Dependability Analysis of Smart Distribution Grid Architectures Considering Various Failure Modes

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

***Abstract*—The future smart distribution grid will be consisting of new components and technologies with enhanced capability whose failure behaviour can not be determined with certainty. In studying the reliability of these distribution grids, it is important to look into various possible failure semantics of the new components and how would they possibly affect the reliability of the distribution grid. This paper aims to investigate/study how the various failure modes of the new components affect the reliability of distribution grids. The focus is on (limited to) reliability evaluation of the feeder protection function of next generation distribution grids considering omission and value type failure semantics. A generic and modular modeling framework based on a stochastic activity networks is used to model the distribution grid. An IEC61850 based automation/substation communication network (SCN) is considered. And, for illustration, different scenarios with different SCN architectures are investigated.**

I. Introduction

Advanced control and communication technologies are the key elements in the development of the next generation Smart distribution grid. New components and technologies has been introduced into the distribution grids. There has been also standards such as IEC 61850 which define protocols for Intelligent electronic devices (IEDs) that can monitor and manage the physical grid. The addition of new functions, technologies and control devices will bring new dependencies and failure behaviour that has to be thoroughly studied.

This paper aims to investigate how various failure modes of the new ICT based components will affect the reliability of distribution grids. The focus is on reliability evaluation of feeder protection function in IEC61850 based next generation distribution grids considering omission failures (a failure yield just a lack of response or action) and value/content type failures (An incorrect response is given or a wrong action taken). A brief description of the failure modes is presented in Section II-C. For protection system of a critical infrastructures, such as the distribution grid, insight into the effect of different failure modes/semantics, e.g., caused by malfunction of software/IEDs, is important since value failure may have sever consequences.

There has been some works that has studied the reliability of distribution grids using the IEC 61850 standard for the substation communication network such as [1], [2], [3], [4], [5], [6]. Most of these works focus on proposing a highly reliable communication network architecture assuming omission type of failure semantics for the components. Thomas & al. [2] presented Ethernet-based logical architecture for the substation communication network (SCN) which takes into account fail-stop/omission and timing failures of the IEDs.

Liu & al. [5] proposed a reliable network based upon cobweb topology for reliability of substation communication network. Thomas & al. [4] proposed a redundant ring network focusing on the importance of utilizing the redundant critical components/communication paths in achieving high reliability and performance while Sidhu & al. [7] presented IEC 61850-based IED models to study the reliability of substation network for different types of network topologies.

A Parallel Redundancy Protocol (PRP) is proposed in the IEC 62493-3 standard which duplicates the LAN in the process bus communication network to provide zero switch over periods in case of any single LAN failure. The study in [6] also presents a PRP scheme where conventional IEDs can be used and cost can be optimized.

To our knowledge, most previous works such as [1], [2], [3], [4], [5], [6], [8] has focused on improving the reliability and performance of IEC based distribution grid with an assumption that the failure is of omission type. In such assumption, a failure in ICT domain will not immediately cause a failure in the physical domain. The propagation of failure into the physical grid will occur only if there is a need to use the ICT control system that has failed. However, in advanced smart distribution grid, there can also be a possibility where a failure in cyber components could instantly propagate into the electrical components and result in a more sever consequence. In a value failure mode, a failure in ICT based control system could produce a wrong result which could induce a failure in the physical grid affecting the service provided to end users. Hence, considering a critical infrastructure such as the distribution grid, all possible failure modes has to be thoroughly investigated [9].

This paper looks into how the reliability of the distribution grid is affected in assuming different failure modes, mainly value and omission type failures. An extended model of a stochastic activity network based model proposed in [10] is used. Furthermore, different architectures of the IEC 61850 based substation communication network, proposed by previous works, are investigated and compared for the different failure semantics considered.

The rest of the paper is organized as follows: The smart distribution grid system and the major assumptions considered in the study are discussed in Sect II. Sect III presents the model. In Section IV, simulation scenarios and an illustration of the results is presented. Lastly, Section V gives conclusive remarks of the work.

II. Major Assumption and System Considered

A. Substation Communication Network (SCN)

The study considers an IEC61850 based substation communication network. The focus is on the protection system which consists of the electronic components such as protection IEDs, Merging Units, Intelligent Switches and circuit breaker IEDs. These components are assumed to be connected to an Ethernet switch through communication links to form a substation communication network.

Merging Unit IEDs collect and transmit sampled value data(current and voltage) to the protection IEDs. Protection IEDs basically receive the sampled values from the Merging Units, perform substation protection functions and send decision/trip signals to circuit breakers connected to the process bus. These devices are also assumed to exchange information such as breaker failure protection or status information among each other by sending Generic Object-Oriented Substation Event (GOOSE) messages. Circuit Breaker IEDs are control device which receive the GOOSE/interlocking commands from protection IEDs and connect/disconnect the physical breaker. Intelligent switch IEDs are operated by controllers to reconfigure the grid topology in fault isolation and service restoration. All IED components are assumed to have a client-server exchange towards substation controller through the communication network. The study is conducted on different IEC 61850 based architectures proposed by some previous works. Below are SCN architectures considered in this study.

1) Architecture A (Arch-A): In this scenario, the substation communication network shown in Figure 1 from [10] is used. It is a traditional IEC 61850 based cascaded SCN where there is no redundancy for either the IED components or the LAN network.

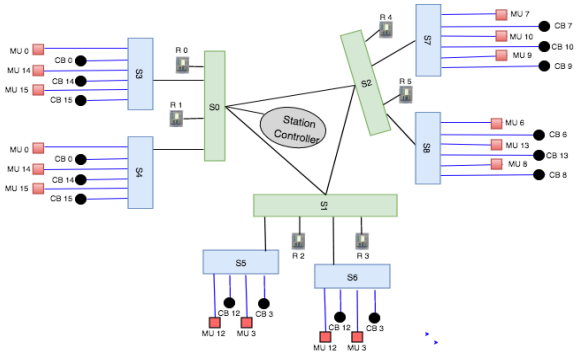


Fig. 1. Substation Communication Network Architecture from [10].

2) Architecture B (Arch-B): The second example SCN architecture considered, shown in Figure 2 is also similar to the above traditional IEC 61850 based architecture but with a single tier of Ethernet switches where protection IEDs, Merging units and breakers are connected to it.

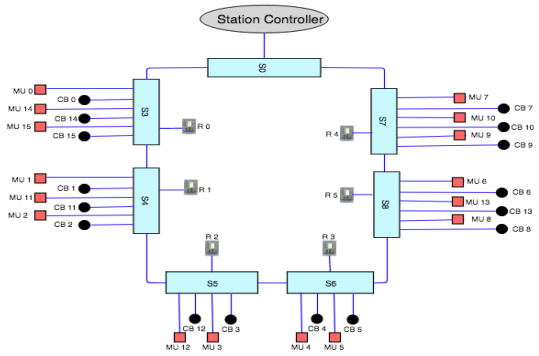


Fig. 2. Substation Communication Network Architecture from [].

3) Architecture C (Arch-C): A substation communication network proposed by Ali et al. [4], shown in Figure 3 is used. Here, the protection system consists of two redundant and independent protection IEDs. Only one protection IED, i.e., primary, out of redundant protection IEDs works at a time to clear the fault. Each dual-port protection IED, Merging Unit IED and Circuit Breaker IED, are connected to two different local(process-level) Ethernet switches, i.e., with its own bay Ethernet switch and to the adjacent bay Ethernet switch. In case of failure in the communication network of a protection system, the Protection IED transfers the control to the redundant port through dual homing protocol (DHP) port switch over mechanism and uses the alternate communication path for further communication [4]. The whole substation is constructed by forming a ring network of bay/ Ethernet switches which provides an alternate data path to the message flow in case of a link failure.

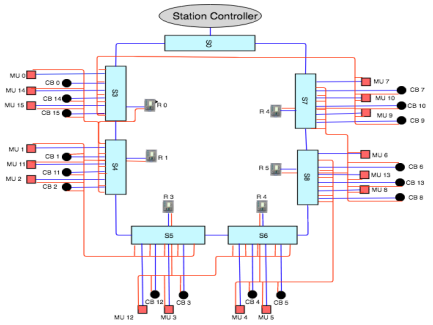


Fig. 3. Substation Communication Network Architecture from [4].

4) Architecture D (Arch-D): The fourth architecture, shown in Figure 3, is based on Parallel Redundancy Protocol (PRP), IEC 62439-3 standard presented in [6]. It propose duplication of the LAN in the communication network to provide zero switch-over periods in case of any single LAN failure. It also has independent LAN rings at the station bus. The PRP

duplicates the incoming message packet and sends them via two different LANs which are independent of each other. On reception the packet which arrives first at the destination is treated as the final packet and the other of the pair is discarded.

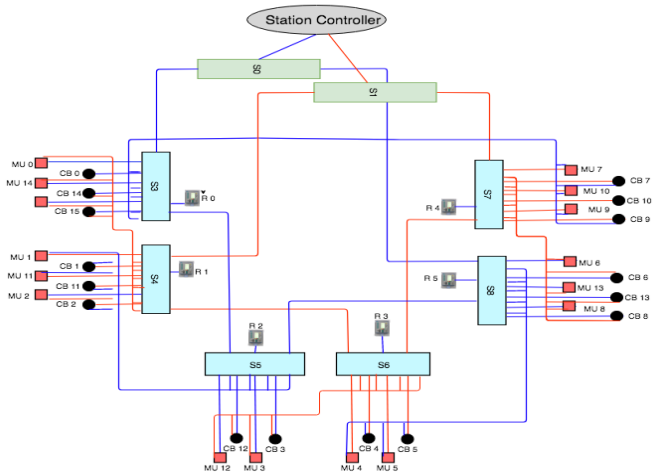


Fig. 4. Substation Communication Network Architecture from [6] .

B. Physical Grid

The physical distribution grid topology from [10] shown in Figure 5, is used in this study. It consists 16 feeders and has a radial topology with normally open intelligent switches providing redundancy between some feeders.

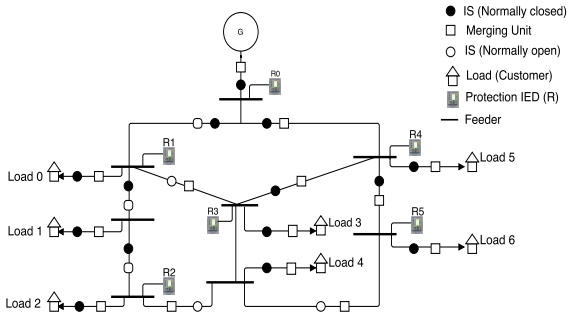


Fig. 5. Distribution grid topology.

C. Failure Modes

For a thorough discussion of faults and failure modes of ICT equipment, see [9]. In this paper we study the effect of the two fundamental failure modes: omission failures and value failures.

1) Omission/Fail-stop Failure Modes: In this failure mode, the component (the Protection IED) stop operation/providing an output when it fails. Other components may detect its failure when trying to communicate with it. In IEC 61850 based substation communications, there are mechanisms/continuous communication exchanges that can be used to detect such failures and trigger a repair process.

2) Value Failure Modes: Here, component may produce wrong values in terms of responses and/or actions that could be interpreted as correct. There may be a wide range of causes of theses failures, among them: software faults, misconfiguration, operation/maintenance mistakes and malicious attacks. Systems may be designed to tolerate some of these, but the authors are not aware of such attempts in the IEC 61850 context. Even with such designs, there is still a probability of vale type of failures. The impact on the power system of such ”active failing” in the ICT system may be significant, and it is important to take them into account in analysis and design.

D. Service Restoration

Once a failure is detected and isolated, the controller is responsible for reconfiguration of the grid topology and updating system state. A limited repair resource is considered for all components. For physical grid components, time to repair is dependent on the availability of ICT infrastructure during the failure.

III. Model

A Stochastic activity network model proposed in [10] is extended and used. The model is developed using the Mobius tool [11]. It is a general and modular stochastic model, which is built from atomic block models.

A. Atomic models

Atomic models are developed for the individual components of the IEC 61850 based control system and the physical grid. Detailed models of each the components and a model of the entire distribution grid are presented in [10]. Below is a summary of the atomic models extended for this study. For the complete model cf. [10].

1) Protection IED: The atomic model of a Protection IED is shown in Figure 6. It consists of five 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), value failure (PR_IED_Value_Failure) and Permanent failure (PR_IED_Failed).

Protection IEDs may fail from all other state to a failed state (of omission/fail-stop type) in PR_IED_Failed which needs maintenance by a repair crew. Failures may be of value type that change the state of the protection IED from a working state in PR_IED_OK to a value failure state in PR_IED_Value_Failure.

The state in PR_IED_Value_Failure results in a wrong value/decisions while it is perceived by others as if it is operating normal. This results in a random failing/tripping of circuit breakers under its control until the failure is detected. This is modeled through the shared extended place, CB_STATUS. A failure discovery mechanism may also be included in the model, which may succeed with some probability and result in a change of the value failure state in PR_IED_Value_Failure into omission type failure in PR_IED_Failed. If the failure

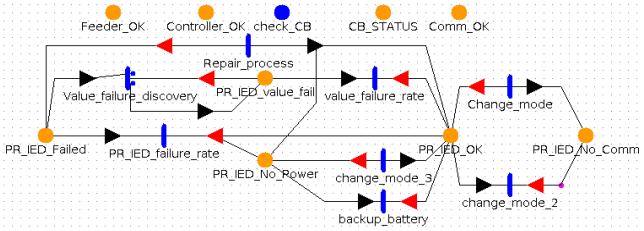


Fig. 6. An atomic model of Protection-IED.

detection do not succeed, the protection IED stay in the value - failure state.

A protection IED, after being powered by battery for some time, will change to a no power state in PR_IED_No_Power if its power supply is failed, i.e., the feeder providing power supply is not in its working state. From the initial working state in PR_IED_Ok, a protection IED may also end up in a no communication state in PR_IED_No_Comm if none of the outgoing communication links are in their working state. A Protection IED may have a local communication to sensors(MU IEDS) and actuators(CB IEDs) it monitors while there is no communication path towards neighbouring protection IEDs or towards the controller. Such cases are modeled by different markings of the PR_IED_No_Comm and PR_IED_Ok extended places.

2) Circuit Breaker: Figure 7 shows the atomic model for a Circuit Breaker IED (CB_IED) which open or close switches that can be remotely operated or tripped. It consists of three extended places; Working states in CB_Ok, failure in communication link- No communication state in CB_No_Comm and permanent failure state in CB_Failed.

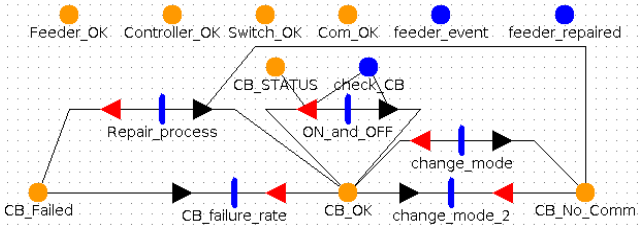


Fig. 7. An atomic model of Circuit Breaker.

The working state in CB_Ok has basically two states, on and off states, modelled by different markings. The marking changes made by protection IED in CB_STATUS changes the state of the circuit breaker between on and off states in CB_Ok. From a working state in CB_Ok, a circuit breaker could end up in a No communication state in CB_No_Comm if all the communication nodes/links towards it are not in their working state. A Circuit breaker may have local communication with protection IEDs while there is no communication path towards the controller. Such cases are modeled by different markings of the CB_No_Comm and CB_Ok extended places. Circuit breakers may fail from all other states to a failed state (CB_Failed), needing attention of a repair crew to become operational.

3) Feeders: Figure 8 shows the atomic model for the feeders. It consists of three extended places: working (Feeder_Ok), permanent failure (Feeder_Failed) and no power (Feeder_No_power). Failure of a feeder in a working state is either handled by the responsible protection IED (safe fail) if the ICT based control infrastructure is in a working state or it might lead to a failure cascading into upstream feeders if the associated ICT based protection system is also failed. These two failure situations are modelled by different markings in the Feeder_Failed extended place. In addition, a working state in Feeder_Ok could be changed into a failed state in Feeder_Failed if the associated circuit breaker is tripped (off state) due to, say a value failure in the ICT based protection system. This is modeled using a transition dependent on CB_OK place.

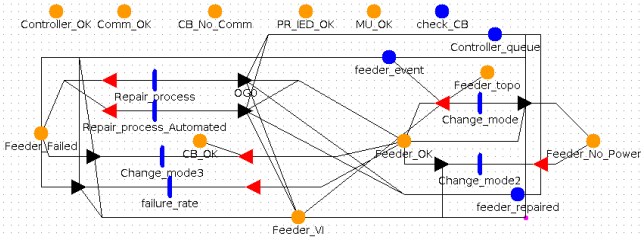


Fig. 8. An atomic model of a feeder.

The feeder may also fail permanently from all other state which needs maintenance by repair crew. A feeder in a working state will instantly switch to 'No Power' state if the feeder from which it gets power is not in a working state. The repair time in a feeder is assumed to be dependent on the failure situation modeled in the failed states in Feeder_Failed extended places. A repair of feeder where the ICT support system has also failed will take a longer time.

B. Composed models

The overall distribution grid is modelled by connecting the atomic sub-models using a 'Join' composed model formalism as shown in Figure 9. Some extended places are shared among two or more atomic models and are used to model the dependencies and interconnection between components as discussed in [10].

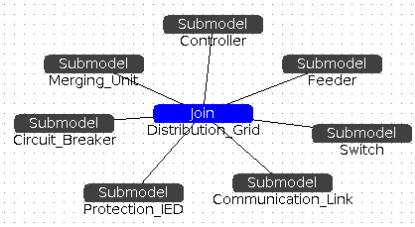


Fig. 9. Composed model of distribution grid

IV. Simulation Study

To demonstrate the effects of different failure modes, a simulation is conducted for measuring the availability of power

to the end user considering omission and value type failure semantics of a protection IED. The ratio of the failure rate between omission and value type failures is varied to study the failure mode that cause a sever consequence. The simulation also looks into how different architectures of the substation communication networks, described in section II-A, behave for the assumed failure modes. An illustration and comparison of the resulting Availability of an end user and of the overall system is also shown in Figure 10 - Figure 14.

The case study mainly considers an over-current protection. If there is an over-current in a feeder, the bay protection IED responsible for the faulty feeder zone should neutralize it by sending a trip signal to a Circuit breaker IED. It should also send a status update to neighbouring IEDs stating that it is handling the situation so that neighborhood protection IEDs, which could operate as a backup, will not act/trip their breakers. For protection coordination and interlocking functions, bay IED components should also communicate to the station controller during fault isolation and service restoration.

As discussed in Section II-C, omission type of failures are assumed to be instantly detected as the IEC 61850 standard has an awareness mechanism that can be used for this purpose. For value type failures, it is assumed that the failure can be discovered with some probability if there is a valid path to a neighbouring Protection IEDs and/or to the station controller. A simplistic approach is to use failure discovery mechanisms through a challenge message exchange among Protection IEDs. The model assumes that if there is a valid path to atleast two neighbouring Protection IEDs and/or to the station controller, a value type failure in Protection IEDs can be discovered. And, the faulty Protection IED can be forced to a fail stop mode. There can also be some consistent value failures which could be difficult to detect. These are modeled with a probability that the faulty protection IED will stay for longer time in value failure mode even if there is a connection to other IEDs and to the controller.

A negative exponential distribution, i.e., $P(T_x > t) = e^{-\lambda_x t}$ is assumed for all failure and repair times, where T_x is the firing times for transitions in the SANs in Figures 6 – 8 and λ_x is the rates in Table I, which are based on [12]. A deterministic distribution, i.e., $P(T_y > t) = 1$ when $t \leq$ 3hr and $= 0$ when $t >$ 3hr, where T_y is used for the backup battery time of controllers, switches and protection relays during power outages. Only 5% of the Value type failures are assumed to be consistent failures. All cases are simulated for 100 years of calender time, each replicated 15 to 20 times for error control. Confidence bands of 95% are shown in Figures 12 and 13 and omitted in the other figures to avoid clutter. The average computational time for one case with replications is in the range 10 to 20 minutes.

The effect of a fraction of the failures being of the value type failure from none (0) to all (1) is shown in Figure 10 obtained for substation architecture A in Figure 1. Similar results are obtained for all other architectures. It is seen that the availability of power to an end user drops significantly

TABLE I
FAILURE RATE AND REPAIR TIME OF THE GRID COMPONENTS

Component type	**Failure rate** λ_x[days^{-1}]	**Repair time** λ_x^{-1}[hr]
Feeder	0.0019 per km	6 Manual rep. 2 Automated rep.
Protection IED	0.0025	2
Merging Unit	0.0026	2
Circuit Breaker	0.0026	2
Communication line	0.0028	3
Switches/router	0.005	3
Controller (permanent failures)	0.00059	3
Controller(Software failures)	0.0333	0.3

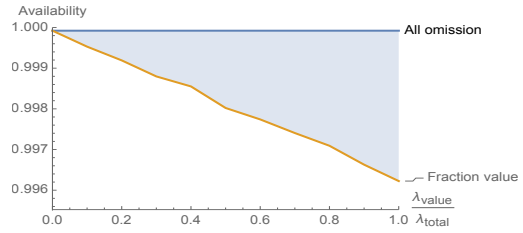


Fig. 10. Availability considering Omission type vs Value type failures

with an increasing ratio of value type failures. There is also a

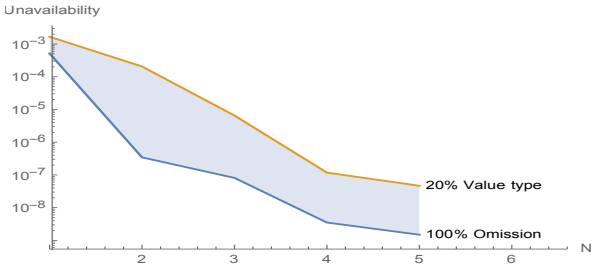


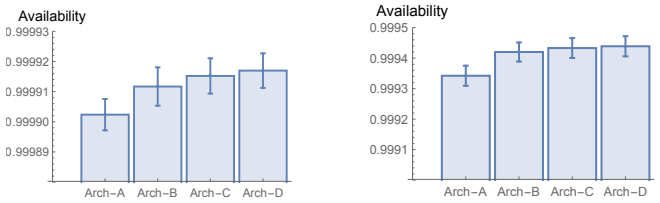
Fig. 11. Unavailability of the service for N or more simultaneous affected users considering the two cases, all failures of omission type, 20% are of the value type

significant drop in the availability of the overall system when there is a fraction of value failures. Figure 11 shows system unavailability condition by N or more simultaneously affected users when 20% of failures are of value type. Note that the relative drop is larger for more than one affected user, i.e., $N > 1$.

Figure 12 shows a comparison of the architectures for omission and value types failures. With only omission failure mode, shown in Figure 12(a), scenario A has the least availability, B slightly better and Scenario C and D has a higher since architecture A and B doesn't have a redundancy in the LAN network while C and D has two LAN networks. Architecture B has a better availability than A due to the placement of protection IEDs closer to the sensors and breaker units.

For value type failure semantics, Figure 12(b), the availability drops from the four nine domain to the three nine domain for all architectures, with some minor relative changes. This mainly due to all the substation communication architectures being proposed/designed with just omission type failure of

ICT components in mind. Here, It is assumed that only 20% of the failures are value type . Considering a potentially higher fraction yield a higher impact.



(a) Omission type of failures only (b) 20% value type of failures

Fig. 12. Availability of power to end-users for the architectures

Though the change in availability of the final service/power to the end user seems small, archtectures C and D may significantly improve the availability of the ICT support system. The availability of the protection function (ICT support system) considering omission type of failure semantics is shown in Figure 13. The protection function/ ICT support system is considered available if the respective Merging units, protection IEDs, breaker units and the communication network behind them is working, otherwise if one of the components fail, the protection function is assumed to be unavailable. Figure 13 shows the gain of the increased redundancy.

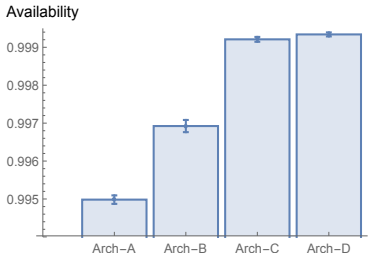


Fig. 13. Availability of the ICT subsystem (Protection function)

Comparison of the architectures on system unavailability shown in Figure 14 for an increasing number of simultaneously affected users. With 20% value type failures, the system unavailability almost independent of the architecture as the value failures are dominant in causing unavailability. However, for only omission type failures, it can be seen that architecture C gives a somewhat lower unavailability than Scenario A and B, especially for more than three simultaneously affected users.

V. Concluding Remarks

In designing a dependable communication architecture for critical infrastructures like distribution grids, it is very important to consider various types of failure modes. This paper has focused on studying how the various failure modes of IEC 61850 based ICT support system components affect the reliability of future distribution grids, by a stochastic activity network simulation model, for four proposed substation communication networks.

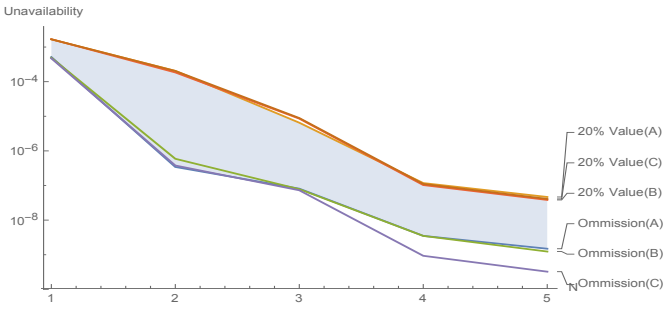


Fig. 14. Unavailability for N or more simultaneous affected users, for the cases with omission failures only and 20% value failures for the architectural options A, B and C

The results shows that there will be a significant change in reliability indexes of the service provided to customers if part of the failure is of the value failure type. Some SCN architectures that has improved the reliability for omission type failure modes fail to do the same when value type failure modes are considered. As future smart grids will be highly dependent on new ICT based components, it is important to consider value type failures of ICT based components in the design of substation communication architectures.

References

[1] H. Hajian-Hoseinabadi, "Availability comparison of various power substation automation architectures," *IEEE Trans. on Power Delivery*, vol. 28, no. 2, pp. 566–574, 2013.

[2] M. S. Thomas and I. Ali, "Reliable, fast, and deterministic substation communication network architecture and its performance simulation," *IEEE Trans. on Power Delivery*, vol. 25, no. 4, pp. 2364–2370, 2010.

[3] I. Ali and M. S. Thomas, "Substation communication networks architecture," *2008 Joint Intern. Conf. on Power System Technology POWERCON*, 2008.

[4] I. Ali & al., "IEC 61850 Substation Communication Network Architecture for Efficient Energy System Automation," *Energy Technology & Policy*, no. 1, pp. 82–91.

[5] X. Liu, J. Pang, L. Zhang, and D. Xu, "A high-reliability and determinacy architecture for smart substation process-level network based on cobweb topology," *IEEE Trans. on Power Delivery*, vol. 29, no. 2, pp. 842–850, 2014.

[6] S. Suhail Hussain et al., "A novel PRP based deterministic, redundant and resilient IEC 61850 substation communication architecture," *Perspectives in Science*, pp. 747–750.

[7] 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.

[8] L. Andersson, K. P. Brand, C. Brunner, and W. Wimmer, "Reliability investigations for SA communication architectures based on IEC 61850," *2005 IEEE Russia Power Tech, PowerTech*, pp. 1–7, 2005.

[9] 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.

[10] 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.

[11] 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.

[12] Statnett SF, "Annual statistics 2016 [In Norwegian]," Tech. Rep., 2016. [Online]. Available: http://www.statnett.no/Global/Dokumenter/Kraftsystemet/Systemansvar/Feilstatistikk/Årsstatistikk 2016 1-22 kV.pdf