used to manage device operation.

In the Figure2.3 a typical network configuration of devices with their roles are shown. The figure can highlight the difference between I/O role and router since I/O devices are not able to route or forward messages (Petersen and Carlsen, 2014).

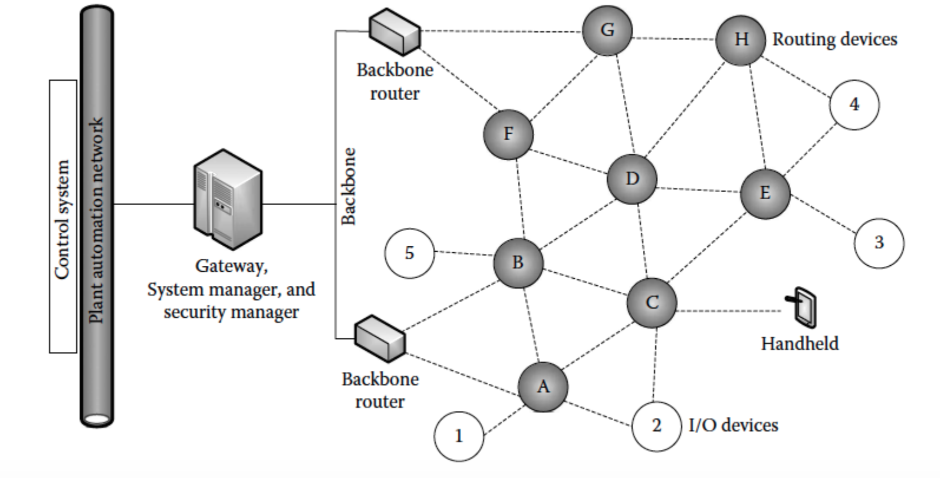

Figure 2.3: Typical ISA100.11a network configuration From ISA100.11a-2011 Standard

WSN Communication Protocol

Since WSN is applied for safety monitoring, the reliability and processing safety time are considered as essential requirements for the network. In order to be ensured about data delivery, a query-based delivery method is applied to WSN where the controller asks about the exposure status of sensors periodically. The delivery report received by the controller guaranties that data received by sensors in the predefined time interval(Petersen and Carlsen, 2014).

A network constitutes of at least two nodes and a connection in between. The queries between the two nodes can be carried out by means of wires or wireless. As far as the communication technology is concerned, all transferred information must be encrypted according to standard communication protocols. This guaranties the accuracy and security of the transferred information. In the other words, a communication protocol is a system of exchanging data between electronic devices. Moreover, a general standard language can prevent mismatch in communication protocols among devices from different vendors (Stripf and Barthel, 2014).

Communication between the sensors and the controller for wired sensors is done by PROFINET protocol. The wired sensor monitors a phenomenon, encrypts the data by using PROFISAFE protocol. In the next step, the data packet is addressed to the destination by PROFINET communication protocol and it is sent to controller. The controller decrypts the data packet and process the information inside the packet (Stripf and Barthel, 2014) (Petersen and Carlsen, 2014). The controller query follows the same procedure which is illustrated in figure2.4.

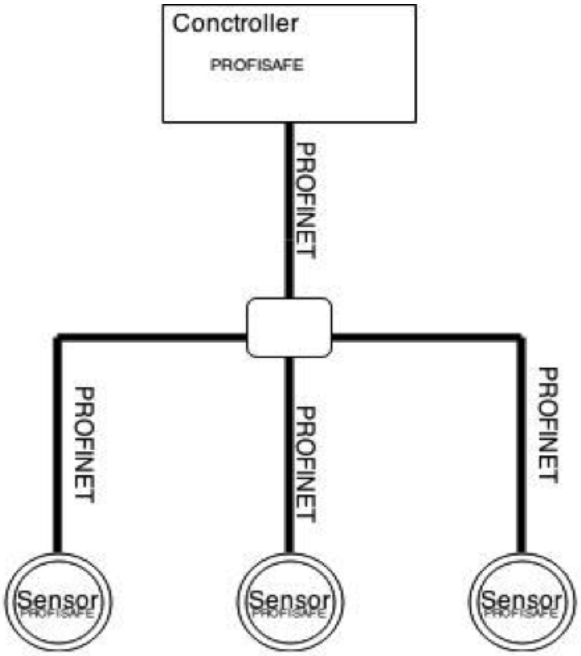

Figure 2.4: Wired Network Protocol

In WSN, the communication protocol changes throughout the data transfer path from sensors to the controller. Such a path includes different hops (jumps) over sensor nodes to access point and a wired connection from access point to the controller. However addressing protocol is changed for wireless communication from PROFINET to ISA100a, the data encryption is remained the same as the wired network. Applying PROFISAFE over ISA100a is considered as a solution for wireless communication because it is certified and proven for safety application

(Petersen and Carlsen, 2014).

In the WSN, query starts from the controller where it inquires about the exposure status of sensors. The query would be packed according to PROFINET communication protocol before being sent on the wire channel to the access point. It should be noted that the information part of the packet is encrypted by PROFISAFE. As the data packet is received by access point, it is readdressed based on ISA100a to the corresponding sensor. The sensor's respond would follow the same procedure to the controller. In the case that the route includes an internal hop among sensors, addressing to destination sensor or the access point is done according to ISA100a (Stripf and Barthel, 2014) (Wenzel, 2014) (Petersen and Carlsen, 2014). Figure2.5 shows wireless communication protocols from sensors to controller.

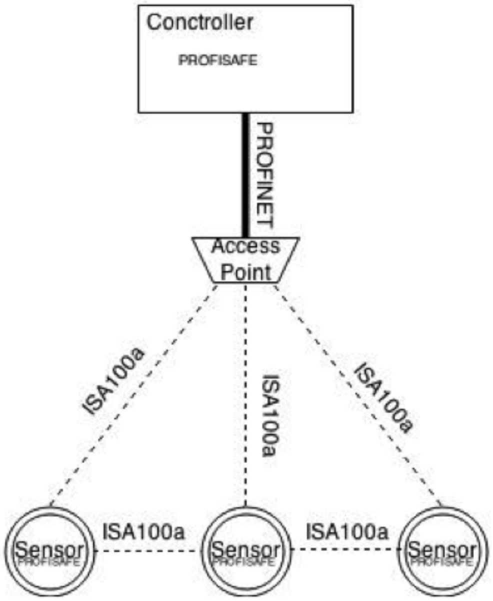

Figure 2.5: Wireless Network Protocol

2.2.2 TDMA and Timeslots

In ISA100.11a, TDMA approach is applied for the main channel access where the communication is done within distinct time-slots of certain duration. As a device is added to the system, the system manger assigns a specific time-slot to it. The accumulation of time-slots creates a superframe, which is repeated over the network lifetime. Figure2.6 shows a super-frame. The communication supervision is handled by the system manger which typically sets a source and a destination to each time-slot. During a times-lot, the source device may send a data packet to a destination, such a data transfer naturally can be successful or unsuccessful. An unsuccessful data packet transmission is named data packet-loss, which has a rate over time. On the other hand for every successful data transmission an acknowledgment packet (ACK) is replied from the receiver to the source device. In case of ACK failure, the receiver sends ACK in the next available times-lot (Petersen and Carlsen, 2014).

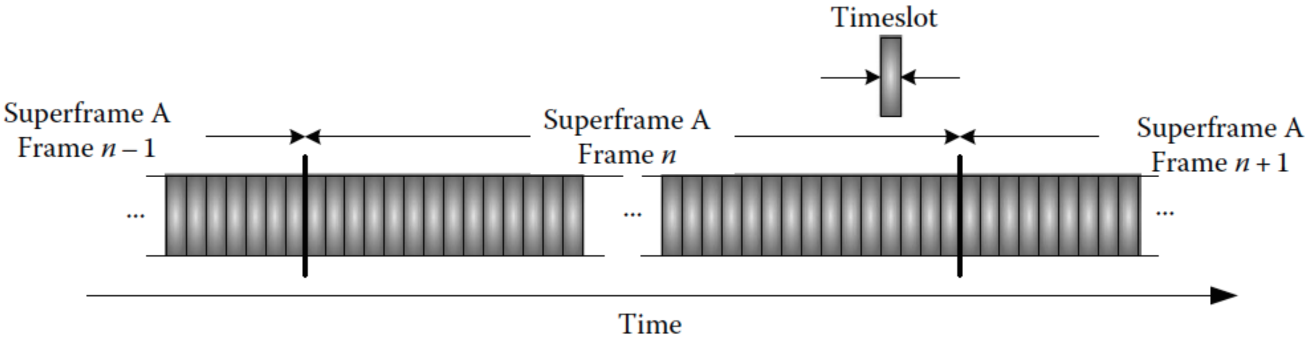

Figure 2.6: Structure of TDMA timeslots and superframes from ICT Handbook

The network performance can be indicated by measuring the time interval between sending and receiving a data packet. Moreover, the packet-loss rate and performance in time are independent. In some cases, the late delivery is regarded as a packet-loss. In the communication network terminology, jitter and message transfer delay (latency) are two widely used terms as the performance indicators and the communication reliability is defined as the amount of data packet reached to destination device or delivery ratio and packet-loss rate (Bhuyan et al., 2010). However, in the safety terminology the reliability of SIS is defined as ability of system to perform its required functions according to the defined time interval to avoid undesired events (Rausand and Høyland, 2004). Therefore, it is important for the reader to differentiate between the communication and SIS reliability in this study.

2.2.3 WSN Constraints

The WSN consists of resource-constrained sensor nodes. Based on the monitored environment and the application such constrains could be listed as the limited amount of energy, short communication range, low bandwidth, and limited processing and storage capability in each node.

The application environment plays a pivotal role in the design of WSN. For instance, outdoor environment requires more sensor nodes in order to cover a wider region while indoor environments could be covered by fewer sensor nodes. Moreover, the obstruction and accessibility of environment affect network connectivity and sensor deployment (Bhuyan et al., 2010).

There are generic (multi-purpose) and gateway (bridge) sensors available in the market. A generic sensor node can measure different environmental phenomena while a gateway sensor node can transfer data from generic node to the base station. Typically , a WSN includes both of these two sensor groups.

In WSN the tasks can be classified into three major groups. The first group of tasks are related to sensor nodes individually while the second group is related to the communication protocol. The third group is the network service, which is the main focus point in this study. This task group is related to efficiency, availability and reliability of the network (Yick et al., 2008). However those task groups are highly linked together. For example, the protocol can strongly influence on end to end delay, energy efficiency and packet-loss rate.

Energy

One of the important concerns in a WSN is energy supply as it is limited to a battery. In order to maximize the network lifetime many intelligent methods are used including retaining the energy through efficient and reliable wireless communication, intelligent sensor placement to achieve adequate coverage, security and efficient storage management, and data aggregation and compression. These alternatives approaches aim to meet the energy constraints as well as providing a quality of service QoS for the network. The parameters such as congestion control, active buffer monitoring, acknowledgments, and packet-loss recovery increases data packet delivery rate (Yick et al., 2008) (Petersen and Carlsen, 2014).

2.2.4 Network Quality

The network quality is an important specification to measure the network performance. The *quality of service* QoS is defined as a set of service requirements that should be implemented while the network transporting data packets stream between sources and destinations. In the other words, QoS is a measurable indicator of network performance, which can be displayed by many indicators including packet loss probability, available bandwidth, end-to-end delay. The required QoS is an agreement between the user and the service vendor (Chen and Varshney, 2004).

The requirements of QoS are expressed according to measurable metrics where different network specification is of the interest. Those metrics have different specifications that are grouped into three categories: additive, multiplicative, and concave (Snigdh and Gupta, 2014).

Additive , let m (n1 , n2) be a metric for link (n1 , n2). For any path P = (n1 , n2 , ···, ni , nj), metric m is: (Note here n1 , n2 , n3 , ···, ni , nj represent network nodes) additive , if m (P) = m (n1 , n2) + m (n2 , n3) + ··· + m (ni , nj). For example, the delay of a path is the sum of the delay of every hop.

Multiplicative , if m (P) = m (n1 , n2) * m (n2 , n3) * ··· * m (ni , nj) Example is the probability sending successful data packet or reliability, in which case 0 < m (ni , nj) < 1.

Concave , if m (P) = min m (n1 , n2), m (n2 , n3), ···, m (ni , nj) For instance the minimum available bandwidth illustrates the bandwidth of a path.

2.2.5 Challenges in WSN Design

using a wireless communication medium introduces a specific set of challenges in network design. Two of these challenges are briefly discussed here:

Energy and delay trade-off as the distance between the source and the destination increases, the power consumption escalates, since it is a proportional to the distance squared. The increment of the distance also results in more exposure to the environment that may influence the data packet-loss probability due to a noisy environment or a non-flat terrain. The proposed solutions includes increasing number of hops which reduces the energy consumption significantly. On the other hand the multi-hop routing can result in the cumulative packet delay. Moreover, multi-hop routing makes the analysis and the handling of delay-constrained traffic complicated (Snigdh and Gupta, 2014).

Support of multiple traffic types applying multi proposes sensors may lead into multiple technical issues related to data routing. Some sensors can detect motions via acoustic signatures and measure the amount of leakage by IR beams. Such a multi-propose sensing can be assembled either in one device or conduct the function independently. In addition using sensors with different data types introduces more challenges in the data routing. Accordingly, the QoS may vary for different groups of data (Snigdh and Gupta, 2014).

2.3 Testing

Similar to conventional sensors, wireless sensors have two types of testing. (i) Functional, and (ii) Diagnostic. Functional tests are typically carried out annually or every sixth month separately among components. In this test most of the *dangerous undetected* (DU) failures are revealed and repaired. For gas detectors failures such as calibration and sensors' position will normally be included during a functional test.

Diagnostic test is a procedure of request and response. The predefined time interval for the controller to conclude that a sensor(s) is in a failed state is within 60 seconds. In this period, the controller has the opportunity to "ask" the sensors about their status. It is important to know that defining the logic of diagnostic test and request/response time frame are mainly related to system developers as well as the programmers' skills (Petersen and Carlsen, 2014).

2.4 Safety Regulations

Generally, the wireless technology requires operating in a specific frequency band. This limits the network communication channels and reduces the probability of interference from other wireless networks operating in the same area(Petersen et al., 2012). However, there is a lack of official standards for wireless applications in safety instrumented systems. Thus, it is suggested to combine general requirements and documented customer requirements for their wireless sensors.

For general SIFs such as gas detection, (Norsok S-001, 2008) requires that:

“The gas detection system shall monitor continuously for the presence of flammable or toxic gases, to alert personnel and allow control actions to be initiated manually or automatically to minimize the probability of personnel exposure, explosion and fire. Typical response times that should be complied with unless faster responses are specified elsewhere:

- IR detector response time (T90) should be less than 5 s for general area applications, and less than 2 s if used in HVAC ducting.
- Acoustic detector response time including delays employed to improve false alarm immunity should not exceed 30 s.
- The time from detector alarm limit is reached until alarm is presented/tagged on operator station should be less than 2 s (i.e. signal transmission time).

There shall be no predefined delays of actions initiated upon gas detection unless a delay is safer. In such a case, this shall be clearly identified in relevant documentation such as FPDS and C and E diagrams.

For gas detection in ventilation inlets IR type detector shall be located as close as possible to the inlet to ensure fast detection".

Technical requirements for wireless instrumentation have been established by the oil and gas industry, regardless of application class (Petersen et al., 2012) (Petersen and Carlsen, 2014). This includes (but are not limited to) the following categories:

- Unlicensed frequency bands
- Friendly coexistence with other wireless solutions
- Standardized and open solutions
- Protection from cyber-attacks and threats
- Quantifiable network performance
- The diagnostic test interval according to IEC 61508

According to the information in this chapter, the safety monitoring of wireless SIS which is done by WSNs has a novelty in design and performance. The wireless SIS may have complexities and new technical features which can create uncertainties concerning their field performance. Due to the change in the communication medium for sensors, it is important to provide a practical and accurate method which can assess the reliability/availability of wireless SISs according to standards and requirements.

In the chapter 3 and 4 methods and techniques for qualitative and quantitative performance and reliability assessment of wireless SIS is introduced.

Chapter 3

Qualitative Reliability Analysis of WSN

As a part of the assessment, it is necessary to have an understanding about system failure modes and mechanisms. In addition, it is important to be aware of any changes in underlying failure causes of the system when the wired sensors are replaced by wireless ones. To identify and analyze the failures, *(Failure Modes, Effects and Criticality Analysis)* FMECA can be an useful method. Similarities between the wired and wireless sensors provided the ability to analyze two systems in one common table. This approach simplifies the comparison between two types of system. In appendix B.2 FMECA for wired and wireless sensors are presented. In the FMECA, wireless network and sensors are taken into consideration for further analysis and other subsystems are not relevant for this report.

3.1 FMECA Technique

A structured bottom-up technique *Failure Modes, Effect, and Criticality Analysis* (FMECA) is a technique for analysis the effect of observed failures in subsystem and system. FMECA approach enables the user to understand how a component failure occurs and what will be the consequences of the failure on the subsystems and system level. The analysis of failure modes and effect is done by tabulating in a worksheet (Rausand and Høyland, 2004) (Rausand, 2014a).

3.1.1 Objectives

Application purposes of FMECA analysis are as follow:

- List the possible failure modes of the systems that are rooted back to components
- Demonstrate the failure causes
- Harmonized between detected and undetected failures

As FMECA is able to list the failure modes and causes, the main objective is to obtain the risk for each failure mode and to what extend are serious the different failure modes. However, FMECA reveals all relevant failure modes, failure rates and severity, it may be only consisted of qualitative data(Rausand, 2014a) .

3.1.2 Assessment Procedure

FEMCA should be carried out by a group of experts that are constituted of system designers, and safety engineers in order to determine a wide range of scenarios for the system failure. In the figure 3.1 the relevant inputs and outputs of the FMECA are illustrated.

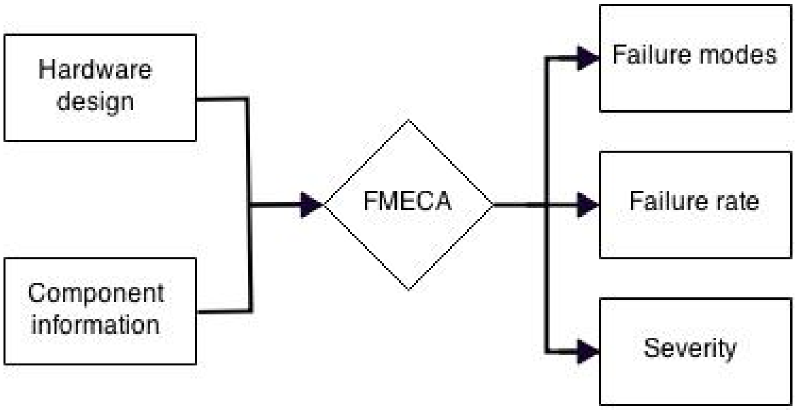

Figure 3.1: Input and output of FMECA

In this study, a FMECA is done for the qualitative failure analysis of WSN subsystem and wireless SIS, but the controller and actuator is not considered as a part of analysis. The FMECA can be find in appendix B.2. The obtained results from the FMECA is used in the new failure analysis (Rausand, 2014a).

3.2 New Failures Analysis

According to the FMECA and (Munir et al., 2015), there can be several failure causes, which are added to the sensor subsystem (WSN). The failures can be divided into two groups, (i) sensor devices failure (ii) network (communication) failure. Both types of failures are detected by diagnostic test and most of them can be labeled as *dangerous detected* (DD) failures.

sensor device failures

New components in wireless sensors add up to some new failure causes with same failure mode as for conventional wired system.

a) *Power source* concerns in this group are mainly related to battery lifetime. Although, the battery failure results in dangerous failure in the sensor device, it is detected within diagnostic test interval. Hence it can be considered as a DD failure. For battery, the failures rate is negligible to have impact on total failure rate of sensor. In addition, battery suffers from degradation (gradual failure) rather than sudden failure, where operator is aware of battery status by constant monitoring (i.e. ignoring operator's error and assuming that timely change of batteries are covered by procedures). However, there can be an increase unavailability of system because of some extra maintenance time for changing the battery compared to wired sensors.

b) *Processing* module can be investigated from two points of view, sensing and communication. From the sensing point of view, this investigation is mainly related to human programming error. The processing module is responsible for analysis of sensor data and encapsulates it in data packets according to the communication protocol. Since the processing logic (calibration) are the same or wired and wireless, the failure rate can be assumed equal. From the network point of view, the processing module is responsible for handling and scheduling the communication. This is discussed more in the communication protocol failure 3.2.

d) *Sensing module* for increasing the battery lifetime is necessary to be redesigned and modified. This involves combining acoustic sensing technology with IR technology in order to reduce power consumption by IR beam. But this redesigning introduces additional failure modes compared to conventional IR sensors. Moreover, IR source must be warmed-up before a measurement is performed, and it must cool-down afterwards. In the discussion section 3.3 this is explained further.

e) *Other failures* there can be other faults in the sensors often related to hardware. Hardware failures related to the wireless communication appear as packet-loss /no communication from a system point of view.

Remarks: There are reported failures in traditional wired sensors that are caused by water intrusion in "Junction boxes" and freezing inside. In wireless sensors the elimination of wires causes exclusion of "Junction box", and consequently no failure of this type.

Moreover, new types of wireless sensors feature so called lifetime calibration, which means that no field calibration is required. However, in some cases, a calibration failure may still be occurred when conventional sensors in field are used with wireless features added to it.

Communication protocol failure

One of the important factors influencing the reliability of a wireless network is programming of the network protocol. The network protocol can bring about several failure causes, which all points back to error in defining the network protocol. There are examples of these errors that may put the diagnosis testing or failure detection in loop and consequently confusion in safety system. Since the programming is done manually, such failures are related either to the programmers skills or to surroundings. In some cases, the system may have delay in transferring the data packet which causes delay in sensing. However, most of the protocol errors are revealed after a while when the operation test (debugging) is performing.

Occupied channel failures

This happens when a specific communication channel, which has the specific frequency, is not available when it is needed. The possible reasons for being occupied can be divided into two categorizes; intentional and unintentional. Intentional occupation is named as "jamming". This is related to a malicious attack on the network and intentional effort to disrupt the communication in the network. This may also be a new reason for false alarm in the system. Unintentional occupation can be classified as follow:

a) Noise that is caused by equipment operating in the same area as the sensors network (e.g. Microwave)

b) *Interference* that is caused by other radio frequency network operating in the same area (e.g. walkie talkie)

c) *Fading* that is caused by the environment where the transmitted data packet fades away due to reflection and attraction effects of surroundings (e.g. Metal pipelines or walls)

d) *Access point failure* since the access point is a device in series with all the detectors, it is important to consider this node as a failure cause of network failure. The access point configuration is similar to detectors without sensing and power modules. A block diagram of access point is shown in Figure3.2.

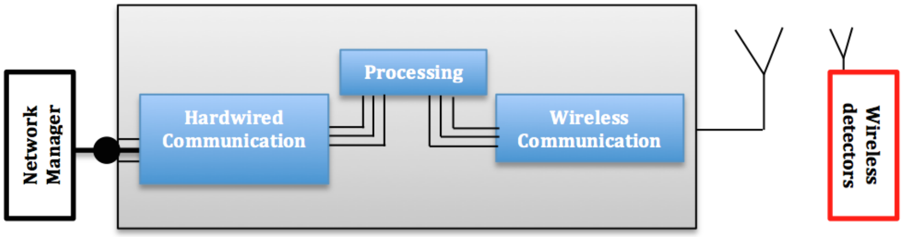

Figure 3.2: Access Point Structural Block

e) *Wireless network management failure* this device has a system manager/security manager/gateway function based on ISA100.11a, and combining this with the field wireless access point composes the field wireless system. This device is located in series with the access point and has its own failure rate. Hence, the failure of the network manager causes network failure and loss of communication. But a failure in the network manager can be detected within the diagnostic test interval.

Remarks wireless gas detectors are dependent on the area and surroundings. This means there are a number of factors influencing the quality of data transmission in wireless systems. For example, if the weather humidity changes the wireless network quality can be changed and as a result the percentage of packet loss may be changed. Therefore, it is possible to have similar sensor models with the same configuration operating in two different areas (e.g. onshore and offshore) with different QoS.

Moreover, there are some factors such as ventilation systems and position of sensors close to areas likely to have leakage that should be taken into account for positioning of sensors. But for wireless there are some added factors such as correct positioning to prevent static fade in network and channel occupation failures, which introduce some additional challenges.

3.3 Discussion

In (Norsok S-001, 2008) it is stated that the time from exposure of sensors to phenomenon until the alarm activation should be less than 7 seconds. This time is calculated as the summation of sensing time, i.e. 5 seconds, and 2 seconds of transmitting the data to controller and activation of the alarm. However, there are some sensing cases for which the process safety time may differ. The reason can be the time frame that each node are allowed to communicate, warming up time and cooling down of sensors, data packet-loss, environmental conditions, etc. Defining a formula correctly for the process safety time is almost impossible, as it involves a lot of uncorrelated parameters from different parts of the system (sensor, processing, time-slots, scheduling), so there will be some cases where the process safety time may be longer than the required time.

As far as the sensors have new design that are featured by IR in standby mode with active acoustic sensing, the warm up time is added to the sensing time. Also, in some cases the system may have additional delays in sensing when it has data packet-loss. In the other words there is a possibility that the system would be unable to meet the response time requirements of a (gas) sensors according to (Norsok S-001, 2008).

The term diagnostic test interval is mentioned in (Norsok S-001, 2008), however the duration of this interval is not specified. The exiting wireless sensors are able to detect a failure in sensors sub-system within 60 seconds. On the other hand, for wired sensors, the detection of failures for the sensors sub-system will be accomplished right at the occurrence of failure, but for wireless due to power saving issues this detection takes longer time.

Based on reliability engineering concepts, adding complexity into a system may reduce its reliability and in best case keeps it at the same level. As can be seen from the failure analysis, there are several failure causes, which results in increasing the unavailability of the system. As a result, a wireless SIS has some reduced reliability and availability compared to a traditional wired system. As it is revealed the main reason behind the failure of WSNs is related to packet-loss. This rate can be measured and monitored by controller where the number of successful reached packets is counted. It is therefore reasonable to focus on the packet-loss rate and the unavailability of SIS for the reliability assessment purpose and modeling in the rest of study.

Chapter 4

Quantitative Reliability analysis

In the chapter 2 and 3 wireless safety system are introduced and investigated in detail. The qualitative analysis reveals some issues, which are introduced to the SIS by shifting the communication medium from wired to wireless. All the efforts is toward illustrating those important issues and establishment of a model is the main step in order to quantify the system reliability. Accordingly, an alternative method for modeling of the system is suggested in this chapter.

4.1 Modeling Key Issues

As far as reliability analysis concerns, packet-loss rate and delay are one of the important metrics for network performance (Chen and Varshney, 2004). The investigation on the system failures reveals that most of the failures are originated from three categories: Hardware, Environment and Human error. The failure of antenna, processor, memory, access point, and battery are regarded as a hardware failure while channel occupation, interference and fading are relevant to environmental factors. However the calibration and programming of wireless protocol are related to human error, it may result in hardware error as well.

According to IEC61508 (2010), the failures can be random hardware failure and systematic failures. Random faults are related to physical damages of the hardware in the system, which are rooted from corrosion, thermal stressing and wear-out. Systematic faults are caused by human error during system development and operation. From this point of view, all environmental factors are lead to random hardware failures while error in programming and defining the network protocol results in systematic failures.

Multi-state modeling

The main idea of the modeling is originated back to multi-state system modeling where the system may have a number of states rather than just working and fail states (Lisnianski, 2007). Defining operating and fail state is a challenge for multi-state systems since there may exist number of intermediate states. In the intermediate states the system is still operating with lower capacity than its maximum. as far as a WSN functions in different operational modes, it can be regarded as a multi-state system. Different states are rooted from different QoS over time. QoS concept that was mentioned in chapter 2 2 can be considered as an indicator of WSN states.

In order to consider QoS as an indicator of the WSN state, a measurable metric must be assigned to QoS. As it was mentioned, well-known metrics include bandwidth, delay, jitter, cost, packet-loss rate and so on (Chen and Varshney, 2004). From the other point of view, it is important to apply the metrics that plays a pivotal role in QoS of wireless SIS. In addition, the most relevant metric must be chosen for this study, considering the important issues in the failure analysis, the study limitations and time constrain. There is a discussion over selection of appropriate metrics for QoS. The data packet-loss rate and time latency are the relevant indicators for the network performance as they are dynamic over time and monitor different levels of QoS in the system. Moreover, qualitative results of the system demonstrated the important effect of these metrics on sub-systems and system. Both of the metrics are relevant for modeling a multi-state system with different functioning states. For instance, the time latency of zero second can be regarded as the best case while infinite latency can be the worst performance and a number of intermediate states can be in between.

The packet-loss rate displays network performance over time in the WSN modeling. Moreover the time latency can be applied as another alternative for indication of WSN performance similar to data packet-loss rate. Hence, different states of the system can be defined based on the data packet-loss rate in every moment of time or the delay for data transmission. For example;

$$\text{State0} = \text{P}(t_0),\ \text{State1} = \text{P}(t_1),\ \text{State2} = \text{P}(t_2),\ \cdots,\ \text{State}N = \text{P}(t_n) \tag{4.1}$$

Where P(t_n) is rate of data packet-loss at time t_n . The states can be illustrated by time latency as follow;

$$\text{State0} = T_0,\ \text{State1} = T_2,\ \text{State2} = T_2,\ \cdots, \text{State}N = T_n \tag{4.2}$$

Where T_n is the delay in transmission for data packet number n.

4.2 Markov Approach

Markov process is a suitable method for dynamic or multi-state systems. This model uses failure rate λ and repair rate μ .and starts from the initiating state. As time passes, the system jumps among its defined states. The Markov model must have finite and discrete number of states over continues time frame that follows Markov process property. The states space is collection of all states and is denoted by X (Rausand, 2014b).

Let $X(t)$ denotes the states of system at time t then $\Pr(X(t) = i) = \mathrm{P_i}(t)$ and it is the probability of being at state i at time t for $i = 0, 1, 2, 3 \ldots, r$ and $r + 1$ is the finite number of states of system. This is called continuous time Markov process because $X(t)$ and probability change over time (Rausand, 2014b).

4.2.1 Markov process property

Markov is a memory less process such that the system jumps to other states, independent of the its background or history of pervious jumps. For example, if the system jumps from state 1 to state 2, in the second jump from state 2 the system would not consider state 1 as a condition for the next jump. This can be formulated by a conditional probability which H_s is the history of system before being in the state i at time s and is going to estimate the probability of jumping into state j at time $t + s$ (Rausand and Høyland, 2004).

$$\Pr(X(t+s) = j \mid X(s) = i \cap H_s) = \Pr(X(s+t) = j \mid X(s) = i) \tag{4.3}$$

More over the probability $\Pr(X(s+t) = j \mid X(s) = i)$ is independent of time s and call homogeneous transition probabilistic process.

$$\Pr(X(s+t) = j \mid X(s) = i) \qquad \text{for } all\ \ s \tag{4.4}$$

It is also assume that the transition probability is continues.

$$\lim_{\mathrm{P_{ij}}\to\infty} = \begin{cases} 1 & i = j \\ 0 & i = j \end{cases} \tag{4.5}$$

The total departure from state i multiply with the probability of jumping from state i to j is transition rate or jump rate and denoted as a_{ij}. So it is possible to assign jump rate between each connected states.

$$\alpha_{ij} = \alpha_i.\mathrm{p_{ij}} \tag{4.6}$$

Where α_i is the total rate of departure from state i and therefore the sum over all possible jumping rate is;

$$\alpha_i = \sum_{\substack{j=0\\ i\neq j}}^{r} \alpha_{ij} \tag{4.7}$$

The transition rate matrix is established as below;

$$\mathrm{A_{m,n}} = \begin{pmatrix} a_{00} & a_{01} & \cdots & a_{0r} \\ a_{10} & a_{11} & \cdots & a_{1r} \\ \vdots & \vdots & \ddots & \vdots \\ a_{r0} & a_{r1} & \cdots & a_{rr} \end{pmatrix} \tag{4.8}$$

Example: Assuming state 0 is working state of a single channel and state 1 is fail stated of channel. More over the failure rate of system is λ and repair rate of system is μ then the sketch of Markov diagram can be illustrated as in figure 4.1.

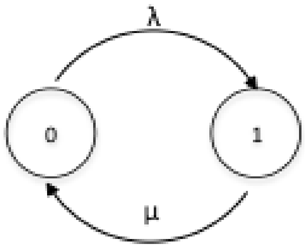

Figure 4.1: two states Markov diagram

The major problem of this method is observed when the target system consists of a large number of components. This can create several states and make the model very extensive and time consuming to establish and run.However, Markov gives "accurate" results, establishing the model by hand would be error prone. It is therefor easier to suffice to a specific category of failures reliability analysis of the system rather than covering the whole aspect of system.

4.2.2 Jump Rate Evaluation

The jump rate plays a pivotal role in reliability quantification however obtaining those rates are not straight forward. One alternative is to monitor the WSN performance and measure the level of data packet-loss, then it is possible to observe how frequent WSN operates with certain QoS level. Those number can be consider as the rate for its assign state.

Jump rates can be called as the failure rate when each jump is a representative of a failure in the system. Therefore, the method for failure rate estimation can be applicable for estimation of jump rates.

Brissaud Approach(Brissaud et al., 2010)

It is common among practitioners to use generic failure rates from data handbooks to handle the lack of reliability feedback data for a specific piece of equipment. However, they may assume these data can be applied in their systems directly without considering details related to technical, operational and environmental conditions underlying the generic data. This may cause uncertainty in reliability estimation of the system

(Brissaud et al., 2010)defines *reliability influencing factors* (RIFs), which act on system's reliability as the internal and external parts of a system. The effects may be positive, by causing a reduction of the failure intensity, or negative, by causing a higher failure intensity. One important aspect of this approach is classification of influencing factors according to life cycle phase of system. The author has also introduced a seven-step methodology for evaluating failure rates. The main steps are as follows:

1. Functional analysis and input data
2. Model definition and influencing factors selection
3. Indicators selection and graduation
4. Influencing factors rating
5. Indicator function
6. Influencing functions
7. Final results

4.3 Modeling of Basic WSN

A simple model is developed by considering a single sensor with the access point as a basic WSN that is a part of a whole SIS with controller and actuator which is shown in figure 4.2. Access point communicate with sensor via wireless which is provide a basic WSN of two nodes and a communication channel in between. The WSN has different packet-loss rate during time due to several influencing factors.

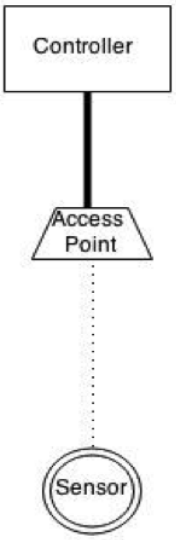

Figure 4.2: Single sensor WSN

As it was mention, the system states can be based on the data packet-loss rate over time. However there are a wide variety of rates over time, it is necessary that Markov states limit to definite number of state. Table 4.1 describes different states of a single channel based on data packet-loss rate in 4 levels. The Markov diagram is illustrated in figure 4.3.

Table 4.1: Markov State of 1oo1 WSN

States	Description
0	The channel is functioning with P_0 rate of data packet-loss
1	The channel is functioning with P_1 rate of data packet-loss
2	The channel is functioning with P_2 rate of data packet-loss
3	The channel is functioning with P_3 rate of data packet-loss

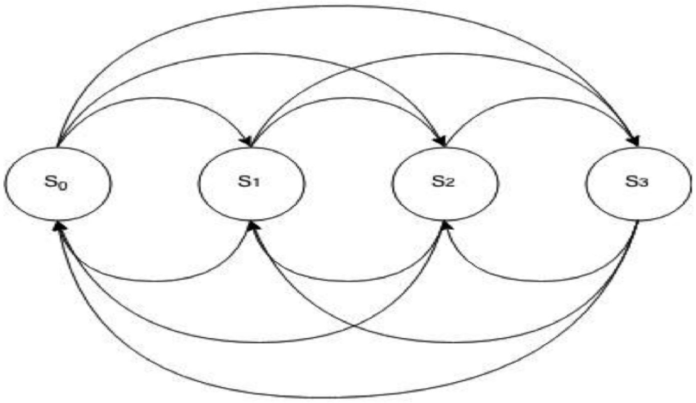

Figure 4.3: Markov Diagram of Single Sensor WSN

4.3.1 Model Description

Figure 4.3 illustrates different jumps of the WSN among these states. As can be seen from the figure system can jump from each state to another state. It starts from initiating state of system S_0, and may jump to other states with different jump rates. It should be noted that the states are ordered in the descending way where S_0 is the best performance for WSN and S_3 is worst. In the other words S_0 has the lowest and S_3 has the highest packet loss rate. It is assumed that the WSN starts the monitoring of environment with S_0 state and then may jump to lower states temporarily or permanently.

4.3.2 Temporary and Permanent Jumps

Temporary jumps

It is important to consider the reason for the degradation of QoS. For example if transient object blocks the communication and reduce the QoS for a short period of time. Then the WSN jump into lower state when the object is presented and jump back to it is initiating state as soon as the object is removed. This type of jump can be considered as a temporary jumps and rooted by temporary blockage, sudden weather change and other transient issues. The contribution of these type of jumps to steady state probability is usually negligible.

Permanent jumps

This jump may be rooted from physical degradation of sensors, installing new wireless system in vicinity or other permanent changes in surrounding. Each of these reasons would result in lower QoS of the WSN and such a low QoS persists until the correction action is performed.

In order to carry out the analysis, modeling most be simplified as much as possible hence it is important to eliminate the jumps that are not realistic to happen. For instance, the QoS would be back to the initiating state S_0 after each correction thus there should not be any intermediate improvement of QoS i.e. jump from S_2 to S_1. Another important issue is the number of states that is defined for the WSN. The WSN can have a wide range of QoS. The definition of WSN performance can be done according to grouping similar performance level of WSN. This can be carried out by the experts and the users. For example, there may be no difference between 70% and 60% packet-loss rate for some users while it is significant for others.

4.4 1oo2 WSN

In this case the WSN is constituted of an access point and two independent sensors which they operate as one out of two voting group. The voting group of 1oon means at least one working element is enough in order to accomplish the system's function. Figure 4.4 illustrates a 1oo2 WSN.

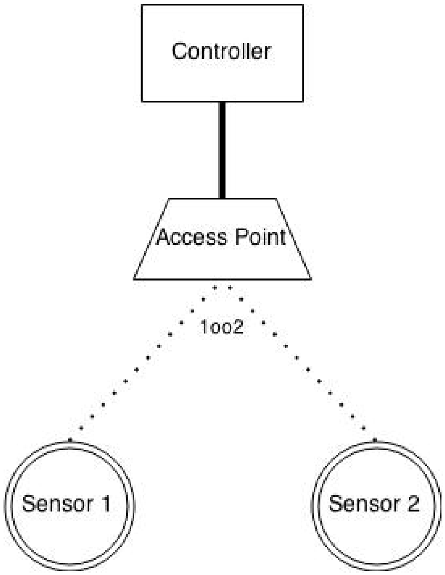

Figure 4.4: 1oo2 Sensors WSN

The following WSN has a slight change over voting group which is due to redundancy. The redundancy is the way to arrange a group of component that can compensate their failure. It is therefore resulted in higher level of QoS since the packet-loss rate should be lower compare to single sensor. However this result is theoretically true, in practice the system may behave in different way due to dependency among sensors.

The modeling of 1oo2 WSN is similar to the single sensor WSN in terms of different states and modeling strategies. In addition, 1oo2 WSN may have more different states due to redundancy but the main difference would be observed in jump rates. The reason beyond that is in regard with the voting and redundancy since the probability of losing two data packets is lower than losing one.

In fact, the proposed model considers the whole group of sensors as a single block with different states. This approach simplifies the complexity of WSN which analytic models such as fault tree are not able to do it. Hence, the techniques would be similar to 1oo1 system with different jump rate values and number of states. Defining the relevant states are an outstanding issue which is necessary to be clarified for Markov method. An alternative technique for defining the states for Markov is introduced in the case study.

Chapter 5

Case Study

This chapter is written according to an experiment carried out by Stig Petersen from SINTEF and Simon Carlsen from Statoil (Petersen and Carlsen, 2009) . In this experiment an specific WSN observed and the results were published in (Petersen and Carlsen, 2009) in 2009. This paper is an investigation over the performance of WirelessHART network in an industrial environment, however an industrial laboratory was chosen in order to have complete control of work activity and operation of other wireless devices.

5.1 Case Description

The WSN is constituted of 9 wireless sensors and one gateway sensor which are located in the lab as figure 5.1. The factors such as signal interference, coexistence of network operating with IEEE802.11g and the jamming from a 2.4GHz device were chosen as an important influencing factor on QoS. By examining different conditions in regard with the mentioned factors, different QoS levels are observed and measured. In order to measure the QoS level packet-loss rate and latency are chosen as indicators of network performance. In this thesis, it is decided to use packet-loss rate as an indicator of QoS due to the limitations.

There is an indicator in the article that is named as reliability and shows the number of successful packets reached to destination. However, the number of successful data packet or reliability can be high due to data re-transmission, there may exist high packet-loss rate at same time. Hence, the system may have high reliability for data delivery while has high packet-loss rate at the same time.

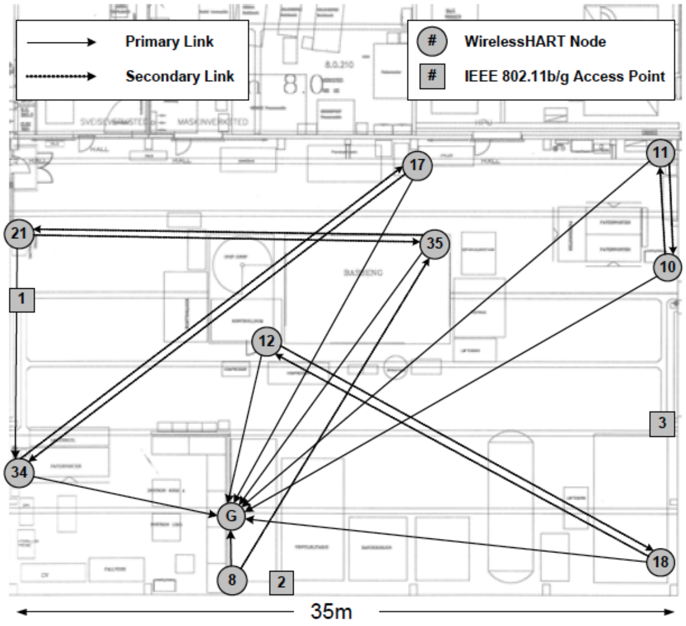

Figure 5.1: Sensors' Location

5.2 Performance

The first part of experiment was related to normal system operation and lasted for 120 hours. During this part,a small fluctuation was observed among 0% , 1% and 2%. Thus, the QoS of 1% is considered as an average QoS when the network is operating in normal condition without any disturbance from environment. Figure 5.2 shows the normal condition packet-lost rate over 120 hours time interval.

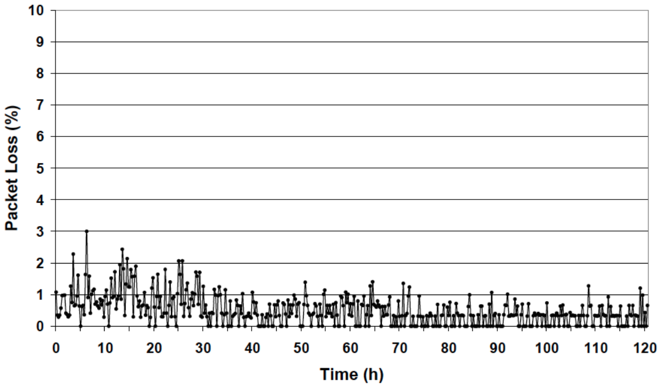

Figure 5.2: Packet-loss Rate-Normal (from Network Performance by Petersen and Carlsen 2008)

It should be noted that in the first 30 hours the packet-loss rate is around 3% which is due to working-related activity in this period.

5.2.1 WSN Performance With Coexistence IEEE 802.11g

The second part of test was to install a WLAN which operate with IEEE802.11g and may influence on QoS of WirelessHART network. Three access points are installed in order to transmit data in the certain time interval. This would results in interference failure that is mentioned in qualitative reliability analysis. It is important to know how much frequent the access points transmit data. Hence, the transmission interval set to 100 ms in the first three hours while it becomes more frequent to 20 ms in the rest of test. The packet-loss rate is displayed in figure 5.3

.

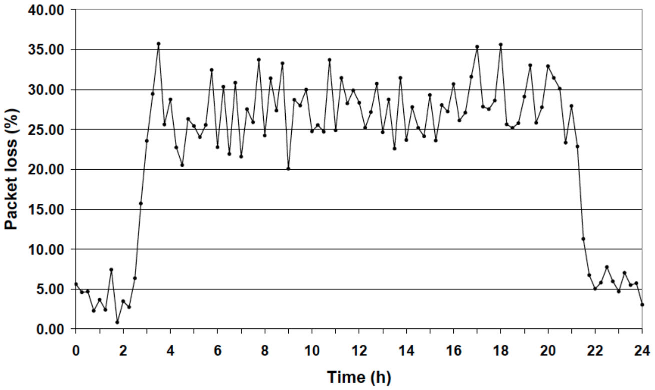

Figure 5.3: Packet-loss Rate-Coexistence IEE802.11g (from Network Performance by Petersen and Carlsen 2008)

As can be seen from the figure the packet-loss probability mounted drastically up to 35% as the data transmission increased and often fluctuated between 25% to 30%.

5.2.2 Jamming

Third part of the test revealed the behavior of system when attacks from a 2.4 GHz linear chirp jamming device are occurred. A chirp is a signal with increasing or decreasing frequency with time, mostly sinusoidal shape. Linear variation of frequency with time gives linear chirp while exponential variation of frequency with time gives exponential chirp.

The jamming device was located in 1 meter distance from gateway node. The figure 5.4 illustrates the packet-loss rate while the device started to operate. The jammer started to send signals from the fifteenth minute and operates for 45 minutes. During this interval packet-loss rate dramatically increased to 100% and resulted in complete network breakdown. This type of attack can be happened intentionally and is dependent in the distance of device to sensors to some extent.

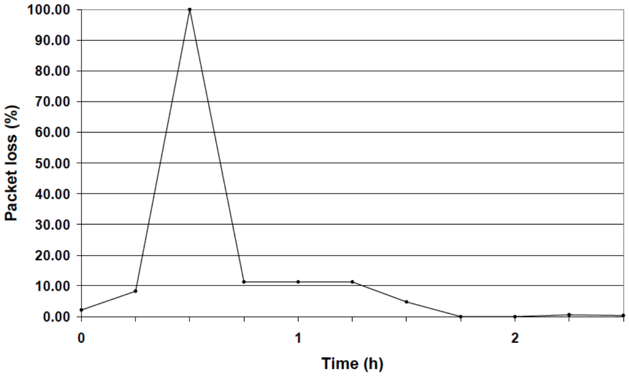

Figure 5.4: Packet-loss Rate-Jamming (from Network Performance by Petersen and Carlsen 2008)

5.3 Modeling

As it was presented before, an alternative way to model WSN which is compatible with WSN specification, is Markov method. In order to apply Markov, it is necessary to define the relevant states of the system and the jump rate values. The results of the experiment over the system performance would provide a knowledge about definition of system states and relevant jumps among different system states. It is therefore straightforward to proceed with Markov method to model the system.

In order to define system state, the QoS should be considered as an alternative indicator of system states. However, the QoS of WSN is not stable over the time and jump several times among different packet-loss rates, the difference is small over time. For example,in the normal condition QoS jumps between 0%, 1% and 2% several times. Since the variation of QoS is not significant in each condition, with consideration of different system performance, it is possible to consider average packet-loss rate. Table 5.1 shows the defined states of the system according to performance analysis.

Table 5.1: Markov State of 1oo10 WSN

States	Description
1	The WSN is functioning with 1% data packet-loss
2	The WSN is functioning with 5% data packet-loss
3	The WSN is functioning with 25% data packet-loss
4	The WSN is failed (100% data packet-loss)

The jump rates over the states are obtained by expert judgment and the experience from the WSN SIS test in the platform. As it was noted, the sufficient method to obtained a jump rate is observation and monitoring. However, in some cases the system is new and there is no available field performance history, RIF method and test data can be another alternative techniques to obtain jump rates. Those methods provide an impression about jump rates but the final results may not be accurate enough and the degree of uncertainty over final results must be taken into consideration. The table 5.2 shows the jump rate.

Table 5.2: Jump Rates

Jump	$1 \rightarrow 2$	$2 \rightarrow 3$	$3 \rightarrow 4$	$1 \rightarrow 4$	$2 \rightarrow 4$	$4 \rightarrow 1$	$3 \rightarrow 2$	$2 \rightarrow 1$
Rate (per minute)	0.74	0.245	0.015	0.0008	0.0001	0.1	1	1

5.3.1 Model Description

The system specification and limitation are caused elimination of some jumps. For instance, there is no sudden jump from 1% packet-loss to 25%, but rather a gradual degradation from 1% to 5% and then to 25%. On the other hand, there are sudden jumps from initiating state to total failure where the system jumps from 1%, 5% and 25% to 100%. Those jumps are happened when the common cause failures occurs. In addition, the repair action can be carried out when the system is fully breakdown (100% packet-loss) and bring system back to its initiating state (1% packet-loss). The intermediate jumps such as jumping from state 2 to 1 or 3 to 2 is due to the fluctuation of QoS over time. Figure 5.5 shows the possible jumps of the WSN over time.

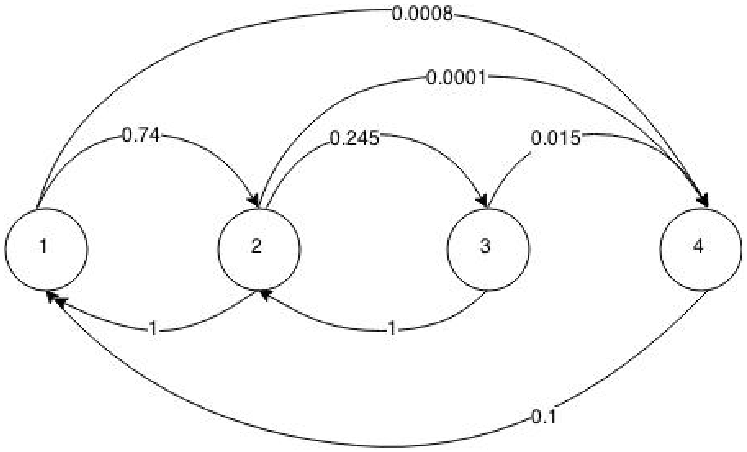

Figure 5.5: Markov Diagram of The WSN Case

5.3.2 Assumptions

First and the most important assumption is that the QoS degradation follows exponential distribution. It means the probability that the QoS of WSN degraded increases exponentially over time. It is also assumed the repair action follows exponential distribution where the repair of the system is accomplished by one maintenance crew. Similarly, the temporary intermediate jumps have the exponential distribution.

There is no repair action in state 2 and 3 since the WSN is still operating. Hence, the system may jump back to states with the better QoS as soon as the temporary issue is removed.

The dependency among states are consider into the jumps from state 1 to 4 or jump from state 2 to 4. There may be a dependency on the probability of intermediate states which is not consider in this modeling. For example If the system jump from state 1 to state 2 it is more probable to jump to state 3.

5.3.3 Steady State Probabilities

In the WSN, it is important to know how much portion of time the system spend in each state. Accordingly the long run probabilities is of the interest. This means the probability that the system spend in each state independent of time ($t \to \infty$) during long run.

$$\lim_{t\to\infty} \mathrm{P_j}(t) = \mathrm{P_j} \qquad \text{for } j = 0, 1, 2, 3, \cdots \tag{5.1}$$

According to (Rausand, 2014b) the steady state equation for the WSN can be established as follow.

$$\begin{pmatrix} \mathrm{P}_1 & \mathrm{P}_2 & \mathrm{P}_3 & \mathrm{P}_4 \end{pmatrix} \times \begin{pmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \\ a_{41} & a_{42} & a_{43} & a_{44} \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & 0 \end{pmatrix} \tag{5.2}$$

There are some techniques such as numerical method to solve the equation 5-2. By increasing the number of states and consequently the rank of matrix, solving of the equation become tedious and time consuming. It is therefore decided to apply software to solve the matrix equation. This approach provide a practical way to solve high rank matrices.

GRIF-Markov Graph Module

GRIF is an analytical software for dependability analysis of the system. This software provides users a wide variety of techniques to choose the method of the interest for the analysis. GRIF-Workshop is designed and has been developed by Total Company.

According to (GRIF-Workshop) the Markov module is able to model and compute small dynamic systems with Markov method. This module applies analytic computation engine Albizia-Markov and is able to solve multi-phase systems. ALBIZIA, engine is developed based on efficient matrix computation algorithms.The user is able to draw Markov diagram easily and insert jump rates in the model, then software computes and delivers results such as, the steady-state probabilities, the sojourn times in each state, the availability/reliability of the system and so on.

The Model graph in the software is provided in Appendix B.1 and steady-state probabilities are illustrated in table 5.3. In addition figure 5.6 shows how the the steady-state probabilities change over time and figure 5.7 show the sojourn time of each state.

Table 5.3: Steady-state Probabilities

P_1	0.5132
P_2	0.3763
P_3	0.09231
P_4	0.01673

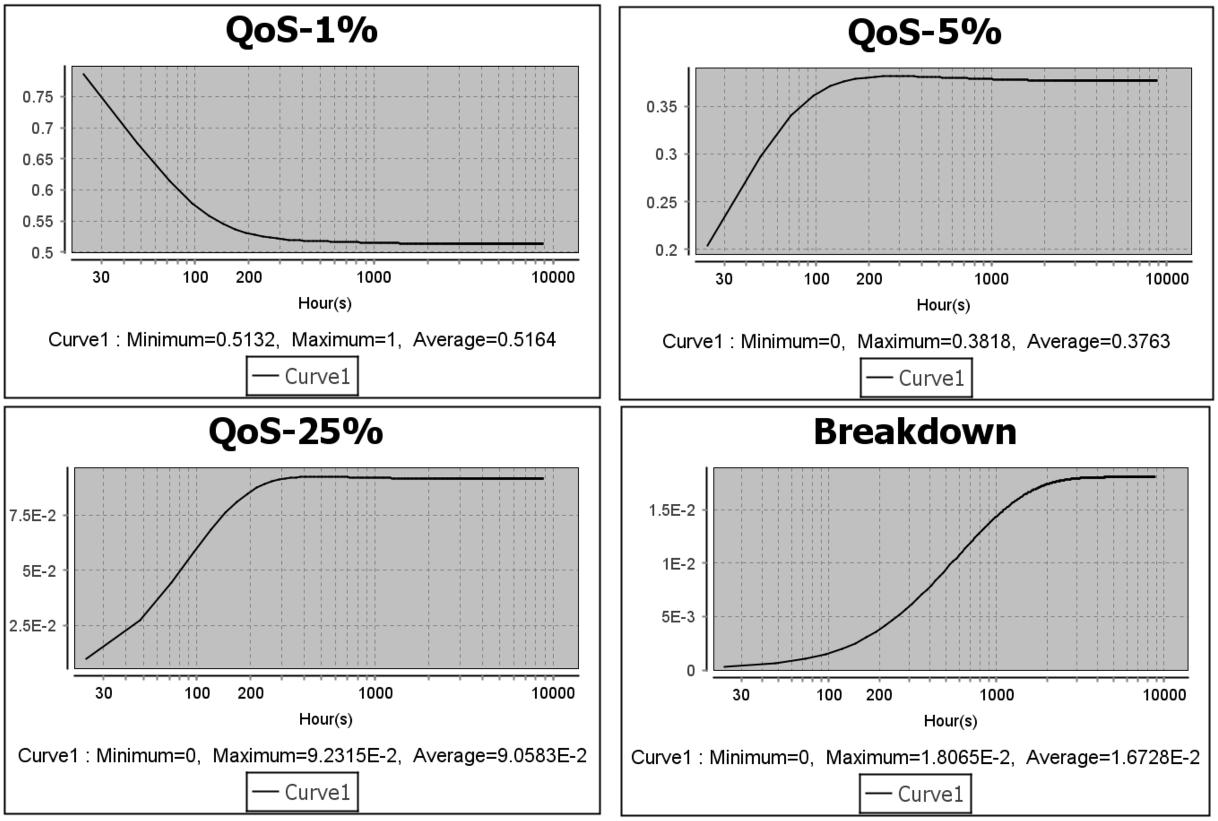

Figure 5.6: Probability of Different QoS Levels

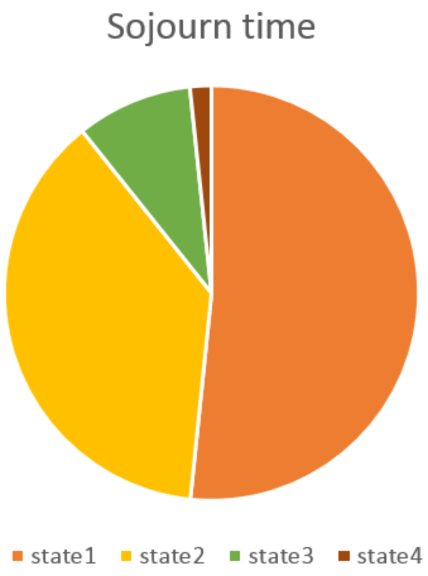

Figure 5.7: Sojourn Time of Each State

5.4 Analysis

It is necessary in the quantitative reliability analysis to elaborate the calculation and the results that are obtained. The most important part is to compare those numbers in order to provide an impression about availability, WSN performance and safety level of the SIF.

The first part of the results is related to the steady-state probability. As can be seen from the figure 5.6 the probability to have 1% packet-loss rate for the WSN has the highest portion with probability of 0.5132 and 5% packet-loss rate has the second place with 0.3763. This level of performance can be an acceptable level for a WSN where the system totally spend 90% of time with high QoS (0% - 5% packet-loss rate).

The availability of sensor network is another issue to analysis. Since it is not straight forward to consider some states as an available state of the WSN, the availability of WSN follows different rules. First of all , it is necessary to define the availability of single sensor where the sensor can transmit data before time-out successfully. On the other hand, each sensor has three opportunities to send the data packet in the time-out interval. If all three chances are lost, then an alarm in the control room signals about failure of the related sensor in such a case. Figure 5.8 shows the chances before time-out.

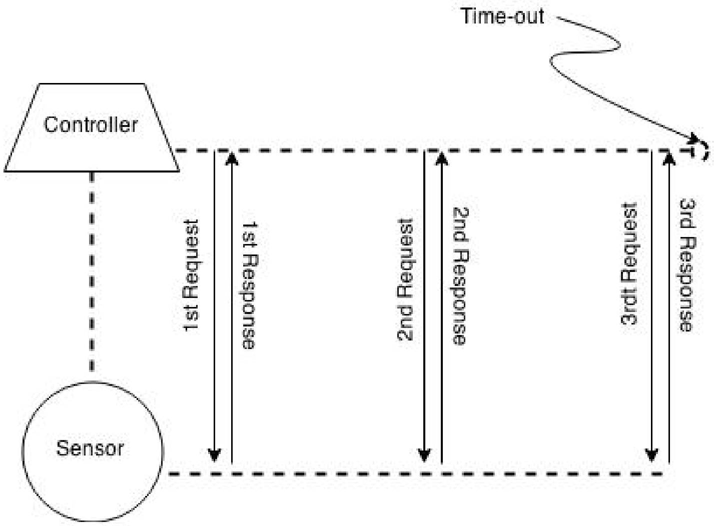

Figure 5.8: Three opportunities for data packet transmission

There are different scenarios about unavailability of a sensor. The sensor can be unavailable either three response or three request data packets are lost in row. Moreover, unavailability can be due to those lost response and request data. All of those scenarios would result in signaling an alarm in control room about unavailability of related sensor. In case of losing 3 sequential data packets, it is expressed that there is a dangerous and detected failure in the system. Figure 5.9 shows different scenarios for unavailability of a WSN due to data packet-loss.

The dependency among different packet-loss scenarios is not considered in the availability calculation but rather an interval is established for unavailability duration. The lower bound is for the unavailability duration when the packet-losses are fully independent and upper bound is when they are fully dependent. The calculation for QoS of 1% is shown as an example. In this way, the total availability is summation over all different QoS levels.

$$\text{Probability of losing 3 sequential data packet } = 0.01 \times 0.01 \times 0.01 \tag{5.3}$$

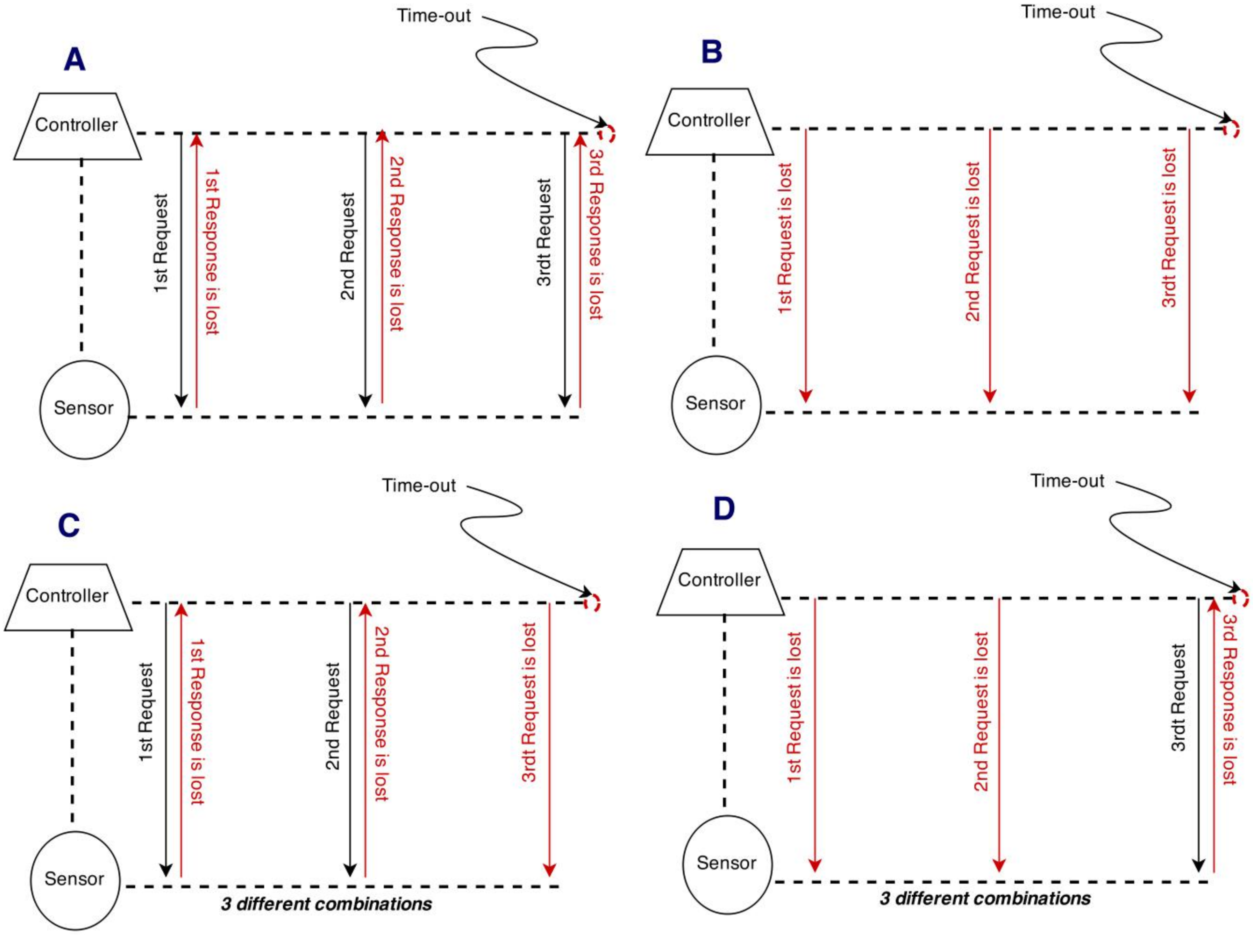

Figure 5.9: Different Data Packet-loss Scenarios

It is assumed that if a response packet is lost then the associated request is lost inevitably and vice versa. The calculated probability of 10^{-6} is unavailability of the system while it has QoS of 1%. As the WSN spends 51.32% of time in long-run with QoS of 1% then the 10^{-6} should be multiplied with 0.5132. This calculation must be done for other QoS levels. Table 5.4 shows the Lower-bound of unavailability for a single sensors for different QoS.

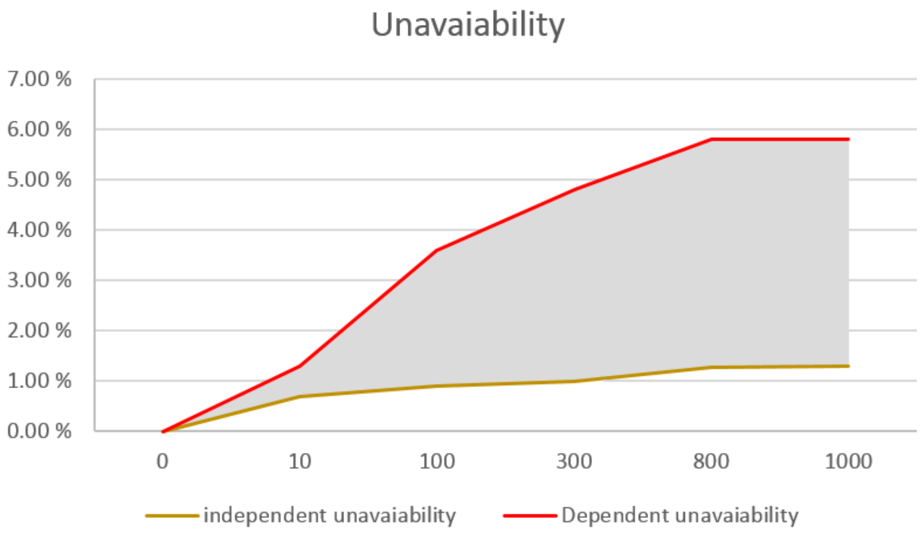

Figure 5.10: Average Unavailability Interval Over Time

Table 5.4: Unavailability Independence Packet-loss

QoS	Unavailability
1%	5.132×10^{-7}
5%	4.703×10^{-5}
25%	1.442×10^{-3}
100%	1.15×10^{-2}
Total	1.294×10^{-2}

Therefore a single sensor is unavailable approximately 1% of time.The calculated number is the lower bound of unavailability interval. In order to calculate the upper bound the full dependency have to be considered. The full dependency of data transmission happens when failure of the first data packet makes an inevitable transmission failure for the second and third packets. The table 5.5 shows the upper bound of unavailability which is related to fully dependent data packets and the figure 5.10 shows the interval of unavailability over time.

Table 5.5: Unreliability-Dependent Packet-loss

QoS	Unavailability
1%	5.132×10^{-3}
5%	1.88×10^{-2}
25%	2.27×10^{-2}
100%	1.15×10^{-2}
Total	5.818×10^{-2}

There is a considerable sensitivity of the unavailability to the number of data transmission opportunities. By increasing the number of transmitted packets in a time-out interval, the availability would be affected but it may consume a lot of energy due to more frequent data transmitting.

However,the whole WSN would be unavailable 0.1 % of time for 1oo10 WSN, the number of sensors unavailability signaling would be increase by 10 due to redundancy of sensors. Table 5.6 illustrate the the number of time an alarm signals in different running duration for 1oo10 WSN.

Table 5.6: Number of Signaling for Unavailability

Days	Number of signaling
100	240
186	446
365	876

This was a sample case of wireless detectors of 1oo10 voting system. Adding sensors to this system would make the system even more robust with respect to redundancy in communication channel. However, the system always suffers from common cause failures, which redundancy cannot overcome. Moreover, adding up to the number of sensors would increase the number of unavailability signaling due to failure of each sensor.

The availability is an performance factor which is important for system users. The investigation about availability is important since there may be a new installed wireless system with an acceptable safety level with very low unavailability. This system has not enough attraction for users as it needs a lot of correction actions during SIS lifetime.

Dangerous Failure

The jump rates that are applied in the model are grouped as dangerous failures where the SIF is not able to perform the safety function. However, those failures result in unavailability of the system, the failure would be detected within the time-out interval. Hence, the modeling and analysis has been over DD failures. The only situation that those failure may not be detected is while unavailability signaling is not able to be done after time-out interval. In this study, the failure of such has not been consider as an alternative reason for occurrence of DU failures. According to FMECA analysis, all the added new failures causes are categorize in DD group of failures. Thus, in the modeling and analysis of the system the availability of the system is more of the interest and the DU failure remains similar to wired system. The *probability of failure on demand* (PFD) of the system remains same as before and the system would have the same quantitative SIL.

Chapter 6

Conclusion

This study demonstrates pros and cons of utilizing wireless safety system with the focus on reliability and failures of wireless SIS. Those system are redesigned by applying WSN instead of traditional wired sensors. Even though SIS reliability entails reliability of each subsystem, the modeling and analysis was centered around WSN due to the fact that the major difference in studying SIS reliability lays in WSN reliability.

Several failure causes are observed using FMECA, which are unique for the wireless SIS. It is shown during the qualitative analysis that most added failure can be categorized as DD failures. Hence, the main focus of the reliability analysis is over unavailability of WSN. Moreover, it is inferred that packet-loss, which is an indicator of wireless QoS, is the obvious underlying reason for the new failures. It is possible to monitor the status of the WSN by linking the packet-loss rate to QoS and accordingly to WSN performance. Therefore, the packet-loss rate is considered as the indicator of WSN performance in a given moment.

Markov approach (Rausand, 2014b) is one of the suitable methods for modeling SIS according to IEC61508 (2010). To do such a modeling, WSNs are considered as a multi-state systems where the state of the system jumps between possible states in time. WSNs are by nature complex structures but the proposed model is required to be simple in order to be practical. Therefore, this study first simplifies the WSN and then proposes the model for the simplified structure. Accordingly the presented model is understandable such that the verification of the SIS performance becomes straightforward and sufficiently accurate for safety applications. Therefore, the proposed study methodology can be used as an alternative guideline for the industries that are going to apply wireless safety systems.

The presented approached is applied to experiment data provided by SINTEF and Statoil(Petersen and Carlsen, 2009). Based on the experiment data relevant system states are defined where the jump in the system are based on significant changes in QoS. Finally, the system unavailability which is the important issue in the qualification analysis is calculated and tabulated.

The main goal of this study was centered on presenting an alternative way to analyze the reliability of wireless SIS. The methodology of this study can be used as a guideline for such an analysis. Knowing system specifications and properties would pave the way in obtaining an acceptable vision about system performance.

6.1 Recommendation for Improvement

In order to improve the wireless SIS the following recommendations can be helpful:

- Since the major failure root are back to error in defining the protocol, it is important to utilize professional programmers who are aware of different failures and consequences in addition to programming skills.
- To improve reliability by using redundant access point and network manager (the new version of the wireless gas detector has redundant access point and network managers).
- Before applying the safety system into field operation, performing a test can be helpful for debugging of network protocol.
- Location of sensors and access points is very important. Training and experience of crew that design and perform installation is therefore important.
- Improving process safety time and elimination of delays in sensing (e.g. by improving battery lifetime)
- Monitoring the environment in order to prevent the interference from other devices.
- It is important to be aware of installing a new wireless network in vicinity of the wireless SIS would affect the QoS of wireless SIS.

6.2 Further Research

However, this study skipped some aspects of the wireless SIS due to limitations. Investigation on the following topics would be of the interests of industries and appliers:

- Dependency analysis among different jumps in the wireless SIS
- Analysis on recovery and maintenance for different packet-loss rate of WSN
- Experiment on effects of climate change on QoS of wireless SIS
- Investigation on the other QoS metrics for WSN modeling such as latency
- Simulating the sensors in a WSN according to latency and packet-loss rate
- Investigation on the reliability modeling of WSN with different voting group(koon) in wireless SIS

Appendix A

Acronyms

ACK Acknowledgment

DARPA Defense advanced research project agency

DD Dangerous and detected

DU Dangerous and undetected

DSN Distributed sensor network

DTU Down time unavailability

EUC Equipment under control

FMECA Failure modes, effect, and criticality analysis

HCF HART communication foundation

ISA International society of automation

MAC Medium access control

PFD Probability of failure on demand

PHY Physical layer

QoS Quality of service

RAMS Reliability, availability, maintainability, and safety

RIF Reliability influencing factor

SIF Safety instrumented function

SIL Safety integrity level

SIS Safety instrumented system

TDMA Time division multiple access

WLAN Wireless local area network

WSN Wireless sensor network

Appendix B

Additional Information

B.1 Markov Diagram GRIF-Markov Module

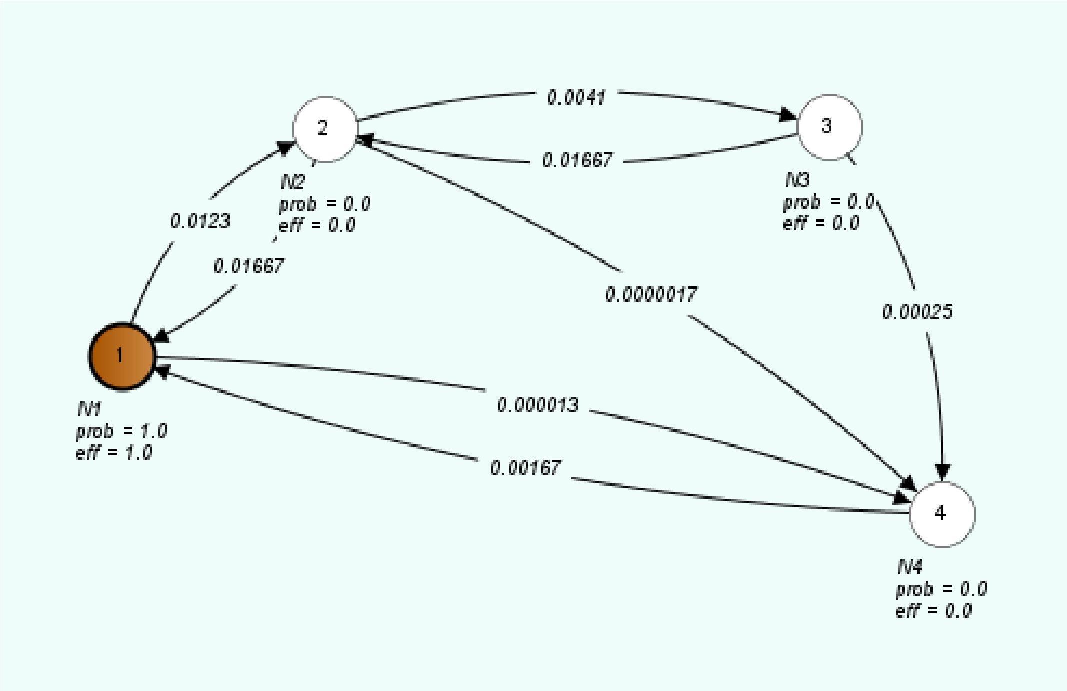

Figure B.1: Markov Diagram in GRIF-Markov Module (rates are per hrs)

B.2 FMECA Table

Description of unit			Description of Failure				Failure Effect		Risk	Comment
Ref. No.	Function	Operational mode	Failure mode	Failure cause by wired detectors	Failure cause by Wireless	Detection of failure	On the sub-system	On the system function	Severity	
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)
1	Activating the alarm	Ready to function on demand	System fails to alarm when it is exposed by gas leak within predefined time interval	—	**Nodes fail to detect when they are exposed due to battery failure**	Detected	Data Packet loss	Unprotected		
				Hard wire or JB is disrupted	**Connection channel is occupied***	Detected	Data Packet loss	Unprotected		
				—	**Communication protocol is not well defined**	Detected	Data Packet loss	Unprotected		
				—	**Access point fail to receive the data packet**	Detected	Data Packet loss	Unprotected		

				—	**Wireless Network management fails**	Detected	Data Packet loss	Unprotected		
				Detectors wrong position	Detectors wrong position	Undetected	Wrong exposure data	Unprotected		
				Detectors wrong calibration	Detectors wrong calibration	Undetected	Wrong exposure data	Unprotected		
			System activates the alarm when it is not exposed to gas leak	Sensors wrong calibration	Sensors wrong calibration	Undetected	Wrong exposure data	Protected		
				Sensing problem (Lens)	Sensing problem (Lens)	Undetected	Wrong exposure data	Protected		
				—	**Malicious attack**	Detected	Wrong exposure data	Protected		

Remark: **Bolds** are new for wireless
Other sub-systems of SIS are not considered
Yellow column is added to FMECA for better understanding of changes in failure causes.

Figure B.2: Wireless SIS FMECA

Bibliography

Bhuyan, B., Sarma, H. K. D., Sarma, N., Kar, A., Mall, R., et al. (2010). Quality of service (qos) provisions in wireless sensor networks and related challenges. *Wireless Sensor Network*, 2(11):861.

Brissaud, F., Charpentier, D., Fouladirad, M., Barros, A., and Bérenguer, C. (2010). Failure rate evaluation with influencing factors. *Journal of Loss Prevention in the Process Industries*, 23(2):187–193.

Chen, D. and Varshney, P. K. (2004). Qos support in wireless sensor networks: A survey. In *International Conference on Wireless Networks*, volume 233, pages 1–7.

Falmmini, A. and Sisinni, E. (2014). *WirelessHART*, pages 1–20. CRC Press.

GRIF-Workshop. MARKOV MODULE. http://grif-workshop.com/grif/markov-module/.

IEC61508, S. (2010). International electrotechnical commission, functional safety of electrical/electronic/progammable electronic safety-related system. *International Electrotechnical Commission Std*, 2.

Ikram, W., Jansson, N., Harvei, T., Fismen, B., Svare, J., Aakvaag, N., Petersen, S., and Carlsen, S. (2013). Towards the development of a sil compliant wireless hydrocarbon leakage detection system. In *Emerging Technologies & Factory Automation (ETFA), 2013 IEEE 18th Conference on*, pages 1–8. IEEE.

Lisnianski, A. (2007). Extended block diagram method for a multi-state system reliability assessment. *Reliability Engineering & System Safety*, 92(12):1601–1607.

Munir, A., Antoon, J., and Gordon-Ross, A. (2015). Modeling and analysis of fault detection and fault tolerance in wireless sensor networks. *ACM Transactions on Embedded Computing Systems (TECS)*, 14(1):3.

Norsok S-001, S. (2008). Technical safety. *S-001, Rev*, 3.

Petersen, S. and Carlsen, S. (2009). Performance evaluation of wirelesshart for factory automation. In *Emerging Technologies & Factory Automation, 2009. ETFA 2009. IEEE Conference on*, pages 1–9. IEEE.

Petersen, S. and Carlsen, S. (2011). Wirelesshart versus isa100. 11a: The format war hits the factory floor. *Industrial Electronics Magazine, IEEE*, 5(4):23–34.

Petersen, S. and Carlsen, S. (2014). *ISA100.11a*, pages 1–14. CRC Press.

Petersen, S., Carlsen, S., et al. (2012). Wireless instrumentation in the oil & gas industry-from monitoring to control and safety applications. *SPE Intelligent Energy International*.

Petersen, S., Doyle, P., Vatland, S., Aasland, C. S., Andersen, T. M., and Sjong, D. (2007). Requirements, drivers and analysis of wireless sensor network solutions for the oil & gas industry. In *Emerging Technologies and Factory Automation, 2007. ETFA. IEEE Conference on*, pages 219–226. IEEE.

Radmand, P., Domingo, M., Singh, J., Arnedo, J., Talevski, A., Petersen, S., and Carlsen, S. (2010). Zigbee/zigbee pro security assessment based on compromised cryptographic keys. In *P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC), 2010 International Conference on*, pages 465–470. IEEE.

Rausand, M. (2011). *Hazards and Threats*, pages 65–76. John Wiley & Sons, Inc.

Rausand, M. (2014a). *Concepts and Requirements*, pages 25–51. John Wiley & Sons, Inc.

Rausand, M. (2014b). *Reliability Quantification*, pages 91–164. John Wiley & Sons, Inc.

Rausand, M. and Høyland, A. (2004). *System Reliability Theory: Models, Statistical Methods, and Applications*. Wiley, Hoboken, NJ, 2nd edition.

Snigdh, I. and Gupta, N. (2014). Quality of service metrics in wireless sensor networks: A survey. *Journal of The Institution of Engineers (India): Series B*, pages 1–6.

Steiner, W., Finn, N., and Posch, M. (2014). *IEEE 802.1 Audio/Video Bridging and Time-Sensitive Networking*, pages 1–14. CRC Press.

Stripf, W. and Barthel, H. (2014). *PROFIsafe*, pages 1–22. CRC Press.

Wenzel, P. (2014). *PROFINET*, pages 1–32. CRC Press.

Yick, J., Mukherjee, B., and Ghosal, D. (2008). Wireless sensor network survey. *Computer networks*, 52(12):2292–2330.

Curriculum Vitae

Name:	**Soheil Sobhani**
Gender:	Male
Date of birth:	11. May 1989
Address:	No63 Herman Keragsvei 20 Moholt. 7050 Trondheim
Nationality:	Iranian
Email (1):	soheils@stud.ntnu.no
Email (2):	soheil.sobhanii@gmail.com
Telephone:	+47 48342763

Language Skills

- English Fluent
- Norwegian Intermediate Level
- Persian Native

Education

- Norwegian University of Science and Technology (NTNU), MSc in RAMS Trondheim, Norway 2013-2015
- University of Science and Culture (USC) BSc in Industrial Engineering-System Planning and Analysis Tehran, Iran 2007-2011

Experience

- Student Assistant for Reliability and Safety Analysis course at NTNU, Trondheim, Norway 2014- autumn
- Research Intern at SINTEF Trondheim, Norway 2014- summer
- Project Planner at AMOOD Engineering consulting Tehran, Iran 2010-2012
- Inventory Planner at MINOO Food Company (internship) Tehran, Iran 2010-summer

Courses and Skills

- Subsea Production System course, NTNU, Trondheim, Norway, 2014
- Responsible negotiation, École des Ponts ParisTech, Paris, France, 2013
- Logistic and supply chain under license of Iranian Industrial Engineering group, Tehran, Iran, 2010
- Entrepreneurship course under authorization of Ministry of Labor and Social Welfare, Tehran, Iran, 2006
- Computer training under authorization of Technical and Vocational skill, Tehran, Iran, 2005
- Turning and milling, 2 years experience

Hobbies and Other Activities

Playing drums, Traveling, Snow boarding, Rock climbing