Permanent Data Loss in Highly Available Substation Automation Systems

Bamdad Falahati, *Student Member, IEEE*, Zahra Darabi, *Student Member, IEEE,* Mehdi Vakilian, *Member, IEEE*, Yong Fu, *Member, IEEE*

***Abstract* — A substation automation system (SAS) is a computer network to which all events, indications and analog measured values collected from entire network are transmitted and logged in a server for future reference. Any SAS disconnection or failure may cause malfunctioning and data loss due to the interruption of data transfer. Highly available networks are the best solution for implementing fault-tolerance techniques for the improvement of SAS reliability. Such networks provide redundancy in appliances and/or data paths to decrease the impacts of failures in the network and increase network reliability.**

This paper studies permanent data loss in an SAS when a fault or failure occurs in the network. Knowledge of the physical characteristics of SAS elements is necessary for measuring this index. The elements that record data should be identified, and then the data lost due to failures in those elements must be determined. Also, as a case study, a typical SAS is examined in four states of failure, and the permanent data loss occurring under each state is calculated.

***Index Terms*-- Substation automation systems, Substation communications, Data loss, Local area networks, Ethernet.**

I. Introduction

The application of digital technologies in power systems has resulted in an evolutionary superseding of electromechanical devices with numerical ones featuring internal digital processors with communication capabilities. A substation automation system (SAS) undertakes substation operation functions, including control, protection, monitoring, and measuring [1]. Ethernet technology and local area networks (LANs) enable the design of SAS architectures that boast greater reliability, availability, speed, and cost savings than traditional hard-wired systems [2].

Two major tasks of an SAS include executing command and recording all event data. Any disconnection or failure in an SAS may cause malfunctioning and data loss due to the interruption of data transfer [3]. The application of highly available networks to mitigate the impact of failures on digital networks is a general point of interest [4], [5]. The fault-tolerant scheme introduced in [6] divides the entire network into several subnets to minimize data loss in the SAS. Another study introduced a fuzzy cognitive map (FCM) for evaluating the impact of non-ideal data quality in a substation system [7]. Path and device redundancy are two major methods by which to increase the reliability of the entire network. Yet, for fail-over switching between the failed path/device and the redundant path/device, different architectures are available [8], [9]. *High-availability* protocols, such as RSTP, PRP and HSR, provide minimum fail-over times [10], [11]. However, certain hardware and topologies are required to make the system fully reliable [4]. Previous studies conceptually emphasized the significance of reliability on minimizing data loss, without providing the numerical evidence necessary to assess the impact of failures on data loss in the network, as well as performance improvement caused by redundancies.

Data loss in an SAS can be categorized as permanent data loss (PDL) or online data loss (ODL). In PDL, the data is lost permanently because of a failure inside the SAS that makes retrieving the data impossible. ODL failures, on the other hand, cause data to become inaccessible only temporarily while the fault exists; the data is restored once the fault is cleared.

This paper investigates permanent data loss in a highly available SAS when a fault or failure occurs in the network. Knowledge of the physical characteristics of SAS elements is necessary for measuring this index. The elements that record data are identified, and then the data lost due to failures in those elements is determined. As a case study, a typical SAS is examined under four states of failure, and the permanent data loss for each state is calculated.

II. Highly Available SAS Network

A highly available SAS network is a digital network in which no single failure point can interrupt the service of hosts by servers [4]. Highly available networks are established on both redundant devices and high-availability protocols. A mathematical model for describing SAS topologies is presented, and based on these mathematical expressions, the mechanisms by which highly available architectures can increase the integrity of the network and accordingly decrease permanent data loss can be investigated.

A. Modeling the Structure of an SAS

A novel SAS consists of three levels, the station, bay, and

B. Falahati and Y. Fu are with Mississippi State University, Department of Electrical Engineering, Starkville, MS, 39759 (e-mail:bf229@msstate.edu, fu@ece.msstate.edu)

Zahra Darabi is with SNC-LAVALIN CONSTRUCTORS INC. Binghamton, NY 13904 USA (e-mail: zahra.darabi@snclavalin.com).

process levels [12]. The station level comprises human-machine interfaces (HMIs), servers, and gateways through which the remote control center can control and monitor the substation. The bay level consists of bay control units (BCUs), bay protection units (BPUs), measuring centers (MCs), and transducers. Finally, the process level connects directly to high-voltage (HV) equipment. This level interfaces between HV equipment and bay-level devices and transfers measurement and status data to the intelligent devices at the bay level. The process level also conveys the commands from the bay level to the HV equipment. It comprises indicators, sensors, actuators, remote I/O and merging units (MUs) connected to circuit breakers, disconnect switches, voltage transformers and current transformers. Fig. 1 illustrates a typical SAS with all three levels.

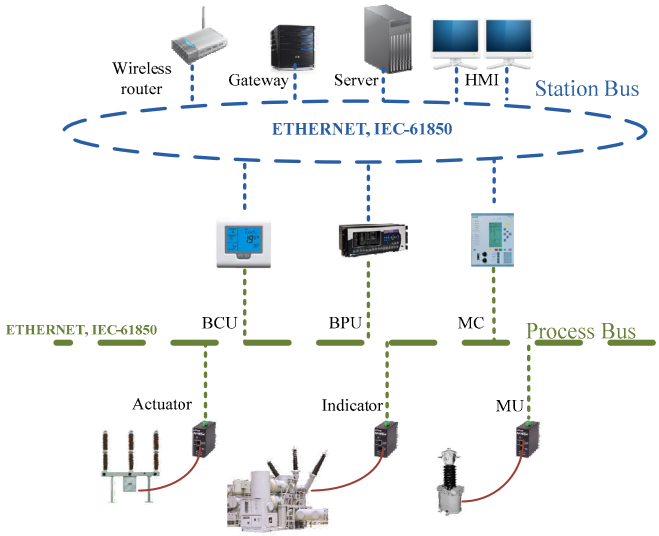

Fig. 1. A typical IEC-61850-enabled SAS

All real devices at all three levels of the SAS, including MUs, BCUs, BPUs, switches, converters, servers and HMIs, are categorized as physical nodes [13]. IEC61850 defines each function as a logical node [14]. An IED is an appliance that incorporates processors, analog and digital inputs/outputs (I/O), and communication capabilities, operating as a meter, controller, indicator, or digital relay in the SAS [15], [16].

TABLE I
ARRAYS OR MATRICES ANNOTATING NETWORK TOPOLOGY

Structure	Full Name	Definition
N	Node	Includes network devices such as computers, switches, and all other real elements.
C	Connection	Includes each cable or path connecting two elements.
S	Source	A virtual structure modeling beginning points.
L	Load	A virtual structure modeling end points.
R	Required (REQ)	Data transfer requirements.

Monitoring data (e.g., statuses, values, indication) usually flow from IEDs to servers, and control commands flow back to the IEDs. A BCU is an IED that controls a breaker and other HV equipment; it controls the opening and closing of the breaker, monitors the breaker's status, and receives the open and close requests from the station level. Also, a BCU reports a breaker's status change events to HMIs and other IEDs through the process bus [1]. The BCU is a source of data in an SAS, and any failure in it causes data loss [14].

Table I defines the structures of the real elements (devices and connections) and virtual elements (sources, loads and required elements) in an SAS. These structures are matrices within which each entry may be a number, plain text, or even another matrix [12]. Physical data connections in the Ethernet network can be made with either fiber optic or copper cables. All information regarding connections is included in the *C* structure. Sources and loads are points among which data travel back and forth; therefore, load and source points are selected arbitrarily. REQs are virtual elements required for data transfer. To address all requirements, it is insufficient to consider only the connectivity between inputs and outputs. REQs are intermediate devices that process the data being transmitted from the source to the load. Therefore, a load exhibits data integrity as long as it has connectivity with all types of REQ elements.

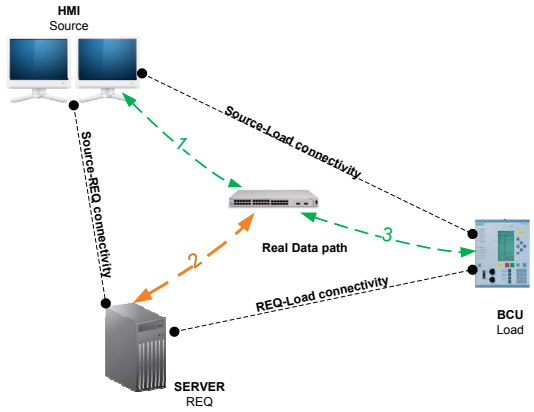

Fig. 4. The role of REQ in transferring data between source and load

Figure 4, which shows the transfer of data between HMIs and BCUs, illustrates that this process actually consists of two instances of data communication:

1- Between the HMI (source) and the SERVER (REQ), paths (1) and (2);
2- Between the SERVER (REQ) and the IED (load), paths (2) and (3);

Array *Nreq* determines whether or not a node is an REQ element, and if so, which type of REQ it is, based on structure *R*. Thus, $Nreq_j$ is *k* if N_j is the k^{th} element of *R*.

REQs are critical points in an SAS network; thus, any failure on such devices diminishes the integrity of the network. Redundant REQs establish a highly available network in that the failure of one REQ causes the redundant one to start working within the fail-over time (*Rst*) [10], [11]. To build the infrastructure that will enable engineers to design a highly available SAS, the architectures, protocols, topologies and applications must support high-availability solutions [4].

Each state of the network is defined in the form of an array (Φ) in which each element refers to the status of a real device in the network.

$$\Phi = (\varphi_1, \varphi_2, ..., \varphi_{n_C}, \varphi_{n_C+1}, ..., \varphi_{n_E}) \quad (1)$$

where φ_k is the status of element k in state Φ. The value 0 for φ_k means that element k is in service, while a 1 represents the outage of element k. Also,

$$n_E = n_C + n_N \quad (2)$$

where n_C *and* n_N represent the number of connections and nodes, respectively.

B. Integrity of Loads

The integrity of a graph is defined as the connectivity between nodes via a single available path or multiple available paths. Likewise, in the SAS, the integrity of a node is maintained if at least one path is available for data transmission.

Load integrity is inspected per each REQ. The model proposed in Equations (3)-(7) is a linear optimization problem that maximizes the integrity of load points.

$$Maximize \quad \sum_{k=1}^{n_R}\sum_{m=1}^{n_N}\zeta_{m,k} \quad (3)$$

Subject to:

$$0 \le \zeta_{m,k} \le 1 \qquad \forall k \in \{1,...,n_R\}, \forall m \in \{1,...,n_N\} \quad (4)$$

$$\sum_{j=1}^{n_N}\psi_{m,j} \times \delta_{m,k} = \rho_{m,k} \times S_{m,k} - \zeta_{m,k} \qquad \forall k \in \{1,...,n_R\}, \forall m \in \{1,...,n_N\} \quad (5)$$

$$\delta_{m,Nreq_m} = 0 \qquad \forall m \in \{1,...n_N\} \quad (6)$$

$$S_{m,k} \ge 0 \qquad \forall k \in \{1,...,n_R\}, \forall m \in \{1,...,n_N\} \quad (7)$$

where $\zeta_{m,k}$ is the integrity of node m to REQ node k; δ_{jb} is the data transferred through the available communication channel j for data source b; $\psi_{m,j}$ is the element of node-channel incidence matrix $\boldsymbol{\psi}$, in which $\psi_{m,j}$=1 if the starting point of the available communication channel j is node m and $\psi_{m,j}$=-1 if the ending point of the available channel j is node m; otherwise, $\psi_{m,j}$=0. After solving the above optimization problem, the multiple integrity index of the data for load point m, ζ_m, is calculated as:

$$\zeta_m = \text{int}\left(\sum_{k=1}^{n_R}\frac{\zeta_{m,k}}{n_R}\right) \quad (8)$$

$$\zeta_i \in \{0,1\}$$

Because $\zeta_{m,k}$ is either 0 or 1, ζ_m is 1 if and only if any $\zeta_{m,k}$ is 1. $\zeta_m = 1$ ensures the integrity of the load point m to all REQs in the network. In other words, for a complete data connection, simple connectivity between each load point and all REQs must be available.

The array ζ of length n_L determines whether or not each load point exhibits data integrity. If load point l^{th} (L_l) has connectivity with all types of REQs, ζ_l is 1; otherwise, it is assumed to be 0.

$$Z_{1\times n_N} = \lfloor \zeta_1 \quad \zeta_2 \quad ... \quad \zeta_{n_L} \rfloor \quad (9)$$

The complement of ζ_m is shown by γ_m, found as

$$\gamma_m = 1 - \zeta_m \quad (10)$$

ζ_m and γ_m are two parameters used in the proposed modeling.

III. Permanent Data loss

All information regarding the status of high-voltage equipment, low-voltage distribution systems, control and protection devices, and indicators is stored temporarily in IEDs, such as BCUs, BPUs, and MCs, and then transferred to the servers for permanent storage. A failure in any IED will cause permanent data loss during the failure period, with no possibility of retrieving the lost data. In this paper, permanent data loss is measured as a numerical index while the network is experiencing a failure. This index can be measured and calculated in duration, bits, bytes, or as a percentage of the total data.

A. Data Loss of a Load without Integrity

When the load loses its integrity to the entire network, the maximum data lost from the time the element failed to the time it returned to the network (MTTR) is measured. When φ_j =1, the element j could be in one of the following four states:

1) Failure of a Connection

If element j is a connection (not a node), the duration of time over which permanent data loss occurs is:

$$\chi_{l,j}^{p} = 0 \quad (11)$$

This means that the failure of a connection does not necessarily cause permanent data loss in the SAS because, once integrity is restored inside the network, the data source will attempt to send the data to be logged in the file server.

2) Failure of a Non-Redundant Node

If element j lacks a backup in the form of a hot or cold standby REQ node, repairing the system requires $1/E\mu_j$. Therefore, the permanent data loss duration is found as:

$$\chi_{l,j}^{p} = \gamma_l \times \varphi_j \times (1/E\mu_j) \times Npdl_{j-n_C} \quad (12)$$

where $E\mu_j$ is the repair time of element j ($MTTR_j$); φ_j is 1 if the element of connection j fails; and γ_l =1 indicates that the network has no integrity. In (12), $\chi_{l,j}^{p}$ is non-zero if γ_l and φ_j are 1 and $Npdl_{j-n_C}$ is a non-zero value. The array *Npdl* is extracted from the *Node* structure, addressing the portion of data loss caused by the failure of each node. *Npdl* is a normalized variable; thus, each entry is a number between 0 and 1. An *Npdl* of 1 means that all data were lost during the downtime and recovery processes of a fault. Element failure is

not the only reason for data loss; data loss can occur in situations in which the connections and devices remain in service. For example, in the case of a cold standby of elements during switchover, data are lost because the switchover process takes time.

3) Failure of a Redundant REQ

Critical devices in the network must be backed up by redundant devices; otherwise, a single failure will cause data corruption over the entire network. If the active REQ fails, the hot or cold standby element is initiated as a substitute. If element *j* is a hot or cold standby REQ node and at least one standby element is *in-state*, then the permanent data loss for element *j* is calculated as:

$$\chi_{l,j}^{p} = \gamma_l \times \varphi_j \times Rst_{Nreq_{j-n_C}} \times Npdl_{j-n_C} \quad (13)$$

where $Rst_{Nreq_{j-n_C}}$ is the fail-over switching time between the redundant REQs of element *j*. In (13), $\chi_{l,j}^{p}$ is non-zero if γ_l and φ_j are 1 and $Npdl_{j-n_C}$ is a non-zero value. γ_l =1 and φ_j =1 indicate that the network loses integrity when element *j* fails.

Rst is related primarily to the network architecture. The network architecture specifically recognizes when the main device stops responding, at which point its workload must be transferred expeditiously and seamlessly to one of the standby devices [17]. The server is the most important REQ in the network because it is responsible for recording data and executing commands.

Among all high availability architecture to provide hot standby redundancy between servers *mirroring* is the easiest one. *Mirroring* entails the active server copying all of its contents to the redundant server. When one server fails, the other is ready to take over within a few minutes [18]. When the principal server fails, some degree of data loss is inevitable because the system will lose data until the standby server completely activates and *forcing service* occurs. The mirror server stops communicating with the principal server and therefore cannot ensure that the server databases are synchronized. Forcing service starts a new recovery fork in that the mirror server starts its service from the last synchronized point.

4) Overall Data Loss

The duration of time over which permanent data loss occurs for load point *l* is the maximum of all data loss caused by various failures in the network:

$$\chi_l^p = \underset{j=1}{\overset{n_E}{Max}}(\chi_{l,j}^{p}) \quad (14)$$

where χ_l^p is the data loss duration of load *l*.

According to the value of each load point, the index of the duration of time over which permanent data loss occurs for all load points in state Φ is:

$$\chi^p = \sum_{l=1}^{n_L} Lv_l \times \chi_l^p \quad (15)$$

where Lv_l determines the value and worthiness of load point *l, and* χ_l^p is the overall permanent data loss duration. Based on the number of logical nodes and their functions, the load points have different values for specific tasks. They are ranked based on the importance of the elements and their risk of failure. To calculate the extent of permanent data loss in bits, it is necessary to determine the parameter *Ntr*, which is an element's average data transfer frequency. Therefore,

$$\chi_{bit}^{p} = F \times \left(\sum_{l=1}^{n_L} Lv_l \times \chi_l^p \times Ntr_{Lp_l} \right) \quad (16)$$

where *F* is the length of the transferred data package in bits, and Ntr_{Lp_l} is the talk rate of load *l* in 1/sec. Hence, χ_{bit}^{p} represents the permanent data loss in bits in state Φ.

B. Data Loss of a Load with Integrity

When a load point maintains its integrity across the entire network, certain circumstances still can cause the SAS to lose data. When a cold-standby device is activated to substitute for a failed device, it is unable to record data. Because this represents a temporary fault inside the network, it does not permanently affect integrity inside the network.

The REQ elements emulate the balance nodes of the network. ζ_l=1 indicates the integrity of load *l* to the network, which generally requires at least one of each type of REQ element. Therefore, in the array $\Phi = (\varphi_1, \varphi_2, ..., \varphi_{n_C}, \varphi_{n_C+1}, ..., \varphi_{n_E})$, when the entry ($\varphi_j$) is 1, if element *j* is not an REQ node ($j>n_C$ and $Nreq_{j-n_c} = 0$), then no data loss occurs. If the j^{th} element is an REQ node ($j>n_C$, and $Nreq_{j-n_c} \neq 0$), then φ_j = 1 causes data loss due to the switching of REQ elements. The duration of time over which data loss occurs in load point *l* in state Φ can be written as:

$$\chi_l^p = \underset{j=n_c+1}{\overset{n_E}{Max}} (Sgn(Nreq_{j-n_C}) \times \zeta_l \times \varphi_j \times Rst_{Nreq_{j-n_C}} \times Npdl_{j-n_C}) \quad (17)$$

where Rst_k is the switching time for the k^{th} REQ, *Max* represents the maximum function, and *sgn* stands for the sign function, which is 1 and 0 when the input number is positive and 0, respectively.

IV. Case Study

In this case study, data loss in a substation control system is investigated. Fig. 3 depicts an SAS with redundant star topology, which consists of three star couplers ($RER111_i$), controllers (NL_i), servers ($SERVER_i$) and protocol convertors ($PCLTA_i$). The station level houses TCP/IP-based Ethernet networks. Redundant connections increase the reliability of the SAS. It is assumed that the switchover process takes four minutes and that repairing each non-redundant device takes 24 hours. The permanent data loss of the SAS is calculated in five different cases.

A. Data Loss Under Various Network States

State 1: *Failure of SERVER1*

A failure in SERVER1 requires the workload of the failed server to be transferred immediately and seamlessly to the standby server. The switchover is assumed to take four minutes, during which time all of the data from the four loads will be lost.

$$\chi^{p}_{NL1,SERVER1} = 240\,s$$

$$\chi^{p}_{NL2,SERVER1} = 240\,s$$

$$\chi^{p}_{NL3,SERVER1} = 240\,s$$

$$\chi^{p}_{NL4,SERVER1} = 240\,s$$

So, the duration of time over which maximum permanent data loss occurs is:

$$\chi^{p}_{NL_1} = \chi^{p}_{NL_2} = \chi^{p}_{NL_3} = \chi^{p}_{NL_4} = 240\,s$$

Assuming an equal value for all loads, the average duration of time over which permanent data loss occurs is:

$$\chi^{p} = \frac{1}{4}\sum_{i=1}^{4}\chi^{p}_{NL_i} = 240\ s$$

With a talk rate of 1 frame per second and 984 bits per data packet, the total number of permanently lost bits equals:

$$\chi^{p}_{bit} = 240s \times 984\ bps$$

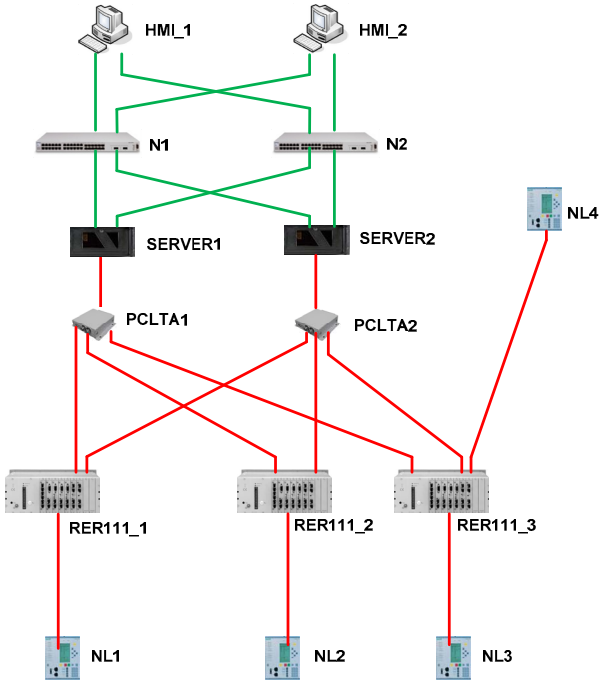

Fig. 3. A typical SAS with star topology

Considering 2^{10} bits as 1kbit, the total amount of data lost in one year is:

$$\chi^{p}_{bit} = 0.23\ Mbit$$

State 2: *Failure of connection between NL3 and RER111_2*

Although a disconnection between NL3 and RER111_2 interrupts the integrity between NL3 and the servers, NL3 will send the recorded data as soon as the integrity recovers. In other words, a failure in the connectors does not cause any data loss (see Eq. (5)).

$$\chi^{p}_{l} = 0$$

State 3: *Failure of RER111_3*

RER111 is a star coupler responsible for data communication and routing inside the network. The *Npdl* values of routing devices are 0 because these types of devices do not record data. Similar to the second state, NL3 will continue sending the locally-recorded data when integrity recovers.

$$\chi^{p}_{l} = 0$$

State 4: *Failure of NL3*

A failure in NL3 prevents all permanent data about the corresponding feeder from being recorded in the system. Nevertheless, other loads (NL1, NL2, and NL4) maintain integrity with the whole system, and their data are recorded in the servers; therefore, they lose no data. The duration of time over which data loss occurs when NL3 fails is calculated based on (6):

$$\chi^{p}_{NL_3} = 24 \times 3600 = 86400\,s$$

For the other three loads, the duration is based on:

$$\chi^{p}_{NL_1} = \chi^{p}_{NL_2} = \chi^{p}_{NL_4} = 0\,s$$

The average duration of time over which permanent data loss occurs is:

$$\chi^{p} = \frac{1}{4}\sum_{i=1}^{4}\chi^{p}_{NL_i} = 21600\ s$$

With a talk rate of 1 frame per second and 984 bits per data packet, the number of bits permanently lost equals:

$$\chi^{p}_{bit} = 20.26\ Mbit$$

State 5: *Failure of NL3, SERVER1:*

The data loss resulting from the failure of NL3 is calculated as 86400 s. Based on (7), the data loss corresponding to the failure of SERVER1 is found as:

$$\chi^{p}_{NL3,SERVER1} = 240\,s$$

So, the maximum duration of time over which permanent data loss occurs is:

$$\chi^{p}_{NL_3} = 86400\,s$$

$$\chi^{p}_{NL_1} = \chi^{p}_{NL_2} = \chi^{p}_{NL_4} = 240\,s$$

Assuming equal values for all loads, the average duration of time over which permanent data loss occurs is:

$$\chi^{p} = \frac{1}{4}\sum_{i=1}^{4}\chi^{p}_{NL_i} = 21780\ s$$

With a talk rate of 1 frame per second and 984 bits per data packet, the total number of bits permanently lost equals:

$$\chi_{bit}^{p} = 20.43\ Mbit$$

B. Comparison and Discussion

Table II compares the results of the five states. States 4 and 5 experience the greatest degree of permanent data loss because both states involve a load failure. A load is an intelligent device that records data regarding all events, statuses and measurements of the corresponding bay of the substation. In states 2 and 3, which involve the failure of a switch or a connection, no permanent data loss occurs because switches and connections do not save any data; they are elements through which data are transferred.

TABLE II
SUMMARY OF RESULTS

State	Description	χ_{bit}^{p} (*Mbit*)
1	Failure of a server	0.23
2	Disconnection of load and switch	0
3	Failure of a switch	0
4	Failure of a load	20.26
5	Failure of a load and a server	20.43

V. CONCLUSION

This paper examined permanent data loss during failures, focusing on the amount of data permanently lost under five failure scenarios. Highly available SASs provides various solutions to alleviate the impact of failures and thereby enhance the reliability of the entire network. Device redundancy helps to reduce total data loss; however, it does not eliminate loss because switching between two redundant elements causes permanent data loss.

The results obtained from the case study show that this index varies based on the state of the network. A comparison of states 1 and 4 indicates that server failure causes the data from all of the loads to be lost, while individual load failure causes only the corresponding load's data to be lost. On the other hand, redundant servers reduce the out-of-service time to only the amount of time it takes to switch between servers, while the relatively lengthy repair time for single loads contributes to significantly more data loss (20.26 *Mbit*) than is suffered under server failures (0.23 *Mbit*).

VI. REFERENCES

[1] T. S. Sidhu and Y. Yujie, "IED modelling for IEC 61850 based substation automation system performance simulation," *Power Engineering Society General Meeting,* 2006, IEEE.

[2] I. Ali and M. S. Thomas, "Ethernet enabled fast and reliable monitoring, protection and control of electric power stations," *IEEE Int. Conf., New Delhi, India*, Dec. 12–15, 2006.

[3] S.S. Tarlochan, Y. Yujie, "Modelling and Simulation for Performance Evaluation of IEC61850-Based Substation Communication Systems," *IEEE transactions on power delivery*, 2007, pp. 1482-1489.

[4] C.M. De Dominicis, P. Ferrari, A. Flammini, S. Rinaldi, M. Quarantelli, "Integration of existing IEC61850-based SAS within new high-availability architectures," *Applied Measurements For Power Systems (AMPS), 2010 IEEE International Workshop on*, 22-24 Sept. 2010.

[5] Yuhui Deng. "RISC: A resilient interconnection network for scalable cluster storage systems." *Journal of Systems Architecture*, vol. 54, pp. 70–80, 2008.

[6] K. Kim, Y. Ryu, J. Rhee, and D. Lee, "SAFE: Scalable Autonomous Fault-tolerant Ethernet," *Proc. IEEE International Conference on Advanced Communication Technology*, Jan. 2009, pp. 365-369.

[7] S. Mohagheghi, "A fuzzy cognitive map for data integrity assessment in a iec 61850 based substation," *in Power and Energy Society General Meeting, 2010 IEEE*, July 2010, pp. 1 –7.

[8] J. M. Rhee, H.A. Pham, S. M. Kim, etc. "Issues of Fail-over Switching for Fault-tolerant Ethernet Implementation", *International Conference on New Trends in Information and Service Science*, 2009, pp. 711-714.

[9] H. Kirrmann, K. Weber, O. Kleineberg, H. Weibel, "HSR: Zero recovery time and low-cost redundancy for Industrial Ethernet (High availability seamless redundancy, IEC 62439-3)," *in proc. of IEEE Conference on Emerging Technologies & Factory Automation, 2009*. ETFA 2009, vol., no., pp.1-4, 22-25 Sept. 2009.

[10] M. Goraj, R. Harada, "Migration paths for IEC 61850 substation communication networks towards superb redundancy based on hybrid PRP and HSR topologies," *Developments in Power Systems Protection, 11th International Conference on* , 23-26 April 2012.

[11] Hubert Kirrmann and Oliver Kleineberg, "Seamless and Low-Cost Redundancy for Substation Automation Systems (High availability Seamless Redundancy, HSR). " *IEEE-Power and Energy Society General Meeting*, Page(s): 1 – 7, 2011.

[12] B. Falahati, Z. Darabi, Y. Fu, and M. Vakilian, "Quantitative modeling and analysis of substation automation systems," *IEEE T&D 2012*, Orlando, FL.

[13] A. Apostolov, "Communications in IEC 61850 Based Substation Automation Systems," *Power Systems Conference: Advanced Metering, Protection, Control, Communication, and Distributed Resources*, 2006. PS '06, PP. 51-56.

[14] T. Sidhu and P. K. Gangadharan, "Control and automation of power system substations using IEC61850 communication," *in Proceedings of the 2005 IEEE Conference on Control Applications*, Toronto, Canada, August 28-31 2005, pp. 1331–1336.

[15] A. Sulistio, G. Poduval, R. Buyya, and C.-K. Tham, "On Incorporating Differentiated Levels of Network Service into GridSim," *Future Generation Computer Systems*, 23(4): 606– 615, May 2007.

[16] T. H. Cormen, C. E. Leiserson, and R. L. Rivest, Introduction to Algorithms. The MIT Press, 1990.

[17] T. Dean, "Network+ guide to networks, 4th edition," Course Technology, 2005.

[18] Intel, "High Availability Server Clustering Solutions, 2002. [Online]. Available:http://www.intel.com/design/network/papers/25157401.pdf

[19] W. Chen, S. Toueg, and M.K. Aguilera, "On the quality of service of failure detectors," *IEEE Trans. Computers*, vol. 51, no. 5, pp. 561- 580, May 2002.

VII. BIOGRAPHIES

Bamdad Falahati (S'08) received the B.S. and M.S. degrees in electrical engineering from Sharif University of Technology in 1999 and 2008 respectively. He is currently with Mississippi State University pursuing his Ph.D. degree in electrical engineering.

Zahra Darabi (S'08) received her Ph.D. in the Department of Electrical and Computer Engineering at the Missouri University of Science and Technology. She is currently working at SNC-LAVALIN.

Mehdi Vakilian received his BSc in electrical engineering (1978) and MSc in electric power engineering (1986) from the Sharif University of Technology in Tehran, and his PhD in electric power engineering (1993) from Rensselaer Polytechnic Institute, Troy, NY, USA.

Yong Fu (M'05) received his B.S. and M.S. degrees in electrical engineering from Shanghai Jiaotong University, China, in 1997 and 2002, respectively, and his Ph.D degree in electrical engineering from the Illinois Institute of Technology, USA, in 2006.