UKACC International Conference on Control 2012
Cardiff, UK, 3-5 September 2012

Developments in Dependability Modeling of Networked Control Systems

Manoj Kumar
Control Instrumentation Division
Bhabha Atomic Research Centre
Trombay, Mumbai 400085, India
Email: kmanoj@barc.gov.in

A.K. Verma
Stord/Haugesund University College
Bjϕrsonsgate 45
Haugesund 5528, Norway
Email: akvmanas@gmail.com

A. Srividya
Department of Civil Engineering
Indian Institute of Technology Bombay
Mumbai 400076, India
Email: asvidya@civil.iitb.ac.in

P.P. Marathe
Control Instrumentation Division
Bhabha Atomic Research Centre
Trombay, Mumbai 400085, India
Email: cnidppm@barc.gov.in

***Abstract*—Networked control systems (NCS) are in existence for quite some time. The network-induced delays and packet drops; and their effect on control system's performance has been a burning topic for last one decade. Dependability in context of NCS has not got much attention. While it is an important aspect of NCS intended to be used in critical application. The paper reviews the present state of developments in NCS and presents open problems pertaining to dependability of NCS. Solutions to these problems may increase the presence of NCS by many folds and in many fields.**

I. Introduction

Networked Control System (NCS) contains a number of interconnected devices that exchange data through shared communication networks. Examples of such systems are found in industrial automation, building automation, office and home automation, intelligent vehicle systems and advanced aircraft and spacecraft. These systems are driven by an important feature, instead of point-to-point connections, all system elements (sensors, actuators and controllers) are connected to the network as nodes. The advantages of this implementation include [1], [2]: reduced system wiring, plug and play devices, increased system agility, ease of system diagnosis and maintenance. These features result in modular and flexible system design, simple and fast implementation and powerful system diagnosis and maintenance utilities [3].

Schematically a typical NCS is shown as in Figure 1. Sensor node samples the process parameters with a given sampling period, convert physical parameters to digital and pack the message to send to controller. The controller node unpacks the message(s) from sensor node and use control algorithm to calculate control signals to be sent to actuator node. Actuator node according to control signal takes the corrective action in process. All these messages are sent over shared network. In NCS, time delay has one more factor in addition to node processing delay, it is network-induced delay, i.e. from sensor to controller and controller to actuator.

Control systems are reactive systems; they need to interact with their environment (i.e. process/plant) constantly in a timely manner. Due to this property, control systems come under the category of real-time systems. They can be hard or soft real-time systems based on the consequences of failure. In NCS, the feedback loop is closed by shared communication network(s) where information is sent by means of packets. These shared communication media are prone to random delay and loss of packets. This leads to two challenging problems in analysis and design of networked control systems (NCS), network induced delays and packet dropouts. Both problems can significantly degrade the NCS's performance and dependability. It has long been realized that network induced communication delay is time-varying and nondeterministic, suggesting that the delay behavior is unpredictable. Packet dropout occurs when communication networks are unreliable or the communication latency is so big that the packet has to be purposely dropped.

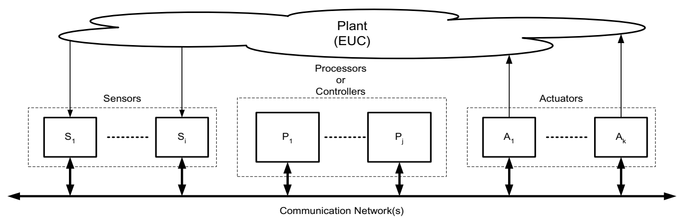

Fig. 1. Schmatic of a typical NCS

Thess inherent issues of NCS - network-induced delay and packet loss - are well acknowledged [1], [2], [4], [5], [6], [7], [8], [9], [3], [10], [11], [12]. The delay and packet loss can degrade the quality of performance (QoP) of control system or even de-stabilize the system, if not properly designed [1], [2], [13], [14], [15], [7], [16], [6], [5], [17], [8], [18]. The two main directions to approach this problem are, i) design a communication protocol that guarantee delays, ii) design control strategies that *a priori* compensate for network-induced delay and packet loss.

When NCS are used for control, then their main objective is

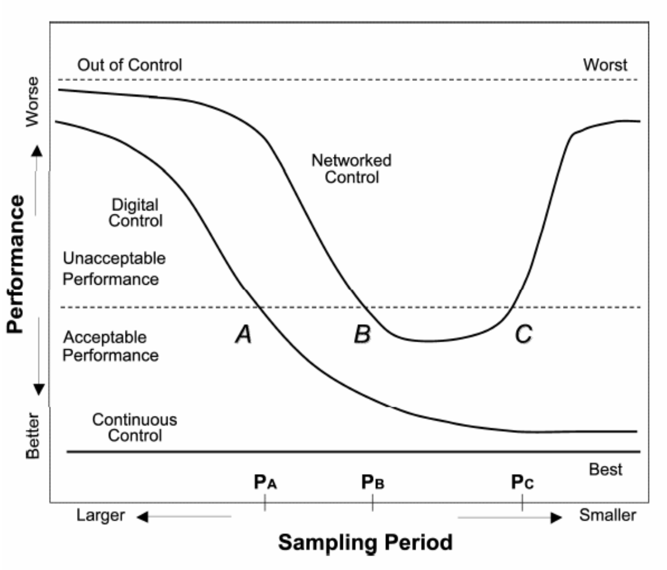

Fig. 2. Performance comparison [2], [9]

to guarantee the stability and performance of plant/equipment under control (EUC), i.e. meet the control system specifications. These specifications include phase margin, gain margin, overshoot, steady state error, response-time, and tracking error etc.

The comparison of control performance versus sampling period for continuous control (analog), digital control, and network control is given in Fig. 2. During the NCS design stage, a performance chart can be derived as shown in Fig. 2. This performance chart provides a clear way to choose the proper sampling periods for an NCS. For a fixed control law, the worst, acceptable, and the best regions can be defined based on control specifications. The performance axis in Fig. 2 could be chosen to reflect a subset of the control system specifications. Since the performance of continuous control is not a function of sampling period, the performance index is constant for a fixed control law. For digital control case, the performance only depends on the sampling period assuming no other uncertainties. The performance degradation point A (sampling period P_A) in digital control could be estimated based on the relationship between control system bandwidth and sampling rate. For the networked control case, point B can be determined by further investigating the characteristics and statistics of network-induced delays and device processing time delays. As the sampling period gets smaller, the network traffic load becomes heavier, the possibility of more contention time or data loss increases, and longer time delays result. This situation causes the existence of point C in networked control.

With the advances in technologies related to NCS and advantages offered by them over conventional systems, NCS are penetrating into almost every aspect of our life. When these systems are used in critical applications, such as, nuclear power plant, avionics, process plants and automobiles etc., failure of these systems could result in loss of huge investment, effort, life or damage to environment. In such cases, dependability analysis becomes an important tool for decision making at all stages of system life cycle - design, deployment, operation and phase-out. In fact for systems concerning safety of people, demonstration of dependability through testing/analysis is a mandatory requirement before system can be deployed.

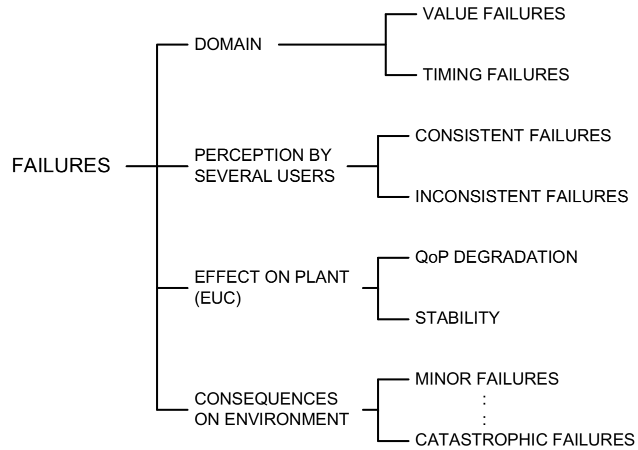

Fig. 3. Failure classification [19], [21]

The paper reviews the related developments in the area of NCS and introduces dependability. Brief overview of dependability aspects are given in section II. Section III reviews the related developments. Dependability models are discussed in section IV. The open issues pertaining to NCS dependability modeling are outlined in section V, followed by conclusion in section VI.

II. Dependability: Basic Fundamentals

Dependability of a system is defined by Algirdas Avizienis et al. [19], [20] as “ability to deliver service/function that can justifiably be trusted”. The service delivered by a system is its behavior as it is perceived by its user(s). User could be another system (physical, human) that interacts with the former. Service is delivered when the service implements the system function, where function is the behavior of the system described by its specification.

A system failure is an event that occurs when the delivered service deviates from correct service. A failure is a transition from correct service to incorrect service. Failure is manifestation of error, which in turn is caused by fault [19], [20], [21]. An error is that part of system state that may cause a subsequent failure: a failure occurs when an error reaches the service interface and alters the service. A fault is the adjudged or hypothesized cause of an error. A fault is active when it produces an error, otherwise it is dormant. Fig. 3, shows the modes characterizing incorrect service. Effect on plant (EUC) has been added considering NCS.

Fig. 4 shows the dependability tree consisting of attributes, means and threats.

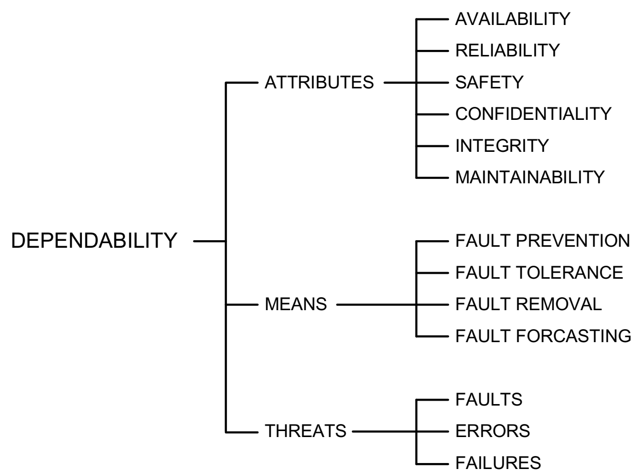

Fig. 4. Dependability tree [19], [21]

The means to attain dependability are a set of four techniques [19], [21]:

1) **Fault prevention:** to prevent the occurrence or introduction of faults
2) **Fault tolerance:** capability to deliver correct service in the presence of faults
3) **Fault removal:** to reduce the number and severity of faults
4) **Fault forecasting:** to estimate the present number, the future incidence, and the likely consequence of faults

The dependability attributes for electronic systems depend on their application or function. An electronic system when used in critical applications can be categorized as safety-critical, mission-critical and economically critical. The definitions of these are given below:

Safety-critical systems: systems required to ensure safety of equipment under control (EUC), people and environment.

Mission-critical systems: systems whose failure result in failure/loss of mission.

Economically-critical systems: systems whose failure result in availability of EUC, causing massive loss of revenue.

Dependability attributes applicable to these systems are safety, reliability and availability, respectively. Fig. 5 shows the applicable dependability attributes pictorially.

III. Review of NCS related research

NCS related research developments can be categorized as, i) network related, ii) control related, and iii) dependability related. Some of the work is reviewed below.

Network related research is in development and performance evaluation of Fieldbus technology. Ethernet related technologies have also been an area of research because of the market share and cost benefit of Ethernet. For Ethernet new development includes traffic smoothing and switched Ethernet.

The real-time industrial network, often referred to as fieldbus, is an important element for building automated manufacturing systems. Thus, in order to satisfy the real-time requirements of field devices such as sensors, actuators and controllers, a number of fieldbus protocols have been developed. These fieldbus protocols have an important advantage over the widely used Ethernet in terms of their deterministic behavior. However, the application of fieldbuses has been limited because of the high cost of hardware and the difficulty in interfacing them with multi-vendor products. In order to solve these problems, computer network technology, especially Ethernet, is being adopted in industrial automation field. The key technical obstacle for Ethernet for industrial applications is that of its non-deterministic behavior [2], [3]. Non-deterministic behavior makes it inadequate for real-time applications, where packets containing real-time information (control command or sensor/actuator signal) have to be delivered within a certain time limit. To overcome the limitations of standard Ethernet, recent development has lead to switched Ethernet, EtherCAT, EPL and PROFInet [3], [22], [23], [24], [25], [26], [27], [28], [29], [30]. These have been adopted in industrial applications because of the elimination of uncertainties in network operation, which leads to improved performance.

Control system related developments can be classified in three categories: i) dealing with only delay, ii) dealing only with packet drops and iii) dealing with both [31], [32], [33].

For quite a long, it has been realized that conventional reliability models are not sufficient to analyze hard real-time systems, since they do not adequately model the temporal properties of such system [34]. A number of methods and techniques have been proposed since then to model and analyze temporal behavior and correctness [34], [2], [33], [30], [31], [26], [24], [12], [1], [29], [35], [36], [37]. A brief review of these is tabulated in Table 1.

IV. Dependability models

To address dependability in context of NCS, available literature has the following:

- techniques to design robust controller for a specified bound on time-delay and packet drop rate.
- a number of networks have been characterized for their time delay and packet drop behavior
- a number of control networks have been proposed with guaranteed behavior
- techniques are being developed to characterize a given network to specify its time-delay and packet drop behavior for specified traffic pattern and network load

Conventional dependability models do not incorporate failures due to not meeting timing constraint and dynamic properties. From literature, it is evident that for NCS functional dependability attributes are more appropriate [37]. For programmable electronic systems functional safety has already been standardized and gaining importance [38].

With respect to dependability modeling of NCSs, there seems to be two different categories of systems - i) failure to meet time deadline leads to system failure and, ii) failure due to not keeping the performance objective.

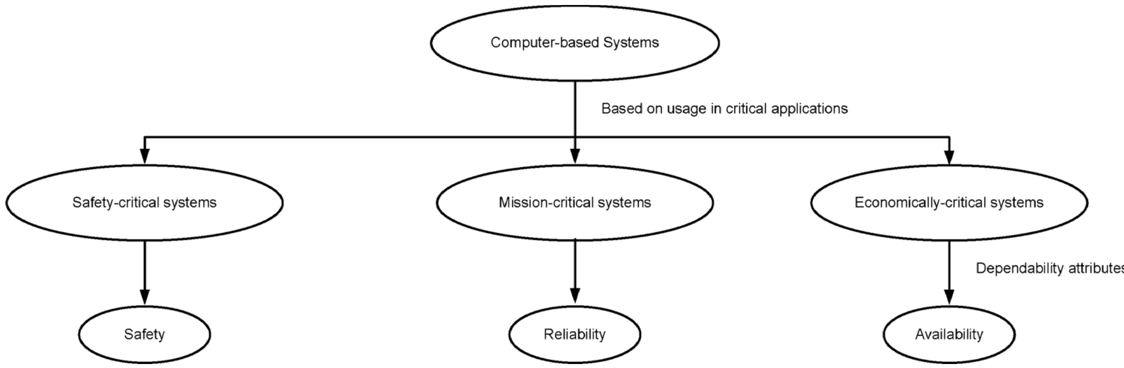

Fig. 5. Failure domains and dependability attributes

Table 1 Review of related literature

Work reference	Study	Method/technique	Outcomes
[2]	time delay of three networks - ControlNet, DeviceNet and Ethernet	theorical formulation and verification by simulation & experimental analysis	- Ethernet has no delay at low network loads - ControlNet provides excellent performance at high network loads - DeviceNet is deterministic protocol for short messages
[28]	traffic smoother for Ethernet	adoptive traffic smoothing	- traffic smoother gives priority to real-time (RT) packets over non-RT packets - reduce collision
[23]	traffic smoother for Ethernet	fuzzy traffic smoothing	- statistical bound on packet delivery time
[25]	switched Ethernet	experimental analysis	- performance evaluation of switched Ethernet
[26]	queuing method for Ethernet with TCP/IP	experiment	- a simple upgrade of bandwidth does not necessarily improve control latency and jitter performance - adding hierarchy into the network introduces extra latency and jitter
[9]	TCP/IP and UDP/IP on Ethernet	experiment	- UDP/IP is better than TCP/IP on Ethernet for real-time systems
[29]	message scheduling over CAN	share-driven scheduling	- share-driven scheduling provides an efficient and predictable scheduling of messages
[1]	effect of network induced delay on control system performance and stability	two delay models - independent and Markov delay	- effect of time stamping and timeouts - optimal controller with independent time delay is combination of state feedback and state estimator - optimal controller with Markov delay requires knowledge of old time delays along with state of the Markov chain
[13][30]	response-time distribution	analytical model	- Model for response-time distribution of CAN and MIL-STD-1553B - Effect of network and node redundancies on response-time distributions
[31]	TCP/IP on Ethernet	experiment	- multifractal nature of network traffic
[17]	stability of NCS with delay	analysis of 9 methods	- random network delays are more difficult to handle than constant or periodic delays
[32]	delay compensation for robust control	experiment and analysis	- Smith predictor based approach control over a network when accurate delay measurements are accessible - Robust control based approach when only upper bound of end-to-end delays available
[26]	NCS with packet drop	parallel queue into the actuator	
[11]	stability of NCS with packet drop	discrete-time hybrid automaton	
[15][33]	NCS with both delay and packet drop	switched system model	- a quantitative relation between the packet drop rate and stability
[7]	NCS with both delay and packet drop	Markovian jump linear system model	- sufficient conditions for stochastic stabilization of NCS with packet drop and time-varying delays
[34]	NCS with delays and out of order packets	analysis	- optimal information processing algorithm for each node
[6]	NCS with both delay and packet drop	analysis	- sufficient conditions for Lyapunov stability are derived in the case of uncertainty due to drops and delays
[36]	fault diagnosis of NCS	time-delay system model and T-S fuzzy model	- fault diagnosis for linear and non-linear NCS with long delay
[37]	dependability of communication	FMEA	- presents a number of means to prevent or avoid or minimize the damaging consequences of failure modes
[35]	reliability of distribued system	Markov chain	- a generic high-level formalism based on Markov chain with lattice structure which represents both time and functional correctness
[38]	reliability of control system	experimental analysis	- Reliability evaluation of control systems considering performance aspects (overshoot, rise-time steady-state error etc.)

The models of these failures which can utilize the available techniques of dependability analysis are the need of the hour. One important failure model is hazard rate. If hazard rate of timing failure and performance-related failure can be obtained, then using available techniques dependability attribute of interest can be estimated.

For systems belonging to first category, response-time distribution can be used to estimate probability of missing the deadline [39], [29], [12].

$$\begin{aligned} & p = R\left(t > t_d\right) \\ & \text{where:} \\ & p: \text{ probability of timing failure} \\ & t_d: \text{ time deadline} \\ & R\left(\cdot\right): \text{response - time distribution (CDF)} \end{aligned} \tag{1}$$

Let system failure criteria is n consecutive deadline violation (or timeliness failures). When $n = 1$, number of cycles at which timeliness failure will occur follows geometric distribution [40].

$$\begin{aligned} & P\left(Z = n\right) = p^{n-1}q \\ & \text{where} \\ & Z: \text{random variable} \\ & q: \text{ probability of occurrence of timeliness failure} \\ & p: 1 - q \end{aligned} \tag{2}$$

Geometric distribution is a memoryless distribution in discrete time and is counterpart of exponential distribution in continuous time [40]. At gross level (larger time scale), it can be easily converted to exponential distribution. In exponential distribution characterizing parameter is hazard rate, which in this case is referred to as "*timeliness hazard rate*".

$$\begin{aligned} & \lambda^T = \frac{1}{t}\ln\left(\frac{1}{P\left(Z > \left\lceil \frac{t}{t_C} \right\rceil\right)}\right) \\ & where \\ & \lambda^T: \text{Timeliness hazard rate} \\ & t: \text{Operating time} \\ & t_C: \text{Cycle time or period} \end{aligned} \tag{3}$$

When $n > 1$, number of cycles for timeliness failure will not follow geometric distribution. This process (number of cycles for timeliness failure) is a memory process and directly cannot be modeled as Markov. Using the technique of additional states [41], Markov model can be used to model this process. This is expalined in [29].

For systems belonging to second category, techniques need to be evolved to derive hazard rates of failure due to performance degradation (overshoot, stability, etc.). The other open issues in dependability modeling of NCS are discussed in next section.

V. Dependability issues in NCS

When systems are used in critical applications, all the means to achieve dependability are employed. Some of them are listed below:

Fault Prevention: Methods to avoid the occurrence of failure. For example,

1) selection and use of reliable hardware components,
2) use of fault-free algorithm and software,
3) use of communication network with predictable delay and preferably no drop during transmission

Fault Tolerance: Means to tolerate the failure. For example,

1) Redundancy for hardware components, including transmission media,
2) software fault tolerance, recovery and roll-back,
3) control algorithm to cope with random packet delay and drop

Fault Removal: Detection and restoration of failed component/unit.

1) diagnosis of hardware component failures,
2) diagnosis of software failures,
3) monitoring of traffic and detection of anomaly

Although some work has been done to improve NCS dependability, but there exist some research gap for dependability modeling and analysis. These are listed as follows:

1) Functional dependability considering *value* as well as *timing* failures
2) Methods to deal with redundancy at node level (mainly actuator node)
3) Methods to deal with redundancy at communication level (mainly controller node)
4) Effect of fault occurrence and removal on system performance
5) Effect of on line repair

The above means try to ensure the uninterrupted operation of system. Like any other critical system, NCS is also expected to have graceful degradation or go a defined state on failure, e.g. *fail-safe* or *fail-silent*. In addition to this, it shall give opportunity for alternate means of control. E.g. in case control system has failed, it shall allow the remote manual control.

Some other issues are:

- Timing of faults: faults affecting the network may have various effects on the control system, depending upon the state of the system, when the failure occurs. E.g. a lost message in transient state does not have the same effect as in steady state.
- Timing model: for safety systems, choice of timing model and indulgent protocol also plays an important role [42].

VI. Conclusion

NCS have been attracting significant interest in the past few years and will continue to do so for the years to come. With the advent of cheap, small, and low-power processors with communication capabilities, it has become possible to endow sensors and actuators with processing power and the ability to communicate with remote controllers through shared networks. In view of these developments, it is expected that NCS will become the more predominant; replacing the current centralized digital control systems that rely on dedicated connections between system elements.

Along with all advantages that NCS offer, they have some inherent limitations. The main issue being the network induced delays, packet drop, out-of-sequence packet and multiple packets. The network quality of service (QoS) related issues affect the quality of performance (QoP) of control systems and sometime lead to in stability. A lot of work has been done in last decade to address these problems.

Dependability analysis is important when NCS is expected to be used for a critical application. To improve dependability, systems are designed with redundancy, maintenance features and diagnosis. These features make the dependability analysis a complex process. The research gap in this direction has been outlined. As can be seen that scope of dependability of NCS is not limited to 'control algorithms' embedded in the controller node or to the traffic behavior on network. It considers the complete system and analyzes all kind of probable failures.

Acknowledgment

The authors would like to thank Shri Y.K. Taly for his continual support and guidance. We also thank Shri U. Mahapatra for his kind guidance and critical comments to improve the work. Continual support and encouragement from Shri G.P. Srivastava is highly appreciated.

References

[1] J. Nilsson, "Real-time control systems with delays," Ph.D. dissertation, Lund Institute of Technology, Sweden, 1998.

[2] F.-L. Lian, "Analysis, design, modeling, and control of networked control systems," Ph.D. dissertation, University of Michigan, 2001.

[3] T. Yang, "Networked control systems: a brief survey," *IEE Proc.-Control Theory Applications*, vol. 153, no. 4, pp. 403–412, July 2006.

[4] J. Hespanha, P. Naghshtabrizi, and Y. Xu, "A survey of recent results in networked control systems," *Proceedings of the IEEE*, vol. 95, pp. 138–162, 2007.

[5] M. Garcia-Rivera and A. Barreiro, "Analysis of networked control systems with drops and variable delays," *Automatica*, vol. 43, no. 12, pp. 2054 – 2059, 2007.

[6] X. Ye, S. Liu, and P. Liu, "Brief paper modelling and stabilisation of networked control system with packet loss and time-varying delays," *Control Theory Applications, IET*, vol. 4, no. 6, pp. 1094 –1100, june 2010.

[7] Y.-C. Tian and D. Levy, "Compensation for control packet dropout in networked control systems," *Information Sciences*, vol. 178, no. 5, pp. 1263–1278, 2008.

[8] M. Das, R. Ghosh, B. Goswami, A. Gupta, A. Tiwari, R. Balasubrmanian, and A. Chandra, "Network control system applied to a large pressurized heavy water reactor," *Nuclear Science, IEEE Transactions on*, vol. 53, no. 5, pp. 2948 –2956, oct. 2006.

[9] F.-L. Lian, J. Moyne, and D. Tilbury, "Network design consideration for distributed control systems," *IEEE Transaction on Control System Technology*, vol. 10, pp. 297–307, 2002.

[10] J. van Schendel, M. Donkers, W. Heemels, and N. van de Wouw, "On dropout modelling for stability analysis of networked control systems," in *American Control Conference (ACC), 2010*, 30 2010-july 2 2010, pp. 555 –561.

[11] B. Lu, "Probabilistic design of networked control systems with uncertain time delay," in *ASME International Mechanical Engineering Congress and Exposition, Proceedings, 9 Part A*, 2008, pp. 355–362.

[12] M. Kumar, A. K. Verma, and A. Srividya, "Probabilistic modeling of network-induced delays in networked control systems," *Int. J. Applied Mathematics and Computer Sciences*, vol. 5, no. 1, pp. 43–54, 2009.

[13] L. Dritsas and A. Tzes, "Robust stability bounds for networked controlled systems with unknown, bounded and varying delays," *Control Theory Applications, IET*, vol. 3, no. 3, pp. 270 –280, march 2009.

[14] W.-A. Zhang and L. Yu, "Modelling and control of networked control systems with both network-induced delay and packet-dropout," *Automatica*, vol. 44, no. 12, pp. 3206 – 3210, 2008.

[15] Y.-B. Zhao, G.-P. Liu, and D. Rees, "Modeling and stabilization of continuous-time packet-based networked control systems," *Systems, Man, and Cybernetics, Part B: Cybernetics, IEEE Transactions on*, vol. 39, no. 6, pp. 1646 –1652, dec. 2009.

[16] Y. Tipsuwan and M.-Y. Chow, "Control methodologies in networked control systems," *Control Engineering Practice*, vol. 11, no. 10, pp. 1099 – 1111, 2003.

[17] F. Hao and X. Zhao, "Linear matrix inequality approach to static output-feedback stabilisation of discrete-time networked control systems," *Control Theory Applications, IET*, vol. 4, no. 7, pp. 1211 –1221, july 2010.

[18] I. Pan, S. Das, and A. Gupta, "Tuning of an optimal fuzzy pid controller with stochastic algorithms for networked control systems with random time delay," *ISA Transactions*, vol. 50, no. 1, pp. 28 – 36, 2011.

[19] A. Avizienis, J.-C. Laprie, and B. Randell, "Fundamental concepts of dependability," in *Proc. of 3rd Information Survivability Workshop*, Oct. 2000, pp. 7–11.

[20] J. Dugan and K. Trivedi, "Coverage modeling for dependability analysis of fault-tolerant systems," *IEEE Transactions on Computers*, vol. 38, no. 6, pp. 775–787, 1989.

[21] A. Avizienis, J.-C. Laprie, B. Randell, and C. Landwehr, "Basic concepts and taxonomy of dependable and secure computing," *IEEE Transaction Dependable and Secure Computing*, vol. 1, no. 1, pp. 11–33, 2004.

[22] L. L. Bello, G. Kaczynski, and O. Mirabella, "Improving the real-time behavior of ethernet networks using traffic smoothing," *IEEE Transaction on Industrial Informatics*, vol. 1, no. 3, pp. 151–161, 2005.

[23] P. Pedreiras, L. Almeida, and P. Gai, "The ftt-ethernet protocol: Merging flexibility,timeliness and efficiency," *Real-Time Systems, Euromicro Conference on*, vol. 0, p. 152, 2002.

[24] K. C. Lee and S. Lee, "Performance evaluation of switched ethernet for real-time industrial communications," *Computer Standards & Interfaces*, vol. 24, no. 5, pp. 411 – 423, 2002.

[25] Y.-C. Tian, Q.-L. Han, C. Fidge, M. O. Tade, and T. Gu, "Communication architecture design for real-time networked control systems," in *Proceedings of the IEEE Conference on Communications, Circuits and Systems*, 2006, pp. 1840–1845.

[26] F.-L. Lian, J. Moyne, and D. Tilbury, "Performance evaluation of control networks: Ethernet, controlnet, and devicenet," *IEEE Control System Magazine*, vol. 21, pp. 66–83, 2001.

[27] S.-K. Kweon, K. G. Shin, and G. Workman, "Achieving real-time communication over ethernet with adaptive traffic smoothing," *Real-Time and Embedded Technology and Applications Symposium, IEEE*, vol. 0, p. 90, 2000.

[28] T. Nolte, "Share-driven scheduling of embedded networks," Ph.D. dissertation, Malardalen University, Sweden, 2006.

[29] M. Kumar, A. K. Verma, and A. Srividya, "Response-time modeling of controller area network (CAN)," in *Int. Conf. on Distributed Computing and Networking (ICDCN09), Lecture Notes in Computer Science, LNCS 5408*. Springer, 2009, pp. 163–174.

[30] Y.-C. Tian, Z.-G. Yu, and C. Fidge, "Multifractal nature of network induced time delay in networked control systems," *Physics Letters A*, vol. 361, pp. 103 – 107, 2007.

[31] N. Vatanski, J.-P. Georges, C. Aubrun, E. Rondeau, and S.-L. Jms-Jounela, "Networked control with delay measurement and estimation," *Control Engineering Practice*, vol. 17, no. 2, pp. 231 – 244, 2009.

[32] W.-A. Zhang and L. Yu, "A robust control approach to stabilization of networked control systems with time-varying delays," *Automatica*, vol. 45, no. 10, pp. 2440 – 2445, 2009.

[33] V. Gupta, A. Dana, J. Hespanha, R. Murray, and B. Hassibi, "Data transmission over networks for estimation and control," *Automatic Control, IEEE Transactions on*, vol. 54, no. 8, pp. 1807 –1819, aug. 2009.

[34] C. Perkins and A. Tyrrell, "A new markov model for dependability and temporal evaluation of hard real-time systems," in *Proceedings of ESS95, The 7th European Simulation Symposium*, 1995, pp. 26–28.

[35] H. Fang, H. Ye, and M. Zhong, "Fault diagnosis of networked control systems," *Annual Reviews in Control*, vol. 31, no. 1, pp. 55 – 68, 2007.

[36] L. Cauffriez, J. Ciccotelli, B. Conrard, and M. Bayart, "Design of intelligent distributed control systems: a dependability point of view," *Reliability Engineering and System Safety*, vol. 84, no. 1, pp. 19–32, 2004.

[37] R. Ghostine, J.-M. Thiriet, and J.-F. Aubry, "Variable delays and message losses: Influence on the reliability of a control loop," *Reliability Engineering and System Safety*, vol. 96, pp. 160–171, 2011.

[38] *IEC 61508: Functional Safety of electric/electronic/programmable electronic safety-related systems*, IEC Std. 0-8, 2000.

[39] K. S. Trivedi, S. Ramani, and R. Fricks, "Recent advances in modeling response-time distributions in real-time systems," *Proceedings of the IEEE*, vol. 91, pp. 1023–1037, 2003.

[40] K. S. Trivedi, *Probability & Statistics with Reliability, Queueing, and Computer Science Applications*. Englewood Cliffs, New Jersey: Prentice-Hall, 1982.

[41] D. R. Cox and H. D. Miller, *The Theory of Stochastic Processes*. London: Methuen & Co., 1970.

[42] I. Keidar and A. Shraer, "How to choose a timing model?" in *Proc. 37^{th} Annual IEEE/IFIP Int. Conf. on Dependable Systems and Networks (DSN'07)*, 2007.