American University in Cairo

Master Thesis

On the Performance Optimization of Reliable Networked Control Systems

Author:
Hassan Hesham Halawa

Supervisors:
Prof. Hassanein Amer and
Dr. Ramez Daoud

A thesis submitted in partial fulfilment of the requirements for the degree of Master of Science in Electronics and Communications Engineering

to the

School of Sciences and Engineering
Department of Electronics and Communications Engineering

January 2015

This page is reserved for the approval sheet.

AMERICAN UNIVERSITY IN CAIRO

Abstract

School of Sciences and Engineering

Electronics and Communications Engineering

Master of Science in Electronics and Communications Engineering

On the Performance Optimization of Reliable Networked Control Systems

by Hassan Hesham Halawa

under the supervision of Prof. Hassanein Amer and Dr. Ramez Daoud

Networked Control Systems (NCSs) consist of sensors, controllers and actuators which are all interconnected via a network fabric. Such an architecture has proven advantageous for industrial communication networks compared to traditional approaches. Lately, Wireless NCSs (WNCSs) have also been rising in popularity due to their ease of installation and maintenance compared to equivalent wired NCSs. However, a significant drawback of WNCSs is the experienced wireless interference which arises from the shared nature of the wireless medium.

In any NCS, the failure of a single component can cause complete control system failure in the absence of fault-tolerance. As a result of the ensuing system downtime due to such failures, large production losses could potentially occur. Thus, fault-tolerance is now becoming a crucial aspect of the design and evaluation of NCSs. Fault-tolerance can be implemented at various levels of an NCS in order to improve system reliability: either at the node level and/or at the network fabric level. Nevertheless, the incorporation of fault-tolerance in NCSs involves additional overhead traffic which can have a noticeable impact on the overall system performance. This overhead traffic may cause the real-time NCS to miss crucial control deadlines. Therefore, minimizing the amount of traffic overhead necessary for the implementation of fault-tolerance is desired.

This research is focused on the design and performance optimization of reliable fault-tolerant NCSs and WNCSs. First, a fault-tolerant WNCS is proposed based on unmodified IEEE 802.11b implementing 1-out-of-3 controller level fault-tolerance utilizing a wired backbone. The interference tolerance of the system was quantified and certain performance optimizations were investigated in order to improve the overall system's interference resilience. Moreover, an additional fault-tolerant WNCS with a reliable wireless backbone is proposed. The proposed WNCS is based on unmodified IEEE 802.11g and implements 1-out-of-2 controller level fault-tolerance in addition to network fabric level fault-tolerance on the critical wireless backbone link using the Parallel Redundant Protocol (PRP).

Second, a network fabric fault-tolerance methodology is investigated for wired Ethernet NCSs utilizing the Rapid Spanning Tree Protocol (RSTP). A performance optimization is proposed which halves the amount of traffic necessary for the implementation of fault-tolerance while guaranteeing system resilience to any individual network fabric failure. Furthermore, a reliability modeling methodology is developed for the proposed model. A case study is subsequently presented to compare reliability of different system architectures using typical industrial parameters. Finally, an expanded two cell model is developed which not only provides the same degree of network fabric level fault-tolerance but also controller level fault-tolerance.

Dedicated to my family, mentors and friends. This work would never have been possible without your guidance and endless support. God bless you all.

Acknowledgements

I would like to acknowledge both my supervisors and my mentors: Prof. H. Amer and Dr. R. Daoud for their constant support and guidance throughout this thesis.

I would also like to acknowledge ex-Provost Prof. Amr Sharaawi for awarding me with an exceptional Graduate Merit Fellowship to complete this work.

I would also like to acknowledge Prof. H. ElSayed, Dr. M. Rentschler, Dr. H. Elgebaly, Eng. T. Refaat, Eng. Y. Hilal, Eng. G. Aziz, Eng. C. Alfi, Eng. M. Mostafa, Mr. R. Mahmoud and Mr. I. Fayez for their generous assistance throughout my work.

I would finally like to acknowledge the thesis examiners: Prof. M. El-Soudani and Prof. S. Abdelazeem as well as the program directors: Prof. A. ElEzabi and Prof. K. Seddik.

Contents

List of Algorithms

List of Figures

List of Tables

List of Abbreviations

A	**A**ctuator
AC	**A**lternating **C**urrent
AP	**A**ccess **P**oint / **A**lternate **P**ort
BEB	**B**inary **E**xponential **B**ackoff
BPDUs	**B**ridge **P**rotocol **D**ata **U**nits
CAN	**C**ontroller **A**rea **N**etwork
CANbids	**C**ontroller **A**rea **N**etwork **B**ased **I**nfrastructure for **D**ependable **S**ystems
CANELy	**C**ontroller **A**rea **N**etwork **E**nhanced **L**a**y**er
Ch	**Ch**annel
COTS	**C**ommercial **O**ff **T**he **S**helf
CSMA/CA	**C**arrier **S**ense **M**ultiple **A**ccess with **C**ollision **A**voidance
CTS	**C**lear **T**o **S**end
DP	**D**esignated **P**ort
FF	**F**ault-**F**ree
FT	**F**ault-**T**olerant / **F**ault-**T**olerance
FTT	**F**lexible **T**ime-**T**riggered
FTP	**F**ile **T**ransfer **P**rotocol
IP	**I**nternet **P**rotocol
ISM	**I**ndustrial, **S**cientific and **M**edical
K	Controller
LAN	**L**ocal **A**rea **N**etwork
MT	**M**ission **T**ime
MTBFs	**M**ean **T**ime **B**etween **F**ailures
NCSs	**N**etworked **C**ontrol **S**ystems
NIC	**N**etwork **I**nterface **C**ard

PROFIBUS	**Pro**cess **Fi**eld**bus**
PRP	**P**arallel **R**edundancy **P**rotocol
PRPT	**P**acket **R**eception **P**ower **T**hreshold
QoS	**Q**uality **o**f **S**ervice
RBD	**R**eliability **B**lock **D**iagram
RedBox	**Red**undancy **Box**
RP	**R**endezvous **P**oint / **R**oot **P**ort
RSTP	**R**apid **S**panning **T**ree **P**rotocol
RTS	**R**equest **T**o **S**end
S	**S**ensor
SAs	**S**ensors and **A**ctuators
SPOF	**S**ingle **P**oint **O**f **F**ailure
SW	**Sw**itch
TCP	**T**ransmission **C**ontrol **P**rotocol
TTF	**T**ime **T**o **F**ailure
UDP	**U**ser **D**atagram **P**rotocol
Wi-Fi	**W**ireless-**F**idelity
WISA	**W**ireless **I**nterface for **S**ensors and **A**ctuators
WLAN	**W**ireless **L**AN
WNCSs	**W**ireless **N**etworked **C**ontrol **S**ystems

List of Symbols

$R(t)$	Reliability at time t	N/A
t	Time	$months$
λ	Failure Rate	$months^{-1}$

Chapter 1

Introduction

In industrial applications, networks are now being used for the transmission of control data such as sensor readings and control actions. Control systems following this arrangement are termed Networked Control Systems (NCSs). NCSs are composed of the same nodes as typical control systems including sensors, controllers and actuators with the only difference being that these nodes are interconnected together via a network fabric composed of links, network interfaces and bridging elements. Compared to traditional point-to-point control architectures, NCSs greatly simplify the wiring and maintenance of complex control systems containing a large number of physically remote but still interconnected nodes.

Recently, wireless communication technologies are being increasingly adopted in industrial applications to form Wireless NCSs (WNCSs). Compared to wired NCSs, WNCSs offer several key advantages including lack of cabling which greatly eases installation and maintenance. However, the shared nature of the employed wireless medium in WNCSs gives rise to several problems more severe than in wired NCSs such as wireless interference and access contention.

With the increase in general complexity and scale of NCSs and WNCSs, the occurrence of failures is no longer a minute possibility. In the absence of fault-tolerance, a failure occurring in any single component is enough to cause the failure of the entire control system. The ensuing system downtime due to such system failures could potentially lead to large production losses.

Therefore, fault-tolerance is now an essential part of the design of evaluation of NCSs and WNCSs. In order to improve the reliability (probability that the system is functioning at a certain point in time) of an NCS, fault-tolerance can as such be applied. The application of fault-tolerance could be on the node level such as at the sensor, controller or actuator nodes and/or on the network fabric level such as at the links, network interfaces and bridging units.

However, the integration of fault-tolerance in an NCS or a WNCS necessitates the addition of overhead traffic which can have a pronounced impact on the overall performance of the control system. Such overhead traffic may congest the control network potentially leading to significant increases in experienced control packet delays and accordingly missed real-time control deadlines. As such, minimizing the traffic overhead associated with fault-tolerant control systems is desired. This research is thus focused on the design and performance optimization (modifying the design parameters in order to achieve gains in system performance evaluation metrics) of reliable fault-tolerant NCSs and WNCSs.

Chapter 2 presents a survey of the literature as well as an overview of relevant previous work in the area of NCSs and WNCSs. Subsequently, the application of fault-tolerance to NCSs and WNCSs is investigated through a survey of multiple fault-tolerant NCSs and WNCSs with fault-tolerance applied at different levels.

Chapter 3 is concerned with fault-tolerant WNCSs. A fault-tolerant WNCS is proposed implementing 1-out-of-3 controller level fault-tolerance. The proposed WNCS is based on unmodified IEEE 802.11b and utilizes a wired high bandwidth Ethernet backbone for inter cell communication. The proposed WNCS's tolerance to external wireless interference was studied and quantified. Some performance optimizations were also carried out on the proposed WNCS in order to improve interference resilience (the maximum tolerable interference).

Moreover, another fault-tolerant WNCS is proposed but utilizing a wireless backbone based on IEEE 802.11g instead of a wired backbone. The Parallel Redundancy Protocol (PRP) is applied on the wireless backbone link in order to improve performance and interference resilience. The proposed WNCS implements two levels of fault-tolerance: 1-out-of-2 controller level fault-tolerance in addition to network fabric fault-tolerance using PRP over the critical wireless backbone link.

Chapter 4 focuses on fault-tolerant NCSs. A network fabric fault-tolerance methodology for wired Ethernet NCSs is investigated. The methodology utilizes the Rapid Spanning Tree Protocol (RSTP) as well as the duplication of key network fabric elements in order to achieve network fabric fault-tolerance against any single fabric failure. A performance optimization is proposed that halves the traffic overhead required for fault-tolerance while maintaining complete immunity to any individual network fabric failure.

Additionally, a reliability modeling methodology is developed for the proposed model. Subsequently, reliability modeling is carried out for the proposed system, a corresponding PRP-based network fabric fault-tolerant NCS as well as a comparable simplex system where no fault-tolerance is implemented. A case study is then presented to compare the reliabilities of the different architectures using typical industrial parameters.

Moreover, an expansion to the proposed optimized RSTP-based network fabric fault-tolerant architecture comprised of two industrial workcells is developed. The proposed expanded model not only offers the same degree of network fabric fault-tolerance against all possible individual fabric failures but also provides 1-out-of-2 controller level fault-tolerance across the two industrial workcells.

Finally, this work is concluded in Chapter 5,

Chapter 2

Literature Review

This chapter provides a survey of the literature as well as relevant previous work.

2.1 Networked Control Systems

Networked Control Systems (NCSs) can be used for a wide range of industrial applications. However, their main components are typically Sensors (S), Controllers (K), Actuators (A) in addition to network fabric elements interconnecting all nodes such as links, interfaces and bridges [1]. Sensors are responsible for monitoring certain phenomena in the environment. Every sampling period, sensor readings are transmitted to a controller which is responsible for processing the data, making control decisions and subsequently transmitting control actions to all actuators as shown in Fig. 2.1. All data transmissions across the network incur a delay (represented by τ in Fig. 2.1) and it is the responsibility of the NCS designers to guarantee that control deadlines are met in the worst case delay conditions.

2.1.1 Classification of Networked Control Systems

NCSs can either be clock-driven (time-driven) or event-triggered based on the existence or lack of a clock signal respectively [2]. On the one hand, for a clock-driven system, constant sampling periods are employed throughout the system with actions taken every

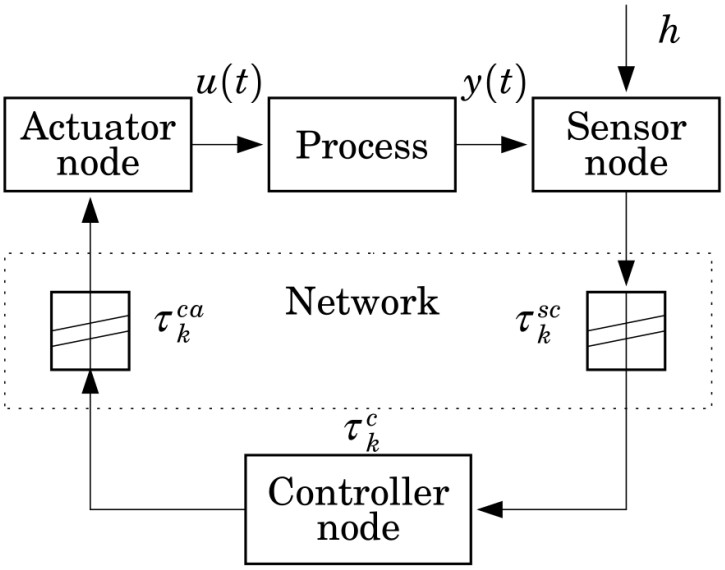

FIGURE 2.1: Networked Control System

sample at discrete time points. On the other hand, for event-triggered systems, sampling is continuous with actions taken immediately once triggered by a certain event.

NCSs can be utilized in a variety of different control applications including real-time as well as non real-time control. Real-Time NCSs typically facilitate the timely communication of small and frequently exchanged control packets [3, 4]. Real-Time control systems can be further subdivided into hard and soft real-time systems [5, 6] the latter of which may tolerate missed deadlines or limited packet losses.

2.1.2 Traditional Networked Control System Approaches

Earlier NCSs had a strict design focus on determinism and predictability of performance. Thus, deterministic protocols were widely developed and employed in traditional NCSs. Of these protocols the Controller Area Network (CAN) [7] and Process Fieldbus (PROFIBUS) [8] protocols have been some of the most widely utilized in industry and consequently researched.

2.1.3 Integrated Control Approach in Networked Control Systems

In [9], an integrated control approach to the design and implementation of distributed NCSs was proposed. The proposed approach is based on the integration of the control

functions locally at the level of the actuator nodes instead of at the level of dedicated controller nodes.

The proposed approach in [9] aims to decrease the total experienced end-to-end delay over the system's control loop. Instead of having a dedicated in-loop controller, all traffic is transmitted directly from the sensor nodes to the integrated control/actuator nodes.

The drawbacks of the approach proposed in [9] is the heavily increased traffic in the control network due to the decentralized nature of the control function. As the number of sensor or actuator nodes increase, the amount of traffic overhead significantly increases thereby requiring a high throughput backbone in order to handle the increased amount of traffic without violating the control system deadline.

2.1.4 Real-Time Modifications to Ethernet in NCSs

With the increased adoption of Ethernet [10] and its subsequent introduction into industrial NCSs, several modification were proposed to offset Ethernet's nondeterminism for use in real-time applications. Some of the most prominent modifications include EtherNet/IP [11], Time Triggered Ethernet [12, 13] and Flexible Time Triggered Ethernet [14].

However, none of these approaches has gained widespread adoption in the industry. Moreover the unmodified Ethernet [10] protocol, despite its nondeterministic nature, has become increasingly popular in NCSs [4, 15, 16].

2.1.5 Ethernet-based In-Loop Networked Control System

An NCS based on unmodified switched Ethernet [10] was proposed in [17]. The proposed NCS was composed of 16 sensors, 1 controller and 4 actuators connected using a switch. Both Fast and Gigabit Ethernet were tested for an integrated real-time and non real-time traffic environment.

It was concluded in [17], through simulations, that Fast Ethernet is unsuitable in a mixed traffic industrial environment due to its low bandwidth which increased experienced delays leading to a failure in meeting the real-time delay constraints. Nevertheless,

Gigabit Ethernet was demonstrated to successfully meet the required real-time delay constraints under various loads.

2.2 Wireless NCSs

Wireless technologies are becoming increasingly popular especially in industrial applications that are unsuited for wired communication technologies such as those requiring mobility or where it would otherwise be difficult or costly to install a wired infrastructure. Generally, Wireless NCSs (WNCSs) benefit from decreased installation and maintenance costs due to the lack of cabling but suffer somewhat from lower available bandwidth and higher potential for interference.

2.2.1 Wireless Interface for Sensors and Actuators

One of the first WNCSs available is Wireless Interface for Sensors and Actuators (WISA) [18–20] developed by ABB (a multinational corporation). The WISA system is composed of two main subsystems: a wireless powering subsystem (WISA-POWER) and a communication subsystem (WISA-COM).

The first subsystem, WISA-POWER, allows the wireless powering of network devices such as sensor nodes through a magnetic induction mechanism. This is useful for industrial applications which may require mobility as motion could cause the breakage of wired power lines.

The second subsystem, WISA-COM, is concerned with the communication protocols employed in the real-time control system. During the development stage, ABB compared the use of Wi-Fi [21], ZigBee [22] and Bluetooth [23] with a specific focus on data rate, coverage and power consumption. Consequently, a modified version of Bluetooth was chosen as the wireless protocol most suitable for use.

The WISA workcell [24], shown in Fig. 2.2 [18], occupies an area around $3 \times 3\ m^2$ and supports up to 120 nodes using a control word size of 1bit [19]. The 1bit control word allows for the most basic forms of On/Off control. The WISA system established a real-time control deadline on the experienced delays over the air links of 20ms [19]. Thus, the delay deadline for the wireless link between the sensors and the controller is 20ms

while the same delay deadline applies for the wireless link between the controller and the actuators.

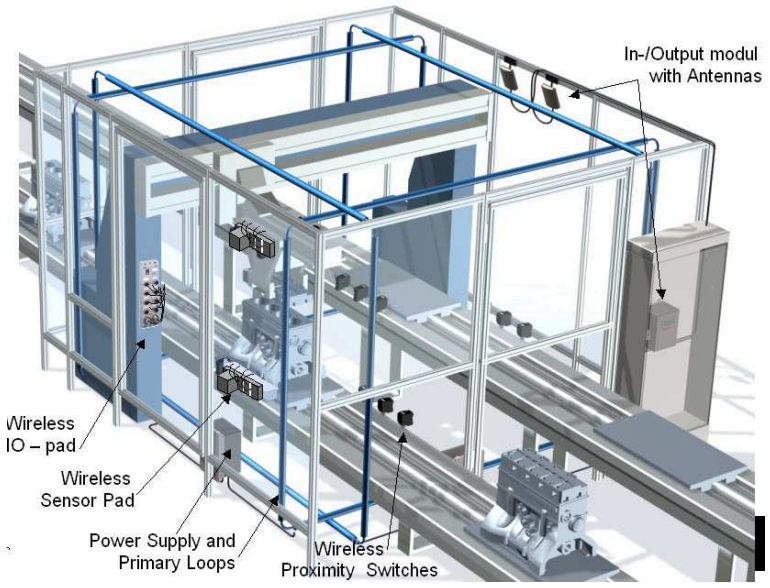

FIGURE 2.2: WISA Workcell

Despite the revolutionary nature of the WISA system at the time of its introduction, especially with its novel wireless powering mechanism, its adoption was hampered by its proprietary nature as well as its use of a nonstandard wireless communication protocol.

2.2.2 Industrial Wireless Interference

For WNCSs, a major issue is wireless interference. Wireless interference may impede control packet transmissions with lost or over delayed packets due to retransmissions. There are many sources of wireless interference both from the external environment or from within the WNCS itself.

One such example is interference on the factory floor emanating from typical industrial operations such as arc/spot welding or mechanical vibrations. An experiment was carried out for the WNCS in [20] in order to study the impact of such typical industrial operations on wireless networks. It was found, using a spectrum analyzer, that the wireless interference caused by such phenomena saturate around the 1.8GHz frequency band.

Thus, for a WNCS system operating in the unlicensed Industrial, Scientific and Medical (ISM) Bands, interference caused by such industrial operations can not have an adverse

impact on wireless communication. Consequently, only ISM band interference may have an impact on a WNCS's performance and should thereby be investigated for non-ideal wireless environments as in [25].

2.2.3 Single Cell Wi-Fi based Wireless Networked Control System

Reference [26] proposed a WNCS utilizing unmodified IEEE 802.11b [21] and switched Ethernet [10] using Commercial Off The Shelf (COTS) hardware. The model is composed of 30 sensors, 1 controller, 30 actuators and 2 Access Points (APs) in a $3 \times 3\ m^2$ area as shown in Fig. 2.3. Since IEEE 802.11b is employed which provides a limited bandwidth, the node traffic is divided over the two APs with each AP serving 15 sensor and actuator nodes.

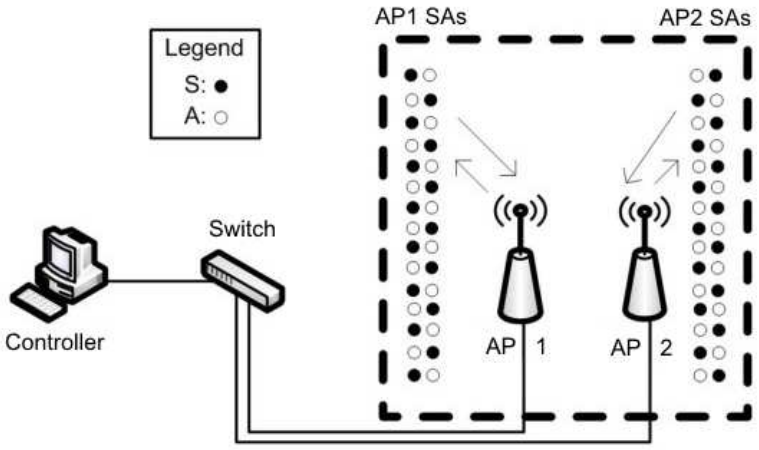

FIGURE 2.3: Proposed Single Cell WNCS

The control word size for the system is fixed to 10Bytes which allows for advanced forms of control in addition to On/Off control [26]. The WNCS employed a sampling period of 40ms strictly following the 20ms per air link benchmark set by [19]. The User Datagram Protocol (UDP) was chosen for the WNCS for performance considerations as opposed to other protocols which require costly packet acknowledgments and retransmissions [15]. Since UDP is employed for all control traffic, transmitter nodes are unable to determine whether a control packet was delivered successfully or not. As such, a strict zero packet loss control criteria is observed by the proposed WNCS in addition to the control packet delay deadline.

In order to study the impact of external interference on the WNCS workcell, an ISM band interferer was employed [26]. The simulated interference models a service engineer using a Wi-Fi enabled laptop while operating in the factory environment. Such usage represents a typical scenario where a service engineer communicates with the workcell's controller through the employed AP for either configuration or diagnostic purposes.

A File Transfer Protocol (FTP) was used to model the communication of the service engineer [26]. The file inter-request time was fixed to 0.5s and the transmitted file size was gradually increased in order to determine the maximum file size that can be tolerated without the WNCS violating its control criteria (zero packets dropped or over delayed packets). The employed benchmark was the same as that in [19].

For all simulations in [26], a confidence analysis was carried out as detailed in Appendix A, in order to mitigate the nondeterminism inherent in the employed wireless protocol which utilizes Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA). CSMA/CA employs Binary Exponential Backoff (BEB) where, when a collision is detected, the transmitter nodes back off for a random number of time slots uniformly chosen between 0 and $2^x - 1$ where x is the number of retransmission attempts.

2.2.4 WNCS Interference Study

A more detailed study of ISM band interference (in the 2.4GHz band) on WNCSs was carried out in [27]. The study investigated various types of ISM band interference on a WNCS workcell utilizing unmodified IEEE 802.11b [21]. The simulated workcell was similar to the one in [26] with a benchmark of 40ms on the total control packet end-to-end delay instead of a 20ms delay per air link.

Different types of Wi-Fi based ISM band interference were modeled in [27] including: network congestion, medium congestion and intentional jamming. For network congestion, an added laptop representing a service engineer communicating with the controller via the cell's AP was simulated. Moreover, medium congestion was investigated where an external Wi-Fi network communicating in the vicinity of the WNCS workcell is employed. Two external laptops communicating through an external ad-hoc network on the same wireless channel as that of the WNCS workcell were used to simulate this type

of interference. Finally, single band jammers (which generate interference across a single frequency band) were used to simulate ambient or even purposeful interference on the simulated workcell.

The interference tolerance of the studied WNCS in [27] was quantified under each interference type. The study showed that intentional jamming is more destructive than medium interference which in turn is more destructive than network congestion.

2.2.5 WNCS Interference and Quality of Service

In [28] the performance of a Wireless Networked Control System based on IEEE 802.11g [21] with Quality of Service (QoS) was investigated under external Wi-Fi interference.

The wireless interference in [28] was modeled by external TCP traffic flows interfering with the WNCS control traffic. The studied external TCP traffic was generated by several interfering FTP sources over Wi-Fi.

It was shown in [28], through a simulation-based study, that the control packet flows are successfully served within the required control deadline when assigned the maximum traffic priority.

2.3 Fault-Tolerant WNCSs

Fault-tolerance is fast becoming a necessity in NCSs and WNCSs as the number of network nodes as well as complexity increases. For a system lacking fault-tolerance, each component becomes a Single Point of Failure (SPOF); the occurrence of a fault in a single component is consequently enough to bring down the entire control system. Such downtime could lead to large production losses which could potentially be extremely costly.

The term fault-tolerance implies that certain faults in one or more components can be tolerated by the system without failing completely [29]. Thus, during a failure, a fault-tolerant system can continue normal operations. However, a system can also be considered fault-tolerant if, upon the occurrence of a fault, the failure is tolerated and the system continues functioning but with degraded performance.

Fault-tolerance can be applied on multiple levels in NCSs and WNCSs: the node level or the network fabric level. This section presents a brief survey of fault-tolerant WNCSs.

2.3.1 Cascaded Fault-Tolerant WNCS using Unicasting and Multicasting

A cascaded 1-out-of-2 controller level fault-tolerant WNCS (where 1 controller is able to takeover the control function of the two workcells in case of a single controller failure) was presented in [30] using unmodified IEEE 802.11b [21]. The presented WNCS was composed of two identical workcells each similar to that in [27] with zero meter inter cell separation as shown in Fig. 2.4. Switched Ethernet was utilized in order to connect the two workcells.

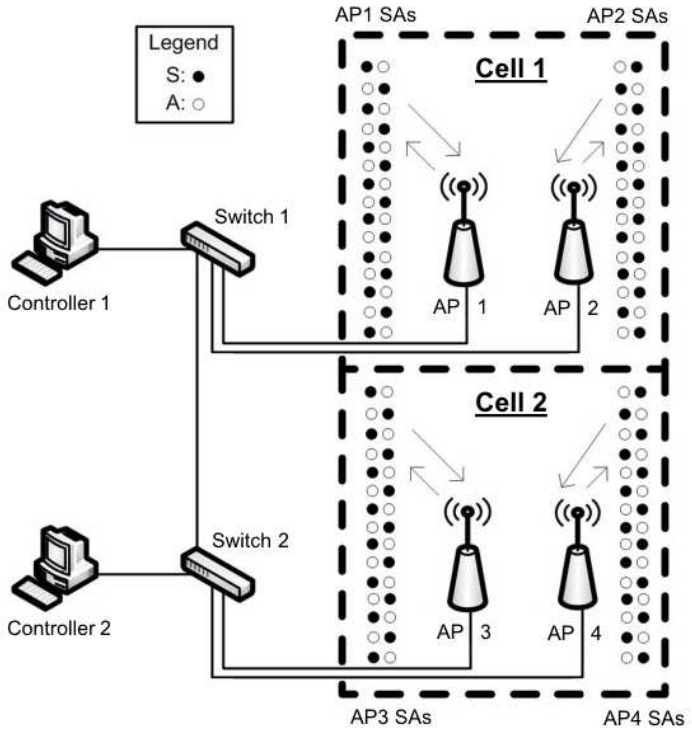

FIGURE 2.4: Proposed Cascaded 1-out-of-2 WNCS

In order to implement controller level fault-tolerance watchdog packets were exchanged between the two controllers as a failure detection mechanism [30]. Watchdog packets were sent twice every sampling period. The absence of watchdog packets would signify the failure of a controller allowing the other to take over operation of its workcell within the same sample.

Thus, in [30], all sensors must send their information to both controllers. Each controller processes this information and subsequently the controller in charge of each workcell sends the required control actions to its cell's actuators. Two approaches to the sensor data transmissions were investigated: Unicasting and Multicasting.

Two approaches for the transmission of control data in [30] were utilized: Unicasting and Multicasting. In Unicasting, each sensor sends two duplicate packets of its data: one addressed to each controller. Such a scheme is simple but bandwidth inefficient. A more efficient approach is to utilize Multicasting where only a single packet is sent by the sensor nodes over the bandwidth constrained wireless link. Afterward, the workcell APs acting as Rendezvous Points (RPs) duplicate the incoming packets and transmit one copy to each controller over the high bandwidth wired backbone.

Moreover, the interference tolerance of the WNCS in [30] was studied under different types of interference. The two employed interference types were network and medium congestion as in [27]. The simulated WNCS was first proven to adhere to the control system constraints, in the absence of interference, using either the Unicasting or Multicasting approaches [30]. However, the WNCS employing Unicasting was unable to tolerate interference; any applied interference would cause the WNCS to violate its control constraints. The WNCS employing Multicasting, however, could tolerate external interference and the maximum interference tolerable by the studied WNCS was quantified.

2.3.2 Cascaded Fault-Tolerant WNCS using IEEE 802.11g

Reference [31] proposed a cascaded 1-out-of-3 controller level fault-tolerant WNCS (where 1 controller is able to takeover the control function of the three workcells in case of a single or double controller failure) utilizing unmodified IEEE 802.11g [21]. The proposed WNCS is composed of three identical workcell each served by a high bandwidth IEEE 802.11g [21] AP connected through a high bandwidth wired Ethernet backbone as shown in Fig. 2.5 [31]. The use of IEEE 802.11g allowed the use of a single AP per workcell instead of requiring two IEEE 802.11b APs per workcell as in [27].

Similar to the system in [30], watchdog packets are employed in [31] in order to detect the occurrence of failures in any of the controllers. Consequently, watchdog packets are

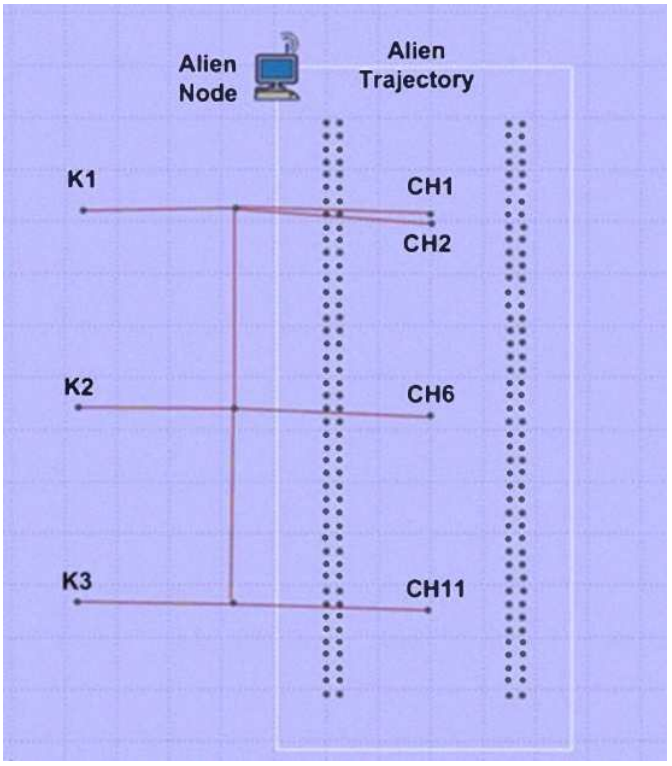

FIGURE 2.5: Proposed Cascaded 1-out-of-3 WNCS

exchanged twice per sampling period between each pair of controllers. Moreover, since the high bandwidth IEEE 802.11g protocol was employed, unicasting was possible for the transmission of multiple copies of the sensor data to all controllers.

The proposed WNCS in [31] was simulated in the absence of any failures and was proven to adhere to the control system constraints in the absence of interference. All possible controller failure scenarios were also investigated including the failure of a single controller or the failure of two controllers. In both scenarios, when no interference was applied, the proposed WNCS was shown to fulfill the required control system constraints.

Finally, the interference tolerance of the proposed WNCS in [31] was quantified under network congestion [27] for all possible controller failure scenarios. The maximum interference tolerable by the proposed WNCS was quantified in each case.

2.3.3 Cascaded Fault-Tolerant WNCS with a Wireless Backbone

Unlike the aforementioned controller level fault-tolerant WNCSs employing a high bandwidth wired Ethernet backbone, the WNCS presented in [32] utilized a wireless backbone

based on unmodified IEEE 802.11g [21]. IEEE 802.11g was chosen due to its high bandwidth which is necessary for the heavily utilized backbone.

The proposed WNCS in [32] implements 1-out-of-2 controller level fault-tolerance over its two identical workcells each employing two APs based on unmodified IEEE 802.11b [21] as in [27]. The two workcells were separated by a fixed inter cell distance in order to decrease the interference between the two workcells as shown in Fig. 2.6 [32].

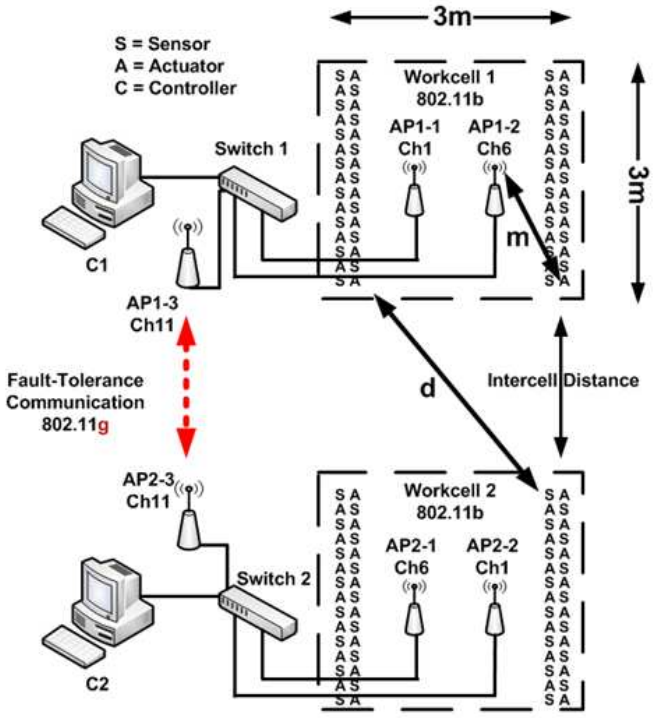

FIGURE 2.6: Proposed Cascaded 1-out-of-2 WNCS with Wireless Backbone

It was shown in [32] that, even with the introduction of the proposed wireless backbone, the control system constraints are fulfilled under all possible controller failure scenarios in the absence of interference. Moreover, interference was applied on the backbone link, in the form of network congestion using external Wi-Fi nodes communicating over FTP as in [27]. It was shown that even under interference on the wireless backbone, the proposed WNCS in [32] is able to fulfill the required control constraints for all possible controller failure scenarios.

2.3.4 Parallel Redundancy Protocol

The shared nature of the wireless communication medium as well as its time-variable nature lead to error-prone communication and nondeterministic error characteristics. As such, for protocols such as Wi-Fi [21], methods of improving performance and robustness are required for real-time control systems with tight deadlines and reliability requirements.

One of the most well studied techniques in order to provide such redundancy is diversity. Diverse communication channels, as shown in Fig. 2.7, could be used in order to counteract the error-prone nature of the channel in addition to improving the characteristics of the wireless communication channel on a stochastic basis [33, 34].

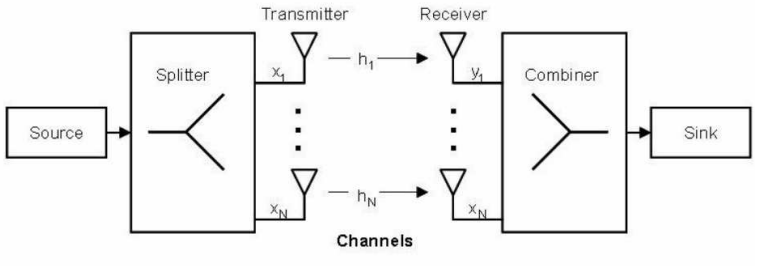

FIGURE 2.7: Wireless Diversity System

A protocol based on this diversity technique is the Parallel Redundancy Protocol [35] which has been recently standardized as IEC 62439-3 [36]. PRP employs a Redundancy Box (RedBox) which is used in both transmitters and receivers. At the transmitter, the RedBox duplicates incoming packets across two separate and independent networks. Subsequently, at the receiver, the RedBox attempts to receive the two duplicate packets with the earliest arriving packet being processed and the other packet discarded. Thus, diversity is made use of across the two independent networks; if packet transmission across one network is unsuccessful then the other network, if independent, should have a high probability of successful packet delivery.

The application of PRP to Wi-Fi networks was investigated through physical as well as simulation experiments. In [37, 38] the feasibility of PRP-WLAN was proven. Moreover, the performance improvements for the use of PRP-WLAN were demonstrated experimentally. These improvements were detailed in a later simulation study [39] focusing on key performance metrics including Maximum End-to-End Delay, Latency and Jitter.

2.4 Fault-Tolerant NCSs

A brief survey of fault-tolerant wired NCSs is presented in this section.

2.4.1 In-Line Fault-Tolerant NCS

A 1-out-of-2 controller level fault-tolerant NCS was presented in [40] using unmodified Ethernet [10]. The proposed NCS consisted of two identical machines working in-line each based on the one in [17]. Both Fast and Gigabit Ethernet were utilized in the model simulations.

It was shown in [40], through simulations, that Fast Ethernet is not sufficient for the studied control application due to its low bandwidth leading to large observed control packet delays as in Section 2.1.5. The proposed NCS in [40], using Gigabit Ethernet, was shown to fulfill the required control system constraints in the fault-free scenario as well as under the failure of any single controller.

2.4.2 Fault-Tolerant Hierarchical Networked Control System

Reference [41] proposed a pyramid control hierarchy where, in an in-line NCS composed of multiple machines, supervisor controller nodes operate on top of machine level controller nodes.

In addition to monitoring the operational status of the NCS, supervisor nodes in [41] are also able to take over operation of factory floor machines in case of controller failure. Supervisors can either be passive or active.

A passive supervisor will only take over control of the factory floor machines after the failure of all other controllers [41]. Typically, for a multiple machine NCS, another controller would take over the operation of the failed controller's machine instead.

In contrast, an active supervisor will immediately take over control of a failed controller's machine upon detection of the failure [41]. The remaining controllers are thus only responsible for managing their own machines.

Two models were investigated in [41]: the first with one supervisor on top of two in-line machines and the second with a single supervisor on top of three in-line machines. Each individual machine is based on that in [17] using unmodified Gigabit Ethernet [10].

A simulation study was carried out in [41] and it was shown that both passive and active approaches are able to fulfill the required real-time control system criteria. However, in case of the three machine scenario, the active supervision approach is preferable to keep a more balanced control traffic load across the network.

2.4.3 Fault-Tolerant Actuation

An actuator level fault-tolerant design was proposed in [42] specifically designed for the electrical steering systems in vehicles. Since a vehicle's steering system is critical to passenger safety then, in case of the occurrence of a fault, a fault-tolerant design must maintain the vehicle's ability to steer until it is brought to a safe stop.

The work in [42] studied the fault-tolerance of a proposed electrical steering system. The presented fault-tolerant architecture utilized a dedicated AC motor design in conjunction with a cheap voltage measurement system in order to ensure that all relevant steering system faults are successfully detected. Instead of duplicating the AC motor, the proposed architecture makes use of a double stator AC motor in order to provide fault-tolerance.

The fault-tolerant capabilities of the proposed work in [42] were successfully demonstrated on the electrical steering system of a warehouse truck.

2.4.4 CAN Enhanced Layer

A node level fault-tolerant NCS architecture was proposed in [43] based on the CAN protocol. The proposed architecture builds up fault-tolerance on top of the CAN protocol without modifications to either the CAN protocol itself or the CAN nodes' hardware.

The proposed work in [43] mainly focused on providing critical fault-tolerance services such as node failure detection and site-membership in a distributed CAN. To that end, a systematic model of CAN was defined then the drawbacks of the unmodified CAN

protocol for fault-tolerant communication were outlined and subsequently solved by the proposed system.

The proposed work in [43] resulted in a set of low-level protocols that are run in software on top of the unmodified CAN system in order to provide node level fault-tolerance.

2.4.5 Fault-Tolerant Flexible Time-Triggered Communication over CAN

A network fabric level fault-tolerant NCS architecture based on FTT-CAN was proposed in [44]. The proposed fault-tolerant architecture takes into account faults caused by electromagnetic interference, defects in addition to external faults.

The proposed work in [44] employed a replicated network fabric using bus guardians. Additionally, the network master nodes were also replicated and a mechanism was proposed to guarantee correct synchronization of the master replicas.

A set of experiments were carried out on a prototype implementation of the proposed architecture in [44] and the fault-tolerance of the system under study was demonstrated successfully.

2.4.6 CAN Based Infrastructure for Dependable Systems

A network fabric fault-tolerant NCS architecture was proposed in [45] based on the CAN protocol. The proposed architecture was named CAN-Based Infrastructure for Dependable Systems (CANbids). The proposed CAN architecture aims to improve data consistency, error containment, fault-tolerance and clock synchronization.

Data consistency in [45] is maintained by a device called a CANsistant which is capable of detecting certain inconsistencies in data transmitted over the CAN protocol.

Additionally, error containment is enabled in [45] through the use of a proposed star topology called CANcentrate which is able to disconnect any CAN nodes or links that fail from the rest of the network.

Moreover, in order to implement network fabric fault-tolerance to protect against single points of failure on the fabric level, the proposed star topology in [45] was modified through active replication. The resulting topology was called ReCANcentrate.

Finally, a clock synchronization subsystem was developed in [45] that is able to tolerate its own faults.

2.4.7 Parallel Redundancy Protocol and High-Availability Seamless Redundancy

Two recent approaches for network fabric fault-tolerance are Parallel Redundancy Protocol (PRP) and High-Availability Seamless Redundancy (HSR). Both are standardized in IEC 62439-3 [36] and can be utilized with a wide variety of communication protocols.

Both PRP and HSR make use of dual interface nodes [36]. In PRP [36], the network fabric is duplicated to form two parallel redundant LANs as in Section 2.3.4. Each node is connected to both independent LANs: one per network interface. All transmitted packets are duplicated across the independent LANs to achieve redundancy. In case of failure of a single component in one LAN, the other parallel LAN is unaffected and the overall control system is able to tolerate the failure. At the receiver, the earliest arriving packet is processed while the other is discarded.

HSR [36], similar to PRP, employs dual interface nodes. However, all nodes in HSR are connected in a ring topology. All transmitted packets between nodes are duplicated across the two interfaces with the earliest arriving packet processed by the receiver. Nevertheless, the required ring topology limits flexibility and scalability. For each added node in the network, the forwarding delays increase leading to longer round trip times as well as increased overall latency.

2.4.8 RSTP-based Network Fabric Fault-Tolerant NCS

A network fabric fault-tolerant architecture based on unmodified Ethernet [10] and utilizing the Rapid Spanning Tree Protocol (RSTP) [46] was proposed in [47].

The proposed fault-tolerant architecture in [47] was shown analytically (through an exhaustive logical traffic analysis) and through simulations to be able to tolerate any single network fabric failure in either the links, interfaces or switches while still fulfilling the required overall real-time control constraints.

Rapid Spanning Tree Protocol Background

In Ethernet, the presence of redundant links can lead to the formation of forwarding loops in the network (which can cause major network outages and packet delivery disruptions). The Spanning Tree Protocol (STP) was developed in order to prevent the formation of such forwarding loops thereby guaranteeing a loop-free network.

Afterwards, the Rapid STP (RSTP) [46] was developed to improve upon STP by offering faster network convergence times while maintaining backwards compatibility with older STP devices [48]. With RSTP, network convergence time is typically in the order of seconds instead of in the order of minutes as in STP [49].

In RSTP [46], all switches exchange Bridge Protocol Data Units (BPDUs) every *Hello Interval*. The *Hello Interval* is a configurable parameter but is set by default to 2 seconds [48]. The BPDUs allow the switches to exchange status information about the network topology and to elect the root bridge in order to build the spanning tree for the network.

Each bridge is assigned a *Bridge Identifier* which is used to determine the priority of the switch during the root bridge election process. A lower value for the *Bridge Identifier* implies a higher priority thus the switch with the lowest value is elected as the root bridge [48].

BPDUs are also used as a failure detection mechanism [46]. Since BPDUs are exchanged every *Hello Interval*, the lack of received BPDUs on a particular port would indicate the failure of the neighboring link or switch on that port. Subsequently, this information is exchanged with the remaining switches in order to update the network topology.

The ports belonging to each switch can operate in one of several roles: Root Port (RP), Designated Port (DP) or Alternate Port (AP) [48]. A RP is the port that is considered to be on the closest path to the root bridge. An AP is the best alternate path to the root bridge other than the root port. An AP is considered as a backup port and kept inactive until required. In case of failure, the AP is activated by switching it to a forwarding state. Finally, a DP is a typical non root port that is connected to an active link and kept in a forwarding state.

Model Description

The proposed fault-tolerant NCS in [47] employed multiple switches interconnected through several main links. Additionally, dual interface nodes were utilized with each network interface connected to an independent switch. A simplified illustration of the proposed architecture is shown in Fig. 2.8 [47].

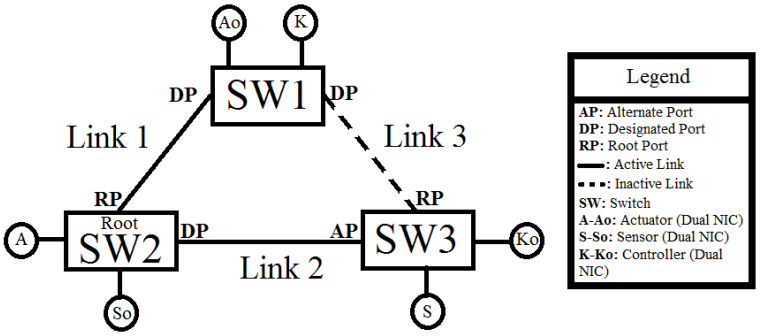

FIGURE 2.8: Simplified RSTP-based Network Fabric Fault-Tolerant Architecture

The proposed architecture in [47] guarantees the existence of multiple redundant paths between the network nodes to be utilized in case of fabric failures. Moreover, for each transmitted packet four copies are sent: two across each interface addressed to the receiving node's dual interfaces.

It was shown in [47], both analytically and through simulations, that the proposed RSTP-based network fabric fault-tolerant architecture is able to withstand any single network fabric failure. The investigated failures included every possible individual link, switch or interface failure. It was shown that the proposed architecture fulfills the required real-time control constraints both under fault-free conditions and in case of any single fabric failure.

It can be argued that the traffic overhead associated with the implementation of fault-tolerance for the proposed architecture might be negligible for small systems with a limited number of nodes. However, this overhead could turn into a scalability bottleneck for larger systems with tight control deadlines.

Chapter 3

Fault-Tolerant Wireless Networked Control Systems

This chapter focuses on the design of reliable fault-tolerant WNCSs. Two WNCS architectures are proposed: the first with controller level fault-tolerance utilizing a wired backbone and the second with both controller level as well as network fabric level fault-tolerance on the critical wireless inter cell backbone.

3.1 Fault-Tolerant WNCS with Wired Backbone

The first proposed WNCS is based on unmodified IEEE 802.11b [21]. The proposed model utilizes a wired backbone which is used for the implementation of 1-out-of-3 controller level fault-tolerance. This work builds upon and expands the 1-out-of-2 controller level FT WNCS presented in [30].

In this section, the proposed model is detailed and subsequently modeled using OPNET Network Modeler [50]. It will be shown that the proposed system satisfies all required control constraints including zero dropped or over-delayed packets.

Moreover, the interference resilience of the proposed system is quantified. Subsequently, several performance optimizations are investigated for the purpose of improving the overall system's interference tolerance.

3.1.1 Model Description

The proposed FT WNCS is composed of three cells, each representing an industrial machine, concatenated together to form an assembly line. Each cell is composed of 30 sensors, 1 controller, 30 actuators and 2 APs as in [26]. The Sensors and Actuators (SAs) belonging to each cell are divided equally into two groups of 15 SAs; each group of 15 SAs communicates wirelessly over one of the two APs belonging to the cell.

Thus, the overall proposed system is composed of 90 sensors, 3 controllers, 90 actuators and 6 APs. The channel allocation scheme, illustrated in Fig. 3.1, is employed. The APs belonging to cell 1 operate on Ch1 and Ch11 respectively while those belonging to cell 2 operate on Ch8 and Ch4 respectively. Finally the APs belonging to cell 3 reuse Ch1 and Ch11 respectively as those are placed furthest away from the APs in cell 1. This channel allocation scheme aims to maximize the frequency separation between the channels employed by the proposed system's APs in order to alleviate the effect of channel interference similar to the work in [30, 51].

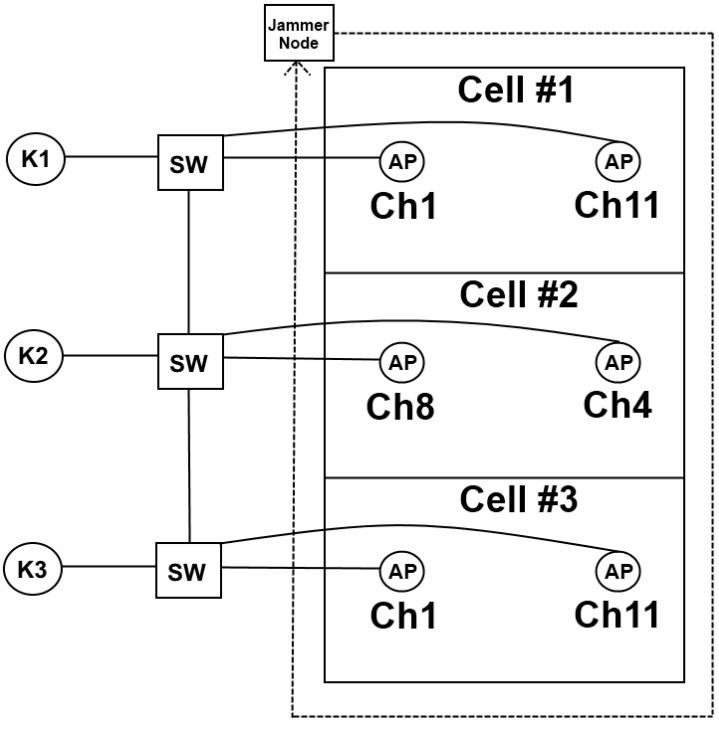

FIGURE 3.1: Channel Allocation and Jammer Trajectory

In the proposed system, each cell is individually managed by its own controller during normal operation (in the absence of failures). However, to implement controller level fault-tolerance, each controller must be ready to take over the operation of any other

cell in case of failure of its main controller. Thus, every sampling period, each sensor sends 10Bytes of data to all three controllers. This 10Byte control word is sufficient for simulating On/Off control with additional room for extra possible information [26]. For each cell, the cell's main controller must process the received data from its sensors then send a 10Byte control word to each of its actuators. Moreover, watchdog packets are exchanged twice in every sampling period as in [30] between every pair of controllers in order to allow for the detection of the failure of any of the three controllers. All control traffic is transmitted using the UDP protocol instead of TCP to decrease network congestion due to acknowledgments [28].

The model specifications are summarized in Table 3.1.

TABLE 3.1: Summary of Model Specifications

Total Number of Sensors/Actuators	90
Total Number of Controllers	3
Total Number of APs	6
Wireless Protocol	IEEE 802.11b
Sampling Period (Guard Time)	40ms (4ms)
Watchdog Period (Guard Time)	20ms (2ms)
Control Word Packet Size	10Bytes
Nodes' Short Retry Threshold	7
APs' Buffer Size	256000bits

3.1.2 Interference Model Description

In order to study the adverse impact of interference on the proposed WNCS and to quantify its interference tolerance, jammers are employed. A jammer node can be used to generate intentional interference on a wireless channel's frequency in order to disrupt communication on that particular channel. The reason behind the usage of such jammer nodes, in the context of factory automation, is to model worst-case ambient interference in the environment along the same lines as in [52]. Moreover, it was concluded in [18] that factory floor operations such as welding do not cause interference on the ISM band.

Hence, for the purpose of this study, a single band jammer is used as in [27]. The utilized jammer is configured to follow the trajectory shown in Fig. 3.1 to induce interference over all studied workcells. The interference tolerance of the system will be quantified by the maximum file size that the jammer can continuously transmit without violating the control system constraints.

3.1.3 Control System Constraints

As a real-time control system, the proposed model must adhere to certain constraints. These constraints apply to both the system's normal control traffic (sensor, controller and actuator traffic) as well as the watchdog traffic necessary for fault-tolerance.

For the control traffic, the overall end-to-end delay for packets transmitted from the sensors to the controllers and subsequently from the controllers to the actuators must not exceed the system's sampling period. Moreover, zero packet drops must be guaranteed. Similarly, for the watchdog traffic, zero packet drops must be ensured. However, the end-to-end delay for the watchdog traffic between the controllers must not exceed half the system's sampling period as in [30]. This is to allow sufficient time for another controller to take over operation in case of failure of any of the controllers.

For all end-to-end delays, a 10% guard time is employed for control system deadlines as in [30]. Table 3.2 presents a summary of the real-time system's constraints.

Table 3.2: Summary of Control System Constraints

Control End-to-End Delay Deadline	36ms
Control Packet Drop Threshold	0packets
Watchdog End-to-End Delay Deadline	18ms
Watchdog Packet Drop Threshold	0packets

3.1.4 Unicasting Approach

One possible approach to implement the traffic necessary for system fault-tolerance is for all sensors to transmit three copies of their control data; one unicast packet addressed for each controller. The controller responsible for each cell subsequently processes its sensors' data and generates one control packet for each actuator within its assigned cell. In case of failure of any controller, one of the remaining operational controllers will take over control of the failed cell in addition to its own assigned cell.

The advantage of this unicast approach is its simplicity; minimal changes are required in comparison to a similar WNCS without fault-tolerance. However, the main problem with this approach is its bandwidth inefficiency. The amount of packets transmitted by the sensors over the wireless links is tripled since a copy must be sent to each of the

three controllers. Such an immense traffic increase is expected to cause heavy network congestion as well increased contention between the wireless nodes.

This expectation was verified through OPNET simulations which demonstrated that, using the unicast approach, the resulting system is unable to meet the required control system constraints as defined in Table 3.2. Chiefly, a significant number of control packets transmitted over the wireless links were dropped due to both exceeding the retry threshold at the sensor nodes as well as overflowing the buffers at the APs.

3.1.5 Multicasting Approach

Compared to the unicasting approach, a more efficient way to implement the traffic necessary for fault-tolerance is to utilize IP Multicasting [53].

To implement such an approach, a static RP scheme was chosen where each AP was configured as an RP as in [30]. Thus, each sensor is able to transmit a single multicast packet over the wireless link instead of multiple unicast copies. The mutlicast stream is then replicated at the RPs and subsequently transmitted across the wired high-bandwidth backbone to all controllers registered as members of the corresponding multicast group at the RPs. Thus, the traffic over the bandwidth constrained wireless links is significantly reduced.

The proposed fault-tolerant model utilizing multicasting was simulated under a variety of different scenarios. In scenario 1, the proposed model was simulated in the Fault-Free (FF) case in the absence of external interference. Subsequently, the maximum interference tolerable by the proposed system was quantified under different scenarios using the single band jammer shown in Fig. 3.1. This interference study was carried out for the FF case in scenario 2 as well as for the Fault-Tolerant (FT) cases where 1 controller or 2 controllers failed in scenarios 3 and 4 respectively.

Table 3.3 summarizes the results of the 4 simulated scenarios. All presented results were subjected to a 95% confidence analysis, as summarized in Appendix A, to offset the non-deterministic nature of the employed protocols. The presented delays include all packet transmission, propagation, queuing, encapsulation and decapsulation delays. Processing delays, which are hard to quantify and application as well as hardware dependent, were assumed to be negligible for the purpose of this study [25].

TABLE 3.3: Maximum Jammer File-Size and Maximum End-to-End Delays for the Simulated Scenarios

Note: All results represent the 95% confidence interval

Scenario		**File-Size (KB)**	**S→K Delay (ms)**	**K→A Delay (ms)**
1	FF	Noiseless	[0.85-0.88]	[6.5-7.81]
2	FF	1.25	[0.89-0.93]	[7.04-8.2]
3	FT-K_1	1.25	[0.87-0.91]	[8.42-9.75]
4	FT-K_1-K_2	1.25	[0.86-0.89]	[8.87-10.09]

It is important to note that, for all presented scenarios, the proposed system using multicasting was able to fulfill all required control system constraints as defined in Table 3.2. In other words, all control traffic end-to-end delays did not exceed the required 36ms deadline while all watchdog end-to-end delays did not exceed the required 18ms deadline. Moreover, no control or watchdog packets were dropped.

3.1.6 Improving Interference Resilience

It can be observed from the results presented in Table 3.3 that the observed control traffic end-to-end delays are much smaller than the maximum possible 36ms delay constraint. The system's inability to tolerate higher interference is because of the occurrence of control packet drops over the wireless links due to both buffer overflows at the APs in addition to exceeding the transmission retry threshold at the sensor nodes thereby violating the system control constraints.

In IEEE 802.11 [21], the number of retransmission attempts for a certain frame are specified using two node parameters: the Short Retry Limit and the Long Retry Limit [54]. If the transmitted frame is larger than the RTS threshold then the Long Retry Limit is used otherwise the Short Retry Limit is used. Thus, for the proposed system, the maximum number of retransmissions is specified by the Short Retry Limit since the RTS/CTS mechanism is disabled.

In order to overcome the observed control packet drops under interference, larger AP buffer sizes as well as larger short retry limits for the sensor nodes are utilized. The impact of those parameters on the system's interference resilience and on the observed control packet delays is studied. Thus, the short retry limit for the sensor nodes is increased to 255 which is the maximum supported value as defined by the standard [21].

Moreover, the AP buffer sizes are increased to 64MBytes, available in commercial APs such as [55], in order to eliminate buffer overflows

OPNET simulations were carried out to investigate the impact of the aforementioned performance optimizations on the proposed system. The focus was on quantifying the maximum interference tolerable by the modified system without violating the control system criteria.

Figure 3.2 shows a sample result (for several seeds) from the fault-free scenario of the delay between a controller and an actuator under the maximum tolerable interference. The x-axis represents the simulation time (in minutes and seconds) while the y-axis represents the observed delay (in seconds). Note that the observed delays are less than the 36ms deadline.

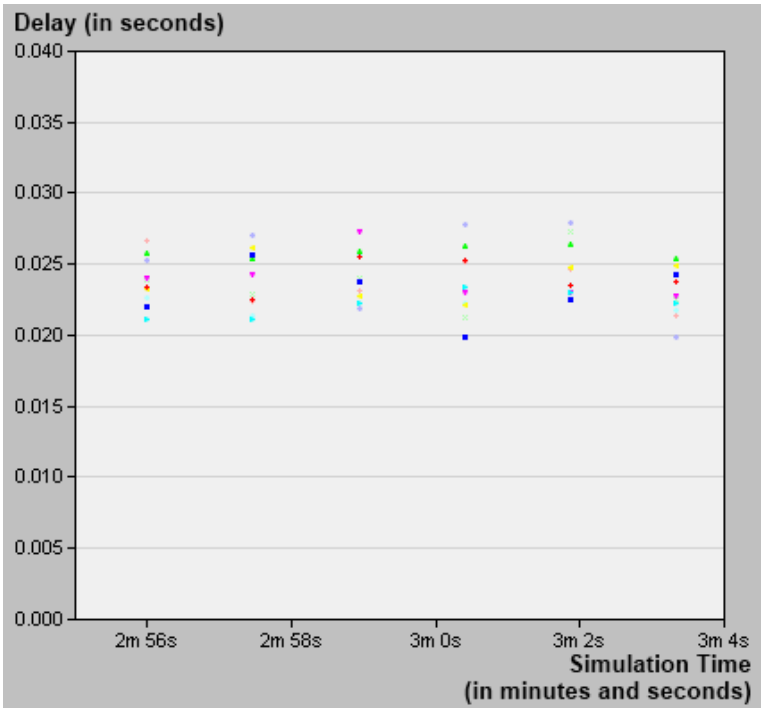

FIGURE 3.2: K→A Delay (several seeds) for the FF Scenario with a 6.5KB Jammer

Table 3.4 presents an overview of the results for all studied scenarios after a 95% confidence analysis.

The results obtained from OPNET simulations for the optimized model show that total end-to-end delays, not control packet losses, are the key measures of adherence to the control system criteria. Through the aforementioned optimizations, the interference

Table 3.4: Maximum Jammer File-Size and Maximum End-to-End Delays for the Simulated Scenarios based on the Optimized System

Scenario		**File-Size (KB)**	**S→K Delay (ms)**	**K→A Delay (ms)**
2	FF	6.5	[1.81-1.9]	[30.65-32.46]
3	FT-K_1	6.25	[1.76-1.82]	[30.84-32.91]
4	FT-K_1-K_2	6	[1.68-1.72]	[29.34-32.23]

resilience of the proposed system was increased by at least 380% without violating the real-time control criteria.

3.2 Fault-Tolerant WNCS with Wireless Backbone

The second proposed WNCS is based on unmodified IEEE 802.11g [21]. The proposed model utilizes a wireless backbone which is not only used for the implementation of 1-out-of-2 controller level fault-tolerance but also for network fabric fault-tolerance across the critical wireless backbone. This work builds upon the 1-out-of-2 controller level WNCS presented in [32] by introducing PRP [36] on the critical wireless backbone link. PRP is employed not only to improve system reliability but also to improve performance across the wireless backbone.

In this section, the proposed model is detailed and subsequently modeled using OPNET Network Modeler [50]. It will be shown that the proposed system satisfies all required control constraints including zero dropped or over-delayed packets. The focus of the study will be on the improvement in performance due to the use of PRP. Finally, the interference resilience of the PRP-WLAN backbone is quantified under various scenarios.

3.2.1 Model Description

The proposed WNCS is composed of two industrial workcells as shown in Fig. 3.3. Each cell is composed of a controller, several SA pairs and a single AP. A wireless backbone is employed to interconnect between the two cells. Due to the high amount of traffic on the backbone necessary for the implementation of controller fault-tolerance as well as the stringent control system constraints, PRP-WLAN is employed across the wireless backbone.

Since the PRP-WLAN backbone requires two independent channels for optimum operation, the single remaining non-overlapping Wi-Fi channel is reused across the two workcells. In order to accommodate the large amount of control traffic across the cells' wireless links, the higher bandwidth IEEE 802.11g is used as in [31] instead of IEEE 802.11b. Thus, the additional throughput of IEEE 802.11g allows a single AP to accommodate the load of an entire workcell instead of having to utilize two APs as in [26]. Thus, the channel allocation for the proposed model utilizes all three available non-overlapping IEEE 802.11g channels (Ch. 1, Ch. 6 and Ch. 11) as shown in Fig. 3.3. Ch. 1 and Ch. 11 are used for the PRP-WLAN backbone while Ch. 6 is reused inside the two industrial workcells.

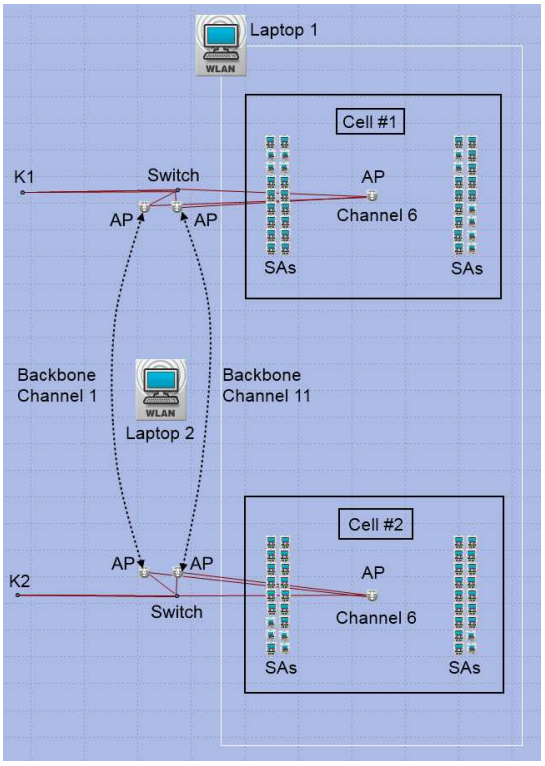

FIGURE 3.3: Proposed Model

To minimize the inter cell interference due to the reuse of Ch. 6, the two workcells are concatenated at a distance of 3m which is composed of a 2m minimum inter cell distance in addition to a 1m safety margin as in [32]. Moreover, the Packet Reception Power Thresholds (PRPTs) of the nodes belonging to each cell were specifically chosen in order to minimize the interference between the two industrial workcells. Finally, to counteract the increased contention on the cell's wireless channel, the short retry limit of the sensor nodes is increased to 255 in order to allow for a larger number of retransmission attempts as in the optimized model proposed in Section 3.1.6.

In each workcell, the sensor nodes are responsible for sensing the environment and transmitting their readings in the form of a 10Byte control word to all controllers every sampling period. The control word simulates On/Off control with additional room for extra possible information as in [26]. The cell's main controller receives its sensors' data, carries out the required processing and subsequently generates the control action to each of the actuators that is managed by that controller at that particular instance of time.

Additionally, watchdog packets are exchanged between the two controllers twice every sampling period as a controller level failure detection mechanism. When a controller fails, the lack of received watchdog packets indicates the occurrence of failure to the

other controller. The remaining controller is then able to take over the operation of the failed controller's cell within the same sampling period.

The UDP protocol instead of TCP is used for the control traffic in order to decrease network congestion due to acknowledgments [28] while TCP is used for the watchdog traffic for increased reliability.

Table 3.5 presents a summary of the proposed WNCS specifications.

TABLE 3.5: Summary of Model Specifications

Parameter	Value
Total Number of Sensors/Actuators	36
Total Number of Controllers	2
Total Number of Workcell APs (Channels)	2 (Ch. 6 reused)
Total Number of Backbone APs (Channels)	4 (Ch. 1 and Ch. 11)
Wireless Protocol	IEEE 802.11g
Transmission Data Rate	54Mbps
Node Transmit Power	1mW
Sampling Period (Guard Time)	40ms (4ms)
Watchdog Period (Guard Time)	20ms (2ms)
Control Word Packet Size	10Bytes
Control Transport Layer Protocol	UDP
Watchdog Application Layer Protocol	FTP
Nodes' Short Retry Threshold	255
APs' Buffer Size	256000bits

3.2.2 Interference Model Description

In order to evaluate the performance improvements offered by the PRP-WLAN backbone, the proposed system is studied under different interference scenarios. Single channel as well as dual channel interference scenarios are investigated. It is important to note that, in all studied scenarios, the workcells themselves were not subjected to interference.

A laptop pair exchanging files over FTP was used in order to simulate external interference. This interference model simulates medium congestion caused by external traffic in a neighboring wireless network operating on the same channel(s) as in [27, 39]. In order to maximize the interference on the PRP-WLAN backbone, one of the two laptops is positioned at the center of the wireless backbone links. The other laptop follows the trajectory illustrated in Fig. 3.3.

For the simulated industrial environment, ISM band interference was employed as the only potential source of interference given that typical factory floor operations such as welding do no cause interference on the ISM band as concluded in [18].

Table 3.6 summarizes the interference model specifications. Interference-Free, Single Channel and Dual Channel interference scenarios are investigated.

TABLE 3.6: Interference Model Specifications Summary

Parameter	Value
Inter Request Time	0.5s
Wireless Protocol	IEEE 802.11g
Transmission Data Rate	54Mbps
Interference Node Transmit Power	5mW
Interference Application Layer Protocol	FTP

Interference-Free Scenario

To establish a benchmark against which the performance of the PRP-WLAN backbone under interference can be compared, the proposed system was first simulated in the absence of external interference.

It is expected that the performance characteristics of the individual channels forming the PRP-WLAN backbone to be almost identical due to the fact that traffic is duplicated across the two independent channels.

It will be shown that the employed PRP-WLAN backbone, even in the absence of interference, offers superior performance characteristics compared to an equivalent single channel wireless backbone.

Single Channel Interference

Interference was first applied on one of the two channels forming the PRP-WLAN backbone. Interference was applied using the laptop pair shown in Fig. 3.3. The file size used by the laptop pair for communication was used to quantify the interference on the channel as in [27].

Due to the symmetrical nature of the traffic across the PRP-WLAN's underlying independent channels, it is expected that interference on either Ch. 1 or Ch. 11 individually

would have an almost identical impact on the performance of the backbone. To confirm this expectation, both scenarios will be simulated.

In this scenario, since interference is only applied on a single channel while the other independent channel is unaffected, the overall PRP-WLAN backbone is unaffected.

Dual Channel Interference

As a worst-case interference scenario, interference can be applied on both the PRP-WLAN's underlying channels simultaneously as in [39]. Thus, an additional laptop pair is needed to cause medium congestion on the other channel.

Due to the nature of the applied interference, a diminishing of the performance improvements offered by PRP is expected. However, it will be shown that PRP improves the interference resilience of the backbone compared to an equivalent single channel backbone.

3.2.3 Control System Constraints

For the proposed real-time system, both control and watchdog packet delays must not exceed their respective hard deadlines. Moreover, zero control and watchdog packet drops must always be guaranteed for correct operation. The control system constraints for the proposed model were summarized in Table 3.2. It is important to note that the watchdog delay deadline is stricter than that for the control traffic.

3.2.4 System Performance Evaluation Metrics

For each of the aforementioned simulation scenarios, relevant performance metrics were studied. These metrics allow the evaluation of the performance of the system as well as the quantification of the performance improvements offered by the PRP-WLAN backbone.

Maximum End-to-End Delay is the maximum observed control packet end-to-end delay for all packets transmitted over the PRP-WLAN backbone. This is a critical

metric for the control system due to the hard nature of the real-time deadlines; any over-delayed packet is considered lost leading to the failure of the control system.

Latency is the average end-to-end delay for all packets transmitted over the PRP-WLAN backbone. This metric serves as a measure of the average overall system performance.

Jitter is the packet delay variation for all packets transmitted over the PRP-WLAN backbone.

3.2.5 Results and Analysis

The aforementioned scenarios were simulated on OPNET Network Modeler. The proposed system was first simulated in the absence of interference. Subsequently, single and dual channel interference were applied on the PRP-WLAN backbone.

It is important to note that, in all presented results, the system experienced no control or watchdog packet drops. Also, all presented delays include packet encapsulation, transmission, propagation, queuing and decapsulation delays. The processing delays are also considered to be negligible based on [25].

Analysis Methodology

For all the outlined system performance evaluation metrics, a 95% confidence analysis (summarized in Appendix A) was carried out on 33 simulation seeds. Note that all values presented in the figures represent the upper bound of the confidence interval.

Interference-Free Scenario

In order to validate that the proposed system does not violate the control system constraints defined in Table 3.2, the proposed model was first simulated in the absence of external interference.

The maximum end-to-end delay results for the control traffic in the proposed system are presented in Table 3.7. From the presented results, the proposed system fulfills

the required control constraints; no control packets are dropped and all control traffic end-to-end delays meet the required real-time deadline.

TABLE 3.7: Summary of Control Traffic Maximum End-to-End Delays

Cell #	**S→K (ms)**	**K→A (ms)**	**Total S→K→A (ms)**
1	[3-3.6]	[16.5-19]	[19.5-22.6]
2	[2-2.5]	[15.9-18.5]	[17.9-21.1]

The watchdog packet delays were also studied in the simulated interference-free scenario. The calculated performance evaluation metrics are presented in Table 3.8 where K_i is the controller in cell i. From the presented results, it can be seen that the watchdog packets' real-time deadline is met. Moreover, the PRP-WLAN backbone improves the system performance for all studied evaluation metrics compared to any single backbone channel taken on its own. PRP improves the experienced jitter by 20%, maximum end-to-end delay by 13% and latency by 13%.

TABLE 3.8: Summary of Watchdog Traffic System Performance Evaluation Metrics

Watchdog Destination	**Maximum Delay (ms)**	**Latency (ms)**	**Jitter (ms)**
K_1 **Ch. 1**	[6.7-7]	[4.6-4.8]	[0.48-0.5]
K_1 **Ch. 11**	[6.7-7]	[4.7-4.8]	[0.46-0.48]
K_1 **PRP**	[5.8-5.9]	[4.4-4.5]	[0.37-0.38]
K_2 **Ch. 1**	[6.8-7]	[4.7-4.8]	[0.47-0.49]
K_2 **Ch. 11**	[6.6-6.9]	[4.7-4.8]	[0.46; 0.48]
K_2 **PRP**	[5.8-6]	[4.4-4.5]	[0.37; 0.38]

The rest of the simulation scenarios will investigate the performance characteristics of the PRP-WLAN backbone under different interference scenarios. Since the individual workcells operate on an independent wireless channel from the channels employed in the PRP-WLAN backbone, therefore the performance of the workcell's control traffic will be unaffected and will remain as shown in Table 3.7.

Single Channel Interference

Interference was applied on each of the PRP-WLAN backbone's two underlying channels (Ch.1 and Ch. 11) individually. The size of the file being exchanged by the laptop pair was swept in order to quantify the impact of external interference on the performance of the PRP-WLAN backbone. As expected, as the interference file-size was increased, the performance of the channel under interference is degraded due to the congestion of the wireless medium.

For the scenario where single channel interference was applied on Ch. 1, Figures 3.4, 3.5 and 3.6 present the simulation results of the interference file-size sweep for the three studied system performance evaluation metrics.

Figure 3.4 shows the maximum observed end-to-end delays for the watchdog packets over the PRP-WLAN backbone. It can be seen, for all simulated interference file-sizes, that the PRP-WLAN backbone offers superior performance than each channel taken individually. This is because the PRP-WLAN backbone makes use of the earliest arriving packet on a packet-by-packet basis from the two underlying channels. For this metric, the experienced improvement in performance was at least 31% compared to the channel under interference for all simulated interference file-sizes.

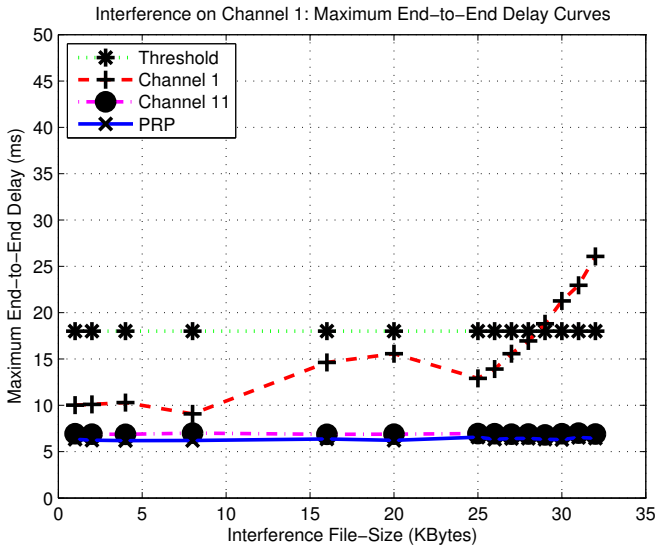

FIGURE 3.4: Maximum Watchdog End-to-End Delay Curves (Interference on Ch. 1)

Moreover, it can be seen from Fig. 3.4 that the PRP-WLAN backbone is completely immune to single channel interference as expected. As the interference file-size is increased, the overall PRP-WLAN maximum end-to-end delay is unchanged. With interference applied on one of the PRP-WLAN backbone's underlying channels, the overall delays over PRP will always be better than or identical to those of the other underlying channel which is unaffected by the interference. It can also be seen that, if a single channel system was employed, then the maximum interference file-size tolerable by the single channel under interference was 28KBytes. The threshold, in this case, represents the real-time deadline for the watchdog packets which is fixed at 18ms. The use of a PRP-WLAN backbone overcomes this single channel interference limitation by providing complete immunity to single channel interference.

Figure 3.5 presents the observed latencies for watchdog packets over the PRP-WLAN backbone. It can be seen that the PRP-WLAN backbone offers better latencies than that of the underlying channels taken individually for all simulated interference file-sizes. For this metric, the PRP-WLAN backbone improved the latency compared to the corresponding single channel under interference by at least 9%.

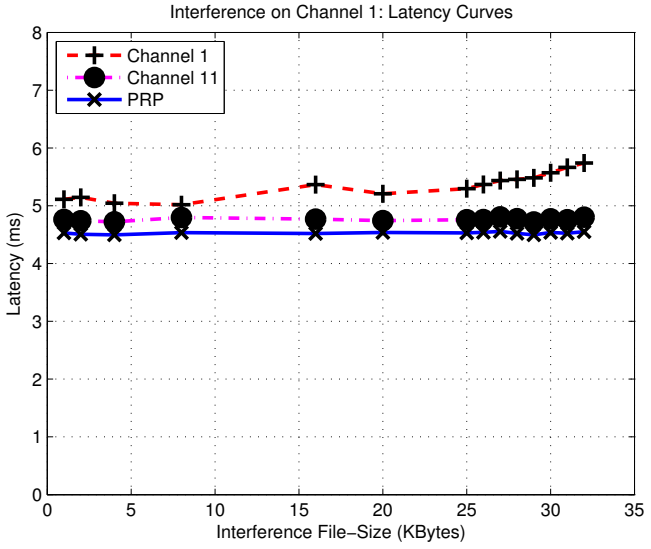

FIGURE 3.5: Watchdog Latency Curves (Interference on Ch. 1)

Figure 3.6 presents the observed watchdog packet delay variations over the PRP-WLAN backbone. It can be seen that the PRP-WLAN backbone consistently offers less jittery packet transmissions. For this metric, PRP-WLAN improved the performance by at least 35%.

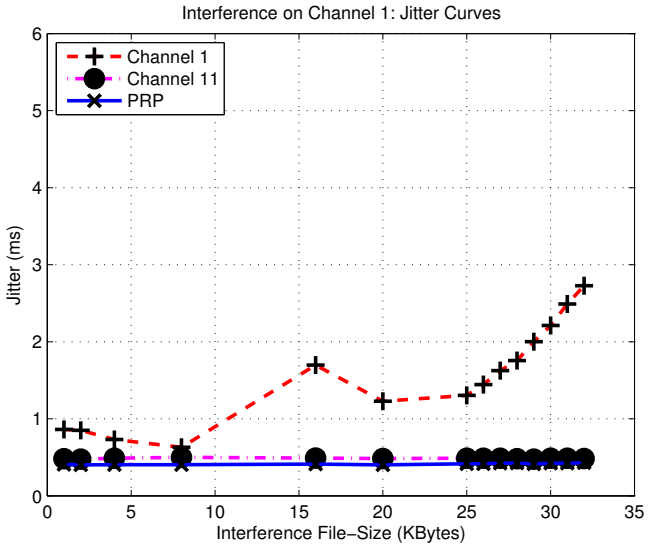

FIGURE 3.6: Watchdog Jitter Curves (Interference on Ch. 1)

In order to verify the previous single channel interference results (on Ch. 1), the same set of scenarios were repeated with interference on the other underlying channel (on Ch. 11). Figures 3.7, 3.8 and 3.9 present the simulation results for the studied performance metrics when the interference file-size was swept on Ch. 11.

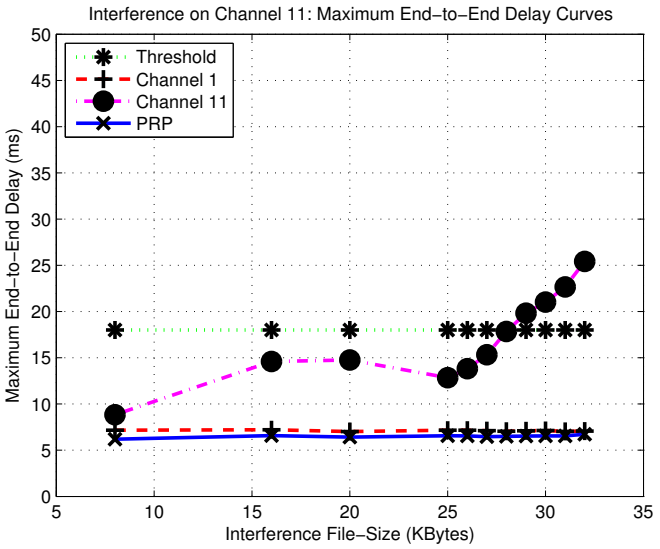

FIGURE 3.7: Maximum Watchdog End-to-End Delay Curves (Interference on Ch. 11)

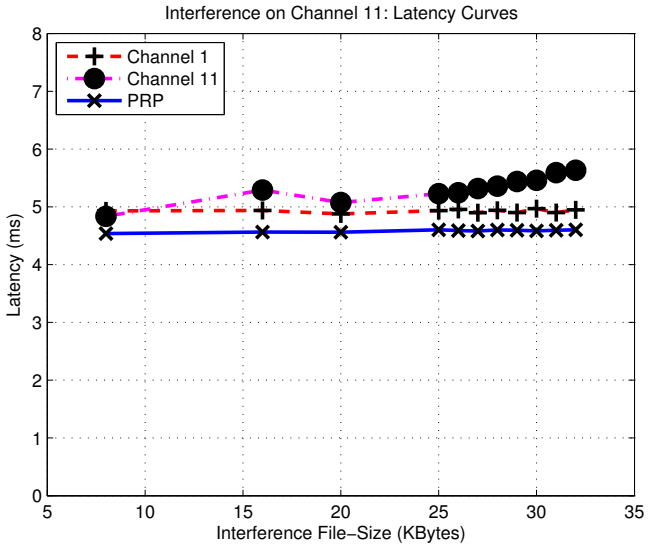

FIGURE 3.8: Watchdog Latency Curves (Interference on Ch. 11)

As expected, the PRP-WLAN backbone's overall performance with interference on Ch. 11 is almost identical to that with interference on Ch. 1. The maximum tolerable interference file-size for the single channel under interference was also found to be 28KByte. The PRP-WLAN backbone demonstrated the same noise immunity to the applied single

channel interference with performance improvements of at least 30%, 6.2% and 32.1% for the three studied metrics: maximum end-to-end delay, latency and jitter respectively.

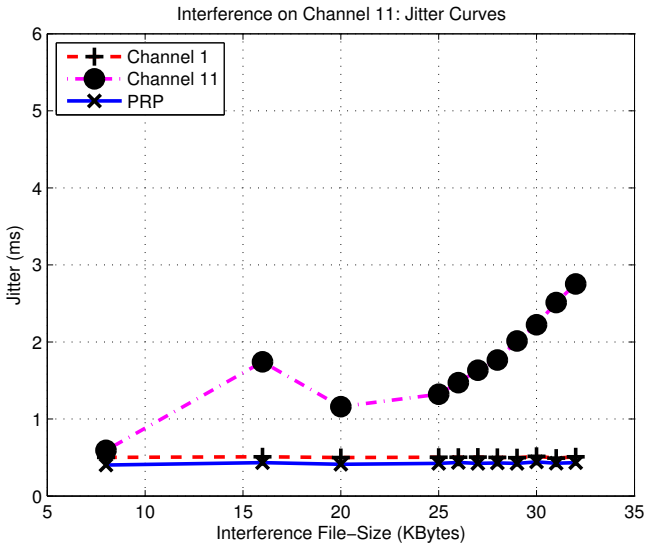

FIGURE 3.9: Watchdog Jitter Curves (Interference on Ch. 11)

Dual Channel Interference

Finally, worst-case interference was applied on the proposed PRP-WLAN backbone where both underlying channels were subjected to interference simultaneously. Figures 3.10, 3.11 and 3.12 present the file-size sweep simulation results for the three system performance evaluation metrics.

For this worst-case scenario, the PRP-WLAN backbone still continues to show noticeable improvement compared to either of the underlying channels under interference. The percentage improvement in performance offered by the PRP-WLAN backbone was found to be at least 8.9%, 6.7% and 13.4% for the three studied system performance metrics (Maximum end-to-end delay, latency and jitter respectively).

It is important to note that, since both underlying channels are subjected to external interference, the PRP-WLAN backbone is no longer completely immune to interference. As the interference file-size is increased, the observed watchdog packet delays over the PRP-WLAN backbone start to increase until the real-time control deadline is exceeded. However, it is worth noting that the maximum interference file-size tolerable by the PRP-WLAN backbone is 30KBytes, a 7% increase over that for a single channel system.

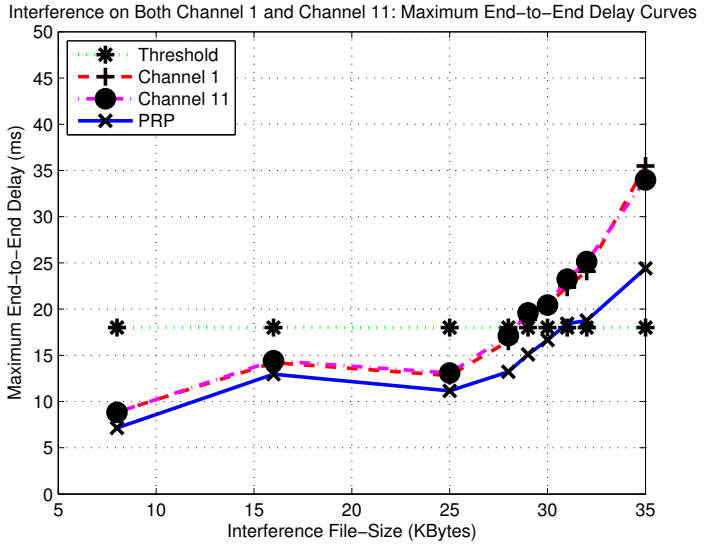

FIGURE 3.10: Maximum Watchdog End-to-End Delay Curves (Interference on both Ch. 1 and Ch. 11)

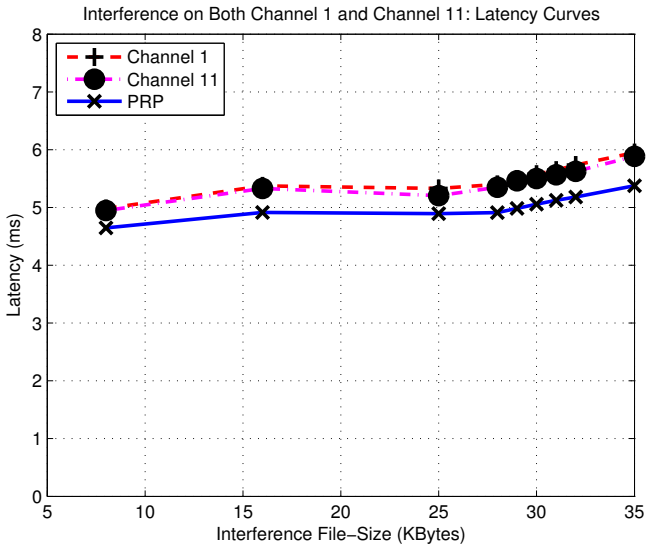

FIGURE 3.11: Watchdog Latency Curves (Interference on both Ch. 1 and Ch. 11)

3.2.6 Summary

For all simulated interference scenarios, the PRP-WLAN backbone offers better performance characteristics across all three studied system performance evaluation metrics (Maximum end-to-end delay, latency and jitter).

Under single channel interference, the PRP-WLAN backbone exhibits complete interference immunity. This is because the PRP-WLAN backbone can always make use of

the packets arriving on the other underlying channel which is not subjected to interference. The net result is that the performance of the PRP-WLAN backbone will always be greater than or equal to those of the underlying channels.

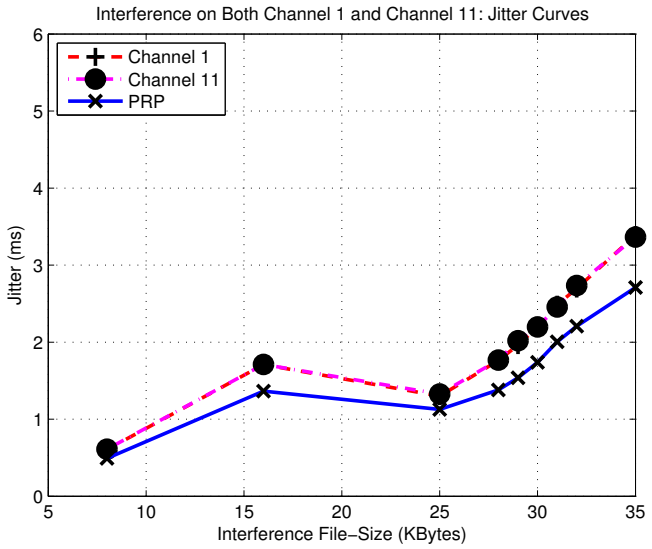

FIGURE 3.12: Watchdog Jitter Curves (Interference on both Ch. 1 and Ch. 11)

For a worst-case analysis, dual channel interference was simulated where interference was applied on both the PRP-WLAN backbone's underlying channels simultaneously. Even under this case, PRP-WLAN continued to offer better performance than any of the underlying channels taken individually. However, interference immunity was lost.

Tables 3.9 and 3.10 present the maximum watchdog packet end-to-end delay results under single channel and dual channel interference respectively. The presented interference file-size values correspond to those at: the worst PRP-WLAN percentage improvement, the maximum tolerable interference file-size and the best percentage improvement respectively.

TABLE 3.9: Maximum Watchdog End-to-End Delay Results for Interference on Channel 1 Only

File-Size (KBytes)	**Ch. 1 Delay (ms)**	**Ch. 11 Delay (ms)**	**PRP Delay (ms)**
8	[8.53-9.08]	[6.71-7]	[6.01-6.21]
28	[15.93-16.95]	[6.67-6.9]	[6.19-6.44]
32	[23.04-26.08]	[6.65-6.9]	[6.18; 6.45]

Table 3.11 summarizes the worst and best percentage improvements for all three studied system performance metrics under the studied single and dual channel interference

scenarios. The results presented in this table where obtained from the figures previously shown for each studied performance metric under the different interference scenarios.

Table 3.10: Maximum Watchdog End-to-End Delay Results for Interference on both Channel 1 and Channel 11

File-Size (KBytes)	**Ch. 1 Delay (ms)**	**Ch. 11 Delay (ms)**	**PRP Delay (ms)**
8	[8.24-8.86]	[8.3-8.83]	[6.82-7.14]
30	[19.41-20.53]	[19.16-20.44]	[15.78-16.66]
35	[32.73-35.48]	[31.33-33.98]	[22.81;24.41]

Table 3.11: PRP Percentage Improvement Summary ([Worst, Best] %)

Metric	**Single Channel Interference**	**Dual Channel Interference**
Maximum	[30, 73.6]	[8.9, 28.2]
Latency	[6.2, 18.3]	[6.7-8.8]
Jitter	[32.1, 84.2]	[13.4, 21.7]

Chapter 4

Fault-Tolerant Networked Control Systems

This chapter focuses on the design of reliable fault-tolerant NCSs. A network fabric fault-tolerant NCS based on RSTP is investigated. An optimization is proposed which halves the total amount of traffic necessary for the implementation of fault-tolerance while still guaranteeing the same level of reliability.

Moreover, a reliability modeling methodology is proposed for the RSTP-based [46] network fabric fault-tolerant architecture. Subsequently, a case study is presented to compare system reliability for different architectures including a PRP-based [36] network fabric fault-tolerant architecture.

Finally, an expanded two cell NCS is presented with the same degree of network fabric level fault-tolerance in addition to controller level fault-tolerance.

4.1 Optimized RSTP-based Network Fabric Fault-Tolerant NCS

The proposed optimized RSTP-based network fabric fault-tolerant architecture builds on that in [47].

4.1.1 Model Description

The proposed architecture is based on unmodified Ethernet [10] as well as unmodified RSTP [46].

The proposed architecture is composed of 16 sensors, 1 controller, 4 actuators as well as three layer 2 switches interconnected as shown in the simplified Fig. 4.1. All nodes connected to the network are equipped with dual Ethernet NICs and, as such, have two points of attachment to the network fabric. In other words, each node is connected via two NICs to two different and independent switches.

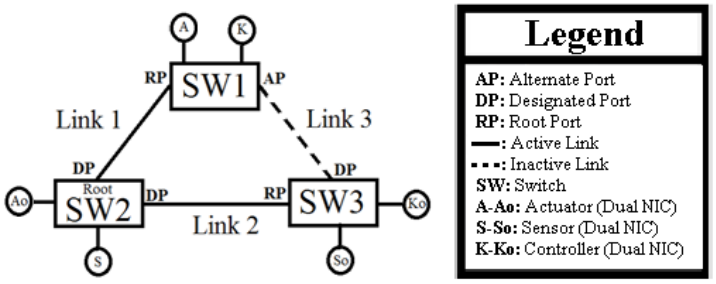

FIGURE 4.1: Simplified RSTP-based FT Architecture for Failure Analysis

Each of the 16 sensors has two interfaces: Si and Si_o where $i \subset \{1, 2, 3, \ldots 16\}$; Si is connected to SW2 while Si_o is connected to SW3. The controller also has two interfaces: K and K_o; K is connected to SW1 while K_o is connected to SW3. Similarly, each of the 4 actuators has two interfaces: Ai and Ai_o where $i \subset \{1, 2, \ldots 4\}$; Ai is connected to SW1 while Ai_o is connected to SW2. Finally, the three switches are interconnected using three Ethernet links.

For this architecture, RSTP is employed and SW2 is configured with the lowest bridge priority identifier and is therefore elected as the root bridge. Consequently, in order to prevent the formation of loops in the LAN which may cause forwarding loops and instabilities, the RSTP algorithm converges on the topology shown in Fig. 4.1 with Link 3 deactivated.

For the proposed network fabric-fault tolerant model, each sensor sends a 100Byte packet using UDP every sampling period to the controller. For fault-tolerance, two copies are sent on the sensor nodes' dual NICs: the first between Si and Ki with the second between Si_o and Ki_o. The first arriving packet is processed by the controller while the other is discarded. Subsequently, the controller transmits a 100Byte packet to each actuator.

Similarly, two copies are transmitted on the controller's dual NICs: the first between Ki and Ai with the second between Ki_o and Ai_o. In total, for the proposed model, only two copies are required for each transmitted packet instead of the four required for the model in [47]. This was made possible by optimizing the distribution of the nodes across the three central switches.

4.1.2 Control System Constraints

The proposed control system must meet definite real-time control constraints. First, the end-to-end delay for all control packets sent from the sensors to the controller and subsequently from the controller to the actuators, must not exceed the system's sampling period. Second, the proposed system must guarantee zero control packet drops; a single lost or over-delayed packet is thus considered as a cause of system failure.

Finally, the proposed architecture must be reliable against any possible single failure at the network fabric level (which includes failures of the main switches, links or NICs). Hence, the occurrence of any single network fabric failure should not have any adverse impact on the control network. The aforementioned control system constraints are summarized in Table 4.1.

TABLE 4.1: Summary of Control System Constraints

Control End-to-End Delay Deadline	1ms
Control Packet Drop Threshold	0packets
Network Fabric Fault-Tolerance Level	All Single Fabric Failures

4.1.3 Fault Analysis

Figure 4.1 illustrates a simplified representation of the proposed single-cell architecture during its fault-free operational state. For the presented system, each possible network fabric fault was individually studied in order to analyze its impact on the overall system function.

For each studied single failure scenario, the overall system was tested against the system criteria outlined in Table 4.1 to ensure that there are no violations under any possible failure scenario. This analysis mainly focuses on the network fabric fault-tolerance aspect

of the control system constraints. Subsequent simulations will validate the end-to-end delay and zero control packet drops criteria.

Since each node has two NICs, a single failure of either one of the two independent interfaces or their connecting links to the switching network will not adversely affect the overall control system. Accordingly, the presented fault analysis focuses on the study of the system fault-tolerance to single failures in any one of the three main switches or in any one of the three interconnecting links. The analysis must verify that traffic flow from the sensors to the controller and from the controller to the actuators is unimpeded for any possible single network fabric failure. In other words, at least one copy of the transmitted control data should be successfully sent over a node's dual NICs.

Table 4.2 presents the aforementioned control traffic analysis for all possible single faults; a ✓ indicates successfully communication between the corresponding nodes whereas a ✗ indicates a communication failure. It is important to note that, for all single failure scenarios, control data was successfully communicated on at least one NIC for all network nodes thereby ensuring fault-tolerance.

TABLE 4.2: Traffic Analysis for the Six Possible Failure Scenarios (SW2 Root Switch)

Scenario	$K \rightarrow A$	$K_o \rightarrow A_o$	$K_i \rightarrow A_i$	$S \rightarrow K$	$S_o \rightarrow K_o$	$S_i \rightarrow K_i$
1. Link 1 Failure	✓	✓	✔	✗	✓	✔
2. Link 2 Failure	✓	✗	✔	✓	✓	✔
3. Link 3 Failure	✓	✓	✔	✓	✓	✔
4. SW1 Failure	✗	✓	✔	✗	✓	✔
5. SW2 Failure	✓	✗	✔	✗	✓	✔
6. SW3 Failure	✓	✗	✔	✓	✗	✔

4.1.4 Simulation Study

The proposed architecture was tested and verified using OPNET Network Modeler [50] Simulations. Table 4.3 summarizes the system specifications for the simulated NCS. The proposed architecture was first tested in the absence of any failures and the control system constraints summarized in Table 4.1 were successfully verified.

Subsequently, all possible single network fabric failures were tested including the failure of any one of the dual NICs of the system's 21 nodes (16 sensors, 1 controller and 4 actuators) as well as any one of the three main switches and the three links interconnecting the switches. For each failure scenario, the simulated system was proven to be

TABLE 4.3: Simulated System Specifications

Number of Dual NIC Sensor Nodes	16
Number of Dual NIC Controller Nodes	1
Number of Dual NIC Actuator Nodes	4
Link Speed	100Mbps (or greater)
Sampling Period	1ms
Control Word Packet Size	100Bytes
STP	RSTP (IEEE 802.1D-2004)
Hello Interval	1s
BPDU Service Rate	38.2 million packets per second
Packet Service Rate	38.2 million packets per second

fault-tolerant while conforming to the control system constraints outlined in Table 4.1 with no dropped or over-delayed control packets.

For the critical failure scenario involving the root bridge (SW2), the proposed system was able to tolerate the failure and to continue normal control operation with no lost or over-delayed packets. For the duration of the failure, illustrated by the dashed rectangle in Fig. 4.2, control packets transmitted from the sensors are not successfully received at interface K whereas the other interface K_o receives the required control packets successfully. Similarly, the control traffic transmitted from the controller to the actuators is not successfully received at the interface A_o whereas the other interface A is able to successfully receive the necessary control packets from the controller.

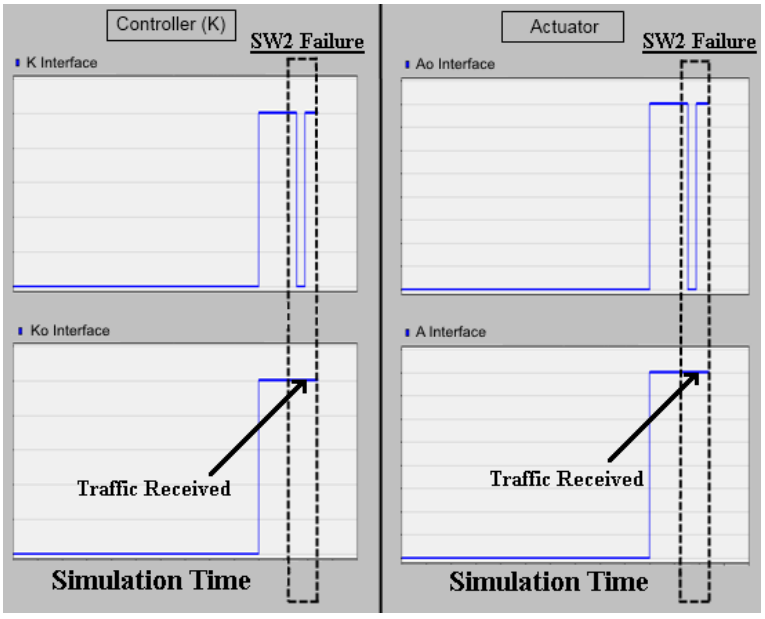

FIGURE 4.2: Failure of SW2 (Root Bridge)

4.2 Reliability Study

The focus, in this section, is on the reliability modeling of network fabric fault-tolerant architectures. A reliability modeling methodology is presented for the proposed optimized single cell RSTP-based network fabric fault-tolerant architecture presented in Section 4.1.

Additionally, for the purpose of comparison, two corresponding architectures are analyzed and modeled: a network fabric fault-tolerant architecture based on PRP [36] in addition to a simplex architecture without fault-tolerance.

Lastly, to compare the reliability of the outlined architectures, a case study is presented. The presented case study employs typical industrial parameters in the reliability modeling of the studied architectures.

4.2.1 Model Description

The number of sensors, controllers and actuators are fixed for a fair comparison of the studied network fabric fault-tolerant architectures. Control information is sent from the sensors to the controller to be processed and subsequently control actions are sent from the controller to the actuators.

PRP Architecture

The PRP network fabric fault-tolerant architecture is composed of two identical LANs operating in parallel. Each network node is equipped with dual NICs with each NIC connected to an independent and parallel LAN. All transmitted packets by the network nodes are duplicated across their two NICs and consequently are carried over the two independent LANs. At the receiving nodes, the earliest arriving packet of the two transmitted duplicates is processed while the other is discarded. Thus, redundancy is achieved through the two independent LANs operating in parallel which ensures fault-tolerance against any single network fabric level failure.

A simplified illustration of the studied PRP architecture is shown in Fig. 4.3. The simplified system is composed of a single sensor, controller and actuator (forming a

1-1-1 system). Each network node is equipped with dual interfaces; the S, K and A interfaces are connected by SW1 to form the original LAN while the S_o, K_o and A_o interfaces form the second parallel redundant LAN.

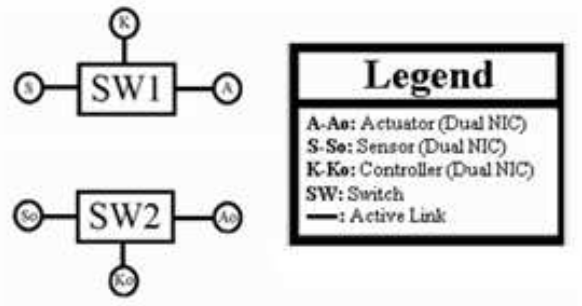

FIGURE 4.3: Simplified PRP Architecture

For any single network fabric level failure occurring in one of the two parallel LANs, the other LAN is unaffected and consequently the necessary control traffic can be communicated successfully.

RSTP-based Architecture

The proposed RSTP-based network fabric fault-tolerant architecture was previously described in detail in Section 4.1. Figure. 4.1 is a simplified illustration of the proposed RSTP-based network fabric fault-tolerant architecture (1-1-1 system).

The proposed architecture is built on the concept of dual interface nodes however, unlike in the PRP architecture, all nodes belong to the same LAN. Instead of having each node's NIC connected to a different LAN, each NIC is connected to a different switch belonging to the same LAN. Also, instead of utilizing two switches as in the PRP architecture, three switches interconnected through multiple links are employed.

4.2.2 Reliability Modeling

Reliability modeling is carried out for each of the outlined network fabric fault-tolerant architectures: the proposed RSTP-based architecture in addition to the corresponding PRP-based architecture. Additionally, reliability modeling is also carried out for a corresponding simplex architecture where no fault-tolerance is implemented in order to act as a benchmark for comparing the two studied fault-tolerant architectures.

Modeling Assumptions

For the purpose of the reliability modeling, an exponentially distributed Time To Failure (TTF) is assumed. Thus, the reliability of a particular system can be expressed as shown in Eq. 4.1.

$$R(t) = e^{-\lambda t} \tag{4.1}$$

where:

λ = failure rate of the system (in $months^{-1}$)

t = time (in $months$)

Reliability modeling is carried out on the two outlined network fabric fault-tolerant architectures in addition to a simplex architecture with no fault-tolerance. For the purpose of this study, TTF is taken in months.

Simplex Architecture

The simplex architecture is used as a benchmark since it lacks any sort of network fabric fault-tolerance. In other words, a single failure in any of the links, switches or interfaces would cause immediate failure of the entire control system.

The studied simplex architecture is composed of the same sensors, controllers and actuators as the other architectures. However, these nodes are connected directly to a single central switch as shown in Fig. 4.4.

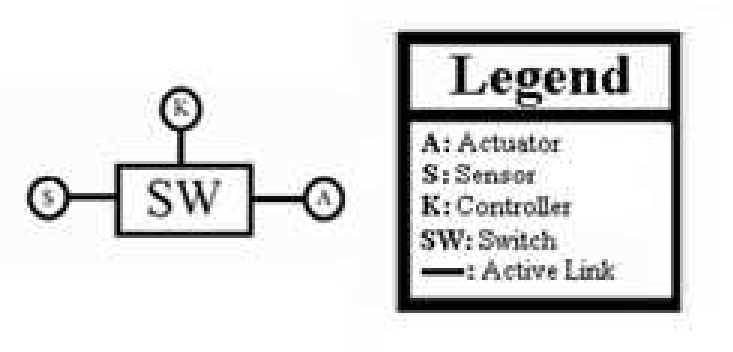

FIGURE 4.4: Simplified Simplex Architecture

Thus, the principle elements affecting the reliability modeling of such a network fabric architecture are the NICs, links and switch. To simplify the reliability modeling analysis, the NIC and connecting link failure rates are combined.

Since no fault-tolerance is implemented in the simplex architecture, any single element can be considered as a single point of failure for the entire system. Thus, the Reliability Block Diagram (RBD) of the simplex architecture can be modeled as in Fig. 4.5.

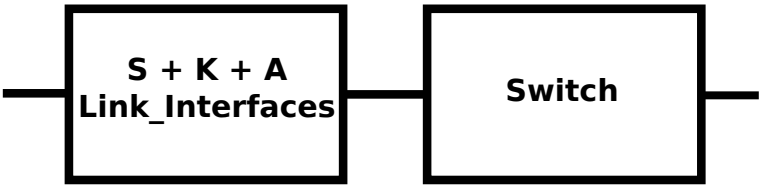

FIGURE 4.5: Simplex Architecture Reliability Block Diagram

Therefore, the reliability of such a series system can be obtained using Eq. 4.2.

$$R(t)_{Simplex} = e^{-t\times((s+k+a)\times\lambda_{link\_interface}+\lambda_{switch})} \tag{4.2}$$

where:

s	= number of sensor nodes
k	= number of controller nodes
a	= number of actuator nodes
$\lambda_{link\_interface}$	= combined failure rate of the interface and its corresponding link
λ_{switch}	= failure rate of the switch

PRP Architecture

In the PRP network fabric fault-tolerant architecture, all nodes are equipped with dual NICs. Each NIC is connected to an independent and identical LAN operating in parallel thereby achieving redundancy.

Consequently, the reliability of the PRP architecture can be modeled as two parallel simplex systems. In case of any single network fabric failure in one LAN, the parallel redundant LAN is unaffected and the overall system can continue normal operation. Thus, the RBD for the PRP architecture can be modeled as in Fig. 4.6.

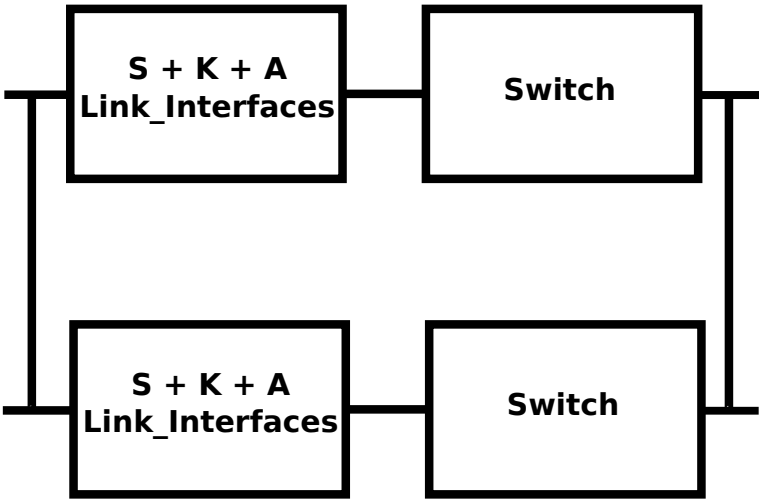

FIGURE 4.6: PRP Architecture Reliability Block Diagram

Since the two parallel LANs are independent, therefore the reliability of such a series parallel system can be obtained using Eq. 4.3.

$$R(t)_{PRP} = 1 - (1 - R(t)_{Simplex})^2 \tag{4.3}$$

where:

$R(t)_{Simplex}$ = reliability of the simplex system as defined in Eq. 4.2

RSTP-Based Architecture

For the proposed RSTP-based network fabric fault-tolerant architecture, the unsymmetrical nature of the interconnections between the network nodes and the network fabric make it infeasible to model the reliability of the system using a series parallel approach; each node is connected to the network fabric at two different points resulting in unsymmetrical behavior depending on the type of failure.

Consequently, two approaches for the reliability modeling of the proposed architecture will be presented. Both approaches will take into account the behavior of the system under all possible failure scenarios. The first approach is an exhaustive approach where all possible failure scenarios are simulated to obtain the overall system reliability. The second approach is a generalization of the first approach which aims to reduce the

required computations by exploiting the independence of multiple nodes of the same type.

Exhaustive Reliability Modeling Approach An alternative approach to the series parallel reliability modeling approach using RBDs is an exhaustive approach which involves calculating the reliability of the system for each possible component state independently. In order to obtain the overall system reliability, a summation of the reliabilities over all the up (operational) states is carried out.

To demonstrate the validity of such an approach, assume a basic system composed of two series subsystems. The failure of any one subsystem would cause the failure of the overall system. Analytically, using the RBD approach, the system reliability can be obtained using Eq. 4.4

$$R(t)_{Total} = \prod_i R(t)_i = \prod_i e^{-\lambda_i t} = e^{-t\times(\sum_i \lambda_i)} = e^{-t\times(\lambda_1+\lambda_2)} \tag{4.4}$$

where:

$R(t)_{Total}$ = reliability of the overall system
$R(t)_i$ = reliability of subsystem i
λ_i = failure rate of subsystem i (in $months^{-1}$)
t = time (in $months$)

Using the alternate exhaustive reliability modeling approach, the reliability of each possible system state must be calculated. Table 4.4 summarizes such an exhaustive analysis for the assumed basic system. For each possible state, due to the independence of the subsystems, the overall system reliability is the product of each subsystem's reliability or unreliability depending on the subsystem's state: operational or failed respectively. Note, for the overall system, a particular state is considered an up state if the overall system is operational under that state.

Table 4.4: Series System Exhaustive Reliability (Basic Series System)

Subsystem 1 State	**Subsystem 2 State**	**State Reliability**	**State Type**
0	0	$(1 - R(t)_1) \times (1 - R(t)_2)$	Down
0	1	$(1 - R(t)_1) \times R(t)_2$	Down
1	0	$R(t)_1 \times (1 - R(t)_2)$	Down
1	1	$R(t)_1 \times R(t)_2$	Up

It is important to note that, in Table 4.4, any subsystem could exist in only one of two possible states: up or down represented by 1 or 0 respectively. Since all possible states are analyzed, a simple validation can be carried out by summing up the reliabilities of all states which must and do evaluate to 1.

Using the exhaustive approach, by summing up the reliabilities of all up states shown in Table 4.4, the total system reliability can be obtained using Eq. 4.5.

$$R(t)_{Total} = \sum_{up\ states} R(t) = R(t)_1 \times R(t)_2 = e^{-t\times(\lambda_1+\lambda_2)} \tag{4.5}$$

It is important to note that, for the studied basic system, the system reliability obtained using the exhaustive reliability modeling approach in Eq. 4.5 is exactly the same as that obtained using the RBD approach in Eq. 4.4.

In applying the same exhaustive reliability modeling methodology on the proposed RSTP-based network fabric fault-tolerant architecture, the total number of possible states can be obtained using Eq. 4.6.

$$Number\ of\ States = 2^n = 2^{2\times(s+k+a)+sw+links} \tag{4.6}$$

where:

n = total number of network fabric elements (interfaces, switches and active links)
s = number of sensor nodes
k = number of controller nodes
a = number of actuator nodes
sw = number of switches
$links$ = number of active links

Nonetheless, identifying whether a particular state is an up or a down state for the proposed architecture is not simple due to the nature of the architecture with the unsymmetrical connections. As such, a traffic analysis must be carried out to verify proper control traffic flow during each possible failure scenario. That, combined with the large number of possible states from Eq. 4.6, make the analysis difficult to carry out by hand.

Therefore, a computer program was developed to carry out the required analysis using Algorithm 4.1.

Algorithm 4.1 Proposed Exhaustive Reliability Modeling Approach

```
1: function EXHAUSTIVE RELIABILITY MODELING(t)
2:     R(t)_Total ← 0
3:     for each possible state do
4:         Construct the network
5:         Discard failed network elements
6:         for each necessary control traffic flow do
7:             Find a path from the source to the destination
8:             if path exists then
9:                 State ← up state
10:            else
11:                State ← down state
12:            end if
13:            Calculate R(t)
14:            Output State Vector, State, R(t)
15:            if State = up state then
16:                R(t)_Total ← R(t)_Total + R(t)
17:            end if
18:        end for
19:    end for
20:    return R(t)_Total
21: end function
```

Consequently, using a computer program implementing Algorithm 4.1, the overall system reliability for the RSTP-based network fabric fault-tolerant architecture can be obtained.

Generalized Reliability Modeling Approach The exhaustive approach for reliability modeling of the proposed architecture becomes more infeasible as the number of network nodes, such as sensors, controllers and actuators, increases. As the number of network nodes increases, the number of scenarios that must be simulated increases exponentially leading to infeasible computational times. Thus, a generalized approach with a fixed computational time is preferable.

A generalization of the exhaustive approach could reduce the required computations by exploiting the independence and similarity in behavior of multiple nodes of the same type. From the exhaustive analysis of the simplified 1 sensor, 1 controller and 1 actuator (1-1-1) system shown in Fig. 4.1, each output vector was analyzed to identify the general behavior of sensor and actuator nodes.

Typically, the sensor and actuator dual interface nodes could only exist in one of three possible states so that the overall system can function correctly. These include the two states where only one interface is operational and the third state where both interfaces are operational. However, a particular interface may become crucial during certain failure scenarios and, as such, there are only two possible states.

After identifying the behavior of the sensor and actuator nodes during all possible failure scenarios, generalizing the exhaustive approach becomes simpler due to the independence of the nodes of the same type. As such, multiple nodes of the same type can be sufficiently modeled using a series RBD approach.

To validate the results obtained using the generalized approach, the results were compared to those obtained using the exhaustive approach for a number of different systems with multiple sensor/actuator nodes. Table 4.5 compares those results and presents the observed percentage error. For the purpose of this comparison, the system reliability was calculated at $t = 0.1$ months for nodes with fixed failure rates of 1 per month.

TABLE 4.5: Reliability Modeling Results Validation (Exhaustive Approach vs. Generalized Approach)

S-K-A	**Exhaustive R(t)**	**Generalized R(t)**	**% Error**
1-1-1	0.83697745	0.8369774	1.06E-13
2-1-1	0.803349113	0.8033491	2.34E-13
3-1-1	0.772504176	0.7725041	7.18E-14
4-1-1	0.744181539	0.7441815	3.72E-13
1-1-2	0.803349113	0.8033491	8.29E-14
1-1-3	0.772504176	0.7725041	7.18E-14
1-1-4	0.744181539	0.7441815	3.72E-13
2-1-2	0.772156974	0.7721569	1.19E-12
3-1-3	0.716897072	0.7168970	3.09E-13
4-1-4	0.669568532	0.6695685	3.58E-12

4.2.3 Case Study

A case study is carried out for a complete 16-1-4 system as in [4, 17] in order to evaluate the reliability improvements offered by the studied network fabric fault-tolerant architectures. The generalized approach, as opposed to the exhaustive approach, was used in the reliability modeling of the RSTP-based architecture due to the large number of possible states shown in Eq. 4.7 by substituting in Eq. 4.6.

$$Number\ of\ States = 2^n = 2^{2\times(16+1+4)+3+2} = 2^{47} \tag{4.7}$$

For this case study, the employed MTBFs are summarized in Table 4.6. For an exponentially distributed TTF, the $MTBF = \frac{1}{\lambda}$.

TABLE 4.6: Node MTBF Case Study Parameters

Parameter	**Value**
Industrial Switch MTBF	42.7 years [56]
Gigabit Ethernet Interface MTBF	106 years [57]
Link MTBF	212 years (assumed 2 × 106 years)

For both studied network fabric fault-tolerant architectures, the resulting system reliability is typically higher than that for a corresponding simplex system with no fault-tolerance as shown in Fig. 4.7 despite the added hardware. More importantly, the reliability of the proposed RSTP-based architecture exceeds that of the corresponding PRP-based architecture over the interval shown in Fig. 4.7.

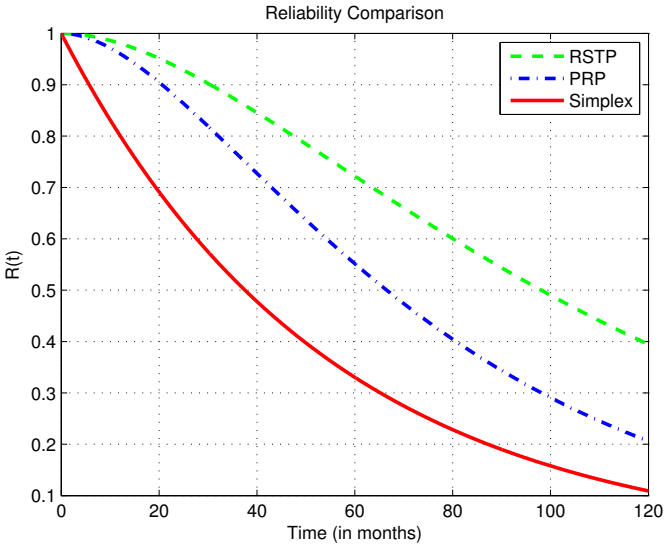

FIGURE 4.7: System Reliability Comparison (RSTP vs. PRP vs. Simplex Architectures)

Figure 4.8 illustrates the percentage improvement in overall system reliability for the architectures under study. It is evident from the positive percentage increase in reliability that the RSTP-based architecture offers a higher total system reliability compared to either the corresponding simplex or PRP architecture.

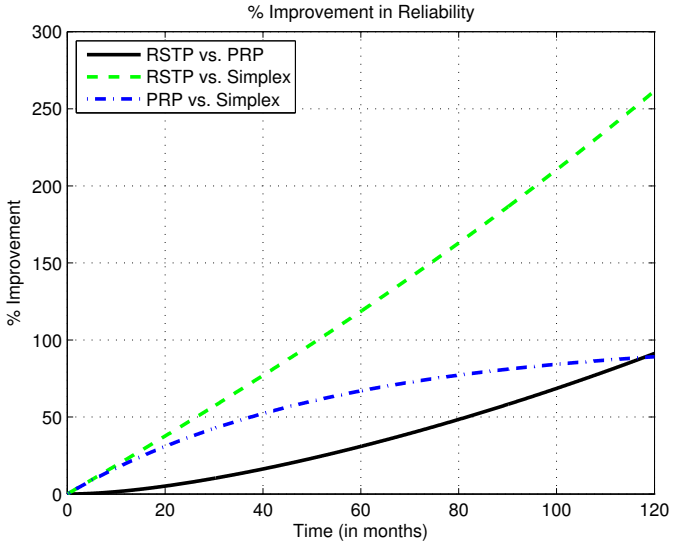

FIGURE 4.8: Percentage Improvement in Reliability vs. Time

For the time interval shown in Fig. 4.8, the fault-tolerant RSTP-based architecture demonstrated a 35% average improvement in reliability compared to the corresponding PRP-based architecture. Moreover, a maximum increase in reliability of 91% for the RSTP-based architecture was observed compared to the PRP-based architecture. Compared to the simplex system, the PRP-based and RSTP-based fault-tolerant architectures increased overall system reliability up to 89% and 261% respectively.

The RSTP-based architecture not only achieves a higher system reliability compared to both the RSTP-based and simplex architectures but is also capable of guaranteeing, with a high probability, the operation of a given NCS for a longer period of time without repair. This time interval is known as the Mission Time (MT) for which the system is guaranteed to remain operational with a predetermined minimum reliability.

From Fig. 4.7, for a minimum reliability of 0.9, the RSTP-based architecture offers an almost 435% and 48% increase in mission time ($\approx$ 30.5 months) compared to the corresponding PRP-based ($\approx$ 20.6 months) and simplex ($\approx$ 5.7 months) architectures respectively.

4.3 Extended In-Line Network Fabric Fault-Tolerant NCS

In this section, the proposed optimized single cell network fabric fault-tolerant NCS proposed in Section 4.1 is extended to two cells. The proposed extended NCS models two industrial machines working in-line as part of an assembly line requiring inter machine communication for synchronization purposes. Additionally, the extended in-line architecture provides not only network fabric level fault-tolerance but also controller level fault-tolerance.

4.3.1 Model Description

The proposed extended in-line architecture is composed of two cells each similar to that shown in Fig. 4.1. The two cells can be interconnected using one, two or three links. One the one hand, if only a single link is used then it would become a single point of failure. On the other hand, having using three links for the interconnection is impractical as the third link would automatically be deactivated by RSTP [46] in order to prevent the formation of forwarding loops. As such, two links are used for connecting between the two cells as shown in the simplified model in Fig. 4.9.

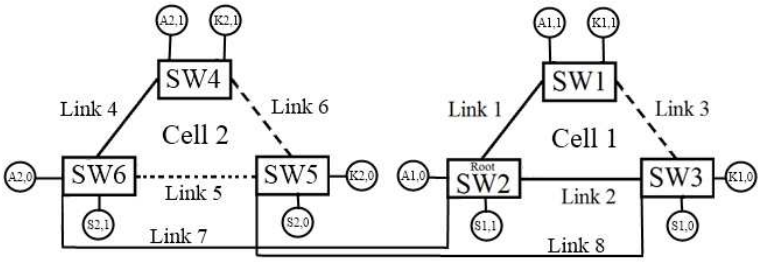

FIGURE 4.9: Simplified RSTP-based FT Extended In-Line Architecture for Failure Analysis

For the proposed architecture, the bridge priorities for the switches (SW2, SW3, SW6, SW4, SW1, and SW5) were configured with SW2 having the highest priority and SW5 have the lowest priority respectively. As such, the proposed network architecture converges to the topology shown in Fig. 4.9 with SW2 elected as the root bridge by the RSTP. Note that the subscripts i and j denote the cell number and interface number respectively.

Similarly to the single cell architecture described in Section 4.1, the control word size is set to 100Bytes. However, in order to implement controller fault-tolerance, each cell's sensors send their control information every sampling period across their dual NICs to the controllers of both cells. As such, each controller has full information regarding both cells and can at any time take over operation in case of the failure of the other controller. Subsequently, the controller responsible for a particular cell then transmits the appropriate control action to all actuators in that cell.

In order to allow for the detection of a failure of any of the controllers, watchdog packets are exchanged between the two controllers over both NICs twice every sampling period (i.e. at half the system's sampling period). The absence of received watchdog packets at a controller would indicate the failure of the other controller and consequently the remaining controller must take over operation of the failed controller's cell in addition to its own.

4.3.2 Control System Constraints

The proposed real-time control system must satisfy the control criteria previously outlined for the single cell architecture in Table 4.1. The proposed architecture must meet the outlined control criteria even in case of failure of any individual network fabric level element. All control packet end-to-end delays must be less than the control system's sampling period (i.e. 1ms). Moreover, zero control packet drops must always be guaranteed.

However, with the introduction of controller level fault-tolerance, additional real-time traffic constraints must be observed on the watchdog traffic. The watchdog end-to-end delays must be less than half the control sampling period (i.e. 0.5ms) in order to allow for the other cell's controller to take over operation in case of a controller failure. Additionally, zero watchdog packet drops must also be guaranteed.

4.3.3 Fault Analysis

The proposed extended in-line architecture will be analyzed under different failure scenarios including all potential single network fabric level failures in addition to controller failures. The analysis will initially focus om verifying that control and watchdog traffic

are not adversely affected by the occurrence of any single network fabric or controller failure. Subsequently, simulations will validate the end-to-end delay and zero packet loss requirements.

Network Fabric Level Fault-Tolerance

An analysis of all possible single network fabric failures was carried out on the proposed model. In the absence of any network fabric failures, the topology shown in Fig. 4.9 is reached according to the RSTP. A complete traffic analysis was carried out similar to that shown in Table 4.2 for the proposed in-line architecture to validate the aforementioned system control criteria.

Since all nodes are connected to the switching network at two different points, then the occurrence of a single failure at a node's NIC or connecting link will not have an adverse impact on the communication; traffic will be transmitted and subsequently received successfully using the other NIC. Moreover, the failure of any link deactivated by RSTP (such as Links 3, 5 and 6) will not have any impact on the proposed architecture. The failures remaining links (Links 1, 2, 4, 7 and 8) as well as the switches (SW1, SW2, SW3, SW4, SW5 and SW6) individually were subsequently investigated.

For all possible single failure scenarios, for any control or watchdog traffic sent between any two nodes, at least one copy (out of the two transmitted over the dual NICs) is successfully communicated over the network to the receiving node. Thus, the proposed system was proven to be fault-tolerant to any single network fabric level failure.

Controller Level Fault-Tolerance

Following the network fabric level fault analysis, controller level fault-tolerance of the proposed extended in-line architecture is investigated. Watchdog packets are utilized as the failure detection mechanism between the two controllers. The absence of watchdog packets in case of a controller failure is used as an indicator for the operational controller to take over the failed controller's cell.

The effect of the failure of each controller was individually studied and it was verified that the control system constraints are not violated; in case of failure of a single controller

the other controller is not only able to successfully receive the required control data from the sensors belonging to the failed controller's cell but also to successfully transmit the necessary control action to the affected actuators. Thus, the proposed system was proven to be fault-tolerant to any single controller failure.

4.3.4 Simulation Study

Using OPNET Network Modeler [50], simulations were carried out on the proposed extended in-line model. The proposed system was first simulated in the absence of any failures and it was verified that the real-time control system constraints were met.

All possible controller failures were individually tested and it was verified that the proposed system meets the required control criteria under all single controller failure scenarios.

Subsequently, all possible single network fabric failures were tested including the failure of any one of the dual NICs of the system's 21 nodes (16 sensors, 1 controller and 4 actuators) as well as any one of the three main switches and the three links interconnecting the switches. For each failure scenario, the simulated system was proven to be fault-tolerant while conforming to the control system constraints outlined in Table 4.1 with no dropped or over-delayed control packets.

For the critical failure scenario involving the root bridge (SW2), the proposed system was able to tolerate the failure and to continue normal control operation with no lost or over-delayed packets. For the duration of the failure, illustrated by the dashed rectangle in Fig. 4.10, at least 1 copy of the duplicated control data is successfully received at the intended destination.

In cell 1, control packets transmitted from the sensors are not successfully received at interface $K_{1,1}$ whereas the other interface $K_{1,0}$ receives the required control packets successfully. While, the control traffic transmitted from the controller to the actuators is not successfully received at the interface $A_{1,0}$ whereas the other interface $A_{1,1}$ is able to successfully receive the necessary control packets from the controller. Likewise in cell 2, control packets transmitted from the sensors are successfully received at both interface $K_{2,1}$ and interface $K_{2,0}$. While, the control traffic transmitted from the controller to the

actuators is not successfully received at the interface $A_{2,0}$ whereas the other interface $A_{2,1}$ is able to successfully receive the necessary control packets from the controller.

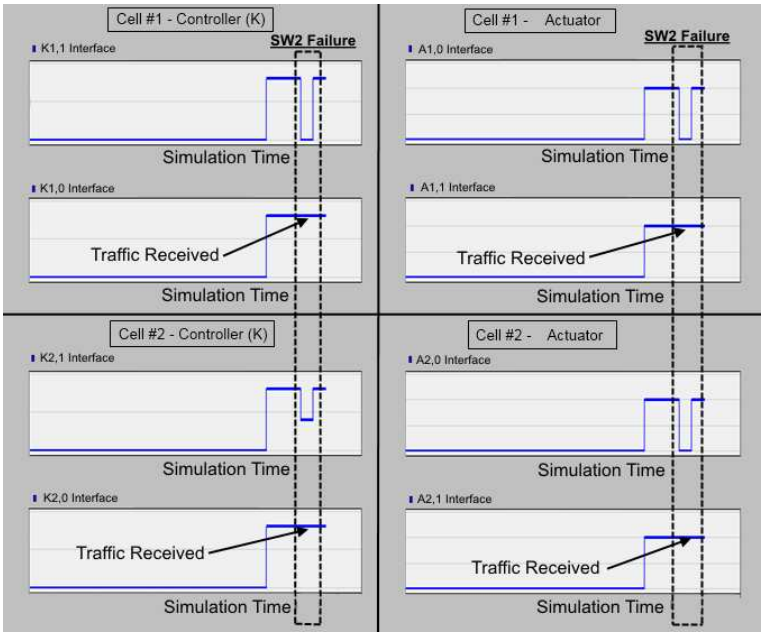

FIGURE 4.10: Failure of SW2 (Root Bridge)

Chapter 5

Conclusions

Networked Control Systems (NCSs), as opposed to traditional approaches such as point-to-point control networks, are now becoming the operative architectures in today's industry. NCSs consist of sensors, controller and actuators interconnected through a network fabric. For NCSs the network fabric is typically wired and employs network communication protocols from a wide family of deterministic and non-deterministic protocols depending on the application and the design of the NCS.

Of late, Wireless NCSs (WNCSs) have been gaining in popularity due to their ease of installation and maintenance especially in industrial applications hindered by physical cabling such as those involving moving robotic arms on an assembly line. However, WNCSs suffer from some significant drawbacks which must be tackled in the design including limited bandwidth as well as experienced interference arising from the shared nature of the wireless medium.

Fault-tolerance is becoming a crucial aspect in the design and evaluation of NCSs and WNCSs. An NCS lacking fault-tolerance can, in case of failure of even a single network node or element, experience a long and costly downtime leading to large production losses. The probability of occurrence of such failures increases dramatically especially for today's complex NCSs with a large number of nodes and, as such, fault-tolerance is fast becoming a necessity not a luxury of NCS design. Fault-tolerance can be implemented at various levels of an NCS: the sensor level, the controller level, the actuator level and/or the network fabric level.

However, the introduction of fault-tolerance requires not only additional hardware but also additional traffic overhead which may have a marked impact on the performance of the NCS. The added overhead traffic may even cause the NCS to miss its required real-time control deadlines. Therefore, minimizing the amount of overhead traffic necessary for fault-tolerance is desired.

The presented work focused on the design and optimization (modifying the design parameters in order to achieve gains in system performance evaluation metrics) of fault-tolerant NCSs and WNCSs. First, a fault-tolerant WNCS was proposed based on the unmodified IEEE 802.11b protocol. The proposed WNCS implemented 1-out-of-3 controller level fault-tolerance over three identical WNCS cells with zero meter inter cell separation connected using a wired backbone. It was proven through simulations that only through the use of multicasting can the system operate within the required real-time control constraints (i.e with no packet drops or over delayed packets). The interference tolerance of the proposed WNCS was also investigated using jammers to simulate worst case interference. The maximum interference tolerable by the proposed WNCS was quantified for all possible failure scenarios: fault-free, failure of 1 controller and failure of 2 controllers. In all scenarios, the proposed WNCS adhered to the required real-time control constraints. Proposed performance optimizations were carried out on the proposed WNCS and led to an improvement in interference resilience (the maximum tolerable interference) of at least 380%.

Moreover, an additional fault-tolerant WNCS with a reliable wireless backbone was proposed based on the unmodified IEEE 802.11g protocol. The proposed WNCS implemented 1-out-of-2 controller fault-tolerance over two identical WNCS cells connected through a fault-tolerant wireless backbone using the Parallel Redundancy Protocol (PRP). It was shown that, even without a high bandwidth wired backbone, the proposed WNCS using a PRP-WLAN backbone was able to meet the required real-time control constraints. Compared to a typical single channel wireless backbone, the proposed PRP-WLAN backbone also provided significant performance improvements which were quantified based on investigated evaluation metrics (Maximum End-to-End Delay, Latency and Jitter). The impact of external interference on the critical wireless backbone link was also investigated under a variety of interference scenarios including single

and dual channel interference. For the single channel interference scenarios, the PRP-WLAN backbone consistently offered better performance across all three studied metrics in addition to complete interference immunity. A minimum improvement of 30%, 6.2% and 32.1% was attained by the proposed PRP-WLAN backbone compared to the equivalent single channel backbone for the three studied metrics. Finally, for the dual channel interference scenario, the proposed PRP-WLAN backbone attained a minimum improvement in performance of 8.9%, 6.7% and 13.4% respectively. Additionally, despite the loss of interference immunity, the maximum tolerable interference by the proposed PRP-WLAN backbone was found to be 7% higher than for a comparable single channel wireless backbone.

Second, a network fabric fault-tolerance methodology for wired Ethernet NCSs based on the unmodified Rapid Spanning Tree Protocol (RSTP) was investigated. A performance optimization was proposed which decreases the amount of overhead traffic necessary for fault-tolerance by half while providing the same level of robustness against any single link, switch or interface failure. The proposed optimized architecture was validated analytically (through an exhaustive logical traffic analysis) and through simulations. It was shown that the proposed architecture fulfills all required real-time control constraints, with no dropped or over delayed packets, both in the fault-free case as well as under all possible single network fabric failures.

Moreover, reliability modeling of different network fabric fault-tolerant architectures was carried out to quantify system reliability (probability that the system is functioning at a certain point in time). The focus was on two main network fabric fault-tolerant architectures including the proposed optimized RSTP-based architecture as well as a PRP-based architecture. The reliability modeling methodology of the PRP-based architecture was outlined and another was developed for the proposed RSTP-based architecture. Additionally, reliability modeling of a corresponding simplex architecture was used as a baseline for the comparison between the two studied network fabric fault-tolerant architectures. A case study, employing typical industrial component parameters and failure rates, was conducted. The proposed RSTP-based architecture consistently offered higher system reliability compared to either the simplex or the fault-tolerant PRP-based architecture. It was shown that the proposed RSTP-based architecture achieves an improvement in reliability of up to 261% and 91% compared to the corresponding simplex and fault-tolerant PRP-based architectures. Moreover, it was shown that the proposed

RSTP-based architecture provides a considerable increase in achievable mission time. Thus, an NCS utilizing the proposed RSTP-based network fabric fault-tolerant architecture can remain operational for a longer period of time without repair with a predetermined guaranteed minimum reliability. For a minimum reliability of 0.9, a 435% and 48% increase in mission time was achieved by the RSTP-based architecture compared to the simplex and PRP-based architectures respectively.

Furthermore, an expanded two cell in-line NCS based on the proposed RSTP-based network fabric fault-tolerant architecture was presented. The proposed expanded in-line NCS made use of the performance optimizations carried out in the single cell architecture in order to allow for an increased amount of network nodes and consequently increased control traffic. The proposed in-line architecture not only provides network fabric fault-tolerance against any single link, switch or interface failure but 1-out-of-2 controller fault-tolerance as well. The proposed architecture was validated both analytically and through simulations and it was shown that, for all possible single failure scenarios, the required real-time control constraints are always met.

Appendix A

Confidence Analysis

All presented simulation results were subjected to a 95% confidence analysis. The confidence analysis was carried out to offset the nondeterministic nature of the studied protocols. This section details the analysis procedure.

Let:

X = Random Variable Under Study (Maximum End-to-End Delay, Latency, Jitter, ...)
μ = Average of the Random Variable X
σ^2 = Variance of the Random Variable X
X_i = i^{th} sample of the Random Variable X (obtained using a different simulation seed)
n = Number of Simulations
x = Sample Mean
s^2 = Sample Variance

$$x = \frac{1}{n}\sum_{i=1}^{n} X_i \tag{A.1}$$

$$s^2 = \frac{1}{n-1}\sum_{i=1}^{n}(X_i - x)^2 \tag{A.2}$$

Most network simulators initialize the various random number generators, employed throughout the simulation, with a certain *seed* value [50]. Thus, multiple distinct seeds are typically simulated in order to capture the randomness inherent in the utilized network protocols.

Based on the Central Limit Theorem, the sample mean of any random variable will approach that of a normal distribution as the number of samples is increased regardless of the underlying distribution of the random variable.

Thus, for a large enough number of samples, the sample mean approaches the normal mean while the sample variance approaches a scaled version of the normal variance [58].

$$x \to \mu; n \to \infty \tag{A.3}$$

$$s^2 \to \frac{\sigma^2}{n}; n \to \infty \tag{A.4}$$

The confidence level is defined as the probability that x is within a certain threshold from μ.

$$Z = \frac{x - \mu}{\sigma/\sqrt{n}} \tag{A.5}$$

where:

Z = Normal Random Variable (with Mean = 0 and Variance = 1)

$$P(-z < Z < z) = 1 - \alpha \tag{A.6}$$

where:

α = Significance Level (1 - Confidence Level)

Therefore, by using 33 simulations (i.e. n ¿ 30), the sample standard deviation s can be used instead of $\sigma/\sqrt{n}$ in order to determine the confidence interval.

For the purposes of this study, the significance level α was fixed to 0.05 for a 95% confidence level.

Appendix B

List of Publications

Parts of this work were published as follows:

1. H. Halawa, R. Daoud, H. Amer, and H. Elgebaly, "Performance Optimization for Reliable Wireless Networked Control Systems in the Presence of Interference," in *Emerging Technologies and Factory Automation (ETFA), 2013 IEEE 18th Conference on*, Sept 2013.

2. H. Halawa, R. Daoud, H. Amer, and M. Rentschler, "On the Performance of a PRP-WLAN Enabled Wireless Backbone," in *Robotics, Control and Manufacturing Technology (ROCOM), 2014 WSEAS 14th Conference on*, April 2014.

3. H. Halawa, Y. Hilal, G. Aziz, C. Alfi, T. Refaat, R. Daoud, H. Amer, and H. El-Sayed, "Network Fabric Redundancy in NCS," in *Emerging Technologies and Factory Automation (ETFA), 2014 IEEE 19th Conference on*, Sept 2014.

References

[1] J.-P. Thomesse, "Fieldbus Technology in Industrial Automation," *Proceedings of the IEEE*, vol. 93, pp. 1073–1101, June 2005.

[2] J. Nilsson, *Real-Time Control Systems with Delays*. PhD thesis, Department of Automatic Control, Lund Institute of Technology, Lund, Sweden, 1998.

[3] F.-L. Lian, W. Moyne, and D. Tilbury, "Network Design Consideration for Distributed Control Systems," *Control Systems Technology, IEEE Transactions on*, vol. 10, pp. 297–307, Mar 2002.

[4] T. Skeie, S. Johannessen, and C. Brunner, "Ethernet in Substation Automation," *Control Systems, IEEE*, vol. 22, pp. 43–51, Jun 2002.

[5] S. Bennet, *Real-Time Computer Control: An Introduction*. Prentice Hall, second ed., 1994.

[6] C. Krishma and K. Shin, *Real-Time Systems*. McGraw-Hill, international ed., 1997.

[7] Bosch, *CAN Specification Version 2.0*, 1991.

[8] "Official Site for PROFIBUS and PROFINET." `http://www.profibus.com`. Accessed: 2014-10-30.

[9] P. Marti, J. Fuertes, and G. Fohler, "An integrated approach to real-time distributed control systems over fieldbuses," in *Emerging Technologies and Factory Automation, 2001. Proceedings. 2001 8th IEEE International Conference on*, pp. 177–182 vol.1, Oct 2001.

[10] "IEEE Standard for Ethernet - Section 1," *IEEE Std 802.3-2012 (Revision to IEEE Std 802.3-2008)*, Dec 2012.

[11] Allen-Bradley, Rockwell Automation, *EtherNet/IP Performance and Application Guide*.

[12] K. Steinhammer and A. Ademaj, "Hardware Implementation of the Time-Triggered Ethernet Controller," in *Embedded System Design: Topics, Techniques and Trends* (A. Rettberg, M. Zanella, R. Dömer, A. Gerstlauer, and F. Rammig, eds.), vol. 231 of *IFIP – The International Federation for Information Processing*, pp. 325–338, Springer US, 2007.

[13] P. Grillinger, A. Ademaj, K. Steinhammer, and H. Kopetz, "Software Implementation of a Time-Triggered Ethernet Controller," in *Factory Communication Systems, 2006 IEEE International Workshop on*, pp. 145–150, 2006.

[14] P. Pedreiras, L. Almeida, and P. Gai, "The FTT-Ethernet Protocol: Merging Flexibility, Timeliness and Efficiency," in *Real-Time Systems, 2002. Proceedings. 14th Euromicro Conference on*, pp. 134–142, June 2002.

[15] F.-L. Lian, J. R. Moyne, and D. Tilbury, "Performance Evaluation of Control Networks: Ethernet, ControlNet, and DeviceNet," *Control Systems, IEEE*, vol. 21, pp. 66–83, Feb 2001.

[16] J.-D. Decotignie, "Ethernet-Based Real-Time and Industrial Communications," *Proceedings of the IEEE*, vol. 93, pp. 1102–1117, June 2005.

[17] R. Daoud, H. Elsayed, H. Amer, and S. Eid, "Performance of Fast and Gigabit Ethernet in Networked Control Systems," in *Circuits and Systems, 2003 IEEE 46th Midwest Symposium on*, vol. 1, pp. 505–508 Vol. 1, Dec 2003.

[18] R. Steigmann and J. Endresen, "Introduction to WISA: WISA – Wireless Interface for Sensors and Actuators," tech. rep., ABB, 2006.

[19] ABB, *Technical Description WISA Wireless Interface for Sensors and Actuators: Planning, Installation and Commissioning Guidelines*.

[20] D. Dzung, C. Apneseth, J. Endresen, and J.-E. Frey, "Design and Implementation of a Real-Time Wireless Sensor/Actuator Communication System," in *Emerging Technologies and Factory Automation, 2005. ETFA 2005. 10th IEEE Conference on*, vol. 2, Sept 2005.

[21] "IEEE Standard for Information technology–Telecommunications and information exchange between systems Local and metropolitan area networks–Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," *IEEE Std 802.11-2012 (Revision of IEEE Std 802.11-2007)*, pp. 1–2793, March 2012.

[22] "IEEE Standard for Local and metropolitan area networks–Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs)," *IEEE Std 802.15.4-2011 (Revision of IEEE Std 802.15.4-2006)*, pp. 1–314, Sept 2011.

[23] "IEEE Standard for Information Technology - Telecommunications and Information Exchange Between Systems - Local and Metropolitan Area Networks - Specific Requirements. - Part 15.1: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Wireless Personal Area Networks (WPANs)," *IEEE Std 802.15.1-2005 (Revision of IEEE Std 802.15.1-2002)*, pp. 1–580, 2005.

[24] S. Morris, *Automated Manufacturing Systems: Actuators, Controls, Sensors, and Robotics*. McGraw-Hill, first ed., 1995.

[25] L. Seno, S. Vitturi, and F. Tramarin, "Experimental Evaluation of the Service Time for Industrial Hybrid (Wired/Wireless) Networks under Non-Ideal Environmental Conditions," in *Emerging Technologies Factory Automation (ETFA), 2011 IEEE 16th Conference on*, Sept 2011.

[26] T. Refaat, R. Daoud, H. Amer, and E. Makled, "WiFi Implementation of Wireless Networked Control Systems," in *Networked Sensing Systems (INSS), 2010 Seventh International Conference on*, pp. 145–148, June 2010.

[27] E. Reheem, Y. El Faramawy, H. Halawa, M. Ibrahim, A. Elhamy, T. Refaat, R. Daoud, and H. Amer, "On the Effect of Interference on Wi-Fi-based Wireless Networked Control Systems," in *Communication Systems, Networks Digital Signal Processing (CSNDSP), 2012 8th International Symposium on*, July 2012.

[28] G. Boggia, P. Camarda, V. Divittorio, and L. Grieco, "A Simulation-Based Performance Evaluation of Wireless Networked Control Systems," in *Emerging Technologies Factory Automation, 2009. ETFA 2009. IEEE Conference on*, Sept 2009.

[29] M. Blanke, M. Kinnaert, J. Lunze, and M. Staroswiecki, *Diagnosis and Fault-Tolerant Control*. Springer, second ed., 2006.

[30] Y. Faramawy, M. Ibrahim, H. Halawa, A. Elhamy, E. Reheem, T. Refaat, R. Daoud, and H. Amer, "Multicasting for Cascaded Fault-Tolerant Wireless Networked Control Systems in Noisy Industrial Environments," in *Emerging Technologies Factory Automation (ETFA), 2012 IEEE 17th Conference on*, Sept 2012.

[31] T. Refaat, R. Daoud, and H. Amer, "Fault-Tolerant Controllers in Wireless Networked Control System using 802.11g," in *Industrial Technology (ICIT), 2012 IEEE International Conference on*, pp. 783–788, March 2012.

[32] T. Refaat, R. Daoud, and H. Amer, "Wireless Fault-Tolerant Controllers in Cascaded Industrial Workcells Using Wi-Fi and Ethernet," *Intelligent Control and Automation*, vol. 4, pp. 349–355, November 2013.

[33] D. Brennan, "Linear Diversity Combining Techniques," *Proceedings of the IRE*, vol. 47, pp. 1075–1102, June 1959.

[34] H. Beikirch, M. Voss, and A. Fink, "Redundancy Approach to Increase the Availability and Reliability of Radio Communication in Industrial Automation," in *Emerging Technologies Factory Automation, 2009. ETFA 2009. IEEE Conference on*, Sept 2009.

[35] H. Kirrmann, M. Hansson, and P. Muri, "IEC 62439 PRP: Bumpless Recovery for Highly Available, Hard Real-Time Industrial Networks," in *Emerging Technologies and Factory Automation, 2007. ETFA. IEEE Conference on*, pp. 1396–1399, Sept 2007.

[36] "IEC Standard for Industrial Communication Networks Technology–High Availability Automation Networks–Parallel Redundancy Protocol–High-Availability Seamless Redundancy," *IEC Std 62439-3-2012 (Revision of IEC Std 62439-3-2010)*, Jan 2012.

[37] M. Rentschler and P. Laukemann, "Towards a Reliable Parallel Redundant WLAN Black Channel," in *Factory Communication Systems (WFCS), 2012 9th IEEE International Workshop on*, pp. 255–264, May 2012.

[38] M. Rentschler and P. Laukemann, "Performance Analysis of Parallel Redundant WLAN," in *Emerging Technologies Factory Automation (ETFA), 2012 IEEE 17th Conference on*, Sept 2012.

[39] M. Rentschler, O. Mady, M. Kassis, H. Halawa, T. Refaat, R. Daoud, H. Amer, and H. ElSayed, "Simulation of Parallel Redundant WLAN with OPNET," in *Emerging Technologies Factory Automation (ETFA), 2013 IEEE 18th Conference on*, Sept 2013.

[40] R. Daoud, H. Elsayed, and H. Amer, "Gigabit Ethernet for Redundant Networked Control Systems," in *Industrial Technology, 2004. IEEE ICIT '04. 2004 IEEE International Conference on*, vol. 2, pp. 869–873 Vol. 2, Dec 2004.

[41] R. Daoud, H. Amer, and H. Elsayed, "Fault Tolerant Two-Level Pyramid Networked Control Systems," in *Emerging Technologies and Factory Automation, 2005. ETFA 2005. 10th IEEE Conference on*, vol. 1, Sept 2005.

[42] J. Thomsen and M. Blanke, "Fault-Tolerant Actuator System for Electrical Steering of Vehicles," in *IEEE Industrial Electronics, IECON 2006 - 32nd Annual Conference on*, pp. 3597–3602, Nov 2006.

[43] J. Rufino, P. Verissimo, and G. Arroz, "Node Failure Detection and Membership in CANELy," in *Dependable Systems and Networks, 2003. Proceedings. 2003 International Conference on*, pp. 331–340, June 2003.

[44] J. Ferreira, P. Pedreiras, L. Almeida, and J. Fonseca, "Achieving Fault Tolerance in FTT-CAN," in *Factory Communication Systems, 2002. 4th IEEE International Workshop on*, pp. 125–132, 2002.

[45] J. Proenza, M. Barranco, G. Rodriguez-Navas, D. Gessner, F. Guardiola, and L. Almeida, "The Design of the CANbids Architecture," in *Emerging Technologies Factory Automation (ETFA), 2012 IEEE 17th Conference on*, Sept 2012.

[46] "IEEE Standard for Local and metropolitan area networks: Media Access Control (MAC) Bridges," *IEEE Std 802.1D-2004 (Revision of IEEE Std 802.1D-1998)*, pp. 1–277, June 2004.

[47] C. Alfi, Y. Hilal, G. Aziz, H. Halawa, T. Refaat, R. Daoud, H. Amer, and H. ElSayed, "Network Fabric Fault-Tolerance for Ethernet-based Networked Control Systems," in *Industrial Informatics (INDIN), 2013 11th IEEE International Conference on*, pp. 636–641, July 2013.

[48] Cisco Systems, "Understanding Rapid Spanning Tree Protocol (802.1w)."

[49] P. Lapukhov, "Understanding STP and RSTP convergence."

[50] "Official Site for OPNET." `http://www.opnet.com`. Accessed: 2014-10-30.

[51] T. Refaat, R. Daoud, H. Amer, and M. ElSoudani, "Cascading Wireless Industrial Workcells," in *Mechatronics (ICM), 2011 IEEE International Conference on*, pp. 51–56, April 2011.

[52] C. Viegas, S. Sampaio, F. Vasques, P. Portugal, and P. Souto, "Assessment of the Interference Caused by Uncontrolled Traffic Sources upon Real-Time Communication in IEEE 802.11-based Mesh Networks," in *Factory Communication Systems (WFCS), 2012 9th IEEE International Workshop on*, pp. 59–62, May 2012.

[53] Cisco Systems, "IP Multicast Technology Overview."

[54] A. Alshanyour and A. Agarwal, "Performance of IEEE 802.11 RTS/CTS with Finite Buffer and Load in Imperfect Channels: Modeling and Analysis," in *Global Telecommunications Conference (GLOBECOM 2010), 2010 IEEE*, Dec 2010.

[55] Cisco Systems, "Cisco Aironet 3600 Series Access Point Data Sheet."

[56] Cisco Systems, "Cisco Industrial Ethernet 2000 Series Switches Data Sheet." `http://www.cisco.com/c/en/us/products/collateral/switches/industrial-ethernet-2000-series-switches/datasheet-c78-730729.pdf`. Accessed: 2014-10-30.

[57] Intel Corp., "Intel PRO/1000 Server Adapter Specifications." `http://download.intel.com/support/network/adapter/1000/spec_en.pdf`. Accessed: 2014-10-30.

[58] K. Trivedi, *Probability and Statistics with Reliability, Queuing and Computer Science Applications*. Wiley, November 2001.