Reliability and Component Importance Analysis of All-Digital Protection Systems

Peichao Zhang, *Member, IEEE*, Levi Portillo and Mladen Kezunovic, *Fellow, IEEE*

***Abstract*— Analysis of the importance of various components of the all-digital protection system is a key part of the system reliability quantification process. The importance analysis for all-digital protection systems was not covered in the literature so far. This paper investigates and selects two appropriate measures of the importance. The first is the Birnbaum's measure used to identify the weak points of the all-digital protection system that needs to be improved if one is to improve overall system reliability. The second measure uses criticality importance to prioritize maintenance actions. To demonstrate the application of the proposed measures, this paper first introduces alternative architectures of all-digital protection systems. The associated reliability block diagrams as well as the exact system reliability are then given. Afterwards, the component importance for the alternative architectures is analyzed and discussed.**

***Index Terms*— Component importance, IEC 61850, reliability block diagram, reliability, protection system, process bus**

Acronyms[1]

IED	intelligent electronic device
TS	time source
MU	merging unit
PR	protective relay
SW	Ethernet switch
EM	Ethernet communication media
MTTF	mean time to failure
FTA	fault tree analysis
RBD	reliability block diagram

Notations

$X_i(t)$	state variable of component i
$X(t)$	state vector: $X(t) = (X_1(t), X_2(t), \ldots, X_n(t))$
$\Phi(X)$	system structure function
p_i, q_i	reliability, unreliability of component i
λ_i	failure rate of component i
h	$Pr\{\Phi(X) = 1\}$: system reliability
$R_{sys}(t)$	system reliability
$Q_{sys}(t)$	system unreliability
$I^B(i\|t)$	Birnbaum's measure of importance of component i
$I^{CR}(i\|t)$	Criticality importance of component i

This work was supported by PSerc project titled, "Digital Protection System Using Optical Instrument Transformers and Digital Relays Interconnected by an IEC 61850-9-2 Digital Process Bus"

P. Zhang is with the Department of Electrical Engineering, Shanghai Jiao Tong University, Shanghai, China (e-mail: pczhang@sjtu.edu.cn). L. Portillo and M. Kezunovic are with the Department of Electrical and Computer Engineering, Texas A&M University, College Station, TX 77843-3128, USA (leviportillo@tamu.edu, kezunov@ece.tamu.edu).

[1]The singular and plural of an acronym are always spelled the same.

I. Introduction

Recent development of non-conventional instrument transformers and wide spread use of digital relays permit implementation of an all-digital protection system. In such a system, the output of the non-conventional instrument transformers is a digital signal, which can be connected to digital relays through an IEC 61850-9-2 digital process bus [1].

The all-digital protection system is expected to have equal or higher reliability than the conventional one. A typical all-digital protection system comprises more electronic devices (merging units, Ethernet switches, time synchronization sources) than the conventional one. This is one of the potential shortcomings of the all-digital protection system, since the count of electronic devices comprising a fully integrated system has a dramatic impact on the availability of the system [2]. There are several solutions to improve the availability of the new system. One known solution is to replace copper wires with fiber optics as intended by IEC 61850, so that the total part count would be greatly reduced. Another solution is redundancy, as the all-digital protection system allows true redundancy ranging from the redundant instrument transformers, merging unit, communication link to protection relay. The third solution is the use of self-testing and monitoring, since the new solution will reduce the number of non-supervised functions and components to almost zero [3]. Any protection system fully designed under the IEC 61850 protocol will make use of each and everyone mentioned feature, hence the reliability models for the all-digital protection system should be constructed to accommodate such approach.

Considerable work has been done to examine different reliability aspects of conventional protection systems. One important technique is to use Markov model. Some reliability indices such as "unreadiness probability" [4], "abnormal unavailability" and "protection unavailability" [5], [6], [7] have been defined. Another important technique is Fault Tree Analysis (FTA) [8], which is an effective way to compare the relative unavailability of various protection schemes [9], [10], [11]. The reliability analysis techniques applied to conventional protection systems can also be applied in all-digital protection systems.

However, reliability analysis of a protection system tells only one part of a story. When the results of a reliability analysis are generated, follow-up questions arise, such as:

- "What are the weak points in an all-digital protection system?"
- "What are the methods and the most cost effective way to improve the reliability of the system?"

- "How to allocate inspection and maintenance resources, and how to prioritize the maintenance actions?"

The answers to these questions require an analysis that identifies importance of each component. This paper aims at investigating and selecting reliability indices to identify the critical components in an all-digital protection system. The paper is organized as follows. Section II proposes alternative system architectures of all-digital protection system. Section III derives associated reliability functions. Section IV focuses on the component importance analysis. Section V discusses some other considerations. Section VI draws the conclusions.

II. System Architectures of All-digital Protection Systems

A. Components Considered

An all-digital protection system is composed of non-conventional instrument transducers, merging units, Ethernet switches, Ethernet interfaces, external time sources and protective relay.

We will assume that the instrument transducers and batteries are extremely reliable. Accordingly, they will not be considered in the reliability models.

We assume a single merging unit can process and provide all signals required by a relay. In the real case, taking distance relay as an example, two merging units may be needed to assemble voltage and current signals separately. But since these merging units are connected in series with each other in the reliability model, the total failure rate is the sum of failure rate of each merging unit given constant failure rates.

As communication plays a very critical role in an all-digital protection system, both Ethernet switch and Ethernet interface should be modeled. The Ethernet interface may be referred to as either Ethernet port or Ethernet communication media [2]. We assume the Ethernet port is a part of the host IED and its reliability has been included in the overall MTTF of the IED. Accordingly, we consider only Ethernet communication media rather than Ethernet port in the reliability models.

A 61850 compatible IED would have an internal clock for time stamping purposes but an external synchronization source will also be needed to provide system wide time synchronization. Capability for time synchronization of sampling data (voltage and current signals from non-conventional CTs and VTs) is required for correct operation of most protection functions [2]. Therefore, the reliability model for the system will consider the time synchronization source connected in series with the other elements. Redundancy of time synchronization would then be needed to maintain the overall system reliability.

B. Alternative System Architectures

This paper defines six alternative system architectures, as shown in Fig. 1. Architecture 1 assumes redundancy only in the relays. Architecture 2 has redundant merging units and relays. Architecture 3 has two redundant and independent protection systems. In architecture 4, the switches are cascaded so as to provide "cross backup" in the merging units and instrument transducers between the two protection systems. Architecture 5 is similar to 3, but adds redundancy in Ethernet switches and Ethernet communication media. Ring communication connection is used in architecture 6, which provides a very high level of reliability. In general, Ethernet does not operate in loops. However, the IEEE 802.1w Rapid Spanning Tree algorithm which is implemented in modern managed switches can detect rings and fix breaks in structures in as little as 5 ms [2], [12]. Besides the ring connection, other fault tolerant network topologies for substation automation are discussed in [12].

From a component redundancy perspective, the proposed architectures can be classified into three categories: (1) providing redundancy in relays and / or instrument transducers (architectures 1-3), which is a typical industrial practice for conventional protection systems; (2) providing redundancy in the Ethernet (architectures 5, 6); and (3) providing "cross backup" at the process level between protection systems (architectures 2, 4, 6).

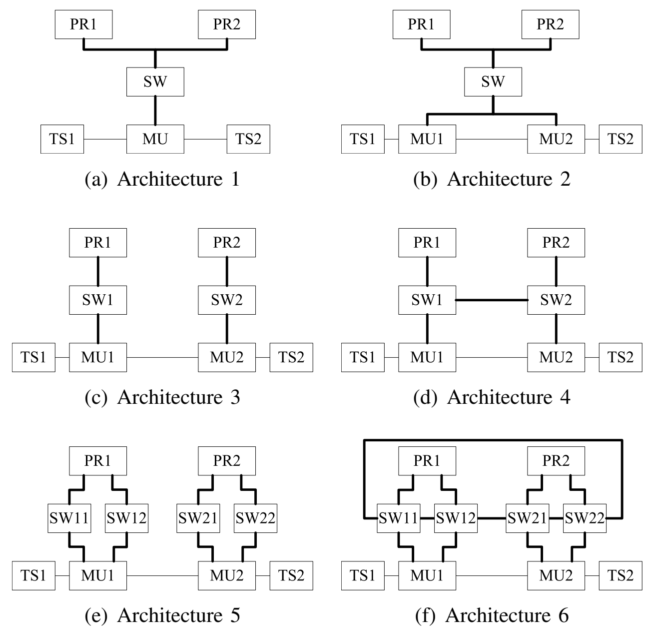


Fig. 1. Alternative system architectures.

III. System Reliability Analysis

A. Reliability Block Diagram

A reliability block diagram (RBD) is a success-oriented network describing the function of the system. It shows the logical connections of components needed to fulfill a specified system function [13].

If the system has more than one function, a separate reliability block diagram has to be established for each system function. Reliability of protective relaying function is a compromise between security and dependability [10]. In this paper, we study only the dependability issue.

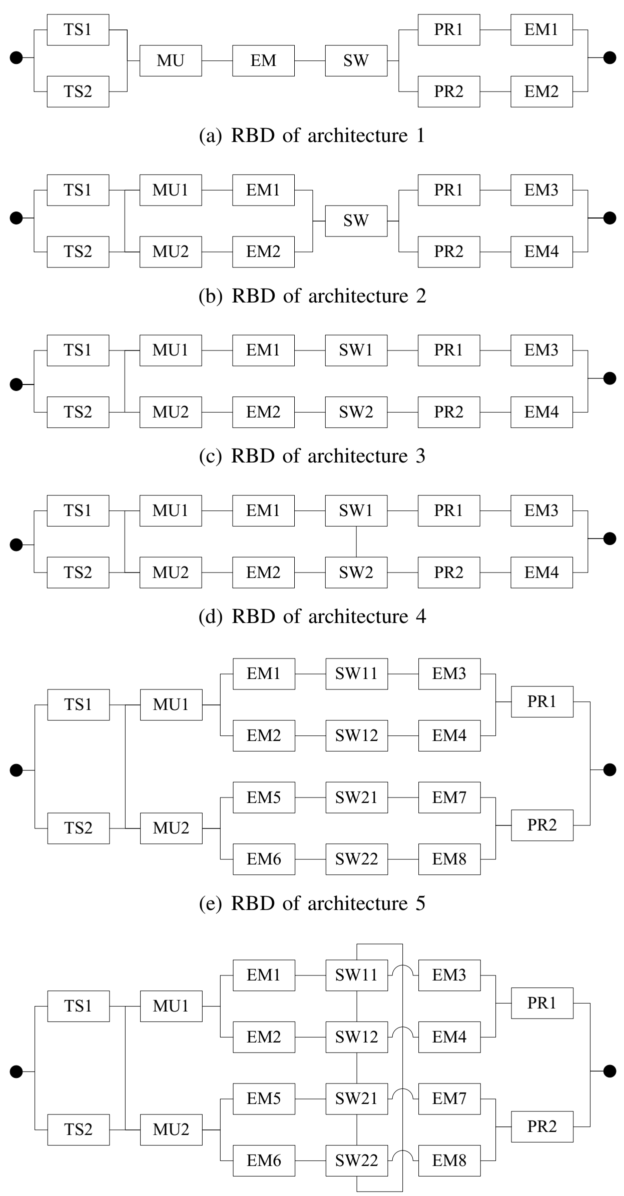
We also assume that, if a fault occurs and is isolated from a redundant (backup) protection system, the fact that the primary relay system did not operate does not constitute a mis-operation. In this case, the whole protection system may degrade but not fully fail.

With the above assumptions, the reliability block diagrams related to alternative system architectures 1 - 6 are constructed and shown in Fig 2. It should be noted that, we assume the links between Ethernet switches are reliable.

Having established the reliability block diagrams, we use the minimal path sets method to calculate the exact system reliability. For a given architecture, when all the minimal path sets $P_1, P_2, \dots, P_p$ are determined, the structure function may be written as

$$\Phi(X) = \coprod_{j=1}^{p} \prod_{i \in P_j} X_i. \tag{1}$$

The structure function is thus written as a multilinear form. $\Phi(X)$ is then expanded, and all exponents should be omitted since $X_i, i = 1, 2, \dots, n$ are binary. The system reliability is obtained by replacing all the X_i's in the structure function by the corresponding p_i's.



(a) RBD of architecture 1

(b) RBD of architecture 2

(c) RBD of architecture 3

(d) RBD of architecture 4

(e) RBD of architecture 5

(f) RBD of architecture 6

Fig. 2. Reliability block diagrams of the alternative system architectures.

B. System Reliability

The reliability of a component i with a constant failure rate λ_i is

$$R_i(t) = p_i(t) = e^{-\lambda_i t}. \tag{2}$$

For simplicity, we assume the components of the same type have the same reliability. Thus, the reliabilities of time sources, merging units, Ethernet switches, Ethernet communication media and protective relays can be denoted by p_{ts}, p_{mu}, p_{sw}, p_{em} and p_{pr} respectively.

There are four minimal path sets in architecture 1, the system reliability of which is

$$\begin{aligned} R^{(1)}_{sys}(t) = &-2p_{ts}p_{mu}p_{pr}^2p_{sw}p_{em}^3 + p_{ts}^2p_{mu}p_{pr}^2p_{sw}p_{em}^3 \\ &-2p_{ts}^2p_{mu}p_{pr}p_{sw}p_{em}^2 + 4p_{ts}p_{mu}p_{pr}p_{sw}p_{em}^2. \end{aligned} \tag{3}$$

There are eight minimal path sets in architecture 2, the system reliability of which is

$$\begin{aligned} R^{(2)}_{sys}(t) = &-2p_{ts}p_{mu}p_{pr}^2p_{sw}p_{em}^3 + p_{ts}p_{mu}^2p_{pr}^2p_{sw}p_{em}^4 \\ &-2p_{ts}p_{mu}^2p_{pr}p_{sw}p_{em}^3 + 4p_{ts}p_{mu}p_{pr}p_{sw}p_{em}^2. \end{aligned} \tag{4}$$

There are four minimal path sets in architecture 3, the system reliability of which is

$$\begin{aligned} R^{(3)}_{sys}(t) = &-2p_{ts}p_{mu}^2p_{pr}^2p_{sw}^2p_{em}^4 + p_{ts}^2p_{mu}^2p_{pr}^2p_{sw}^2p_{em}^4 \\ &-2p_{ts}^2p_{mu}p_{pr}p_{sw}p_{em}^2 + 4p_{mu}p_{pr}p_{sw}p_{em}^2. \end{aligned} \tag{5}$$

There are eight minimal path sets in architecture 4, the system reliability of which is

$$\begin{aligned} R^{(4)}_{sys}(t) = &-p_{mu}^2p_{pr}^2p_{sw}^2p_{ts}^2p_{em}^4 + 2p_{mu}^2p_{pr}^2p_{sw}^2p_{ts}p_{em}^4 \\ &+2p_{mu}p_{pr}^2p_{sw}^2p_{ts}^2p_{em}^3 + 2p_{mu}^2p_{pr}p_{sw}^2p_{ts}^2p_{em}^3 \\ &-4p_{mu}p_{pr}^2p_{sw}^2p_{ts}p_{em}^3 - 4p_{mu}^2p_{pr}p_{sw}^2p_{ts}p_{em}^3 \\ &-2p_{mu}p_{pr}p_{sw}^2p_{ts}^2p_{em}^2 - 2p_{mu}p_{pr}p_{sw}p_{ts}^2p_{em}^2 \\ &+4p_{mu}p_{pr}p_{sw}^2p_{ts}p_{em}^2 + 4p_{mu}p_{pr}p_{sw}p_{ts}p_{em}^2. \end{aligned} \tag{6}$$

There are eight minimal path sets in architecture 5, the system reliability of which is

$$\begin{aligned} R^{(5)}_{sys}(t) = &-2p_{mu}^2p_{pr}^2p_{sw}^4p_{ts}p_{em}^8 + p_{mu}^2p_{pr}^2p_{sw}^4p_{ts}^2p_{em}^8 \\ &-4p_{mu}^2p_{pr}^2p_{sw}^3p_{ts}^2p_{em}^6 + 8p_{mu}^2p_{pr}^2p_{sw}^3p_{ts}p_{em}^6 \\ &+4p_{mu}^2p_{pr}^2p_{sw}^2p_{ts}^2p_{em}^4 + 2p_{mu}p_{pr}p_{sw}^2p_{ts}^2p_{em}^4 \\ &-8p_{mu}^2p_{pr}^2p_{sw}^2p_{ts}p_{em}^4 - 4p_{mu}p_{pr}p_{sw}^2p_{ts}p_{em}^4 \\ &-4p_{mu}p_{pr}p_{sw}p_{ts}^2p_{em}^2 + 8p_{mu}p_{pr}p_{sw}p_{ts}p_{em}^2. \end{aligned} \tag{7}$$

There are fifty-six minimal path sets in architecture 6, the system reliability of which is (after being simplified)

$$\begin{aligned} R^{(6)}_{sys}(t) = &-p_{em}^2p_{mu}p_{pr}p_{sw}p_{ts}(p_{ts}-2) \\ &((2p_{em}(p_{em}+(p_{em}((p_{em}-4)p_{em}+2) \\ &+2)p_{mu}) + p_{em}(p_{em}((p_{em}-4)p_{em}(p_{mu} \\ &(p_{em}-2)^2+2)+4)+4)p_{pr}-4)p_{sw}^3 \\ &+4((1-p_{em})((p_{em}-4)p_{em}p_{mu}+2) \\ &+p_{em}(p_{em}(p_{mu}(p_{em}-2)^2-p_{em}+5) \\ &-4)p_{pr})p_{sw}^2 + 2(p_{em}^2-2(p_{mu} \\ &+p_{pr}+2)p_{em}+4)p_{sw}+4). \end{aligned} \tag{8}$$

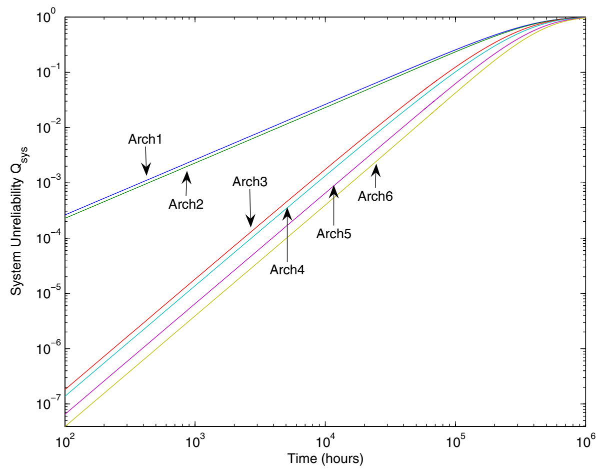


Fig. 3. System unreliability *vs* time of the alternative architectures.

TABLE I
SYSTEM UNRELIABILITY AND MTTF

Architecture #	Q_{sys} ($t = 1000$ hours)	$MTTF$) (years)
1	2.60E-03	31.5
2	2.30E-03	32.7
3	1.81E-05	37.3
4	1.37E-05	40.1
5	6.52E-06	46.0
6	3.92E-06	50.4

MTTF is defined as

$$MTTF = \int_0^\infty R_{sys}(t)dt. \tag{9}$$

The system unreliability is calculated by

$$Q_{sys}(t) = 1 - R_{sys}(t). \tag{10}$$

We assume the Ethernet communication media has a failure rate of 0.003 year^{-1} (MTTF $\approx$ 300 years), and the rest components have the failure rates of 0.01 year^{-1} (MTTF $=$ 100 years). The system unreliabilities vs time are shown in Fig. 3. The system unreliabilities at mission time = 1000 hours and MTTF are listed in Table I.

C. Observations

The following observations can be made based on the experiment results:

1) Architecture 1 and 2 have unreliability numbers by orders of magnitude higher when compared with the others. This is reasonable since they have non-redundant components like Ethernet switch, which constitute the bottleneck of the system reliability.
2) Introducing redundancy in the Ethernet has greater impact on improving system reliability than introducing "cross backup" at the process level. For example, from architecture 3 to 5, the MTTF is increased by 8.7 years by introducing Ethernet redundancy, while from architecture 3 to 4, the MTTF is increased by only 2.8 years by introducing "cross backup".

Since architecture 1 and 2 have much lower reliability levels, they will not be studied further in the following component importance analysis.

IV. COMPONENT IMPORTANCE ANALYSIS

The importance of a component depends on two factors: (1) the location of the component in the system; (2) the reliability of the component in question.

How a component importance measure is applied depends on the phase in the system's life cycle. In the system design phase, the importance measure may be used to identify weak points and components that should be improved to improve the system reliability. Once identified, the reliability of a component may be improved by using a higher quality component, by introducing redundant components, or by improving the maintainability of the component. In the operational phase, the component importance measure may be used to allocate inspection and maintenance resources to the most important components.

A. Component Importance Measures

Several importance measures (e.g., Birnbaum's measure, [14], Fussell-Vesely's measure [15], risk achievement worth, risk reduction worth [16], criticality importance) for components have been proposed in the past. After investigating these measures, we select Birnbaum's measure and criticality importance measure to quantify the component importance in an all-digital protection system.

1) Birnbaum's Measure: Birnbaum's measure of importance of component i at time t is

$$I^B(i|t) = \frac{\partial R_{sys}(t)}{\partial p_i(t)}, \tag{11}$$

where $i = 1, 2, \ldots, n$.

Semantically, the Birnbaum's importance of component i can be interpreted as the rate at which the system reliability improves as the reliability of component i improves.

Birnbaum's measure can also be written as

$$I^B(i|t) = h(1_i, R_{sys}(t)) - h(0_i, R_{sys}(t)), \tag{12}$$

where $h(1_i, R_{sys}(t))$ denotes the conditional probability that the system is functioning when it is known that component i is functioning at time t, and $h(0_i, R_{sys}(t))$ denotes the conditional probability that the system is functioning when component i is in a failed state at time t.

From the definition, the Birnbaum's measure may serve as a good indicator for selecting components that are the best candidates for efforts leading to improving system reliability. But $I^B(i|t)$ only depends on the structure of the system and reliability of other components. It is independent of the actual reliability $p_i(t)$ of component i. This is a weakness of Birnbaum's measure [13].

2) Criticality Importance: The criticality importance $I^{CR}(i|t)$ is another popular measure. As compared with Birnbaum's measure, the reliability attribute of the studied component is integrated into the measure. Analytically, the criticality importance is defined by

$$I^{CR}(i|t) = \frac{I^B(i|t) \cdot (1 - p_i(t))}{1 - R_{sys}(t)}. \tag{13}$$

Criticality importance can also be written as

$$I^{CR}(i|t) = \frac{Pr(C(1_i, X(t)) \cap (X_i(t) = 0))}{Pr(\Phi(X(t)) = 0)}, \tag{14}$$

where $C(1_i, X(t)$ denote the event that the system at time t is in a state where component i is critical.

Semantically, the criticality importance $I^{CR}(i|t)$ measures the probability of a specific component i being responsible for system failure before time t. For component i to cause system failure, component i must be critical, and then fail. Component i will then, by failing, cause the system to fail. When component i is repaired, the system will start functioning again. As a result, criticality importance is particularly suitable for prioritizing maintenance actions in complex systems. Here the maintenance may refer to preventive maintenance, corrective maintenance or failure-finding maintenance [13].

B. Measure Results

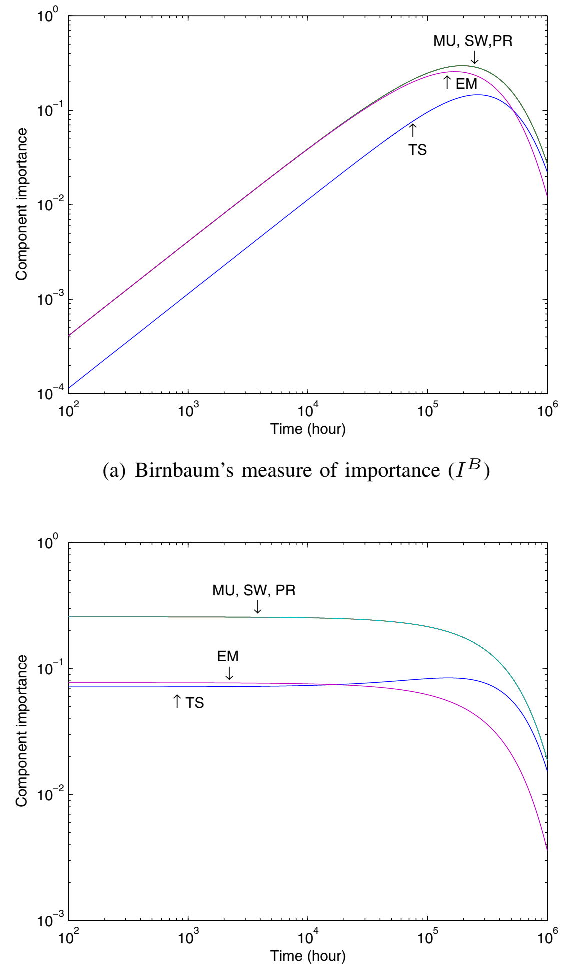
Figs. 4 - 7 show the component importance for architectures 3 - 6. Tables II - V list the exact component importance at mission time = 1000 hours and the ranking of components by their importance.

C. Discussions

The following observations can be made based on the experimental results.

1) Time source. By introducing redundancy in the time sources, they are not the most critical components in architectures 3-5. In architecture 6, the time sources are not more critical than merging units and protective relays.
2) Ethernet. By introducing redundancy in the Ethernet in architecture 5 and 6, the Ethernet switches and communication media are no longer the critical components in the systems.
3) Merging unit and relay. Merging units and relays have the same component importance as they occupy similar positions and have the same failure rates in the studied systems. By introducing "cross-backup" in architecture 4, the criticality of merging units and protective relays are reduced as compared with architecture 3.

It can also be observed that the Birnbaum's measure and criticality importance measure may lead to different rankings. Taking architecture 3 as an example, the Birnbaum's measures show that the Ethernet communication media has almost the same importance as the switch. It means that almost same rate numbers are expected at which the system reliability improves as the reliabilities of the two components improve.



(a) Birnbaum's measure of importance (I^B)

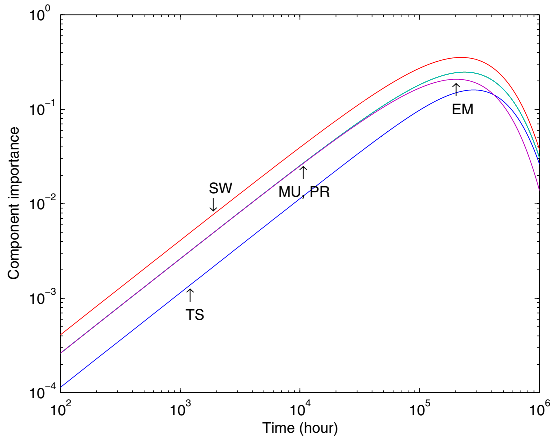
(b) Criticality importance measure (I^{CR})

Fig. 4. Component importance for architecture 3.

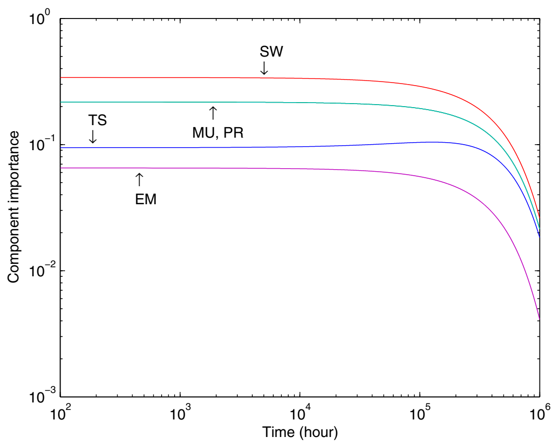
TABLE II
COMPONENT IMPORTANCE FOR ARCHITECTURE 3

Meas.	TS	MU	SW	PR	EM
I^B	0.001	0.004	0.004	0.004	0.004
	Order: (MU = SW = EM = PR) > TS				
I^{CR}	0.072	0.257	0.257	0.257	0.077
	Order: (MU = SW = PR) > EM > TS				

The Birnbaum's measures may induce misleading conclusions in terms of prioritizing system maintenance. It is clear that the Ethernet communication media should be ranked lower in the maintenance checklist than the switch, because although they occupy similar positions in the system, the Ethernet communication media has a lower failure rate. As compared with Birnbaum's measure, the criticality importance gives a more reasonable measure, which indicates the Ethernet communication media is less important than the switch as expected. After checking the results of architectures 3 - 6, it can be concluded that the criticality importance measure is more dynamic and informative. The importance analysis using I^{CR} can result in a more deterministic ranking of the components.



(a) Birnbaum's measure of importance (I^B)



(b) Criticality importance measure (I^{CR})

Fig. 5. Component importance for architecture 4.

TABLE III
COMPONENT IMPORTANCE FOR ARCHITECTURE 4

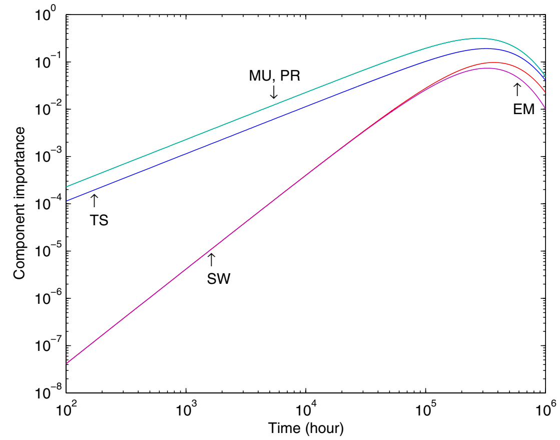
Meas.	TS	MU	SW	PR	EM
I^B	0.001	0.003	0.004	0.003	0.003
	Order: SW $>$ (MU $=$ PR $=$ EM) $>$ TS				
I^{CR}	0.095	0.217	0.340	0.217	0.065
	Order: SW $>$ (MU $=$ PR) $>$ TS $>$ EM				

According to the above observations and analyses, we suggest two general rules for selection of appropriate measures.

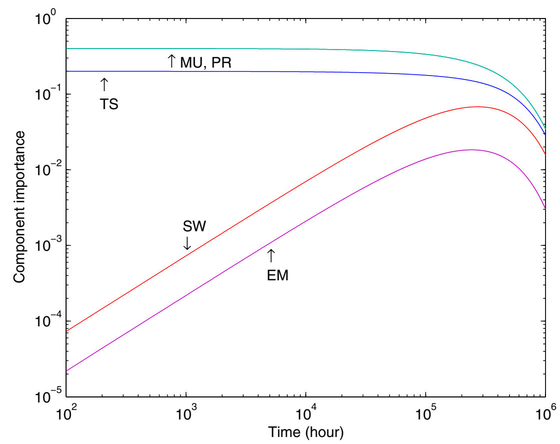
1) If the objective is to assist system designers, and if the reliability of each component can be increased by a specified amount with the same effort, the Birnbaum's measure is an appropriate one.
2) If the objective is to prioritize maintenance actions, or if improvements can be made only to components that have low reliability, the criticality importance measure is an appropriate one.

V. Other Considerations

Because of space limitations, we mainly focus on the dependability and hardware reliability issues in this paper.



(a) Birnbaum's measure of importance (I^B)



(b) Criticality importance measure (I^{CR})

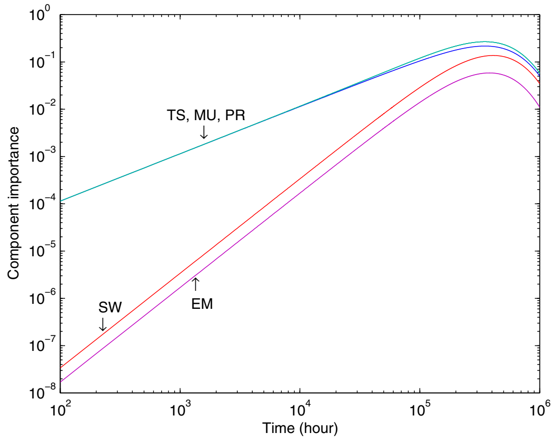
Fig. 6. Component importance for architecture 5.

TABLE IV
COMPONENT IMPORTANCE FOR ARCHITECTURE 5

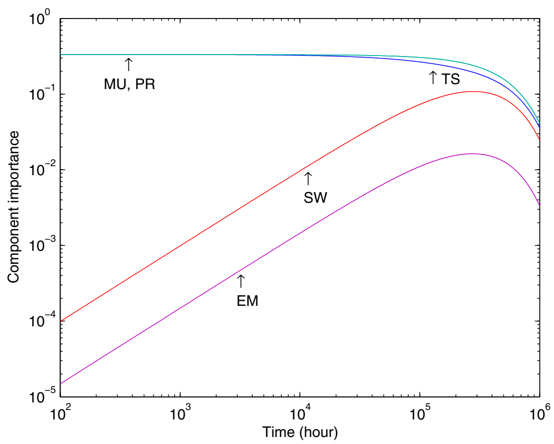
Meas.	TS	MU	SW	PR	EM
I^B	0.001	0.002	0.000	0.002	0.000
	Order: (MU $=$ PR) $>$ TS $>$ (SW $=$ EM)				
I^{CR}	0.200	0.399	0.001	0.399	0.000
	Order: (MU $=$ PR) $>$ TS $>$ SW $>$ EM				

Other important considerations that should not be neglected when evaluating the reliability of all-digital protection systems are discussed briefly in this section.

One important consideration is the security failure. When compared with operational failure, the security failure has two main differences: (1) not all of the components that contribute to an operational failure are capable of contributing to a security failure. For example, of the considered components, the Ethernet components including the Ethernet switches and Ethernet communication media are not security failure risks; (2) the redundancy in the protection systems will improve the system reliability in terms of dependability, whereas it may decrease the system reliability in terms of security [10]. Taking architecture 5 as an example, the reliability block diagram with



(a) Birnbaum's measure of importance (I^B)



(b) Criticality importance measure (I^{CR})

Fig. 7. Component importance for architecture 6.

TABLE V
COMPONENT IMPORTANCE FOR ARCHITECTURE 6

Meas.	TS	MU	SW	PR	EM
I^B	0.001	0.001	0.000	0.001	0.000
	Order: (TS = MU = PR) > SW > EM				
I^{CR}	0.332	0.333	0.001	0.333	0.000
	Order: (TS = MU = PR) > SW > EM				

respect to the security failure is shown in Fig. 8, which is much simpler than that the one with respect to the operational failure shown in Fig. 2(e).

Another important consideration is software reliability. The nature of a software failure is quite different from that of a hardware failure. Because of the complexity of software, over 200 models have been developed since the early 1970s, but how to quantify software reliability still remains largely unsolved [17]. In this paper, we suggest a Logarithmic Exponential Model proposed in [18], which assumes that as software bugs are found and fixed, the failure rate of software will decrease. The expression is:

$$\lambda(\mu)^S = \lambda_0 e^{-\theta\mu}, \tag{15}$$

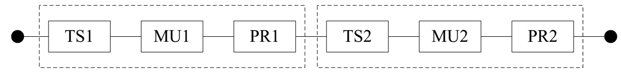


Fig. 8. Reliability block diagram of architecture 5 w.r.t. security.

where λ_0 is a constant, θ is the failure decay parameter and μ is the number of failures found.

As an example, assume $\lambda_0 = 0.1$ year^{-1}, $\theta = 0.2$, $\mu = 10$, the estimated software failure rate is 0.014 year^{-1} according to (15). It should be noted that, as hardware, the software also has two kinds of failures, namely operational failure and security failure of software.

If we take software also as a component of the protection system, the "software component" and the host "hardware component" are connected in series in the reliability model. Taking relay as an example, the combined operational failure rate when considering both the hardware failure and software failure is:

$$\lambda_{pr} = \lambda_{pr}^H + \lambda_{pr}^S. \tag{16}$$

As can be seen from the above discussions, the method proposed in this paper can be applied to both the issue of operational failure and the issue of security failure. After being extended, the method can cover not only the aspect of hardware failure, but also the aspect of software failure.

VI. Conclusion

Redundancy has always been regarded as an important way to increase system reliability. But redundancy is expensive and needs to be limited to mission-critical components. This work focuses on establishing reliability indices for critical components of all-digital protection system. The Birnbaum's measure is suggested as a quantifier of component importance for identifying the bottleneck of the system reliability. The criticality importance is suggested as yet another important quantifier which is useful for diagnosing failures and generating repair or inspection checklists.

The component importance analysis is also useful when facing decisions on equipment cost versus reliability. Our future work will involve developing importance indices which can be used for calculating component contribution to the total system failure cost.

VII. Acknowledgement

The work was done while Dr. Peichao Zhang was working as a visiting scholar at Texas A&M University during June 2005 to July 2006.

References

[1] *Communication networks and systems in substation-Part 9-2: Specific communication service mapping(SCSM)- Sampled analogue values over ISO 8802-3*, IEC Std. 61 850.

[2] B. Kasztenny, J. Whatley, E. A. Udren, J. Burger, D. Finney, and M. Adamiak, "IEC 61850 - a practical application primer for protection engineers," in *59th Annual Conference for Protective Relay Engineers*, Texas A&M University, College Station, Texas, USA, 2006, pp. 309–374.

[3] L. Anderson, C. Brunner, and F. Engler, "Substation automation based on IEC 61850 with new process-close technologies," in *IEEE PowerTech Conference*, vol. 2, Bologna, Italy, June 2003, p. 6.

[4] C. Singh and A. D. Patton, "Protection system reliability modeling: unreadiness probability and mean duration of undetected faults," *IEEE Trans. Rel.*, vol. 29, no. 4, pp. 339–340, Oct. 1980.

[5] P. M. Anderson and S. K. Agarwal, "An improved model for protective-system reliability," *IEEE Trans. Rel.*, vol. 41, no. 3, pp. 422–426, Sept. 1992.

[6] J. J. Kumm, D. Hou, and E. O. Schweitzer, "Predicting the optimum routine test interval for protective relays," *IEEE Trans. Power Delivery*, vol. 10, no. 2, pp. 659–665, Apr. 1995.

[7] P. M. Anderson, R. F. Ghajar, G. M. Chintaluri, and S. M. Magbuhat, "An improved reliability model for redundant protective systems - Markov models," *IEEE Trans. Power Syst.*, vol. 12, no. 2, pp. 573–578, May 1997.

[8] N. H. Roberts, W. E. Vesely, D. F. Haasl, and F. F. Goldberg, *Fault Tree Handbook*. NUREG-0942, U. S. Nuclear Regulatory Commission, Washington, DC, 1981.

[9] I. E. O. Schweitzer and P. M. Anderson. (1998) Reliability analysis of transmission protection using fault tree methods. [Online]. Available: http://www.selinc.com/techpprs/6060.pdf

[10] P. M. Anderson, *Power system protection (Part VI : Reliability of protective systems)*. IEEE Press, 1998.

[11] G. W. Scheer and D. J. Dolezilek. (2000) Comparing the reliability of Ethernet network topologies in substation control and monitoring networks. [Online]. Available: http://www.selinc.com/techpprs/6103.pdf

[12] IEEE Power System Relaying Committee (PSRC) H6. (2005) Application considerations of IEC 61850/UCA 2 for substation Ethernet local area network communication for protection and control. [Online]. Available: http://www.pes-psrc.org/Reports/

[13] M. Rausand and A. Hoyland, *System reliability theory : models, statistical methods, and applications (second edition)*. John Wiley Sons, 2004.

[14] Z. W. Birnbaum, *On the importance of different components in a multicomponent system. In Multivariate Analysis*. Academic, San Diego, 1969.

[15] J. B. Fussell, "How to hand-calculate system safety and reliability characteristics," *IEEE Trans. Rel.*, vol. 24, no. 3, pp. 169–174, 1975.

[16] EPRI, *PSA Application guide*. EPRI TR-105396, Electric Power Research Institute, 1995.

[17] J. Pan. (1999) Software reliability. [Online]. Available: http://www.ece.cmu.edu/~koopman/des_s99/sw_reliability/

[18] J. D. Musa, A. Iannino, and K. Okumoto, *Software reliability: measurement, prediction, application*. McGraw-Hill, 1987.

Peichao Zhang (M'06) was born in 1970 in Jiangsu province, China. He received his M.S. and Ph.D. degrees from Shanghai Jiao Tong University, all in electrical engineering, in 1996 and 2004, respectively. Dr. Peichao Zhang is an associate professor in Shanghai Jiao Tong University. His main research interests are power system protection, system-wide disturbances, as well as signal processing and artificial intelligence applications in power systems.

Levi Portillo was born in 1979 in the state of Zulia, Venezuela. He received his B.S. in Electrical Engineering from Zulia University in 2000. He is currently pursuing the M.S. degree in the Department of Electrical Engineering, Texas A &M University, College Station. Email: leviportillo@tamu.edu.

Mladen Kezunovic (S'77, M'80, SM'85, F'99) has been with Texas A&M University since 1987 where he is the Eugene E. Webb Professor and Director of Electric Power and Power Electronics Institute. His main research interests are digital simulators as well as application of intelligent methods to control, protection and monitoring. Dr. Kezunovic is a registered professional engineer in Texas, and a Fellow of the IEEE.