GUIDANCE NOTES ON

RESPONSE TIME ANALYSIS FOR PROGRAMMABLE ELECTRONIC ALARM SYSTEMS

SEPTEMBER 2018

American Bureau of Shipping
Incorporated by Act of Legislature of
the State of New York 1862

© 2018 American Bureau of Shipping. All rights reserved.
ABS Plaza
16855 Northchase Drive
Houston, TX 77060 USA

Foreword

The response time analysis of programmable electronic alerts and indicators onboard marine and offshore structures helps to demonstrate how real-time alarm deadlines are satisfied under worst-case operational conditions. The ABS requirements for Response Time Analysis of alarms generated by Category III systems (defined in the ABS Rules and IACS UR E22), offer digital design clarification that the paramount situational awareness function of any standalone programmable electronic alarm or any integrated alarm within the Alarm and Monitoring System remains intact, regardless of any additional computational or network load introduced from sensory elements provided in excess of those required by the ABS Rules and statutory regulations.

ABS defines deadlines for response time analysis of alerts and indicators within its Rules so as to effectively harmonize class requirements with national and international standards (e.g., IEEE 45.2) on real-time systems deterministic behavior.

However, considering further the complexity of processors and communication protocols used to implement a real-time, programmable electronic alarm system, as well as the ever increasing utilization of such systems by additional or retrofitted sensory elements, ABS has developed a proposed methodology to further support Response Time Analysis efforts. The proposed methodology described in these Guidance Notes utilizes block diagrams for programmable electronic alarms system architectural modeling. The proposed methodology also introduces the concept of the response time table and offers applicable equations for calculating the Worst Case Response Time. These concepts aim to introduce both an optional unified terminology and a generalized methodology for Response Time Analysis efforts, targeting similar quality and consistency of engineering review submittals subject to ABS requirements for Response Time Analysis of alarms generated by Category III systems.

Alternative calculations and methods used to estimate the Worst-case Response Time (WCRT) of programmable electronic alarm systems can be reviewed and evaluated on an individual basis.

Users are advised to check periodically on the ABS website www.eagle.org to verify that this version of these Guidance Notes is the most current.

These Guidance Notes become effective on the first day of the month of publication.

We welcome your feedback. Comments or suggestions can be sent electronically by email to rsd@eagle.org.

Terms of Use

The information presented herein is intended solely to assist the reader in the methodologies and/or techniques discussed. These Guidance Notes do not and cannot replace the analysis and/or advice of a qualified professional. It is the responsibility of the reader to perform their own assessment and obtain professional advice. Information contained herein is considered to be pertinent at the time of publication, but may be invalidated as a result of subsequent legislations, regulations, standards, methods, and/or more updated information and the reader assumes full responsibility for compliance. This publication may not be copied or redistributed in part or in whole without prior written consent from ABS.

GUIDANCE NOTES ON

RESPONSE TIME ANALYSIS FOR PROGRAMMABLE ELECTRONIC ALARM SYSTEMS

CONTENTS

SECTION 1 General

1 Application

These Guidance Notes can be of relevance to any Category III system (defined in the ABS Rules and IACS Unified Requirement E22), with real-time performance requirements for its alerts and indicators on board ABS Classed vessels, as required by ABS Rules and statutory regulations.

1.1 Audience

These Guidance Notes are intended for use by Programmable Electronic System suppliers, vendors and system integrators.

1.2 Purpose

With the increasing complexity and utilization of Programmable Electronic Alarm Systems, ABS developed a proposed methodology to further support response time analysis of alarms generated by Category III systems.

The objectives of these Guidance Notes is to utilize block diagrams for programmable electronic alarms system architectural modeling, identify the critical elements of the design by means of a response time table and to suggest applicable equations for calculating the Worst Case Response Time. The aim of these Guidance Notes is to introduce both an optional common terminology and a generalized methodology for Response Time Analysis (RTA) efforts, targeting similar quality and consistency of engineering submittal to demonstrate meeting ABS Rules requirements for Response Time Analysis.

It is also the purpose of these Guidance Notes to further clarify the proposed methodology by means of example RTA calculations.

Alternative calculations and methods used to estimate the Worst-case Response Time (WCRT) of programmable electronic alarm systems can be reviewed and evaluated on an individual basis.

2 Scope

These Guidance Notes, provide recommended methods for documenting both the real-time scheduling and the medium access control (MAC) protocols latency of processors and networks, respectively, in order to demonstrate that the expected response time of the design is achieved under worst-case operational conditions.

It is further within the scope of this document to discuss methods for showing that the software execution times of the system under design assessment, are always lower or equal to their specified deadlines under worst-case conditions during a fault-free, normal operation.

3 Background

Alerts and indicators required by ABS Rules and conditionally by statutory requirements are critical to safety and form part of a vessel's safety systems. Their proper functioning within the required timeframe are also critical to safety and need to be verified when the systems are new, throughout their full lifecycle and in particular following modifications that increase network load or modify its real-time response.

In addition to those alerts and indicators required by classification regulations, the Code on Alerts and Indicators, 2009 provides the type, location and priority for those alerts and indicators which may be required by the International Convention for the Safety of Life at Sea, 1974 (1974 SOLAS Convention), as amended; associated codes (BCH, Diving, FSS, Gas Carrier, 2000 HSC, IBC, IGC, IMDG, LSA, 2009 MODU, and Nuclear Merchant Ship Codes); the International Convention for the Prevention of Pollution from Ships, 1973, as modified by the Protocol of 1978 relating thereto (MARPOL 73/78), as amended; the Principles of Safe Manning; the Guidelines for Inert Gas Systems (IGS); the Standards for Vapour Emission Control Systems (VEC); the Performance Standards for a Bridge Navigational Watch Alarm System (BNWAS); and the Revised Performance Standards for Integrated Navigation Systems (INS), according to IMO Resolution A.1021(26).

Although relevant international standards on Programmable Electronic Systems explicitly require a response time assessment for operator's control commands (e.g., IEC 60092-504:2016/10.4.9), the response time requirements of Alerts and Indicators (e.g., IEC 60092-504:2016/9.3.3.6, MSC 87/26/Add.1 Annex 21/13.1.2.1) and their necessary assessment are not explicitly stated. Also, continuous advancements in data acquisition, software and network technologies allow additional monitoring channels to be integrated with the programmable electronic alarm systems, in excess of those required by both the statutory and the classification regulation, resulting in increased situation awareness. As a result, several IACS members including ABS, state requirements for response time assessment of critical alarms in their Rules to better promote and verify the dependability of programmable electronic alarm system designs.

The importance of response time assessment of critical alarms becomes even more apparent considering the required automatic safety functions onboard. In several programmable electronic alarm system designs, especially if they are part of an Integrated Automation System, a variable number of monitoring channels have additional functionalities that satisfy the requirements in 4-9-2/9.5.2(a) of the ABS *Rules for Building and Classing Marine Vessels (Marine Vessel Rules)*, "Threshold Warning for Safety System Activations". Consequently, the lower the real-time deadline for reaching the remote control station(s) and the bridge, the greater the time for situation assessment by the crew, manual override and intervention. Lower real-time deadlines of both alarms and safety output signals are even more important for those monitored processes where the manual intervention is not an option, as it can result in total failure of the engine and/or propulsion equipment within a short time, for example, in the case of over speed.

However, lowering the real-time deadline of any alarm signal, below the two seconds requirement included in 4-9-3/5.1.7 of the *Marine Vessel Rules*, requires response time analysis historical trends and independent benchmarking. Such design documentation that calculates the response times of current programmable electronic alarm system designs is not an easy task to complete as trends in Commercial Off-The-Shelf (COTS) hardware and software products run contrary to the drive toward response time predictability. The level of detail for the Response Time Analysis is therefore very important and is addressed herein.

4 General Definitions and Nomenclature

The following definitions and nomenclature are used in these Guidance Notes.

4.1 Definitions

Programmable Electronic System (PES): A system based on one or more programmable electronic devices, connected to (and including) input devices (e.g., sensors) and/or output devices/final elements (e.g., actuators), for the purposes of control, protection or monitoring. The term "PES" includes all elements in the system, including power supplies, extending from sensors or other input devices, via data highways or other communicating paths, to the actuators, or other output devices, associated software, peripherals and interfaces.

Worst-case Execution Time (WCET): The WCET of a computational task is the maximum length of time the task could take to execute on a specific hardware platform.

PES Worst-case Response Time (WCRT): The maximum time taken from the input to the sensor (or input device), to the output device (final element) completing its required action. This time period includes the time taken for the Programmable Electronic System to carry out any software processing under WCET and communicate with the sensors and final elements.

Task Deadline: The instant of time by which an output signal of the system (or component) is required to be produced.

Message Deadline: The instant of time by which an output network signal of the system (or component) is required to be delivered.

Medium Access Control (MAC): Controlling when data is sent and when a delay is necessary to avoid congestion and collisions, especially for topologies with a collision domain (bus, ring, mesh, point-to-multipoint topologies).

Network Load: The fractional load relative to full network capacity.

4.2 Abbreviations

FMEA: Failure Mode and Effect Analysis

ETA: Event Tree Analysis

FTA: Fault Tree Analysis

HMI: Human Machine Interface

IODM: Input Output Direct Memory

CPU: Central Processing Unit

UTP: Unshielded Twisted Pair

4.3 Lowercase Symbols

d: Cable distance between the Programmable Device and the HMI,

s: Wave propagation speed, approximately 2×10^8 m/sec for both the UTP cable and the fiber optic cable.

4.4 Uppercase Symbols

R: Worst-Case Response Time

D_{SD}: State Detection Delay

D_P: Processing Delay

$E(I_i)$: Worst-case reception time of Input i.

$E(X_i)$: Worst-case execution time of Processing Task i.

$E(O_i)$: The worst-case transmission time of Output i.

D_{PR}: Propagation Delay

D_{RT}: Retransmission Delay

N: Number of bits per frame

RT: Rate of transmission (e.g., 10 Mbps, 100 Mbps, 1 Gbps)

D_{QL}: Average latency due to queuing

D_{RT}(max): Store and forward latency of a full-size (1526 bytes) packet.

4.5 List of Applicable Rules, Regulations and International Standards

ABS *Rules for Building and Classing Marine Vessels*

ABS *Rules for Building and Classing Offshore Support Vessels*

ABS *Rules for Building and Classing Mobile Offshore Units*

ABS *Rules for Building and Classing High Speed Craft*

ABS *Rules for Building and Classing High Speed Naval Craft*

IMO Resolution A.1021(26)

IMO Resolution MSC.302(87)

IACS UR E22: On Board Use and Application of Computer based systems

IEC 61508: Functional safety of electrical/electronic/programmable electronic safety-related systems

IEC 61511: Functional safety – Safety instrumented systems for the process industry sector

IEC 60092-504: Electrical installations in ships – Part 504: Special features – Control and instrumentation.

ISO 17894:2005: Ships and marine technology – Computer applications – General principles for the development and use of programmable electronic systems in marine applications

IEC 61069-1:2016: Industrial-process measurement, control and automation – Evaluation of system properties for the purpose of system assessment

IEEE Standard 45.2: IEEE Recommended Practice for Electrical Installations on Shipboard – Controls and Automation

SECTION 2 Methodology

1 General

The proposed Response Time Analysis methodology in these Guidance Notes addresses the submittal requirement in 4-9-1/7.3.9 of the *Marine Vessel Rules*. Alternative methodologies used in submittals concerning the above Rule requirement would be considered.

2 Documentation

2.1 Architectural Models

The system under study could be simplified and generalized by means of the procedure described in Section 3 or similar. For every product model, a separate architectural model can preferably be submitted, clearly stating the product model number.

2.2 Response Time Table

Each Architectural model can be accompanied by a Response Time Table, as clarified in Section 3. Response Time Tables could be submitted in a spreadsheet format.

2.3 Calculations or Timing Diagrams

Four sets of calculations are proposed as clarified in Section 3. If Timing Diagrams are used to illustrate the necessary Worst Case Response Times scenarios defined in Section 3 in lieu of required calculations, then they can be created manually or with software.

2.4 Real-Time Scheduling Analysis or Affidavit of Schedulability

For each Central Processing Unit (CPU) included in the above diagrams, a Real-Time Scheduling Analysis for all critical alarm processing tasks could be provided to demonstrate a tighter upper bound in the Worst-Case Execution time. If Real-Time Scheduling Analyses are not available from earlier design steps, then an affidavit that the system is schedulable under Worst-case conditions can be provided, according to the template in Appendix 2. In such case, the task deadlines can be used instead of Worst-case Execution time for the Response Time Analysis as explained in Section 3.

3 Systems Categories

Systems subject to Response Time Analysis are of Category III and of Category III reduced to Category II, due to independent effective back up or other means of averting danger for the manual and automatic control functions (such as mitigation of alarms missing deadlines), according to 4-9-3/7.1 of the *Marine Vessel Rules*. Examples of assignment to system categories are shown in Section 2, Table 1 but are not all-inclusive.

4 List of Alarms

ABS *Marine Vessel Rules*, Part 4, Chapter 9, provide a list of alarms that can be considered the minimum scope of analysis in certain vessels. It is the responsibility of the analyst to also consider all other applicable systems, including but not limited to, alerts and indicators that may be required by the ABS *Guide for Dynamic Positioning Systems*, the ABS *Guide for Bridge Design and Navigational Equipment/Systems*, steering control system alarms, auto-pilot alarms, fire detection system alarms and gas detection system alarms.

SECTION 3 Response Time Analysis

1 Identification of Critical Elements

The complexity level of the response time analysis is primarily dictated by two factors. The first factor is the number of critical elements in the programmable electronic alarm system design. The second factor is the required modeling accuracy of the real-time performance aspect of each critical element, that the response time analysis can be contacted.

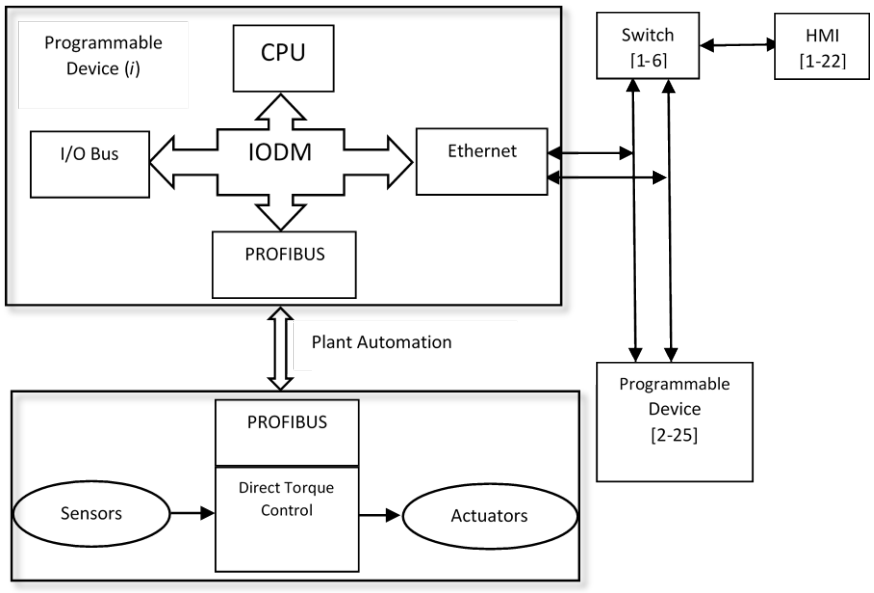
Considering the holistic PES definition in 1/4.1, it is necessary to remove from the Response Time Analysis studies all elements of the programmable electronic alarm system design that do not contribute to response time delays (i.e., power supplies and other peripherals). As a result, a generalized and simplified architectural model of the system under study, can be created.

For the purpose of these Guidance Notes it is assumed that the generalized and simplified architectural model consists of maximum three different types of hardware elements:

1. A processor that computes data,
2. A memory that allows access to stored data (read and write), including databases, and
3. A bus, which is the communication medium through which nodes of a distributed network send and receive data.

See Section 3, Figure 1 for an example of an Alarm and Monitoring System Architectural model. It denotes block diagrams as a recommended submittal for the above requirement. The numbers in the square brackets indicate how many instances of the specific component are present in the design. Other forms of architectural modeling may be considered, provided that the required information is not more complicated than the proposed block diagrams.

FIGURE 1
Example of an Alarm and Monitoring System Architectural Model in Block Diagram Format



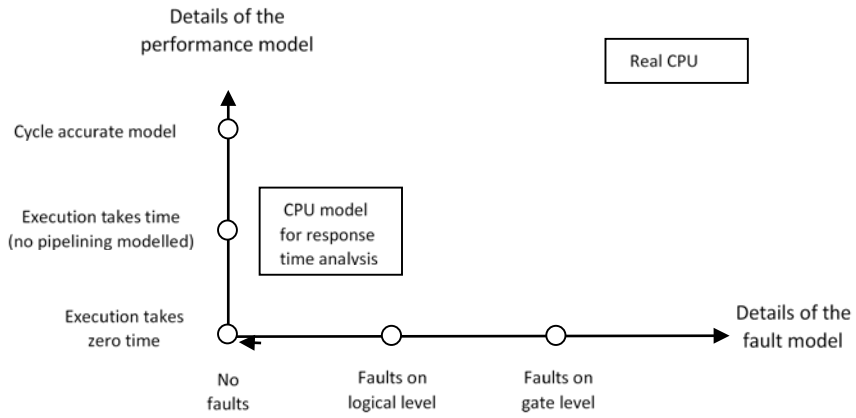
The architectural model in Section 3, Figure 1 simplifies the overall system design by omitting power supplies and other peripherals, which do not contribute to the response time performance under normal operation. It retains, however, a model of a process under Direct Torque Control (DTC), so as to illustrate two distinct automation levels with completely different response time requirements. The DTC level may have response time requirements in the region of 25 μs and it is not currently within the scope of these Guidance Notes as it does not involve a human in the control and monitoring loop.

It is noted that for the Response Time Analysis described herein, no hardware or software faults are considered. This is primarily because hardware and software faults may contribute greatly towards response time malfunctions of a real-time system and can further be considered during a risk assessment of the product unit, taking into consideration any additional sensory element interfaced for the specific ABS classed asset. For initial guidance on risk assessment processes, see Appendix 3.

2 Level of Performance Abstraction for Critical Elements

International standard IEC 61069 defines four attributes for the performance of a process measurement application: Accuracy, Precision, Resolution and Response Time. As the first three attributes primarily describe sensory elements' performance, only the fourth attribute is relevant for these Guidance Notes. Additionally, as discussed earlier and clarified further by J. Ehret's *Validation of Safety-Critical Distributed Real-Time Systems*[1], the response time performance and the fault model of any programmable, real-time electronic system are highly correlated. Consequently, deviations from the Worst-Case Response Time may provide an early indication of developing potential malfunctions in hardware, software, network (including dual transceivers used for redundancy) or even a potential for a cyber security threat. An example of the two-dimensional Fault-Performance classification scheme is presented in Section 3, Figure 2.

FIGURE 2
Example Classification of a CPU



The vertical dimension of Section 3, Figure 2 illustrates that hardware elements (CPU, Memory, Network Controller, network aggregation point) can delay alerts and indicators of a physical process because analog to digital signal processing, digital signal computation, network transmission, and storage of data takes a finite, non-zero amount of time in a PES. The horizontal dimension of Section 3, Figure 2 illustrates the fact that a programmable electronic component can fail unexpectedly during its life cycle, thus producing additional delays and/or erroneous values. Accordingly, any deviation from the Worst-case Response Time may provide early indication of developing increasingly risky conditions. Modern Integrated Automation Systems with embedded Alarm and Monitoring functionality should be able to analyze Worst-case Response Time deviations in greater depth and notify maintenance personnel accordingly. This self-monitoring feature becomes even more important in the context of Smart, Remotely Controlled, Partially Unmanned and Autonomous Ships where such early response time faults could be transferred to shore-based personnel for real-time operational risk assessment.

In the two-dimensional Fault-Performance classification scheme denoted in Section 3, Figure 2, the CPU is considered a delaying critical component due to the delay it causes in the overall Response Time Analysis. According to J. Ehret's *Validation of Safety-Critical Distributed Real-Time Systems* [1], the delay caused by a CPU operating free of faults is due to the finite, non-zero amount of time to first schedule and then to execute a software task. Every instruction set that is executed on a CPU takes a certain amount of time, regardless how short that period of time may be. Therefore, a CPU is considered as a shared resource for the programmable electronic alarm system design, since more than one alarm processing software tasks wait some predefined time to be scheduled and run on each CPU of the programmable electronic alarm system. If the programmable electronic alarm system design utilizes a Real Time Operating System, then a scheduler manages the CPU resources based on assigned task priorities and task durations.

As a result of scheduling, alarm processing software tasks do not run instantly on the assigned CPU after they have requested the computational resource, but wait for higher priority tasks and/or interrupts to complete their execution. In addition, since commercially-available CPUs are designed primarily for average case performance, advanced CPU features for average case performance such as speculation, out-of-order execution, branch prediction and complex cache replacement strategies can create additional unexpected delays in scheduling of a real-time processing task, generally referred to as "jitter". During verification it is assumed that the software program running on each programmable electronic alarm system CPU has been partitioned in a finite number of tasks and that a Worst-Case Execution Time analysis has been completed for all tasks having real-time deadlines. Furthermore, it is assumed that an appropriate task scheduling algorithm exists within the operating system of the CPU so as any real-time scheduling analysis can be realized. As such, both WCET and Real-Time Scheduling analysis (e.g., Rate-Monotonic, Earliest Deadline First, etc.) can be included in the Response Time Analysis, if they have indeed been completed in a previous design stage. In the event that such studies are not available or it is very difficult to complete due to multiprocessor architectures, the Response Time Analysis documentation can consider the deadlines of the real-time tasks as their WCET and an affidavit can be provided stating that the programmable electronic alarm system software is schedulable under worst-case conditions following the template in Appendix 2.

Similarly, the time delays caused by the networks are because an access to the physical medium and the transmission of data through the physical medium take time. This is a function of the available bandwidth, the network load and the implemented communication protocol. Depending on the Medium Access Control (MAC) sub-layer of the layer 2 of the Open Systems Interconnection (OSI) model [11], the Response Time Analysis of the network may be precisely calculated or statistically estimated. References to the various methods for calculating the Worst-Case Response Times of the most common networks found onboard ABS classed vessels are provided in the below Section 3, Table 1. Note that Section 3, Table 1 is not exhaustive and additional entries may be included in later versions of these Guidance Notes. In addition, a few simplified equations are provided in Subsection 3/4, for easy reference.

TABLE 1
Worst-Case Response Time References

Network Name	*Medium Access Control Protocol*	*Worst-Case Response Time Reference*
CAN	Carrier Sense Multiple Access with Arbitration on Message Priority (CSMA/AMP)	[4], [5], [6]
DeviceNet	Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)	[3]
IEEE 802.11e	Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)	[8]
Profibus DP	Token-Bus (IEEE 802.4 and ISO 8802.4)	[2]
ControlNet	Token-Bus (IEEE 802.4 and ISO 8802.4)	[3]
ProfiNet IRT	Token-Bus (IEEE 802.4 and ISO 8802.4)	[9]
Ethernet	Carrier Sense Multiple Access with Collision Detection (CSMA/CD)	[3]
EtherCat	Carrier Sense Multiple Access with Collision Detection (CSMA/CD)	[9]
Modbus/TCP	Carrier Sense Multiple Access with Collision Detection (CSMA/CD)	[3]

It should be noted that with the CSMA/CD protocol, any network device can try to send a data frame at any time, but each device will first try to sense whether the line is idle and available for use. If the line is available, the device will begin to transmit its first frame. If another device also tries to send a frame at approximately the same time (perhaps because of cable signaling delay), then a collision occurs and both frames are subsequently discarded. Each device then waits a random amount of time and retries its transmission until it is successfully sent. For that reason it is impossible to bound message response times in networks employing the CSMA/CD access protocol, unless switched or industrial Ethernet variations are used, like EtherCAT. In a switched Ethernet, a deliberate effort is made to suppress the standard CSMA/CD protocol in order to increase determinism. This is done by using Ethernet switches to interconnect devices, connecting only one device per switch port. With only one device per switch port, there can be no collisions and devices communicate full-duplex, at effectively double the base data rate.

However, several programmable electronic alarm system designs are based on the standard CSMA/CD access protocol and as such, a Quality of Service statement can be accepted for these designs, including a statistical estimation of the best case, average and worst-case response times, until a deterministic network can be adopted. It should be noted that requirements in MSC 87/26/Add.1 Annex 21/13.1.2.1 dictate that the alert-related communication protocol should follow a standardized concept to provide a unique identification of an alert divided into cluster, function, alert code and time. Therefore time stamping requirements may be interpreted as a mandatory function in the field input device which acquires the sensor signals, processes the values and creates the network packet with individual alarm conditions. For designs that have implemented timestamping functionality inside the field device, then consideration of a distributed real-time clock synchronization protocol may be appropriate. Then again, IEC 60092-504:2016/9.3.3.6 indicates that the *arrival* of alerts should be clearly recorded in chronological order with date and time stamp. Therefore certain designs may implement timestamping at the destination. For these designs when all three conditions above hold true (i.e., timestamping at origin, real-time clock synchronization protocol and timestamping at destination), the Quality of Service statement can be a sufficient approach until upgrading to a deterministic protocol as stated earlier. All other designs can be considered, subject to the statistical estimation of their worst-case network load.

Considering further the required modeling of critical elements, it should be noted that the origin of the above two-dimensional Fault-Performance classification scheme of Section 3, Figure 2 represents a situation in which the critical elements have neither a response time performance limitation nor a fault constraint [1]. The models of processors, networks, and memories located in the origin of Section 3, Figure 2, do not affect the response time of the system during computation, transmission, or storage. In the terminology of these Guidance Notes such models are called “ideal”, because they do not contribute significantly to the Worst-Case Response Time of the system. For example, a Dynamic Random Access Memory element delays data because a read/write action takes time as well. Very often however, the time delays caused by memory can be neglected because they are on a different scale in comparison to delays caused by CPUs or MAC protocols.

Consequently, the Response Time Analysis study may identify each critical hardware component as “ideal” or “delaying” and provide justification of such choice by means of the following example in Section 3, Table 2 (based on the Architectural Model example of Section 3, Figure 1).

TABLE 2
Response Time Table

Critical Component	*Response Time Model*	*Response Time Parameters*	*Values (sec)*
DTC PROFIBUS Controller	Ideal	Interrupt Service Routine Duration, FIFO buffer latency	2×10^{-6} sec, 5×10^{-6} sec
PROFIBUS Network	Delaying	Scan Rate	50×10^{-6} sec
PD(*i*) PROFIBUS Controller	Delaying	Interrupt Service Routine Duration, FIFO buffer latency	2×10^{-6} sec, 50×10^{-6} sec
PD(*i*) IODM	Delaying	Read/write latency	50×10^{-6} sec
PD(*i*) CPU	Delaying	Task deadline	$100 \times$x 10^{-6} sec
PD(*i*) Ethernet Controller	Ideal	Interrupt Service Routine Duration, FIFO buffer latency	2×10^{-6} sec, 3 x 10^{-6} sec
Ethernet Network	Ideal	Propagation delay	See Equation 3
Ethernet Switch(*i*)	Ideal	Average queuing latency	See Equation 5
Real Time Database	Delaying	Read and Write transaction	See Equations 6 and 7
HMI(*i*)	Ideal	Refresh rate	2×10^{-6} sec
Software Induced Delay	Delaying	Software Induced Delay	5 sec

3 Response Time Estimation

When Section 3, Table 2 has been completed, the next set of submittals denotes the estimation of all Worst-Case Response Time scenarios identified below. Following the recommendations found in IEC 61508-7/C.5.20, this can be achieved by means of either functional models (including the below test cases for simulation), timing diagrams, or using equations similar to the ones outlined in Subsection 3/4. If the same combination of hardware, software and network properties are used for all alarms under the same Worst-Case Response Time scenario, the estimation can be submitted once for all applicable alarms. Alternatively, a new estimation can be submitted for any different combination of hardware, software and networks' properties.

Worst-Case Response Time scenarios required are:

i) Alarms of systems as per 4-9-1/7.3.9 if the *Marine Vessel Rules* can be analyzed for alarm state transition immediately after the field device's read actions. This scenario is explained in Example 1 where the requirement in 4-9-3/5.1.7 of the *Marine Vessel Rules* is verified.

ii) Especially for alarms generating a safety-slow down or safety-shutdown, automatic reactions can be analyzed further for the effects that parametrized software-induced delays may have on manual override actions. This scenario is explained in Example 2 where a deadline greater than the requirement of 4-9-3/5.1.7 of the *Marine Vessel Rules* is used (software induced delay) that equals auto safety signal activation.

iii) Alarms specified in the above tables (as applicable), connected to a single I/O board can be analyzed for concurrent tripping. This scenario is explained in Example 3 where message queuing jitter and queuing latency for the selected fieldbus is analyzed.

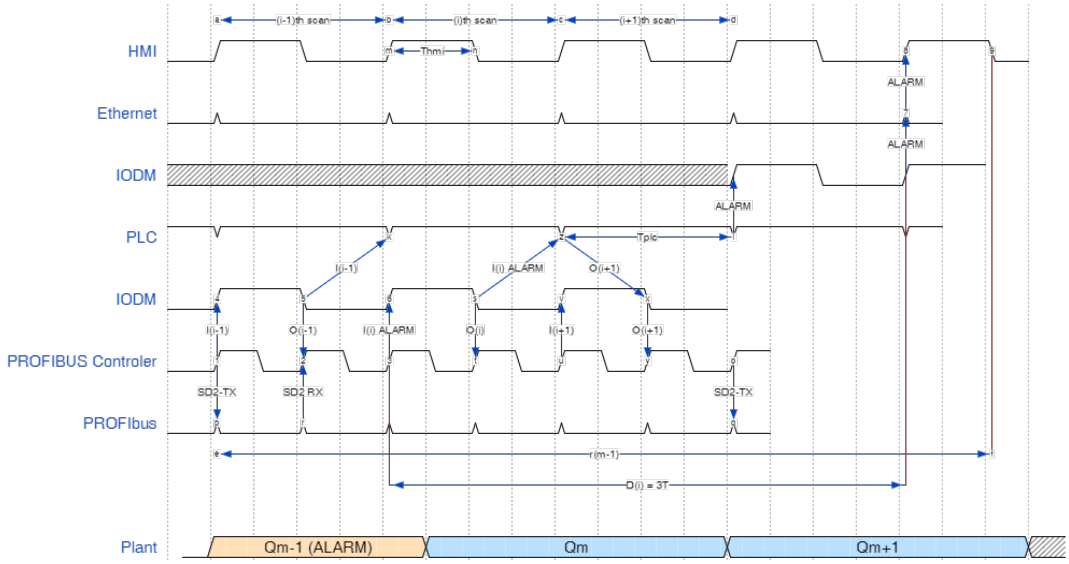
iv) Applicable alarms specified in the above tables, with permanent correlations (under the same alarm group or not), can be analyzed for concurrent tripping. The final scenario is explained in Example 4, where the performance of the HMI network load and database load (as applicable), is analyzed.

For Alarm and Monitoring System designs transmitting time-series of measurements in addition to alarm states, refer to Appendix 4.

3.1 Example 1

In Section 3, Figure 3, a digital timing diagram for the first worst-case scenario is offered as an example, based on the architectural model example of Section 3, Figure 1 and the performance modeling of Section 3, Table 2. A digital timing diagram is a representation of a set of signals in the time domain. It is a tool commonly used in digital electronics, hardware debugging, and digital communications. Besides providing an overall description of timing relationships, the digital timing diagram can help find and diagnose digital logic hazards. Note that both ideal and delaying critical components are present in the example timing diagram, so as to illustrate the different response time effects. In actual submissions of timing diagrams, ideal components can be omitted.

FIGURE 3
Example Timing Diagram



Section 3, Figure 3 above describes the first worst-case scenario of the system modeled in Section 3, Figure 1. At the i_{th} scan interval (top line), the single PLC processing task starts before the input data, $I(i)$ ALARM have been written in the Input-Output Direct Memory (IODM). This task performs an IODM read at the very beginning of each execution. As a result, the i_{th} PLC processing task is executed with the input data $I(i-1)$ stored already in IODM. The output data transmission, $O(i)$, also starts before the completion of the i_{th} PLC processing. As a result, the output data of the i_{th} PLC processing, $O(i+1)$ are transmitted over to the plant at the $(i+1)_{th}$ scan interval. In the worst-case scenario illustrated in Figure 3, the plant goes into an alarm state, $Q(m-1)$, at the exact point in time when the $(i_{th}-1)$ PLC processing task starts. The alarm reaches the IODM after the delay caused by the PROFIBUS scan rate and the PD(i) PROFIBUS Controller FIFO latency. It will then be processed at the next PLC scan interval, $(i+1)$. After input data processing, the alarm condition will be identified and written back at the IODM. The PD(i) Ethernet Controller has been defined as "ideal" and was omitted for simplicity. The switched Ethernet Network has been defined also as "ideal", but included in order to depict the insignificant delays involved. Finally, the worst-case response time for the state change, $Q(m-1)$, is calculated by Equation 1 in Section 4. The example above has the following values:

$$D_{SD} = 2 \cdot 50 \times 10^{-6} = 2 \cdot \textit{PROFIBUS Network Scan Rate}$$

$$E(I_i) = 2 \cdot 50 \times 10^{-6} = \text{PD}(i)\text{PROFIBUS Controller} + \text{PD(i) IODM}$$

$$E(X_i) = 100 \times 10^{-6} = \text{PD}(i)\ \text{CPU}$$

$$E(O_i) = D_{PR} + D_{RT} + D_{QL} << D_{SD} + E(I_i) + E(X_i), \text{ therefore}$$

$$R = D_{SD} + E(I_i) + E(X_i) = 300 \cdot 10^{-6} \text{ sec} << 2 \text{ sec deadline}$$

3.2 Example 2

The same system is used to analyze the effects of a software-induced delay on a Threshold Warning for Safety System Activation. In this case, the deadline for activating the safety signal equals the software-induced delay. However, the setup results in an error as the automatic safety signal is activated prior to the warning reaching the crew.

D_{SD} = $2 \cdot 50 \times 10^{-6} = 2 \cdot$ *PROFIBUS Network Scan Rate*

$E(I_i)$ = $2 \cdot 50 \times 10^{-6}$ = PD(*i*)PROFIBUS Controller + PD(i) IODM

$E(X_i)$ = 100×10^{-6} = PD(*i*) CPU

$E(O_i)$ = $D_{PR} + D_{RT} + D_{QL} + D_{St} = 5$ sec

R = $D_{SD} + E(I_i) + E(X_i) + E(O_i) = 5.3$ sec ≥ 5 sec DEADLINE ERROR

In a different situation under the same scenario, the software-induced delay may be greater than the duration of the abnormal condition altogether and after auto-slow down or auto-shutdown activation, the alarm condition may disappear entirely. In such situation, the machinery slows or shuts down with no previous warning. Especially in the case that such safety activation is initiated by optional condition monitoring signals, integrated in the Alarm and Monitoring System (e.g., Bearing Wear Monitoring), crew manual override reaction time can be verified by including such cases in the second scenario.

3.3 Example 3

In the third example, the ability of the field devices to concurrently process all their inputs is calculated (worst-case condition). The packaging of the network response frame (if different than the single alarm case), the additional processing time (if any) and the transmission delay from the field input/output device to the process controller is calculated. In the below calculations, it is assumed that all alarm inputs (16 or 32) are always included in the fieldbus response frame so the Worst-case Response Time is the same as Example 1. In such case, the third Worst-case Response Time scenario can be omitted.

D_{SD} = $2 \cdot 50 \times 10^{-6} = 2 \cdot$ *PROFIBUS Network Scan Rate*

$E(I_i)$ = $2 \cdot 50 \times 10^{-6}$ = PD(*i*)PROFIBUS Controller + PD(i) IODM

$E(X_i)$ = 100×10^{-6} = PD(*i*) CPU

$E(O_i)$ = $D_{PR} + D_{RT} + D_{QL} << D_{SD} + E(I_i) + E(X_i)$, therefore

R = $D_{SD} + E(I_i) + E(X_i) = 300 \times 10^{-6}$ sec << 2 sec deadline

3.4 Example 4

Depending on the Alarm and Monitoring System design, class requirements for the response time of alarms impose real-time constrains in the transactions of the Alarm Database. Consequently, database transactions require response time validity as a late commit may result in an alarm missing its deadline. Quality of Service (QoS) statements are more accurate than Worst-case Execution Times at this level, due to the dynamic variation of the database workload and the access patterns of transactions. Exceptions may be Alarm and Monitoring System designs utilizing Real-Time databases.

For the Alarm and Monitoring System under study there are two distinct transaction types. The first is the alarm(s) update transaction, containing the alarm data objects and the second is the HMI alarm(s) refresh query. The former transaction has a higher priority than the later. Also the operation(s) of the former transaction is always a *write* where the operation(s) of the later transaction is always a *read*. There is a certain execution time associated with each operation and the execution time of a transaction is the sum of the execution time of all its operations. However, it is very rare to be provided explicitly in real applications. As a result, the notion of *Execution Time Estimation Error*, as defined by Y. Wei et al., in *QoS Management in Distributed Real-Time Databases*[7] is used, having normal distribution with a mean of 20% and a standard deviation of 10%. For the purpose of this example, the time required for one *read* or *write* operation is a maximum of 2.4 msec including the additional average *Execution Time Estimation Error*[7]. In the example Alarm and Monitoring System there are 10 alarms (of the same alarm group) with permanent correlations (i.e., always activated at the same time).

D_{SD} = $2 \cdot 50 \times 10^{-6} = 2 \cdot$ *PROFIBUS Network Scan Rate*

$E(I_i)$ = $2 \cdot 50 \times 10^{-6}$ = PD(*i*)PROFIBUS Controller + PD(i) IODM

$E(X_i)$ = 100×10^{-6} = PD(*i*) CPU

$E(O_i)$ = $D_{PR} + D_{RT} + D_{QL} + D_{b\_write} + D_{b\_read} = 48 \times 10^{-6}$ sec

R = $D_{SD} + E(I_i) + E(X_i) + E(O_i) = 348 \times 10^{-6}$ sec << 2 sec deadline

4 Recommended Equations

4.1 Equation 1: Worst-case Response Time

$$R = D_{SD} + D_P$$

where

R = Worst-case Response Time

D_{SD} = State Detection Delay

D_P = Processing Delay

4.2 Equation 2: Processing Delay

$$D_P = E(I_i) + E(X_i) + E(O_i), \qquad i \in N$$

where

D_P = Processing Delay

$E(I_i)$ = worst-case reception time of Input *i*

$E(X_i)$ = worst-case execution time of Processing Task *i*

$E(O_i)$ = worst-case transmission time of Output *i*

4.3 Equation 3: The Worst-case Transmission Time of Output *i*

$$E(O_i) = D_{PR} + D_{RT} + D_{QL} + D_{db} + D_{HMI} + D_{SI}$$

where

D_{PR} = Propagation Delay

D_{RT} = Retransmission Delay

D_{QL} = Queuing Latency

D_{db} = average database queuing latency

D_{HMI} = HMI refresh rate

D_{SI} = Software Induced Delay

Note: The above delays are design-specific and as such may or may not be applicable to all designs. It is the responsibility of the response time analyst to include all applicable delays affecting Output *i*, including repeated calculations for network segments with different transmission rates.

4.4 Equation 4: Propagation Delay

$$D_{PR} = d/s$$

where

D_{PR} = Propagation Delay

d = cable distance between the Programmable Device and the HMI,

s = wave propagation speed, approximately 2×10^8 m/sec for both the standard Cat 5 UTP cable and the fiber optic cable

4.5 Equation 5: Retransmission Delay

$$D_{RT} = N/RT$$

where

D_{RT} = Retransmission Delay

N = number of bits per frame

RT = rate of transmission (e.g., 10 Mbps, 100 Mbps, 1 Gbps)

Note: Ethernet Switches must allow a minimum idle period between transmissions of Ethernet packets known as the Inter-Packet Gap (IPG). A brief recovery time between packets allows devices to prepare for reception of the next packet. The standard minimum IPG is $96t_{bit}$, so it can be omitted.

4.6 Equation 6: Queuing Latency

4.6.1 Average Queuing Latency for Switched Ethernet

$$D_{QL} = Network\ Load \times D_{RT}(\max)$$

where

D_{QL} = average latency due to queuing

Network Load = fractional load relative to full network capacity

D_{RT}(max) = Store and forward latency of a full-size Ethernet frame

4.6.2 Queuing Latency for CAN

$$D_{QL(m)}^{n+1} = B + \sum_{\forall j \in hp(m)} \left\lceil \frac{D_{QL(m)}^{n} + J_j + t_{bit}}{T_j} \right\rceil C_j$$

where

$D_{QL(m)}^{n+1}$ = latency due to queuing of $n + 1$ iteration for message m. Because the recurrence relation monotonically increases in $D_{QL(m)}$, the iteration should start with a value $D_{QL(m)}^{0} = 0$ until convergence

B = blocking time of the network due to transmission of lower priority messages. For worst-case calculations, B = 130 μsec for 1Mbit/sec transmissions

$hp(m)$ = set of all messages in the system with higher priority of message m

J_j = jitter in the queuing of message j

t_{bi} = time required to transmit one bit

T_j = period of message j

C_j = time taken to transmit message j on the bus including all overhead bytes. It is a function of bytes in the message.

4.7 Equation 7: Database Write Delay

$$D_{b\_write} = F \times \frac{W}{F} \times OT$$

where

F = number of Alarm Frames in the queue

$\frac{W}{F}$ = *Write* operations per frame

OT = *Write* Operation Time

4.8 Equation 8: Database Read Delay

$$D_{b\_read} = F \times \frac{W}{F} \times OT$$

where

F = number of Alarm Frames in the queue

$\frac{W}{F}$ = *Read* operations per frame

OT = *Read* operation Time

4.9 Equation 9: TCP/IP Packet Length Probability Distribution for Non-switched Ethernet

Each TCP/IP packet length produced by each Programmable Electronic Controller initially presents a uniform distribution [10], if no network measurements have been completed in priory.

$$P_{(x)} = \frac{1}{L_M - L_m}$$

$x \in [L_m, L_M]$

where L_m and L_M are the minimum and maximum normalized packet lengths respectively defined as below:

$$L_m = \frac{\text{minimum packet length}}{MTU} = \frac{\text{20 Bytes IP Header}}{MTU} = \frac{28}{1500}$$

$$L_M = \frac{MTU - \text{LLC header}}{MTU} = \frac{1500 - 8}{1500}$$

Other values for L_m are possible depending how the protocols are combined.

When the TCP/IP packet passes through an aggregation point (i.e., hub, non-dedicated switch), it suffers a non-linear transformation depending on the aggregated traffic at that point. According to E. Castro, et al., in *Probability Density Functions Of The Packet Length For Computer Networks With Bimodal Traffic* [10], the probability density function transformation, at the aggregation point is given by:

$$\ell = \frac{M - \cos(x)}{2}$$

$x \in [0, \pi]$

where

M = normalized MTU (1500 bytes/1500 bytes)

ℓ = output that represents the packet length (size) and it is a function of x

x = input random variable

Accordingly, the probability density function of the packet length after the aggradation point is given by:

$$P_{(\ell)} = \frac{P_{(x)}}{\left|\frac{d\ell}{dx}\right|} = \frac{P_{(x)}}{\frac{1}{2}\sqrt{1-(M-2\ell)^2}} = \frac{\frac{1}{L_M - L_m}}{\frac{1}{2}\sqrt{1-(M-2\ell)^2}}$$

APPENDIX 1 References

1. Ehret J., *Validation of Safety-Critical Distributed Real-Time Systems*, Doctoral Thesis, Munich Technical University, Munich 2003.
2. E. Tovar, F. Vasques, *Cycle time properties of the Profibus timed-token protocol*, Comput. Commun. 22(13), 1206–1216 (1999)
3. F.L. Lian, J.R. Moyne, D.M. Tilbury, *Performance evaluation of control networks: Ethernet, ControlNet, and DeviceNet*, IEEE Control Syst. Mag. 21(1), 66–83 (2001)
4. K. Tindell, A. Burns, *Guaranteeing message latencies on control area network (CAN), in Proceedings of the 1st International CAN Conference*, Mainz, Germany, September 1994
5. K. Tindell, A. Burns, A.J. Wellings, *Calculating controller area network (CAN) message response times*, Control Eng. Pract. 3(8), 1163–1169 (1995)
6. M. Di Natale, *Scheduling the CAN bus with earliest deadline techniques*, in Proceedings of the 21st IEEE Real-Time Systems Symposium, Orlando, Florida, USA, September 2000
7. Y. Wei et al., *QoS Management in Distributed Real-Time Databases*, [Online], Available: https://www.cs.virginia.edu/~stankovic/psfiles/rtss03.pdf , [Accessed 18 08 2016].
8. Yunli Chen, Qing-An Zeng and Dharma P. Agrawal, *Performance evaluation for IEEE 802.11e enhanced distributed coordination function*, WIRELESS COMMUNICATIONS AND MOBILE COMPUTING, 2004; 4:639–653
9. Gunnar Prytz, *A performance analysis of EtherCAT and PROFINET IRT*, 13th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA) in Hamburg in September 2008.
10. E. Castro, et al., *Probability Density Functions Of The Packet Length For Computer Networks With Bimodal Traffic*, International Journal of Computer Networks & Communications (IJCNC) Vol.5, No.3, May 2013
11. International Organization for Standardization *(1989-11-15). "ISO/IEC 7498-4:1989 – Information technology – Open Systems Interconnection – Basic Reference Model: Naming and addressing"*.

APPENDIX 2 Affidavit of Schedulability Templates

Declaration of Central Processing Units Schedulability, for Components, Products or Systems included in and offered for the ABS Type Approval Program

Email the completed form to: The ABS Technical Office closest to you.

Company Name:

ABS Client Number:

In accordance with the submittal requirements in the Guidance Notes on Response Time Analysis, all Central Processing Units identified as critical delaying components during the analysis, deploy tasks that are schedulable by a real-time scheduling algorithm and their worst-case Execution Time is lower than the assigned deadlines under normal operational conditions.

Print Name: _____

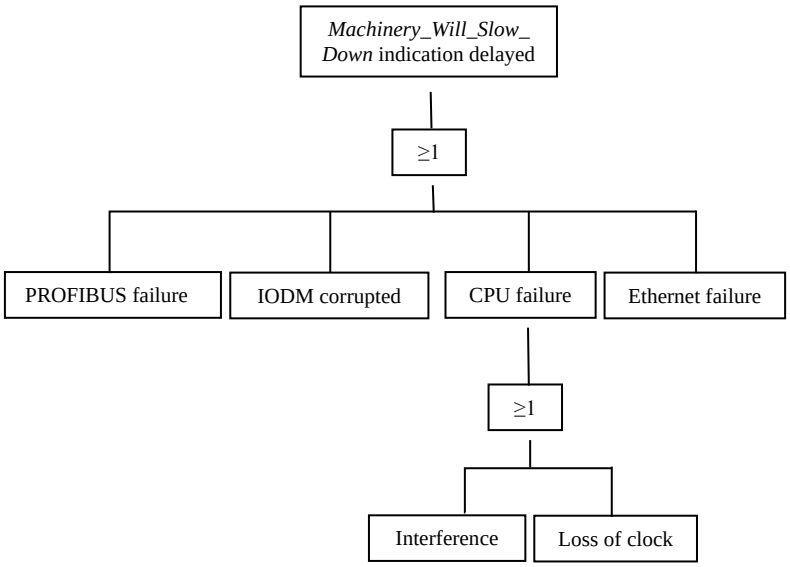
Title: _____

Date: _____

APPENDIX 3 Risk Assessment Discussion

For initial guidance on the risk assessment process targeting the PES designs, it should be noted that commonly used risk assessment techniques include, but are not limited to Failure Mode and Effect Analysis (FMEA), Event Tree Analysis (ETA) or Fault Tree Analysis (FTA), and can reduce the number of physical faults of hardware elements and faults caused by physical interferences within a complex automation system that need to be considered during plan approval. For example, Appendix 3/Figure 1, shows a simple fault tree of an Alarm and Monitoring System (Alarm and Monitoring System) as a result of a Fault Tree Analysis (FTA), based on the example Architectural Model of 3/Figure 1. Note that this example fault tree is mostly incomplete and shown here to demonstrate the principle of this approach only.

FIGURE 1
A Simple Fault Tree



The top level (hazardous event), is that the Threshold Warning for Safety System Activation *Machinery_Will_Slow_Down*, has been delayed (one or more times) before reaching the HMI level, thus missing its predefined deadline. A consequence of such delay can be that the crew is not able to manually override this slow down signal prior reaching the actuator denoted in Appendix 3, Figure 1, resulting to an unnecessary slowdown of the process under control. This event can be caused either by a fault within the PROFIBUS network, or by a corrupted segment of the IODM component, or by a failure of the CPU, or by a fault within the Ethernet network. A failure of the CPU can be caused either by interference or by losing the CPU clock. Note that only one fault at a time is considered (single-fault assumption) in the FTA. When a fault in a CPU is present, a task running on that CPU is either delayed by a specified amount of time (e.g., caused by spurious interrupt load of a CPU) or is not processed at all (e.g., caused by a reset of a CPU).

Evidently, an idealized fault model of the critical elements is more appropriate during Response Time Analysis design verification as certain commissioning details (e.g., CPU locations and EMI levels) are still undefined at this stage.

For additional guidance on required Failure Mode and Effect Analysis submittals, interested readers are referred to the ABS *Guidance Notes on Failure Mode and Effects Analysis (FMEA) for Classification*.

APPENDIX 4 Alarm and Monitoring Systems with Optional Digital Measurements Transmission

Regardless of the physical processes that need to be monitored by digital equipment, the Nyquist–Shannon sampling theorem dictates the minimum sampling rate. Specifically:

> *If a function x(t) contains no frequencies higher than B hertz, it is completely determined by giving its ordinates at a series of points spaced 1/(2B) seconds apart.*

However, if the physical process is digitized faster than the network can transmit the digital values, then the network will be saturated and data will be queued at the buffer (unless it is discarded). In designing an integrated monitoring functionality, both the effective bandwidth and the physical processes sampling rate must be considered. Although high sampling rates improve signal reconstruction in traditional data acquisition systems, they also induce high traffic loads on the network medium for integrated monitoring systems. High traffic loads can increase mandatory network messages time delays and can degrade the Alarm and Monitoring System performance in case of erroneous network sharing. A general rule is that the control networks' response time under worst-case conditions should be less than the sample time of data being gathered.

For calculating the induced network load based on the monitoring of a new analogue process, the following example calculations can be used:

Analogue to Digital Converter Resolution (ADC): 16 bits

ADC Total Measurement Range: 0-5 V

ADC Shunt Resistor: 100 Ω

1. Voltage Drop across the Shunt Resistor for a typical 4-20 mA signal: (20 mA – 4 mA) × 100 Ω = 1.6 V
2. Total Measurement Percentage consumed by the 4-20 mA loop: 1.6 V × 100/5 V = 32%
3. ADC counts applied to the 4-20 mA loop = 2^{16} × 32% = 20971 counts
4. Digital Signal Resolution or Least Significant Bit (LSB): (max Process Value)/20971
5. Define the dead-band step, usually ten to one hundred times more the (max Process Value)/20971.
6. Define how often the signal value will be updated while in the dead band (i.e., smoothing function) for proper Alarm and Monitoring System network utilization.
7. Define how often the signal will be updated when outside the dead band once (step change) for proper Alarm and Monitoring System network utilization.
8. Define how to transmit continuous signal changes (i.e., always outside the dead band) so as not to saturate the network and not to lose signal information (i.e., local processing with accurate timestamps and then transmit once all values when possible).
9. Define network message size for each new signal including network overhead.
10. Include new network message length and frequencies in the response time analysis.
11. Submit the analysis to ABS for review of the calculations.