A Method for Performability Study on Wide Area Communication Architectures for Smart Grid

Tesfaye Amare
Information Security and Communication Technology
NTNU – Norwegian University of Science and Technology
Trondheim, Norway
Email:tesfayez@ntnu.no

Charles M. Adrah
Information Security and Communication Technology
NTNU – Norwegian University of Science and Technology
Trondheim, Norway
Email:charles.adrah@ntnu.no

Bjarne E. Helvik
Information Security and Communication Technology
NTNU – Norwegian University of Science and Technology
Trondheim, Norway
Email:bjarne@ntnu.no

***Abstract*—An extensive use of ICT is a key feature in the development of next generation smart grids. The ability of the ICT system to meet the real time requirements of the powers system, even when it is degraded due to failures, is essential. This simultaneous study of dependability (reliability) and performance are referred to as performability.**

This paper presents a method for a performability study on ICT support system of smart grid. It looks into how performance associated properties (timing failures) can be modelled together with properties affecting dependability such as omission or conventional component failures. A two tier model using ns-3 and SAN is developed to study the peformability of an IEC 61850 based communication infrastructure for a protection application. For illustration, a simulation is conducted to study the reliability and unavailability of an IEC 61850 based communication architecture, where the impact of both timing failures and omission failures are investigated and compared. The result revealed that the availability and reliability is highly dependent on the requirements for the protection application, maximum delay per packet and maximum number of consecutive delayed packets the protection application can tolerate. It also shows that timing failures have a higher impact than omission failures for a protection application with shorter time requirement.

***Keywords*—Performability, Smart Grid, Stochastic Activity Networks,IEC 61850, Modeling**

I. Introduction

In Smart grid, the electricity distribution and management is upgraded by incorporating advanced ICT support system and extensive computing capabilities for improved control and reliability. Massive use of distributed energy resources, advanced data acquisition, smart metering and automation of the grid operation is increasing the complexity of the grid and forcing the grid to highly rely on the underlying ICT support. Thus, the digital communication between Intelligent Electronic Devices (IEDs) has become a key feature in the development of the next generation smart distribution grid. The grid, being a very critical infrastructure,the dependability (availability, un-interrupted service) and performance (latency/real-time, throughput) of this ICT support system has to be carefully studied.

Dependability and performance are properties of systems that are commonly studied separately and a complete assessment of the system is often obtained by taking the results of each type of evaluations. For ICT systems of even moderate complexity, individual assessment of performance and dependability can not be combined in this fashion to determine the overall quality of service [1]. This is mainly due to properties of one affecting the other. For instance, in a fault tolerant system with redundancy, a fault may not necessarily result in failure of the service, but it may degrade the performance, i.e., the system might be regarded as available (from conventional dependability point of view), but it may not meet the timing requirements. What we refer as *Performability* is used to capture the combined influence of dependability and performance.It measures the ability of the system to provide a particular service with sufficient performance over a certain time, even in the presence of failures [1].

The aim of this paper is to propose a method for a performability study of ICT support system of smart grid. The focus will be on a communication infrastructure for a protection of power lines connecting substations where a wide area network based on IEC 61850 is considered.

The rest of the paper is organized as follows. The next section give a summary of related work on dependability and performance of communication systems for protection in smart grid and put this paper into that context. A brief background knowledge and presentation of the wide area communication architecture is discussed in Section III. Section IV presents the proposed method and model. In Section V, the simulation scenario and an illustration of the results is presented. Lastly, Section VI gives conclusive remarks of the work.

II. Related work

The dependability and performance of communication systems for protection in smart grid has been studied by some, but not in a comprehensive way. Papers such as [2], [3], [4], [5] studied the reliability of an IEC 61850 based substation communication networks (SCN). Various techniques has been used; Chen et al. used reliability block diagrams (RBD) and fault tree techniques, Wafler et. al used RBD and Markov modeling while Zeng et. al used stochastic petri nets for studying the dependability of wide area networks in smart grid

substations. A probabilistic model checking for conducting the safety-critical reliability analysis of the protection systems of smart grids is used in [2]. Most of these works has focused on studying the dependability of the SCN focusing on omission failures. They do not look into performance related issues; for e.g. failure to meet the timing requirements are not considered. For the ICT support in a smart grid, timing issues are an integrated part of the system specification (such as the protection application) and the dependability evaluation shall also verify that the system is doing what it should do, in a timely way.

On the other hand, some works such as [6], [7], [8], [9], [10], [11], [12], [13], [14], [15] studied the performance of communication systems in smart grid. Paper such as [9], [10], [8], [11] looked into performance analysis in SCNs. Kanabar et. al[8] evaluates the performance of sampled value packets over the IEC 61850-9-2 based substation. Xiang Lu et. al [12] conducted experimental study on the delay performance of DNP3 over TCP/IP communication in smart grids. In [13], the performance of a communication network for a Nordic 32 power system is studied under different QoS mechanisms. Ferarri et. al [14] studied the delay performance of communication in substations in the case of most common network failures. Performance evaluation of various possible communication systems between IEC 61850 based DAS and DER is presented in [15]. Few papers such as [6], [7] have also looked into the performance analysis in communication between substations. Yiming Wu et. al. [6] presented a study on the effect of bursty traffic on delay measurement on a wide area communication for IEEE 14 bus system. Ali et. al [7] studied the performance of IEC 61850 for peer-to-peer communications between substations. Similarly, most of the papers that has looked into the performance analysis does not consider factors associated with dependability analysis such as failure of components that could also affect the performance. With such approaches (individual evaluation of dependability and performance), decision making would be challenging as it lacks the ability to give a comprehensive measure(full picture) of the QoS.

This paper looks into how performance associated properties (timing failures) can be modelled together with properties affecting dependability of the ICT support system in smart grid. A two tier model is presented where Ns-3 is first used to study the performance characteristics. Then, the result from the Ns-3 model are stored in a C++ static library for a use in the second tier stochastic activity network model which is used to study the reliability and dependability of the communication infrastructure for protection in the smart grid. To demonstrate the capabilities of the model, the impact of timing failures on the dependability of the communication system is investigated and compared with (omission) failure of components.

III. System Considered

The study considers a communication infrastructure for a protection of power lines connecting substations where a wide area network based on IEC 61850 is part of the system. The communication architecture and major assumptions are presented below.

A. Wide area communication in smart grid

Wide area networks form the communication backbone to connect the highly distributed smaller area networks that serve the power systems at different locations [16]. They are used to transport real-time measurements or local SCADA information taken at the electric devices (from substations) to the control centers or to neighbouring substations and carry instruction or actuator commands from control centers to electrical devices in the substations.

B. Communication architecture

An IEC 61850 based wide area communication between substation using a V-LAN tunneling setup is considered. It is a ring architecture, as shown in Figure 1, where gateway switches from each substation are connected through a ring network by a fiber line. The substation networks are connected to the control center or SCADA controller through the gateway switch at substation 4. Each substation are assumed to generate a background traffic (k) from inside which has to be carried through the ring network towards the control center. In addition, all substations are assumed to exchange control information (such as sampled value and GOOSE messages) to each other.

C. Latency requirement

Real time performance, i.e., the latency of packets trough the network, is critical in smart grid communications. The messages communicated between various entities within the smart grid have different network latency requirements. The protection function is among the applications that are most demanding [16]. The protection information exchange between intelligent electronic devices is useful only within a predefined time frame. If the communication delay exceeds the required time window, the information does not serve its purpose and the grid may be damaged. Based on the IEC 61850, the maximum latency for a protection information external to substations, is in the range of 10 to 100 ms [16].

D. Failure Semantics

The communication in smart grid may fail in a number of different ways. In this study the two failure modes *omission* and em timing are considered. Based on [17], the failures where no service /message is delivered are referred as omission failures. In a separate dependability analysis, discussed in the introduction, typically just these are regarded. Timing failures occurs when the system does not meet its specified timing requirements. These are important in smart grids as discussed in section III-C.

IV. Modeling

This section presents the model used for studying the performability, i.e., a comprehensive dependability analysis of the communication system for a protection in smart grid, incorporating the impact of timing failures. It is based on the

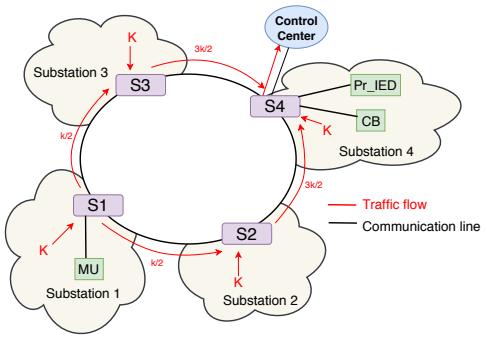


Fig. 1. Ring architecture of the ICT support system.

stochastic activity network (SAN) formalism [18] and uses the Möbius tool [19] in combination with the Ns-3 network simulator [20]. This is described in Subsection IV-A, which gives a high level description of the method employed. Then, the Ns-3 based model for the traffic handling of a single link is presented in Subsection IV-B. Finally, the details on the components SAN model are described in Subsection IV-C.

A. Method

In designing the tool, the main goal is to propose a method which is able to model the packet level dynamics of the communication infrastructure, capture timing failures and include these failures into the dependability study of the whole distribution network.

Performance studies often require modeling the packet level detail of the system while reliability/dependability studies usually take into account a relatively rare events such as failures, repairs, dependencies and interaction between components. In order to properly characterize timing failures, it is necessary to model the packet dynamics. However, modeling the ICT support system with such level of detail together with dependability simulation models with rare event failures that occur once in years, will be very time consuming and inefficient. Hence, the main issue in a performability study of the grid is the inclusion of timing failures with the other (omission) failures in the system, despite the two have different characteristics.

Figure 2 shows the employed method and Figure 3 illustrates the schematic representation of the proposed tool. As shown in Figure 2, the communication architecture has to be first identified together with the failure and recovery rates of its components. The types of traffic, traffic flow pattern and traffic parameters have also to be defined and set. Then, the background traffic is classified into a number of sets ranging from the minimum to maximum values the network can potentially carry.

The proposed method has two stages. On the first stage, a simple model is used to study the delay performance on a single link (delay on a switch towards a link). Then, the results from this model are used on another model which is used to study the performability of the whole architecture. The first stage single link model is presented in Figure 4. It consists two end points (MU and Pr_IED) that are connected with an Ethernet switch. As shown in Figure 3, Ns-3 is used to model the single link for a set of cases with the different environment, i.e., a set of possible background traffic scenarios a given link could have. For each background traffic scenario, Ns-3 simulations are done to study and measure the delay introduced to sample values that are sent between the two endpoints. A real time hardware in the loop set up (HIL) is also used to model the single link for the purpose of validation and calibration of the Ns-3 model. For a selected set of background traffic, measurement from the HIL is used to validate the results from Ns-3 simulation.

The measurements from Ns-3 are then used to create a static C++ library (*Delay.a*) that maps the delay measurements with the various set of background traffic. The C++ static library is made for a use in the second stage model where the performability of the ICT support system is studied.

A stochastic activity network model (SAN) is used to study the performability of the whole communication infrastructure. All major events such as failure and repair of components are modeled with the SAN using the Möbius tool [19]. Timing failures are also modeled by SAN, but with the data from the static C++ library externally linked with the Möbius compiler.

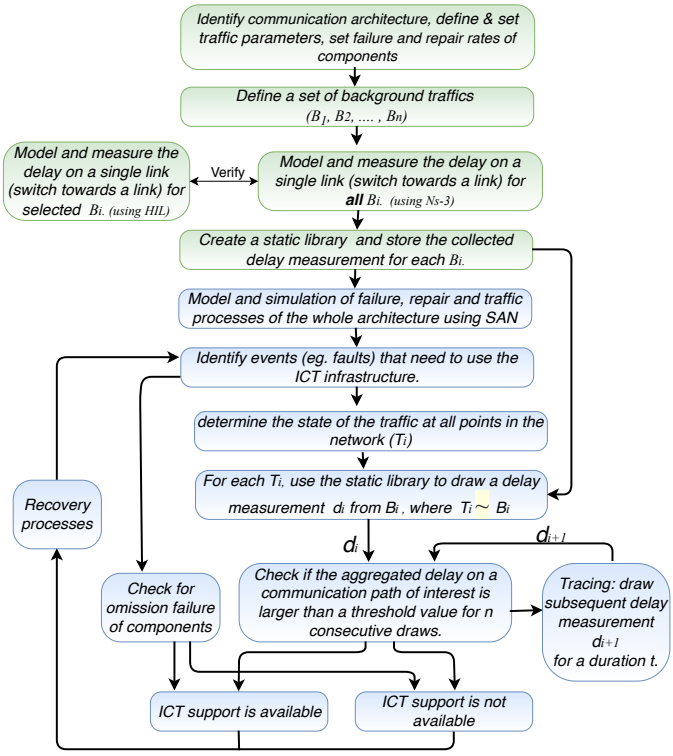


Fig. 2. The proposed method.

The SAN model is developed for an event driven simulation. Whenever an event(for e.g., power failure) that need to use the communication infrastructure occurs in the simulation, the model first determines the state of the traffic through out the communication network. Then, it will use this information to

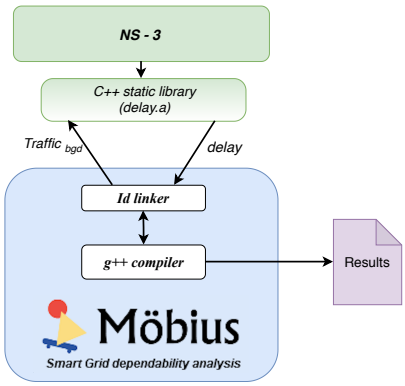


Fig. 3. Schematic representation of the proposed tool.

draw the delay measurement of each link (switch towards a link) from the external library.

The collected measurements are then recorded as values in the extended places in Möbius , and might be acted upon in further simulations, i.e., once the measurements are known at all points in the network, decisions are made if there will be a timing failure or not by comparing the aggregated delay from a path (communication line) of interest with a threshold value. The ICT support is considered as unavailable if either a timing failure as stated above occurs or if there is omission failure of components that are necessary for the protection application.

B. Methods to capture network delays

In this section, we show how network delays and effects on the single link model are measured. Both approaches, the Ns-3 model for studying all the scenarios and the HIL for validation, are presented.

1) Real time Hardware-in-the-loop prototyping: Hardware-in-the loop testing platform combined with communication network emulator have been proposed for testing of protection algorithms in inter-substations and even wide area networks. It enables modelling of communication network impairments to study impact on overall protection performance [21], [22].

In this work, we set up a simple HIL involving OPAL-RT simulator, communication emulator, practical network switch and relays to measure the delays experience in the network by a specific protection application traffic. Two substations made to share sample value (SV) measurements for a protection application. A separate background traffic which is generated from a simulated video traffic source, is added to the network traffic mix. Then, we measure the delay incurred on the SV traffic for a 1 minute duration. Different background traffic sources are used and the delay impact on the SV traffic is measured for each cases.

2) Ns-3 prototyping: Ns-3 [20] is an open-source discrete event simulator that provides support for network protocol simulations. In studying the various scenarios, Ns-3 model is easy to setup the experiment and gives full control in setting the model/traffic parameters. For these reasons, all cases of network delays incurred on SVs are modelled in Ns-3. However, the Ns-3 may not be as representative as the HIL. To improve the accuracy of the Ns-3 model, HIL results are used to calibrate it before taking measurement for all the scenarios. For a selected background traffics, HIL measurements are used to validate the result from the Ns-3 simulator.

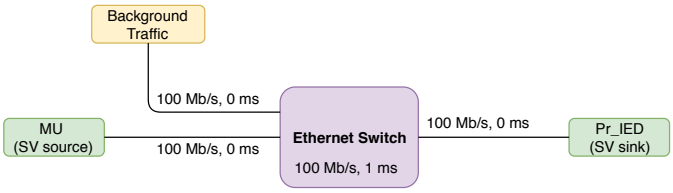


Fig. 4. The single link Ns3-HIL model

The Ns-3 prototyping is achieved by modelling the SV as a traffic source with the IEC61850 properties. SV are sampled measurements of current and voltage generated from devices called merging units. Assuming $50\,\mathrm{Hz}$ and a sampling rate of $80\,\mathrm{samples/cycles}$, SV generated will be $4000\,\mathrm{packets/second}$. Hence we set our traffic source as a constant bit rate traffic source to achieve this property of $4000\,\mathrm{packets/second}$.

The background traffic source is modelled using video trace files obtained from Telecommunication Networks (TKN) Group at Technical University Berlin [23] (The trace library is available at http://www-tkn.ee.tu-berlin.de/research/trace/trace.html). Different combinations of this sources are used to create different background traffic scenarios. The two sources, SV and background traffic, are then connected to an Ethernet switch as shown in Figure 4. A sink node on the other side of the switch is used to look into the time stamps of the packets and collect the network delay measurements.

.

C. SAN models

A Stochastic activity network model using the Möbius tool [19] is used. It is a general and modular stochastic model, which is built from atomic block models. First, a Möbius atomic model is developed for all individual components of the communication architecture proposed in Section III-B. Then, the overall system is modelled by connecting the atomic sub-models using the Join formalism in Möbius . The reward model functionality in Möbius is used to collect statistics of interest.

Atomic models are developed for the individual components of the IEC 61850 based architecture shown in Figure 1. Detailed models of components can be found in [24]. Below is a summary of some of the atomic model types extended for this study. The extended places in Möbius are used to create instances of the model types. Extended places are special elements in the SAN formalism that allows the model to handle the representation of structures and arrays of primitive data-types(places). Input and output gates, red and black boxes of Figure 5 - 7, are used to define the enabling condition and consequences of an activity or state transitions in the model.

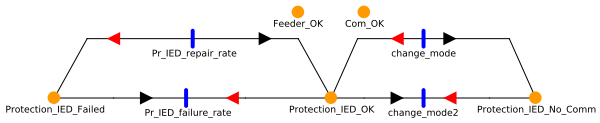


Fig. 5. An atomic model of Protection-IED.

1) Protection IED:- : Figure 5 shows the atomic model for a protection IED, one of the important components in the communication architecture for smart grid protection presented in Figure 1. It consists of four extended places; Working (*PR_IED_Ok*), failed power supply - No power (*PR_IED_No_Power*), failure in communication link - No communication (*PR_IED_No_Comm*) and Permanent failure (*PR_IED_Failed*). From initial working state in *PR_IED_Ok*, a protection IED could end up in a *PR_IED_No_Comm* state if the communication nodes/links towards it are not in their working state.

A working state in *PR_IED_Ok* instantly switch to a no power state in *PR_IED_No_Power* if its power supply is lost. Protection IEDs could fail(omission failure) from all other states to a failed state in *PR_IED_Failed* which needs maintenance. Shared states between the *Protection_IED* and other components are modeled by the unconnected extended places at the top, (*Feeder_OK* and *Com_OK*). This two shared states are used to model the interaction and dependencies with the other atomic models.

2) Background traffic generator:-: Figure 6 shows the atomic model for background traffic generator. It is used to model the varying background traffic carried by the switches of Figure 1. It is also used to determine the delay a packet would experience when it passes through on a certain switch interface towards a link at a given instant of time. In this study, we have considered video traffic (such as for monitoring power lines) as a background traffic which flows from the substations to the control center. It is assumed that an average rate of K Mps is injected to each switches accounting for the video traffic generated from inside the substations.

The model consists of three extended places; Normal, Peak and *Delay_On_Switch*. A set of regular and peak background traffic values are defined and modeled by different markings of the *Normal* and *Normal* extended places. *Normal* is used to model regular traffic conditions while *Peak* is used to model peak traffic that rarely occurs.

Rates are defined to vary the background traffic either within the normal/peak values or between peak and normal values. The following parameters are used to characterize the background traffic:-

- K_n:-an average rate of the normal traffic in Mps.
- K_p:- an average rate of the peak- time traffic in Mps.
- K_{n_var}:- the maximum and minimum variation/deviation within the normal traffic in Mps. This are modeled by the normal_var transitions from/to the *Normal* extended place.
- K_{p_var}:- the maximum and minimum variation/deviation within the peak traffic in Mps modeled by the peak_var transitions from/to the *Peak* extended place.
- $\lambda_{n\_to\_p}$:- the rate at which the peak traffic occurs. It is modeled by the normal_to_peak transition
- T_p:- average duration of peak traffic, modeled in the peak_to_normal transition.

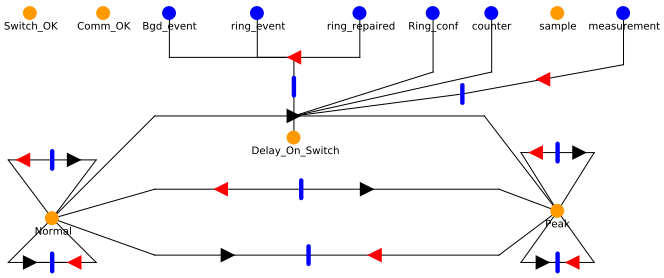


Fig. 6. An atomic model of Background traffic generator.

Whenever a fault in the power system occurs, the background traffic generator learn about it through *measurement* shared extended place. This initiate the process to determine the instant state of background traffic in the network and measurement of delay in the switches. If there are any changes in the topology of the communication system that may affect the traffic, it will be captured through the shared extended places: *comm_event* and *ring_config*. Then, based on the instantaneous traffic values, this model queries the static library (delay.a from the Ns-3 simulation) to obtain the delay measurement for all the switches in the network. The *Delay_on_Switch* extended place is used to store the measured delay values. Once the first measurement is taken, tracing is used to obtain the consecutive measurements until the fault is neutralized. A different marking on *measurement* shared place is used for this purpose, to continually query the static library for a certain mission critical time (a requirement from the protection application).

3) Protection function:-: the protection function atomic model, shown in Figure 7, is used to model the protection function and its performability assessment. It is not a model for a physical component, but rather it is used to model the impact of both timing and component (omission) failures on the availability and reliability of the ICT support for protection application. Timing failures are determined by the requirements for the protection application i.e. how resilient is the protection application to delay in the sampled value packets. This characteristics is mainly described by two parameters; the maximum delay per packet (t_max) and maximum number of consecutive delayed packets (n_max) the protection application can tolerate.

The model consists of four extended places; *Pwr_Line*, *Fault*, *Safe_Mode*, *Unsafe_Mode*. The *Pwr_Line* is used to model a normal working state of a power line while the *Fault* extended place represent the immediate state after a fault occurs in the power line. The fault state is communicated to the traffic model through *measurement* extended place and a

different marking on this extended place is used for tracking and tracing the delay measurement from the traffic model until the isolation is done by the protection application.

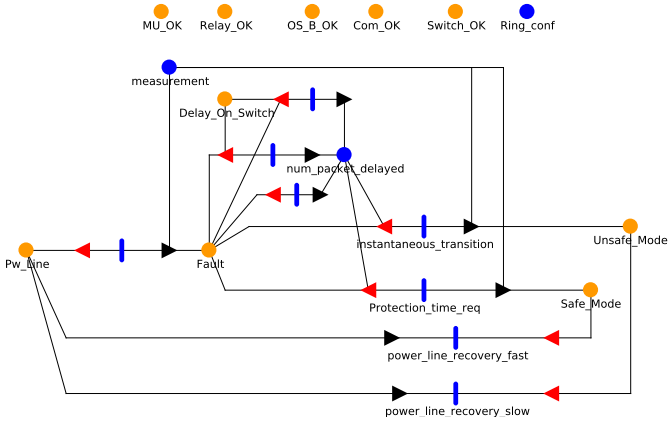


Fig. 7. An atomic model of Protection function.

The fault will be neutralized safely if the protection function is continually available during the critical mission time.This is represented by a transition to *Safe_Mode* extended place. Otherwise, it will go to the *Unsafe_Mode* state.

Considering timing failures, a protection function is said to be unavailable if the packet delay on the switches (those on the communication path of interest) is greater than the threshold (t_max) for n_max consecutive packets. This is modeled by a fault to safe/unsafe mode transitions dependent on the *Delay_On_Switch* extended place, which is a shared place with the traffic model. The *num_packet_delayed* place is used to count the number of consecutive packets delayed by more than the threshold value. If the number exceed n_max before the protection IED handle the fault, it will result in unsafe isolation of the power line. Otherwise, if the number of delayed packets is less than n for a protection time t, it will go to safe mode and halt taking the delay measurement (through the *measurement* extended place).

For modeling omission failures, the safe/unsafe mode transitions are made dependent on *MU_OK*, *Protection_IED_OK*, *Switch_OK*, *OS_B_OK* and *Com_OK* extended places which are shared places with different components of the communication architecture shown in Figure 1. If one of these necessary components are in a failure state, the fault will not be cleared safely, a transition to *Unsafe_mode*. Otherwise, it will go to *safe_mode* if there are no timing failures within the protection mission time.

V. Simulation Study

A. Scenario

To demonstrate the capabilities of the proposed method and model, a simulation is conducted for studying the performability of the ICT support for an (over-current) protection application on a power line connecting substations of Figure 1. It is assumed that when there is an over-current in a feeder connecting two substations, a merging unit on one of the substations will send the fault current information (sampled value) to a protection IED on the other substation. And, this protection IED is responsible to neutralize it by sending a trip signal to a Circuit breaker IED under its control.

TABLE I
Traffic Parameter Values

Traffic Parameters	Values used
$\lambda_{n\_to\_p}$	1 day^{-1}
T_p	2 hr
t_max	4 ms - 15 ms
n_max	8 - 40
K_n	4 - 9 Mbps
K_p	6 - 12 Mbps
K_{n_var} and K_{p_var}	1 Mbps

1) Communication subsystem architecture: The communication architecture shown in Figure 1, is considered. The study investigates the dependability of the communication between substation 1 and substation 4, assuming a protection application for a power line connecting these substations. Substation 1 is represented by a merging unit connected to a gateway switch while substation 4 is equipped with a protection IED, merging unit IED and a breaker IED connected to its gateway switch. The protection IED in substation 4, with the sampled value information gathered from both substations, is responsible to neutralize the fault on the power line connecting the two substations.

2) Traffic Assumption: The study focuses on the influence of the delay, which is due to a varying background traffic, on the dependability of the protection application. Merging units are assumed to generate a constant traffic of sampled value (SV) packets with a rate of 4000 packets per second. The gateway switches on each substation are also assumed to carry a varying background traffic ranging from 10 to 50 Mbps. In addition, to account for a constant background traffic (for e.g., SV exchange between other devices) and propagation delays, a 1 ms constant delay is introduced to all the switches.

In the considered architecture, a two way ring topology, the traffic can be carried through two alternative directions. This study considers background traffic to be carried through a shortest path towards the control center. In the case of multiple path with equal number of hops, the traffic is assumed to be divided and directed to the controller in both directions. If there is a failure in the ring architecture, all the traffic will be directed through the other/redundant working path of the ring architecture, which may affect the performance i.e. increase the probability of timing failures.

The traffic model parameters used in this study are shown in Table I. Some parameters such as the maximum delay per packet (t_max), maximum number of delayed packets (n_max) and protection function time requirement t are varied to study the impact of timing failures. In all simulations, the background traffic is set into the following three classes:-

- *Lower traffic (T1)*:- The normal average traffic K_n is set to 4 Mbps while the peak traffic is set to 6 Mbps.

TABLE II
FAILURE RATES AND RECOVERY TIMES OF THE SYSTEM COMPONENTS

Component type	Failure rate [days^{-1}]	Mean recovery time [hr]
Protection IED	$6.3 \cdot 10^{-4}$	2
Circuit Breaker	$6.6 \cdot 10^{-4}$	2
Merging Unit	$2.8 \cdot 10^{-4}$	3
Communication Line/cables	$1.8 \cdot 10^{-4}$	6
Router/Switches	$5.7 \cdot 10^{-5}$	3
Power line failure	$1.9 \cdot 10^{-3}$	3

- *Medium traffic (T2)*:The normal average traffic K_n is set to 6 Mbps while the peak traffic is set to 9 Mbps.
- *Higher traffic (T3)*:The normal average traffic K_n is set to 9 Mbps while the peak traffic is set to 12 Mbps.

3) Failure and recovery models: A negative exponential distribution, i.e., $P(T_x > t) = e^{-\lambda_x t}$ is assumed for all failure, repair and the rate at which the traffic varies, where T_x is the firing times for transitions in the SANs in Figures 5 – 7 and λ_x is the rates in Table II.

4) Metrics: The following metrics are used to measure the comprehensive dependability (performability) of the communication system considered:

- Availability of the ICT support system(A_p): measure the steady state availability of the ICT support system for the protection function. When only timing failures are considered, a protection function is assumed to be available if the delay requirement on the line between the two communicating substations is met. It is said to be unavailable if n_max consecutive packets are delayed by more than the threshold value, t_max.
  For the cases where all types of failures are considered, a protection function is available if both the delay requirement is met and all the ICT components used by the protection application are in a working state. In the presentation of numerical results, the unavailability is used, $U_p = 1 - A_p$.
- Mission Reliability ($R(t)$): Once a failure occurs that require the intervention from a protection application, this metrics measure the probability that the ICT support for the protection function will be continually available for a certain mission time. i.e. no n_max consecutive packets are delayed by more than t_max ms.

B. Evaluation and Discussion

For the scenario presented in Section V-A, a simulation is conducted to study the performability of the ICT support for protection of a power line between substation 1 and substation 4 of the architecture shown in Figure 1. First, to study the impact of timing failures, a sensitivity analysis is conducted by varying some traffic parameters. Then, for a set of specified traffic parameters, the impact of timing failures is compared with other (omission) failure modes of the ICT components.

All cases are simulated for 30 years of calendar time. A replication of 20 to 30 times is carried out for error control. The average computational time for one case with replications is in the range 20 to 120 minutes.

1) Sensitivity Analysis:-: In this section, the aim is to first study the characteristics of timing failures before incorporating it to a performability assessment where omission failures are also considered. A sensitivity analysis is used to study the effect of timing failures on the performability of the ICT support for a protection application. This study considers traffic class T1 and T2. Some parameters such as the delay threshold (t_max), maximum number of delayed packets (n_max), and the protection time requirement t are varied for a range of values shown in Table I.

Figure 8 and Figure 9 shows how the the mission reliability is affected by the assumption and parameters used to describe the resiliency of the protection application, t_max and n_max. It also shows the impact of background traffic on the reliability measure for the different assumptions of t_max and n_max parameters.

In Figure 8, the maximum delay per packet (t_max) is set to 8 ms and the n_max is varied. For a lower n_max assumption, the result shows that the mission reliability is low for both traffic classes. This is partly due to the fact that t_max is set close to the average delay measured on the switches. Hence, there is a significant probability that eight packets could be delayed by more than the threshold $t\_max = 8ms$, especially during bursty traffic periods. The Ns-3 delay measurements for the traffic class shows that the mean duration between bursty traffic ranges between 55 ms to 70ms which is also manifested by a steep drop upto 60 ms in Figure 8.

Increasing n_max to twelve, $T1$ becomes highly reliable while $T2$ shows some gain but still with a reliability lower than 60% for a protection with a 100 ms requirement. As the duration of bursty traffic in T1 is relatively shorter than T2, increasing the tolerance (n_max) to 12 results in a significant change on T1's reliability while it does not result in a considerable change for T2.

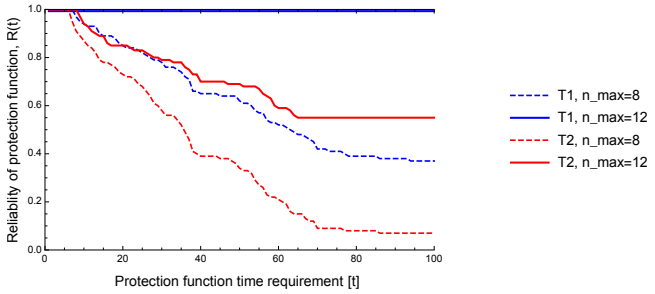


Fig. 8. Reliability of the ICT support system considering different set of background traffic when n_max = 8 and when n_max = 12.

Figure 9 shows the effect of varying the maximum delay per packet where the n_max is set to 8 packets.It shows that traffic class T1, in both $t\_max = 10ms$ and $t\_max = 15ms$

cases, has a relatively higher reliability than T2. For traffic class T1, the average delay measured on the line between substation 1 and substation 4 is around 7.5 ms. Hence, setting the threshold ($t\_max = 10ms$) above the average delay results in a fairly high reliability for T1. Whereas, for traffic class T2, the $t\_max = 10ms$ is lower than the average delay (13 ms) which results in a lower $R(t)$. The figure also shows that setting $t\_max = 15ms$ well beyond the average delay for traffic class T1, results in a very high reliability. However, T2 has some gain but still low $R(t)$.

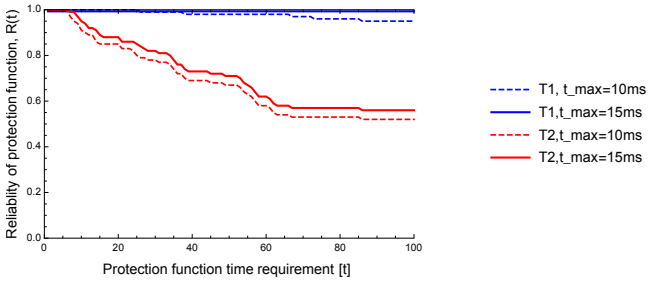
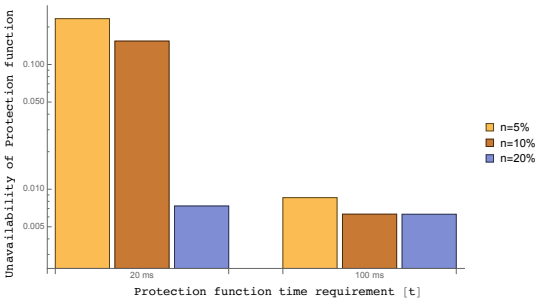


Fig. 9. Reliability of the ICT support system considering different set of background traffic when t_max = 10 ms and when t_max = 15 ms.

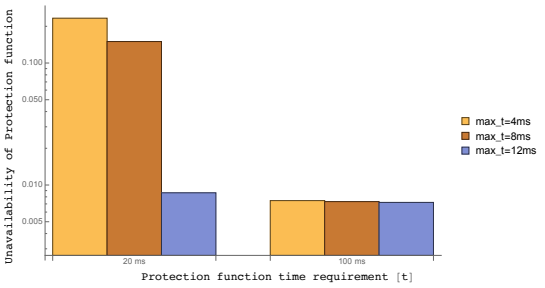
A sensitivity analysis on the unavailability of the ICT support system for a protection applications with different time requirements is shown on Figure 10. This study investigates two types of protection applications considering traffic class T1; one with a shorter time requirement of 20 ms, and another with a relatively higher time requirement of 100 ms. The two protection applications are assumed to have different characteristics which is described by the maximum number of consecutive delays that can be tolerated (n_max) and the maximum delay per packet (t_max). This investigation assumes that a protection application is said to be failed if n_max packets equivalent to $n\%$ (fraction) of packets expected to be transmitted in protection time t has a delay greater than or equal to t_max.

Figure 10 shows how the unavailability of both the 20 ms and 100 ms protection applications are affected by the n_max (described by $n\%$) and t_max parameters. In Figure 10(a), n is varied between 5% to 20% where the t_max is set to 8 ms. The figure shows that the unavailability for the 20 ms protection application is very high when the 5% and 10% fraction tolerance is considered. Whereas, for the 100 ms protection application, the same assumption results in a ten fold lower unavailability figure. This is due to the fact that the 20ms protection applications has a stricter time requirement and a failure in small number of packets will result in unavailability of the protection function. For $n = 20\%$, the unavailability is very small for both the 20 ms and 100 ms protection application. Prediction mechanisms in the case of packet losses and delays are taken into consideration for the the $n = 20\%$ assumption. This provide enough room for both protection applications to be available for situations with higher number of packet delays.

Figure 10(b) shows how the unavailability is affected by the variation in the maximum delay per packet setting the n to 10%. The result shows that the 20 ms protection function has a very high unavailability for $t\_max = 4ms$ and $t\_max = 8ms$. This indicates that when the maximum tolerable delay for a packet (t_max) is lesser or close to the average delay (7.5 ms considering T1), the unavailability of the ICT support become significantly high. However, the 100 ms protection application results in a very small unavailability as it requires large number of packets to be delayed which is a very rare situation considering traffic class T1. When t_max is set to 12 ms, both the 20 ms and 100 ms protection applications will perform good as the t_max is set well beyond the average.



(a)



(b)

Fig. 10. Unavailability of the ICT support system for a varying (a) fraction of packets with a delay greater than th threshold, $t > T\_threshold$ (b) delay threshold for each packet, t_max

2) Comparative Analysis: Setting the traffic parameters to a certain value, the performability measurements of the case where only timing failures are modeled, is compared with the case where other (omission) failure modes of all the ICT components are considered.

The comparison between timing failures and omission failures is shown on Figure 11. The unavailability of a 20 ms and 100 ms protection application are compared for the three different background traffic classes, where $t\_max = 8ms$ and $n\_max = 10\%$ is considered. It can be seen that the timing failures has a higher impact on the 20 ms protection application. The contribution of omission failure is quite small when compared with the timing failures. The background traffic variation has also significant impact on the unavailability of the 20 ms protection application ranging from 0.13 for T1 to

0.29 for T3. The omission failure is the same in all the cases as it is assumed to be not dependent on the traffic behaviour, i.e., only environmental/hardware failures are considered. For the 100 ms protection application, the impact of timing and omission failure is comparable. The change in unavailability due to a variation in the background traffic is also negligible. This is mainly due to the relatively larger time window and hence larger number of packets has to be delayed for the protection application to be unavailable.

Overall, the results are highly dependent on the assumption of the n_max and t_max parameters. If these parameters were assumed to be more relaxed/increased, the performance of the 20 ms protection application would also become better and comparable with the 100 ms protection application.

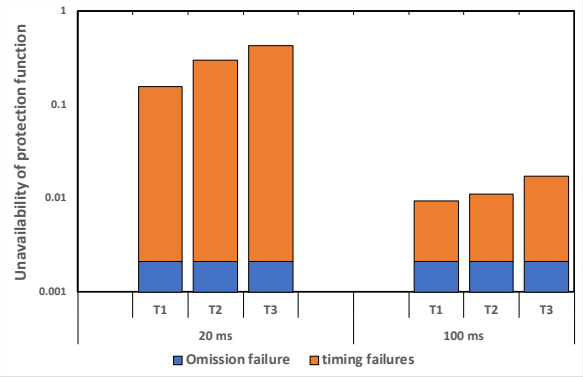


Fig. 11. Comparison of unavailability of timing failures and omission failures for a varying background traffic T.

VI. Concluding Remarks

In future smart grid, there will be a large scale use of ICT support system which makes it a complex cyber-physical system. It is important to study the totality of such complex systems and determine the combined influence of failures and workloads, i.e., performability. This paper looked into how performance associated properties (timing failures) can be modelled together with properties affecting dependability of the ICT support system in smart grid. A two tier model using Ns-3 and SAN is developed to study the peformability of an IEC61850 based communication infrastructure for protection of lines between substations.

Simulation studies were conducted to illustrate how the method is able to capture the two properties and to study their effect on the reliability and availability of the ICT support system. The result shows that the reliability and availability is highly dependent on the requirements for the protection application, maximum delay per packet (t_max) and maximum number of consecutive delayed packets (n_max) the protection application can tolerate. A higher reliability is observed when the maximum delay per packets is set well beyond the measured average delay and when the maximum number of consecutive delayed packets is set larger than the number of packets that could be sent within the bursty period of the background traffic. The result also showed that timing failures have a significant impact on the unavailability of the ICT support; higher for the critical protection applications with shorter time requirement (20 ms) than those with a relatively higher time requirement (100 ms).

References

[1] B. R. Haverkort, g. R. Raymond Marie, and K. Trivedi, *Performability Modelling: Techniques and Tools*. John Wiley Sons, Ltd, 2001.

[2] A. Mahmood, O. Hasan, H. R. Gillani, Y. Saleem, and S. R. Hasan, "Formal reliability analysis of protective systems in smart grids," in *Proceedings - 2016 IEEE Region 10 Symposium, TENSYMP 2016*. Institute of Electrical and Electronics Engineers Inc., jul 2016, pp. 198–202.

[3] L. Chen, K. Zhang, Y. Xia, and G. Hu, "Scheme design and real-time performance analysis of information communication network used in substation area backup protection," *Proceedings - Power Engineering and Automation Conference, PEAM 2012*, pp. 1–4, 2012.

[4] J. Wäfler and P. E. Heegaard, "A combined structural and dynamic modelling approach for dependability analysis in smart grid," in *Proceedings of the 28th Annual ACM Symposium on Applied Computing*. ACM, 2013, pp. 660–665.

[5] R. Zeng, Y. Jiang, C. Lin, and X. Shen, "Dependability analysis of control center networks in smart grid using stochastic petri nets," *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 9, pp. 1721–1730, 2012.

[6] Y. Wu, L. Nordstrom, and D. E. Bakken, "Effects of bursty event traffic on synchrophasor delays in IEEE C37.118, IEC61850, and IEC60870," in *2015 IEEE International Conference on Smart Grid Communications, SmartGridComm 2015*, 2016, pp. 478–484.

[7] N. Das, T. T. Aung, and S. Islam, "Process-to-bay level peer-to-peer network delay in IEC 61850 substation communication systems," in *2013 Australasian Universities Power Engineering Conference, AUPEC 2013*, vol. 1, no. 3. Springer Science and Business Media LLC, dec 2013, pp. 266–275.

[8] M. G. Kanabar and T. S. Sidhu, "Performance of IEC 61850-9-2 process bus and corrective measure for digital relaying," *IEEE Transactions on Power Delivery*, vol. 26, no. 2, pp. 725–735, apr 2011.

[9] S. Kumar, N. Das, and S. Islam, "Performance analysis of substation automation systems architecture based on IEC 61850," in *2014 Australasian Universities Power Engineering Conference, AUPEC 2014 - Proceedings*, 2014.

[10] N. Das, W. Ma, and S. Islam, "Analysis of end-To-end delay characteristics for various packets in IEC 61850 substation communications system," in *2015 Australasian Universities Power Engineering Conference: Challenges for Future Grids, AUPEC 2015*, 2015.

[11] T. S. Sidhu and Y. Yin, "Modelling and Simulation for Performance Evaluation of IEC61850-Based Substation Communication Systems," *Power Delivery, IEEE Trans. on*, vol. 22, no. 3, pp. 1482–1489, 2007.

[12] X. Lu, Z. Lu, W. Wang, and J. Ma, "On network performance evaluation toward the smart grid: A case study of DNP3 over TCP/IP," in *GLOBECOM - IEEE Global Telecommunications Conference*, 2011.

[13] Y. Wu, D. Babazadeh, and L. Nordstrom, "Modeling of communication infrastructure compatible to Nordic 32 power system," in *IEEE Power and Energy Society General Meeting*, vol. 2016-Novem. IEEE Computer Society, nov 2016.

[14] P. Ferrari, A. Flammini, S. Rinaldi, E. Sisinni, and G. Prytz, "Advanced networks for distributed measurement in substation automation systems," in *2013 IEEE International Workshop on Applied Measurements for Power Systems, AMPS 2013 - Proceedings*. Institute of Electrical and Electronics Engineers (IEEE), nov 2013, pp. 108–113.

[15] P. M. Kanabar, M. G. Kanabar, W. El-Khattam, T. S. Sidhu, and A. Shami, "Evaluation of communication technologies for iec 61850 based distribution automation system with distributed energy resources," in *2009 IEEE Power & Energy Society General Meeting*. IEEE, 2009, pp. 1–8.

[16] W. Wang, Y. Xu, and M. Khanna, "A survey on the communication architectures in smart grid," pp. 3604–3629, 2011.

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

[18] W. H. Sanders and J. F. Meyer, "Stochastic Activity Networks : Formal Definitions and Concepts," *Lectures on formal methods and performance analysis*, vol. 315-343, no. 9975019, pp. 315–343, 2002. [Online]. Available: http://dx.doi.org/10.1007/3-540-44667-2{_}9

[19] S. Gaonkar, K. Keefe, R. Lamprecht, E. Rozier, P. Kemper, and W. H. Sanders, "Performance and dependability modeling with Möbius," *ACM SIGMETRICS Perf. Ev. Review*, vol. 36, no. 4, p. 16, 2009.

[20] T. R. Henderson, S. Roy, S. Floyd, and G. F. Riley, "Ns-3 project goals," in *Proceeding from the 2006 Workshop on Ns-2: The IP Network Simulator*, ser. WNS2 '06. New York, NY, USA: ACM, 2006. [Online]. Available: http://doi.acm.org/10.1145/1190455.1190468

[21] C. Adrah, O. Kure, Z. Liu, and H. Hoidalen, "Communication network modeling for real-time HIL power system protection test bench," in *Proceedings - 2017 IEEE PES-IAS PowerAfrica Conference: Harnessing Energy, Information and Communications Technology (ICT) for Affordable Electrification of Africa, PowerAfrica 2017*, 2017.

[22] K. Pandakov, C. M. Adrah, H. K. Hoidalen, and O. Kure, "Experimental validation of a new impedance based protection for networks with distributed generation using co-simulation test platform," *IEEE Transactions on Power Delivery*, pp. 1–1, 2019.

[23] F. H. Fitzek and M. Reisslein, "MPEG-4 and H.263 video traces for network performance evaluation," *IEEE Network*, vol. 15, no. 6, pp. 40–54, 2001.

[24] T. Amare, B. E. Helvik, and P. E. Heegaard, "A modeling approach for dependability analysis of smart distribution grids," in *Design of Reliable Communication Networks (DRCN 2018)*, 2018.