Fault Tolerant Two-Level Pyramid Networked Control Systems

Ramez M. Daoud
IEEE Student Member
Electronics Eng. Dept.
American University in
Cairo, 113 Kasr El Aini,
Cairo 11511, Egypt
rdaoud@ieee.org

Hassanein H. Amer
IEEE Member
Electronics Eng. Dept.
American University in
Cairo, 113 Kasr El Aini,
Cairo 11511, Egypt
hamer@aucegypt.edu

Hany M. Elsayed
IEEE Member
Electronics and Comm.
Engineering Dept.
Cairo University,
Giza, 12613, Egypt
helsayed@ieee.org

Abstract

In this paper, a pyramid control hierarchy is proposed. It is based on the presence of a supervisor controller on top of separate controller nodes. A simulation study is conducted to test the functionality of the system.

The proposed model is an enhancement of machine modeled in form of Networked Control Systems (NCS). Two models are tested: one supervisor/two sub-controllers, one supervisor/three sub-controllers. All possible combinations of supervisor-controller inter-communication are tested. Also, all supervisor/controller inter-changeability possibilities are taken into consideration. Results are illustrated and discussed. Recommendations are drawn out.

All machine models of this study are built using switched Gigabit Ethernet in Star topology.

1. Introduction

Manufacturing control is migrating towards implementation of distributed control systems [1]. Networks play an important role in distributed implementation of control systems [2]-[7].

Distributed control systems are typically implemented in a hierarchy of functions comprising a supervisory control level. The role of this level is to monitor whether the control objectives are met, and to support the overall coordinated control in different phases of normal operation. In addition, this level should allow the diagnosis of all foreseeable faults, and should be able to take the necessary corrective actions, including the change of controller parameter or structure [8].

In [9], individual machines running on-top-of Fast and Gigabit switched Ethernet to form automated workcells, were tested. It was shown that Gigabit Ethernet had better performance implementing such NCS model, especially when dealing with mixed traffic of real-time and non-real-time loads, and no message priorities are used.

In [10] and [11] the possibility of having more than one machine controlled by only one controller was investigated. This case simulated the failure of one machine controller. Since all sensors and actuators are connected over the machine network, and several machines have their control network inter-connected together, the control traffic of one machine can be received by another machine's controller (publisher/subscriber mode of communication) [1], [10], [12], [13]. [11] showed the limitations on controllers to back-up other controllers, while [10] introduced the idea and started the first phase tests.

In this paper, a hierarchical mode of operation is introduced based on NCS. Keeping the same idea introduced in [10] and [11], for inter-machine operation, a supervisor node is added. Supervisor and controllers resembles tree hierarchy: supervisor node is the root and controller nodes are the leaves. The model consists of having several machines running in an in-line production scheme. This mandates inter-controller communication for synchronization purpose [10], [11]. Also, having a supervisor node on-top-of these controllers, they report on frequent basis to that supervisor to keep track of the complete process.

Two supervisor modes of operations are suggested, namely passive and active modes of operations. In the passive mode, the supervisor only collects information from controllers under its supervision. It intervenes in control in very limited cases as will be described later. In the active mode, the supervisor has the major role of keeping controllers under its supervision in full synchronization, which makes inter-controller communication virtually not present.

The real-time traffic is unchanged for each individual controller from the one introduced previously in [9]-[11], while the non-real-time traffic is increased. This is because each controller has to report to the supervisor node its status through FTP sessions. This will add to the FTP session already existing for inter-controller communication, the telnet sessions, the HTTP sessions, and the e-mail sessions already loading the system [9]-[11].

0-7803-9402-X/05/$20.00 © 2005 IEEE

Two main sets of simulations are conducted: first, a pyramid of 2 controllers and a supervisor, second, a pyramid of 3 controllers and a supervisor. Each set is tested for passive and active supervisor.

The rest of this paper is organized as follows: previous work overview is given in section 2. Section 3 explains the proposed model. Section 4 gives the simulated scenarios and results. Section 5 concludes this research.

2. Previous Work

In previous research Ethernet was presented as communication media for control packets in Networked Control Systems (NCS). It was studied for work in individual machines at low speed [9] and at high speeds [11]. Also, building in-line production lines, and connecting controllers of these machines together for information back-up and synchronization was investigated at low and at high speeds [10] and [11]. Markov models were used to estimate the reliability and availability of the fault-tolerant models in [14].

It was found that Fast Ethernet as well as Gigabit Ethernet can be used to build automated workcells in a mixed traffic environment. That is, machines having their control network using Ethernet technology in Star Topology can absorb implicit messaging (real-time traffic) as well as explicit messaging (non-real-time traffic). It was also found that under same operating conditions, Gigabit Ethernet had better safety margins (because of the bigger bandwidth). It was then concluded that Gigabit Ethernet was more suitable to implement NCS machines [9]. No priority is given to real-time packets over non-real-time ones, i.e. the IEEE 802.3z std is used as it is [15].

Based on this conclusion and the one that Ethernet can be used to build control networks demanding hard time limits constraints (hard real-time control systems), research moved towards complex architectures. Building in-line production Ethernet machines was tested. In-line production schemes of up-to 4 machines were successfully simulated. It was found that the system can tolerate the failure of up-to 3 controllers and still run. The traffic of the failed controller is automatically switched to be handled by another operating controller on the same production line [10], [11].

This led to the modelling of the system using Markov models to estimate its reliability and/or availability [14].

Simple machines are built to run at a nominal speed that can be increased for increased productivity. This is not done for long operating periods, especially because of the induced mechanical inertia on the system. This model was also simulated using OPNET [16]. Individual machine speed up as well as in-line machines speed up was tested. This gave an idea on the limitations of Ethernet to meet critical time constrains in control [11].

3. Proposed Model

In this paper, a Pyramid Architecture is presented. This model is built in the sense of having running machines for in-line production, and these are monitored by a supervisor controller. This supervisor is either passive or active. This means that, in normal operation, when all controllers are running and no production difficulties exist, the supervisor simply collects information from the controllers it is mastering. It is more like a tree structure with the supervisor as the root and the controllers as the leaves. Inter-leaves communication is present when these controllers are part of an in-line production scheme. So, the root collects information to be displayed on the main control room screen, in the passive mode.

In case of any controller failure, the supervisor node turns on to be active depending on the proposed switching technique. That is, the supervisor can take over control of the machine with failed controller, or it can switch the control of this machine to another operating controller on the same network. The last scenario can usually be done in the case of in-line production schemes and it resembles what was introduced in [10] and [11]. The main difference here is that a new redundant node in the new scenario exists (the supervisor), i.e., if the only remaining controller is now out of service for any reason, still the system is not down because the supervisor node can take over the control.

This research presents two Pyramid models: two machines with a supervisor, and three machines with a supervisor. Simulations are run to test all possible points of failure and the capability of the proposed system to absorb these failures.

The supervisor-controller communication in normal conditions is mainly of FTP sessions for gathering information about the machine operation. This kind of explicit messaging is jamming real-time operation of machine controllers [9]-[11]. Another FTP is present for inter-controller communication. This is for system synchronization and data back-up [9]-[11]. Every FTP session must be accompanied by a telnet session for authentication and security measures. Another added non-real-time traffic of e-mail check and HTTP is introduced in the simulations. These are the four non-real-time traffic flavors always present in all previous researches [9]-[11], and [14].

The maximum permissible round-trip delay is of 694usec. This is equivalent to a sampling frequency of 1,440Hz. Under such conditions, the machines are running at a speed of 1 revolution per second producing 60 strokes a minute.

4. Simulated Scenarios

Mainly two sets of simulations were run using OPNET; one set focusing on the two machine model with a supervisor and the other set focusing on the three machine model with a supervisor.

4.1. Two-Machine Model

This model consists of two machines running under a supervisor node. It simulates the case of having 2 machines for in-line production with inter-controller communication. In the proposed design the control is carried out by the supervisor in case one controller failed. This is justified below.

All given delays are round-trip delays, i.e., the sum of delays a packet undergoes originating at the sensor node, travelling over the network to reach the controller node, the processing delay at the controller node and the propagation delay once more from the controller to the actuator. All data encapsulation/de-capsulation on different levels are taken into account. They are also maximum delays, since they are measured under the most critical conditions. These are during FTP sessions. Recall that in [9], it was found that the maximum measured delays were always during FTP sessions.

4.1.1. Passive Supervisor

When the supervisor is passive, it monitors the other controllers only and does not make control actions. The controller of each machine reports from time to time to the supervisor node its status vector (all information concerning production rate, cam position, number of defected parts …etc…). Also, for the purpose of synchronization, it sends another file to the controller of the other machine. The maximum measured delay in this scenario is during an FTP session and is 508us (Figure 1), this is less than the maximum permissible round-trip delay: 694us. Here synchronization is done by inter-controller communication; it can also be done through supervisor. This last scenario will be explained in the next subsection.

The failure of the supervisor will not harm the control scheme. This is because synchronization is conducted by inter-controller communication. Supervisor failure causes the system to be disconnected from the outside world communication. That is, the controller nodes are connected to the internet for HTTP and e-mail checks through the supervisor node. Its failure forces the system to work in a closed network over the industrial floor. Moreover, the failure of a machine controller will make the system work in a critical mode with only one controller taking control of both machines. Such a scenario was studied beforehand and results were reported in [10].

With an operational supervisor and upon the failure of one controller, two scenarios are suggested. First, the other controller can take over the control of the machine with failed controller automatically (as described in [10]). This is done through back-up software running on both controller node platforms. The maximum measured delay is 776us and average delay of 638us (Figure 2). This exceeds the maximum permissible delay of 694us. Accordingly, the system will not be observed by the supervisor (no FTP) to run smoothly. This is the same conclusion of [10]. This leads to the next simulated scenario.

Second, the supervisor node comes into operation and takes control of the machine with failed controller. In this case, the operational controller node load is not changed: it still reports to the supervisor node and collects synchronization information from the supervisor instead of the other controller. The maximum delay measured is in the link between the operational controller and the supervisor: 562us (Figure 3). The failure of the second controller causes the supervisor to take control of both machines. The maximum measured delay is of 632us (Figure 4).

In the previous case, where the supervisor is engaged and one of the controllers is active, supervisor failure engages the operating controller to take control of both machines. This will again give a scenario similar to the one introduced in [10].

4.1.2. Active Supervisor

The supervisor in this scheme does not only collect information from individual controllers, but it has a vital role in machine synchronization. The inter-controller communication is virtually not present. This is because the synchronization information needed is transferred from one controller to the other through supervisor. Here, it can be said that the supervisor is an upper layer controller for the machine controllers. It is clear that supervisor node failure drives the system to complete failure for in-line production schemes.

Upon the failure of one of the machines' controllers, the supervisor node must take over control of this machine. The maximum measured delay in the control scheme of the machine with a failed controller is of 551us (Figure 5). Upon the failure of both machines, the supervisor must take control of both machines (similar to the proposed scheme of [10]). The maximum measured roundtrip delay through supervisor node is of 632us (Figure 6). Complete system failure occurs when the supervisor node goes out of operation for any hardware or software failure.

4.2. Three-Machine Model

This model consists of three machines running under a supervisor node. It simulates the case of having 3 machines for in-line production with inter-controller communication, same as in the previous section. Again, two cases can be analyzed. These are passive and active supervisor.

4.2.1. Passive Supervisor

In these scenarios, the supervisor node only collects information from different controllers on the line (here 3 controllers). These collected information are to be displayed in the control room.

In normal operating conditions, the maximum measured delay is of 517us [9]. Here, all controllers are running, reporting to the supervisor, and having inter-controller communication for synchronization.

Upon the failure of one controller node, the supervisor node is automatically engaged to take over control action of the machine with failed controller. This is based on the conclusion of the previous section. The maximum measured round-trip delay in all links is of 562us, recall that the maximum permissible round-trip delay is 694us.

Another controller failure must drive the supervisor node to take control of both machines. Also, FTP sessions between the remaining operating controller and the supervisor must be switched OFF. This is a result of the study conducted in [10]: the supervisor node acts like a controller node having the charge of two machines control. Accordingly, if FTP is switched OFF, no communication will take place between the operating controller and the supervisor. In this case, the average measured round-trip delay is in the links communicating information from machine nodes with failed controllers, and supervisor node is of 673us. Any FTP session will cause the system to violate round-trip delay constraint of 694us. To overcome this problem, the processing rate of the supervisor node has to be doubled. This will create an average round-trip delay of 465us with a maximum round-trip delay of 503us (Figure 7).

The failure of the third controller drives the supervisor to take charge of complete control of the system. Now no FTP sessions are present for the model having supervisor switching capability the same as any other controller node and the average measured round-trip delay is of 598us. If the supervisor processing capabilities are increased to the double, the maximum round-trip delay is of 548us, and the average round-trip delay is 485us (Figure 8).

Increasing the supervisor's processing capabilities is not a drawback of the proposed system. A conclusion from previous studies in [10] and [11] was that FTP sessions must be switched OFF in critical operating conditions. This is acceptable for normal machine controller implementation. The proposed machines' controllers processing capabilities are of 28,800 packets per second [9] and [10]. The supervisor when running with such processing speed and supervising two machines showed success (previous section). In the case of monitoring 3 machines and requiring intervention when two or three machines' controllers fail, this switching speed will be very low and the supervisor node will fail to fulfil its duties. An increase of its switching speed by a factor of 2 to reach 57,600 packets per second is not that expensive when a need to have a robust control scheme is there. It is mainly a software modification to make the system able to handle a maximum of 57,600 packets per second instead of 28,800 packets per second.

4.2.2. Active Supervisor

In these scenarios, the supervisor node takes action in control and synchronization between machine controllers in addition to collecting information to be displayed in the control room. It is clear that supervisor node failure drives the whole system to go off-line.

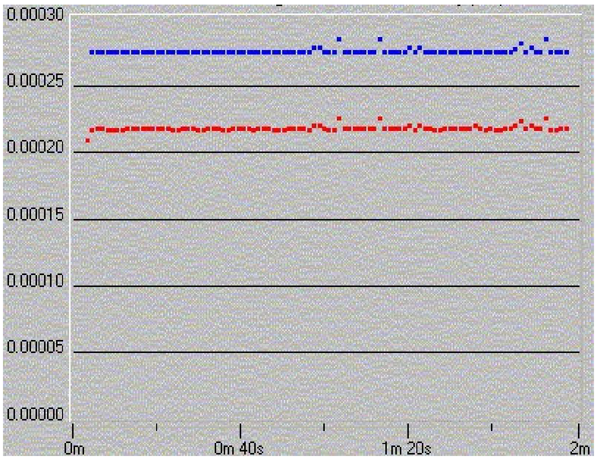
Upon the failure of one controller, the supervisor node takes care of control of that machine and the maximum measured round-trip delay is of 517us. Upon the failure of two controllers, the maximum round-trip measured delay is of 503us with a doubled switching capability. Upon the failure of all three controllers, the maximum measured round-trip delay is of 548us. Again, this measured delay is using a supervisor having the capability to handle 57,600 packets per second.

5. Conclusions

A pyramid control hierarchy is introduced based on NCS scheme. Gigabit Ethernet machines for in-line production where tested using OPNET. Machines' sampling frequency is 1,440Hz with 694us sampling period. All controllers and supervisor are interconnected using switched Gigabit Ethernet. All machines' sensors and actuators are smart having network capabilities. Two main scenarios where suggested for this research: 2 machines in-line and a supervisor, and 3 machines in-line and a supervisor. Each of these models was tested for passive and active supervisor node.

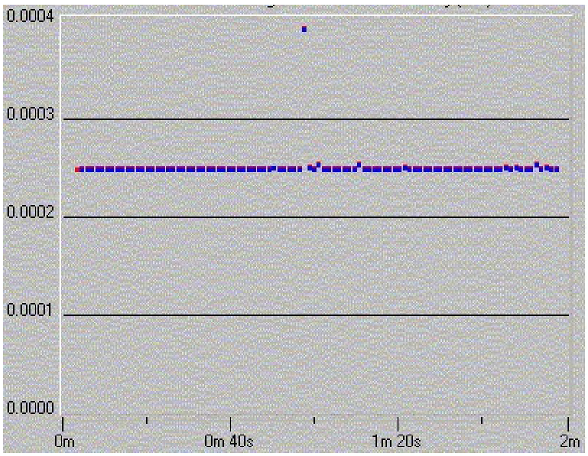
The two-machine scenario showed that the best back-up scenario for failed controller is to be replaced by the supervisor node. Upon the failure of the second controller node, the supervisor takes control of both machines. This is valid for both models: passive and active supervisor. Having an active supervisor means that it takes part in the control scheme and has a vital role in inter-machine synchronization. Accordingly, supervisor failure drives the whole system to stop operation. Passive supervisor means that it collects information and does not intervene in control scheme unless it is necessary. This occurs upon the failure of one of the controller nodes it is supervising.

The three-machine model scenario showed that the best back-up scenario for failed controller is again to be replaced by the supervisor, not by one of its neighbouring controllers. This is to keep balanced traffic load among controllers. Also, it is recommended to have the supervisor computational capacity double that of any other controller it is supervising. This is to be able to back-up two failed controllers and have successful communication with the remaining controller (in case of two controller failure). Again active supervisor failure drives the entire system to go out of service because it has the major role in inter-machine controllers' communication. Passive supervisor is engaged in control action upon the failure of any of the controllers it is supervising.



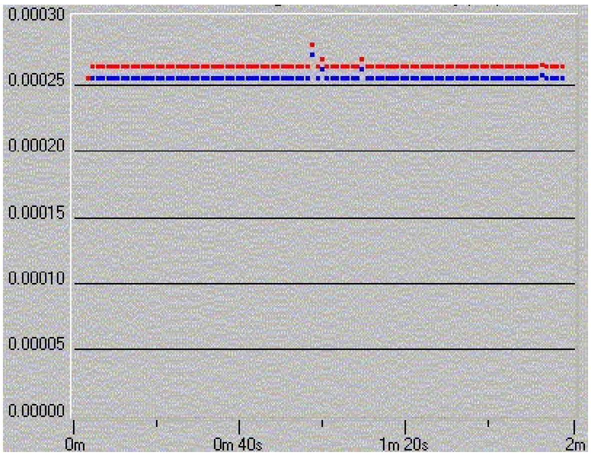
Packet Delay (seconds) vs. Simulation Time (minutes, seconds)

Figure 1. The end-to-end delays for 2 machines, 1 supervisor, normal operation



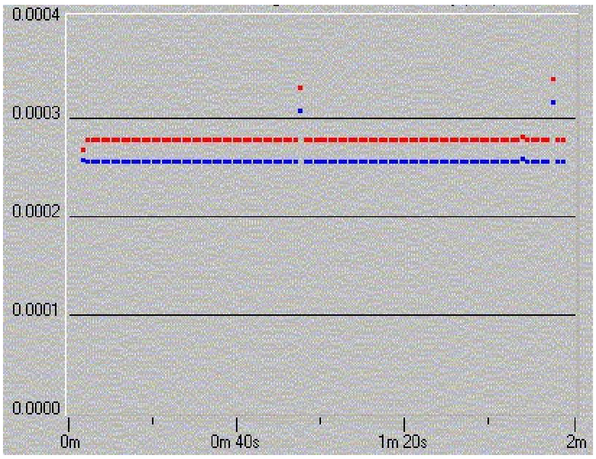
Packet Delay (seconds) vs. Simulation Time (minutes, seconds)

Figure 2. The end-to-end delays for 2 machines, 1 supervisor, controller back-up



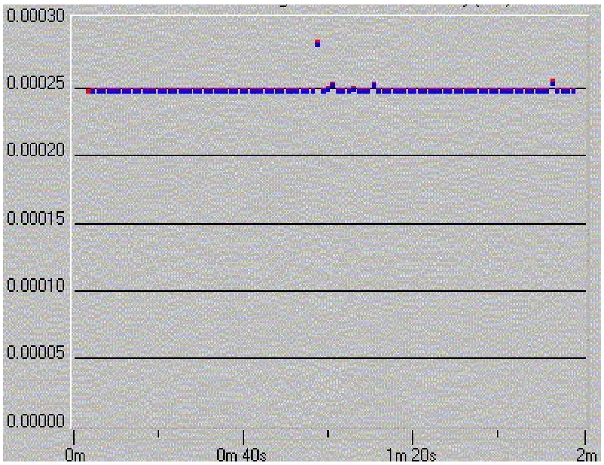
Packet Delay (seconds) vs. Simulation Time (minutes, seconds)

Figure 3. The average end-to-end delays for 2 machines, 1 supervisor, supervisor back-up.



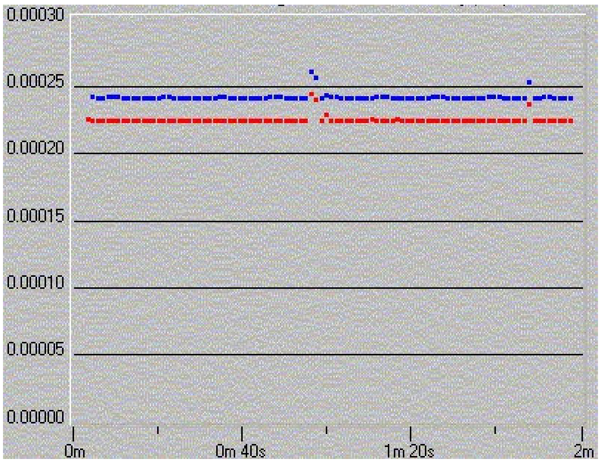
Packet Delay (seconds) vs. Simulation Time (minutes, seconds)

Figure 4. The maximum end-to-end delays for 2 machines, 1 supervisor, supervisor back-up.



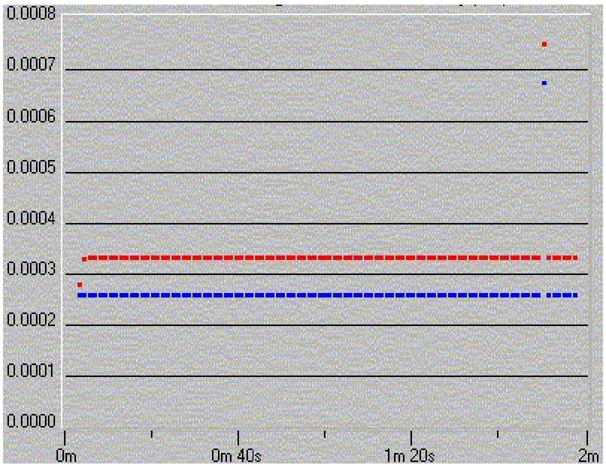
Packet Delay (seconds) vs. Simulation Time (minutes, seconds)

Figure 5. The end-to-end delays for 2 machines, 1 active supervisor, supervisor back-up.



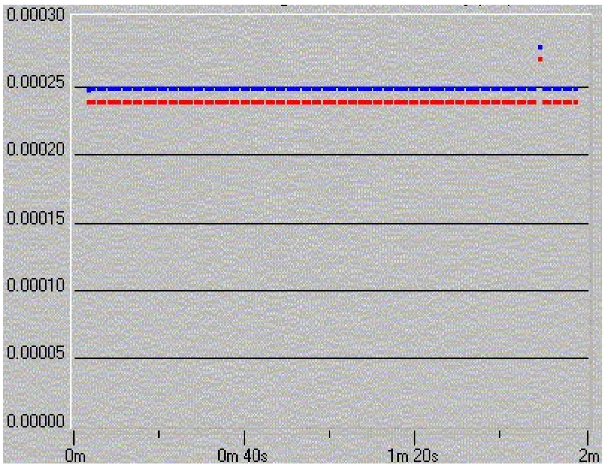
Packet Delay (seconds) vs. Simulation Time (minutes, seconds)

Figure 6. maximum The end-to-end delays for 2 machines, 1 active supervisor, supervisor back-up.



Packet Delay (seconds) vs. Simulation Time (minutes, seconds)

Figure 7. The end-to-end delays for 3 machines, 1 supervisor, supervisor back-up for 2 machines.



Packet Delay (seconds) vs. Simulation Time (minutes, seconds)

Figure 8. The end-to-end delays for 3 machines, 1 active supervisor, supervisor with double processing back-up for 2 machines.

References

[1] F.L. Lian, J.R. Moyne, and D.M. Tilbury, "Performance Evaluation of Control Networks: Ethernet, ControlNet, and DeviceNet," *IEEE Cont. Sys.*, pp. 66-83, Feb. 2001.

[2] J. Nilsson, "*Real-Time Control Systems with Delays*," PhD thesis, Department of Automatic Control, Lund Institute of Technology, Lund, Sweden, 1998, Available: http://home.case.edu/ncs

[3] F.L. Lian, J.R. Moyne, and D.M. Tilbury, "Performance Evaluation of Control Networks: Ethernet, ControlNet, and DeviceNet," *IEEE Cont. Sys.*, Vol. 21, No. 1, Feb. 2001, pp.66-83.

[4] B. Wittenmark, B. Bastian, and J. Nilsson, "Analysis of Time Delays in Synchronous and Asynchronous Control Loops,", *37th CDC, Lund Institute of Technology*, Tampa, Dec. 1998.

[5] B. Moss, "Real-time Control on Ethernet," *Dedicated Systems*, No. 00q2, April 2000, pp.53-60.

[6] ODVA, "Volume 1: CIP Common," Available: http://www.odva.org/10_2/03_events/03_ethernet-homepage.htm

[7] ODVA, "Volume 2: EtherNet/IP Adaptation on CIP," Available: http://www.odva.org/10_2/03_events/03_ethernet-homepage.htm

[8] M. Blanke, M. Staroswiecki, and N. Wu, "Concepts and Methods in Fault-Tolerant Control," *Proceedings of the American Control Conference*, Arlington, VA, June 2001, pp. 2608-2620.

[9] R.M. Daoud, H.M. Elsayed, H. H. Amer, and S.Z. Eid, "Performance of Fast and Gigabit Ethernet in Networked Control Systems," *Proceedings of IEEE International Mid-West Symposium on Circuits and Systems, MWSCAS03*, Cairo, Egypt, Dec. 2003.

[10] R.M. Daoud, H.M. Elsayed, and H.H. Amer, "Gigabit Ethernet for Redundant Networked Control Systems," *Proceedings of IEEE International Conference on Industrial Tecnology, ICIT04*, Tunis, Dec. 2004.

[11] R.M. Daoud, H.H. Amer, and H.M. Elsayed, "Fault-Tolerant Networked Control Systems under Varying Load," *Proceedings of IEEE Mid-Summer Workshop on Soft Computing in Industrial Applications, SMCia/05*, Espoo, Finland, June 2005.

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

[13] B. Lounsbury, and J. Westerman, "Ethernet: Surviving the Manufacturing and Industrial Environment," *Allen-Bradley white paper*, May 2001.

[14] H. H. Amer, R.M. Daoud, "Reliability and Availability of Fault-Tolerant Networked Controlled Systems," *1st International Computer Engineering Conference ICENCO04*, Cairo, Egypt, Dec. 2004.

[15] IEEE 802.3 Std, 2000 Edition

[16] Official Site for OPNET: www.opent.com