Improvements in Dependability and Usability for a Substation Automation System with Redundancy

HACHIDAI ITO[*+], KEIICHI KANEDA[#], KOICHI HAMAMATSU[#],
TATSUJI TANAKA[#], KOICHI NARA[$]

* Graduate School of Science and Engineering
Ibaraki University
Hitachi-Shi, Ibaraki 316-8511
JAPAN

Power Systems Control Dept.
Toshiba Corporation
Fuchu-Shi, Tokyo 183-8511
JAPAN

+ Energy Automation Systems Engineering Dept.
Toshiba Corporation
Minato-Ku, Tokyo 105-8001
JAPAN
ha.ito@toshiba.co.jp

$ Fukushima National College of Technology
Iwaki-Shi, Fukushima 970-8034
JAPAN

Abstract: - Substation Automation Systems (SAS) are widely used for the purpose of control, protection, monitoring, communication etc. in substations to improve the reliability of the power supply. SASs adopting IT based solutions such as Ethernet LAN have recently become more common although hardwired control has been used in the past in earlier versions of SAS utilising simple communication methods. Moreover, IEC 61850 which is the international standard for communications within substations has been published, and the application of SAS based on IEC 61850 is increasing.

It is necessary to select each component and the configuration of the SAS from the viewpoint of dependability so that the dependability of the SAS, i.e. reliability, availability, and serviceability may have a very big impact in the stability of the power supply in the electric power transmission and distribution systems.

In this paper, we will describe the configuration policy of an IEC 61850 based SAS, its actual system configuration and the redundant configuration to improve dependability. In addition, we will explain some of the new functions not currently covered by IEC 61850 that we have developed to improve usability and availability. Following which we will present an evaluation of the dependability for MTTF (Mean Time To Failure), Availability, and FMEA (Failure Mode and Effects Analysis) for these configurations of SAS based on the dependability requirements for SAS. Furthermore, other measures have been adopted in the design to ensure fail-safe and fool-proof operation and thus improve system dependability in a much wider sense.

Key-Words: - SAS, Substation Automation System, IEC 61850, Reliability, Dependability, Availability, System Architecture, Redundant System

1 Introduction

Substation Automation Systems (SAS) are widely used for the purpose of control, protection, monitoring, communication etc. in the substation to improve the reliability of the power supply [1]. The monitored and recorded information also can be integrated and used for such power system control applications as shown for example in references [2][3][4]. SAS using IT such as Ethernet LAN has recently become more common although hardwired control has been used in the past in earlier versions of SAS utilising simple communication methods [5][6]. Moreover, IEC 61850 which is the international standard for communications within substations has been published [7], and the application of SAS based on IEC 61850 is increasing [8][9]. Furthermore, the method to transmit the current and voltage data at the process level using a network has been developed and examined [10][11][12]. In addition the process bus has been standardized within IEC 61850.

However, it is necessary to select each component and the configuration of the SAS from the viewpoint of dependability so that the dependability of the SAS, i.e. reliability, availability, and serviceability may

have a very big impact on the stability of the power supply in the electric power transmission and distribution systems. It is common to use various levels of redundancy within the equipment and the network used in a SAS to improve dependability. Moreover, it is often necessary to have sufficient level of redundancy in very important substations to achieve a high level of dependability, because the level of redundancy implemented is usually decided based upon the trade-off between the importance of the substation in the power transmission network and the available budget. Since users such as electric power utilities and SAS manufacturers are interested in the dependability of SAS, various considerations on the dependability of SAS have been performed [13][14][15][16].

The main objective of recently published standard, IEC 61850 is to facilitate interoperability and it aims to enable logical configuration of the SAS by connecting various types of equipment from different vendors through an Ethernet LAN. However, the current version of IEC 61850 does not standardise the redundant configuration. Therefore each manufacturer uses different measures to realise the redundancy which results in different dependability levels and hence difficulty in ensuring interoperability. It is also a very important requirement to maintain interoperability between different manufacturers, different generations of equipment even from the same manufacturer, to enable easy configuration based on a common technology and to achieve better cost/performance.

In this paper, we will explain the concept of system configuration of a SAS using IEC 61850, its actual system configuration and approach to redundancy to improve dependability. In addition we will explain some of the new functions not currently covered by IEC 61850 that we have developed to improve usability and availability. Following which we have performed a dependability evaluation for MTTF (Mean Time To Failure), Availability, FMEA (Failure Mode and Effects Analysis) etc. based on the dependability requirements which are necessary for SAS.

2 Overview of Substation Automation System (SAS)

In this section, we will provide an overview of the purpose, function and system configuration of SAS.

2.1 Background of SAS application

The SAS is a system that provides the automation functions for monitoring, control and protection within a substation and utilises recent improvements in the fields of electronics, information and communication technologies. Application of SAS has increased to fulfil a market requirement to decrease the total cost, including life cycle costs of substation equipment, highly effective operation or near-limit operation of the substation equipment, and the optimization of maintenance costs etc.

Application of SAS to substations began in the 1980's, and systems applied in accordance with international standard specifications such as Ethernet and TCP/IP, etc. as well as systems that utilised proprietary methods from different manufacturers have been applied from the 1990's. IEC 61850 which is the international standard for communications within substations was established from 2003 to 2005 and has become very popular and its application has increased very rapidly in recent years.

A major break-through has been achieved with the application of the IEC 61850 standard. This is the realization of “Interoperability” which is also an objective of this standard. It is expected that the system will be easier to configure in answer to the market requirements by having flexibility in the system configuration. The new standard continues to have a large impact on the design and implementation of SASs and very positive active discussion has continued based on practical experience from

Table 1 Overview of SAS functions

Basic functions	Typical examples of functions
Monitoring functions	• Monitoring of switchgear status, tap position and status of transformer and tap changer, status of protection and control equipment, etc. • Monitoring of electrical quantities, e.g. current, voltage, frequency, power and reactive power, etc.
Control functions	• Control for switchgear and transformer tap • Synchronism check and interlocking • Voltage regulating control and voltage-reactive power control
Recording functions	• Recording the monitoring data and manipulation/control of facility/device • Fault record of facility and device Disturbance fault record
Protection functions	• Protection for Transmission line, Transformer, Busbar, Generator, Distribution feeder, Shunt reactor, Shunt capacitor etc.

manufacturers, system integrators and end-users. This has resulted in further improvements to the standard and this work continues.

2.2 Basic functions of SAS

The basic functions of a SAS are categorised into 4, i.e. monitoring, control, recording and protection. Most SAS systems have the functions described in Table 1, even though these may vary from project to project.

2.3 Basic system configuration of SAS before IEC 61850

Fig. 1 shows a basic system configuration example of SAS before IEC 61850 is adopted. This system configuration, which is still widely used all around the world is based on a distributed-bay configuration policy and utilises Ethernet and TCP/IP for the LAN in the substation. The substation LANs consists of a Station-level LAN and a Bay-level LAN. The Bay-level LAN can be separated into different voltage-levels which is one of the measures used to improve system reliability.

Furthermore, a Standard Time Signal provided by GPS (Global Positioning System) is distributed to each BCU (Bay Control Unit) through a Time Distributor in order to realise an accuracy of 1ms for event recording by each BCU which is a general requirement. Dedicated optical fibre is used for transmission of the Time Signal from the Time Distributor enabling time synchronisation between substation devices such as the BCU of better than 1ms.

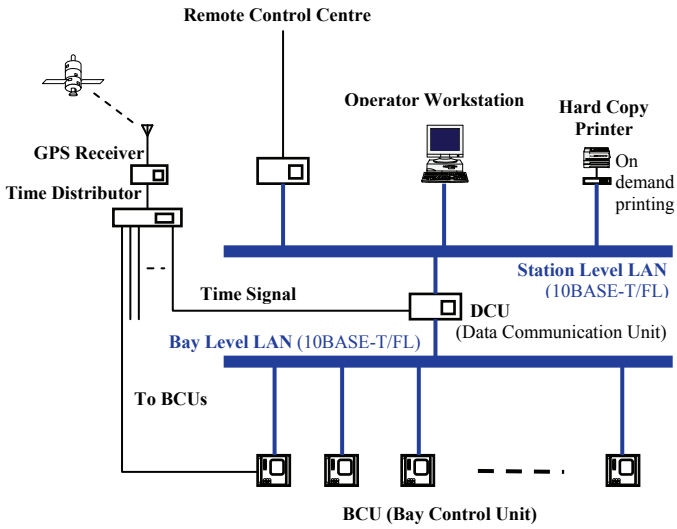


Fig. 1 Example of Basic system configuration for SAS without IEC 61850

3 Improvements Related to System Configuration of SAS

In this section we will describe improvements related to system configuration when applying IEC 61850, and the basic system configuration of SAS adopting IEC 61850.

3.1 SAS adopting IEC 61850

A basic system configuration for a SAS having a distributed Bay approach adopting the IEC 61850 communication standard within a substation is shown in Fig. 2. In this configuration we have implemented the following improvement and simplification to the system from the viewpoint of achieving higher system dependability, and a better balance between redundancy and efficiency.

- Unification of some devices to simplify system configuration (Integration of DCU, Gateway and Substation Server into one Station Computer). The result is a 30% reduction in hardware which in turn reduces the overall failure rate of the system.
- Integration/simplification of Station-level LAN and Bay-level LAN into Station Bus.
- Removed the dedicated communication lines for Time Signal by adopting IEC 61850 based SNTP (Simple Network Time Protocol).
- Instead of the Star topology LAN used in the past, we have adopted a Ring topology LAN which has the advantage of achieving a higher redundancy and shorter cable length. The system uses RSTP (Rapid Spanning Tree Protocol) for the Ring-topology LAN so that the system can remains less complicated and inexpensive whilst still providing a high level of redundancy.

Station-level LAN, Bay-level LAN, the LAN for protection relay maintenance, and the time distribution network have been implemented separately in the past and still applied to most of the SAS around the world. Different protocols are often used for these networks. But by applying improved SNTP (Simple Network Time Protocol) technology which enables 1ms resolution over an Ethernet LAN, and by adopting the IEC 61850 standard, we have succeeded in integrating these networks onto one Ethernet LAN and thus simplified the system as mentioned above.

Although this is the minimum configuration that will achieve all of the SAS functions, the system still

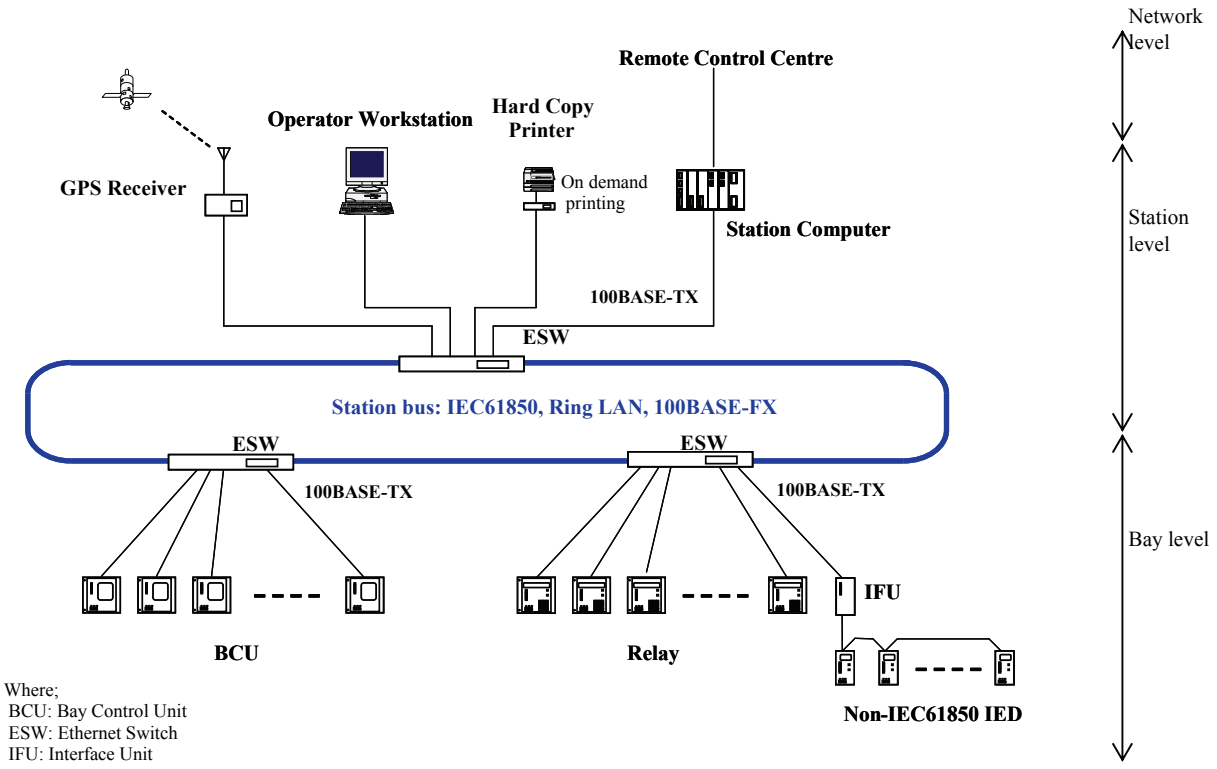


Fig. 2 Example of basic system configuration with ring network topology

has sufficient flexibility in terms of maintenance and future expansion by using a Bay distributed configuration and ring LAN. This system configuration is in widespread application today.

An outline of the main system components is given below;

(a) Operator workstation:

This is an HMI (Human Machine Interface) device which is used to perform control and monitoring operations for the entire substation. Engineering tasks, such as database maintenance and relay setting can be equipped in this HMI device.

(b) Station computer:

The station computer is a substation server device providing control and monitoring functions, a remote control centre interface function, data recording function, etc. Moreover, as it is one of the most important devices in the system the hardware that is used is for industrial applications, with the emphasis on dependability.

(c) BCU (Bay Control Unit):

This is a multifunction control and monitoring unit equipped with a control and monitoring function at the bay level for a single line. BCUs are provided for each line and mounted in the LCP (Local Control Panel) or control device. The BCU executes control processing in response to commands from the operator workstation or remote control centre under normal operational conditions. It is also provided with an LCD (Liquid Crystal Display) having a system display function. Local control from the BCU can also be achieved.

(d) Station bus:

This shows an intra-substation LAN which is compliant with the IEC 61850 standard for establishing connection with the various IEDs (Intelligent Electronic Devices). The ring topology shown in Fig. 2 has the following features:

- Shorter total cable length
- Redundant communication path
- Prevention of data looping for broadcasting data using RSTP (Rapid Spanning Tree Protocol, IEEE 802.1w)

Therefore the ring-type configured LAN with the application of RSTP is more widely used. RSTP is a protocol through which communication paths are logically formed in a star configuration and controls the transmission paths in such a way as to prevent a loop of multi-address transmission data. In addition, in the event of a failure in one of the transmission paths it

also provides a function to reconfigure the paths at high speed. Even if a failure occurs in the communication paths, reconfiguring the paths through this protocol enables continuous transmission over the station bus and system operation to be performed. See Fig. 3.

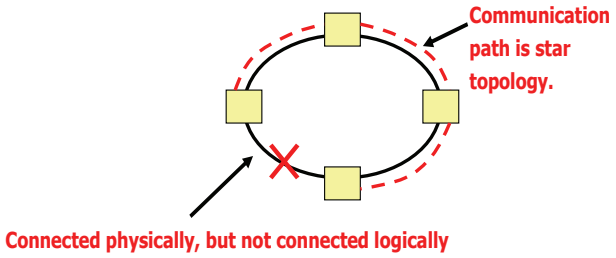


Fig. 3 Outline of RSTP

3.2 Communication method

To ensure improvements in system maintainability and scalability, it is important to use a communication method that is excellent with regard to it being open and being able to provide connectivity in accordance with the relevant international standards. In view of this, the communication methods which are compliant with the following IEC standards are applied to the SAS:

- Communication between remote control centre and substation control and monitoring system: IEC 60870-5-101/104
- Communication between protection relay and substation control and monitoring system: IEC 60870-5-103/IEC 61850
- Communication within substation control and monitoring system (Station bus): IEC 61850

3.3 Further improvements to the system

In addition to the implementation of the IEC 61850, we have developed and implemented a number of functions to improve SAS in terms of usability and availability etc. The functions described in Sub-sub sections 3.3.1 and 3.3.2 out of those many functions we developed have important features in a highly reliable SAS. By utilising these functions the users of the system will be quickly informed as to the status of the system or be able to shorten the repair time when a failure occurs within the system. These improvements result in shorter MTTR (Mean Time To Repair) and higher dependability of the system.

3.3.1 Dedicated logical node for IED failure

Logical nodes of physical devices or logical devices defined in the current version of IEC 61850 have only "Health" attribute to show the status of the system as illustrated in Table 2. As a consequence the attribute can only show the difference in the status of normal, light failure or heavy failure conditions. This results in the SAS operator only being informed of which IED has failed. In this case the operator will have to replace the complete IED unit which usually takes about 4 to 6 hours, even after obtaining the new IED, including re-wiring, re-configuration of the IED, confirmation tests etc. The user may also inspect the IED in location in order to determine which part inside the IED has failed, but it also may take hours.

The solution to this problem can be quite straightforward by either modifying the definition of the LPHD Logical Node or implementing a proprietary information transfer measure to be able to indicate which circuit board has failed. But these approaches disable "interoperability" which is one of the main objectives of the IEC 61850 standard.

Table 2 Standard Logical Node LPHD for IED failure

LPHD class				
Attribute Name	**Attr. Type**	**Explanation**	**T**	**M/O**
LNName				
Data				
PhyNam	DPL	Physical device name plate		M
PhyHealth	INS	Physical device health		M
OutOv	SPS	Output communications buffer overflow		O
Proxy	SPS	Indicates if this LN is a proxy		M
InOv	SPS	Input communications buffer overflow		O
NumPwrUp	INS	Number of Power ups		O
WrmStr	INS	Number of Warm Starts		O
WacTrg	INS	Number of watchdog device resets detected		O
PwrUp	SPS	Power Up detected		O
PwrDn	SPS	Power Down detected		O
PwrSupAlm	SPS	External power supply alarm		O
RsStat	SPS	Reset device statistics	T	O

LPHD : Logical Node Physical Device
DPL : Device name plate
SPS : Single point status
INS : Integer status

Table 3 Dedicated Logical Node for IED Failure

GGIO class				
Attribute Name	**Attr. Type**	**Explanation**	**T**	**M/O**
LNName		Shall be inherited from Logical-Node Class (see IEC 61850-7-2)		
Data				
Common Logical Node Information				
		LN shall inherit all Mandatory Data from Common Logical Node Class		M
EEHealth	INS	External equipment health (external sensor)		O
EEName	DPL	External equipment name plate		O
Loc	SPS	Local operation		O
OpCntRs	INC	Resetable operation counter		O
Measured values				
AnIn	MV	Analogue input		O
Controls				
SPCSO	SPC	Single point controllable status output		O
DPCSO	DPC	Double point controllable status output		O
ISCSO	INC	Integer status controllable status output		O
Status Information				
IntIn	INS	Integer status input		O
Alm1	SPS	General single alarm1		O
⋮	SPS	⋮		O
Alm50	SPS	General single alarm 50		O
Ind	SPS	General indication (binary input)		O

Therefore we have developed and implemented dedicated logical nodes and mechanisms as shown in Table 3 within our IEDs to notify the operator which circuit board has failed. In order to maintain as high a level of interoperability as possible when an IED has failed, the logical node is implemented as a "GGIO (Generic Process I/O)" logical node as defined in IEC 61850. This dedicated logical node is used to inform the operator of where the failure has occurred in order that it is only necessary to replace the failed circuit board rather than the complete IED. With this approach the repair time of the system is dramatically shortened to about 10 minutes for an I/O board up to 1 or 2 hours maximum for a more complex CPU board which requires re-configuration etc.

3.3.2 Usability improvement by unselect report

The SBO (Select Before Operate) control method is used in IEC 61850 and most SASs. The state transition of SBO control is shown in Fig. 4. When an unselect condition occurs after entering the "Ready" state, a method of how to notify the unselect state from an IED to the HMI is not defined in the current version of IEC 61850. Although the "stSeld" attribute is provided in IEC 61850, it will notify only "Select" or "Unselect". With this notification alone, i.e. without any reason for the "Unselect" condition, the operator has to find out why it has occurred by him/herself.

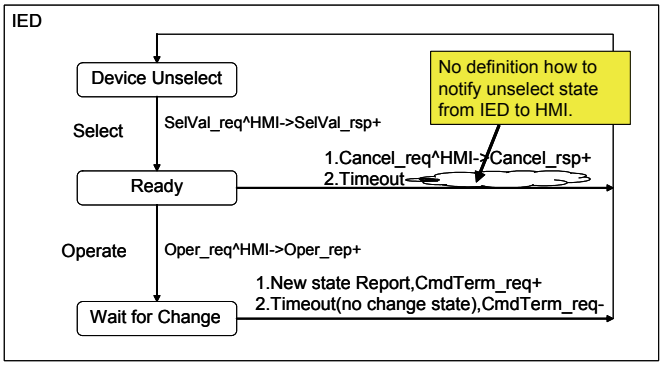


Fig. 4 SBO (Select Before Operation) control state transition

To improve this situation, we developed and implemented a dedicated logical node utilising "GGIO" to notify the type and reason for the "Unselect" error in the IED. With this mechanism, when an unselect state occurs within the IED between the ready state and the operate state, e.g. IED failure, interlock condition unsatisfied, control privilege unsatisfied etc., the type and reason for the error, i.e. unselect, can be notified immediately to the operator.

Without this function, the operator must investigate the reason of the unselect. Since there are nearly 20 possible reasons, it may take about 10 minutes or more for the operator to find out the real cause of the error. The new feature we implemented assists the SAS operator in improving availability and shortening the repair time of the system.

4 System Architecture for SAS

Investigation into optimisation of dependability and connection between substation equipment and devices using IEC 61850 is shown in this section.

4.1 Concepts of system configuration

When IEC 61850-based SAS is applied to a substation, the following two points should be considered by system integrators;

(a) To avoid system unavailability due to a single point of failure
(b) To provide an integration solution for non-IEC61850 devices/signals in an equipment/substation

Item (a) is very important and should be carefully considered in order to ensure dependability of operation for the substation. However, too much emphasis on dependability may cause complexity in system configuration and result in an increase in costs. Therefore a system integrator must propose an appropriate configuration for a particular system.

The point covered in (b) above is an issue to be considered because not all IEDs are IEC 61850 compliant since IEC 61850 is a rather new standard. Furthermore (b) is important for instances where the input information required is only available via mechanical contacts such as in-service or blocked status of relays in a protection relay panel. Generally contact information is captured at the BCU and translated into IEC 61850 information. But inputs to the BCU may not be allowed in order to separate control functions from protection functions by users. In addition, minimising the cable length for contact inputs may be a consideration.

4.2 Solutions for system configuration

System integrators need to propose solutions based on the concept of the system configuration described in Subsection 4.1. It is especially important to minimise the effect of one failure, but at the same time cost effectiveness has to be considered. Therefore system

integrators should keep the following observations in mind;

- Dependability of the system can be doubled by duplicating everything, i.e. server, BCU, communication path etc. But the cost and the failure rate of the system will also be doubled.
- Considering the balance between cost and dependability, the best balance may be achieved by duplicating devices that are common to several functions and ensuring that each bay has a single configuration.
- Having Ethernet switches in every bay will result in an increased the number of switches which will have a big impact on cost and reliability.
- Port failure and power supply failure are the main failure modes of the Ethernet switch. The MTTR can be reduced by exchanging the failed port for the spare port when a port failure occurs. But a power failure within an Ethernet switch will affect all devices connected to it.

With consideration to the observations made above, the redundant architecture described below can have a large impact on improving the dependability of a SAS;

(a) To adopt redundant configuration of the station computer and operator workstation, these are the common devices at the station level in order to prevent the loss of the total system due to one failure.
(b) To ensure communication reliability by adopting a redundant configuration of Ethernet switches at the station level connecting the station bus with the station computer and operator workstation which are redundant as mentioned in (a).
(c) To ensure redundant paths by adopting a ring topology with redundant feature for the station bus. Furthermore separating the ring configuration into several rings can also improve the dependability.
(d) Ethernet switches at the IED side are used by several IEDs in common. Failure of the power supply will have the greatest impact as it will result in the total loss of function of the switch itself. Therefore it would be better that the power supply for each switch were redundant to increase reliability. Also, ensuring the availability of spare ports in each Ethernet switch is recommended to reduce the MTTR.

Information exists on non-digital devices or non-IEC 61850 devices in the substation or in protection relay panels. To integrate this information into the system, an IFU (Interface Unit) can be used which has interface functions for serial communication and binary inputs/outputs.

It will be possible to optimise system configuration and cost by paying heed to the measures described above.

4.3 A system configuration

Fig. 5 shows the actual system configuration adopting the concept and solutions described in Subsections 4.1 and 4.2. The main features of the system are as follows;

(a) Redundancy in equipment at station level enables higher dependability. The Ethernet switches are redundant because they are used to connect equipment at station level to the station bus.
(b) To minimise the effect of device failure, a distributed bay configuration is used for IEDs such as the BCU or protection relays.
(c) The most suitable number of Ethernet switches at the IED side is selected based on the number of IEDs and ports per switch. When considering the number of switches to be employed it is necessary to consider the impact on the system at the time of failure of the switch and optimisation of the cost. However, there are possibilities to use several independent switches for control IEDs because of the importance of communication for control when compared to than for protection. The same issue may apply to the ring configuration of the Station bus, and then it is possible to have several separate ring LANs instead of a single ring LAN.
(d) An IFU is used when it is necessary to integrate mechanical contact information and/or protection relays which are not compliant with IEC 61850 or analogue-type relays.

5 Dependability Evaluation

As one of the indicators that can be used to evaluate a SAS, dependability evaluation is described in this section.

5.1 Dependability calculation method

Formulae to calculate MTTF, MTTR and Availability which are parameters that can be used to evaluate the dependability of a system as follows [17][18];

$$MTTF = 1 / \lambda \quad (1)$$

$$MTTR = 1 / \mu \quad (2)$$

$$Availability = MTTF / (MTTF+MTTR) \quad (3)$$

where λ is failure rate and μ is repair rate.

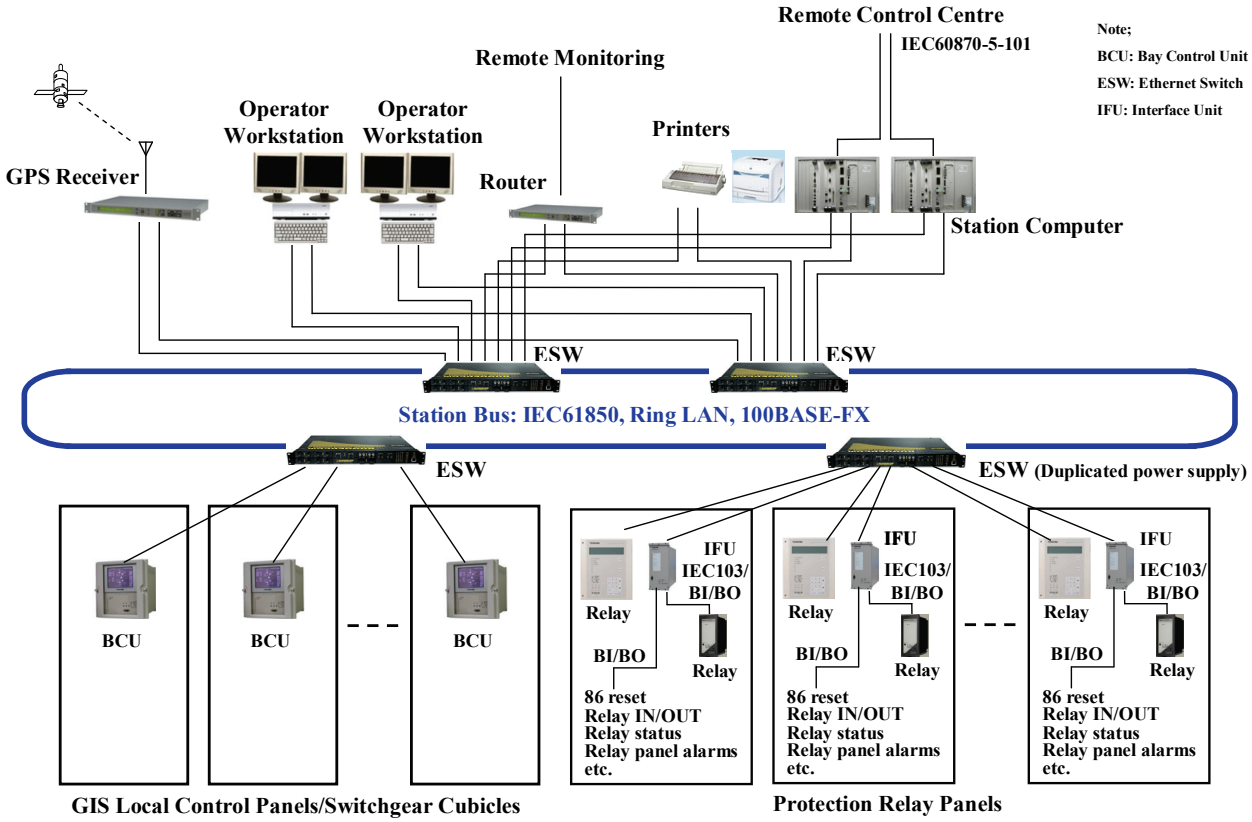
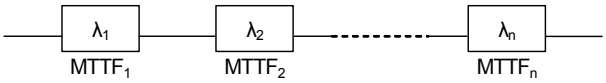


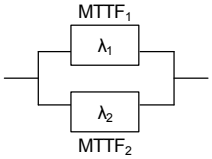
Fig. 5 Example of redundant system configuration

MTTF of the serial model below is calculated as follows;



$$MTTF = 1/\Sigma\lambda = 1/\{(1/MTTF_1)+(1/MTTF_2)+\ldots+(1/MTTF_n)\} \quad (4)$$

MTTF of the redundant model (parallel model) below is calculated as follows supposing $\lambda=\lambda_1=\lambda_2$;



$$MTTF = (3\lambda+\mu)/2\lambda^2 = (3MTTF/2)+(MTTF^2/2MTTR) \quad (5)$$

5.2 Dependability calculation

We evaluated the dependability of the basic configuration of the SAS shown in Fig. 2 and the redundant configuration shown in Fig. 5. For the dependability of the system, we evaluated the Availability of monitoring and control system in one bay. Table 4 shows the MTTF of the main components of the system. These MTTF values were calculated from the supply experience of Toshiba SASs.

Table 4 MTTF for main components

Components	MTTF (year)	Remarks
Station Computer	41	With HDD for historical data recording
Bay Control Unit (BCU)	154	
Ethernet switch	12	16 optical ports, Single power supply
Ethernet switch	20	16 optical ports, Re-dundant power supply

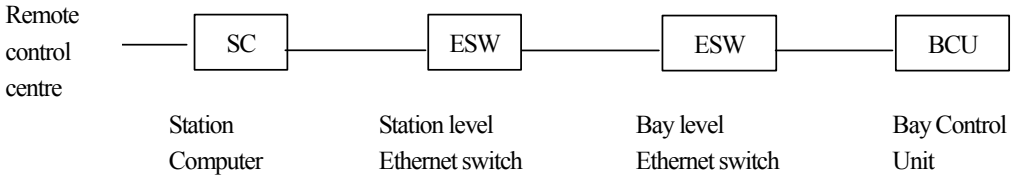


Fig. 6 Dependability calculation model for basic system configuration

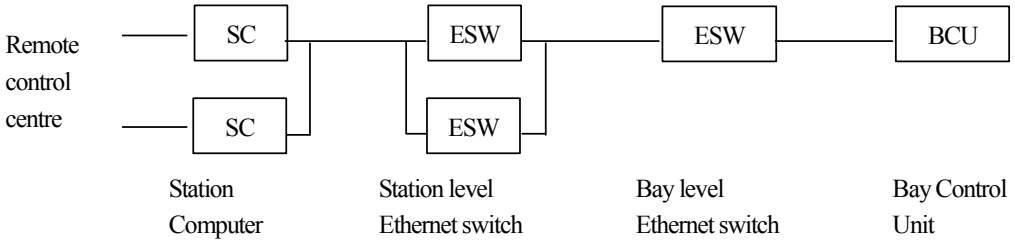


Fig. 7 Dependability calculation model for redundant system configuration

The average repair time is 4 hours based on our experience and with the new features described in Subsection 3.3 to improve repair time. Therefore an MTTR = 4 hours is used in the following calculation.

During remote control operation, the basic and redundant configurations can be modelled as depicted in Fig. 6 and 7 when focusing on one of the bays.

The availability for the basic system configuration shown in Fig. 2 (Case 1) is 99.9820% based on the model shown in Fig. 6, calculation using formula (4), MTTF in Table 4 and MTTR=4 hours.

Series connection of two Ethernet switches in the basic system configuration lowers the availability. Therefore the overall availability will be higher if the MTTF of the switches is higher by using redundant power supply circuits in the switch for example. The availability for the basic system configuration with Ethernet switches adopting redundant power supplies (Case 2) is 99.9880%.

On the other hand, the redundant system configuration shown in Fig. 5 results in a much higher Availability, since the station computer and the Ethernet switches, which are common parts in the system, are redundant. The Availability for the redundant system configuration (Case 3) is increased, being 99.9918% or 99.9948% when applying Ethernet switches with redundant power supplies (Case 4) based on the model shown in Fig. 7, calculation using formula (4) and (5), MTTF in Table 4 and MTTR=4 hours.

Table 5 summarises the availability evaluation described above with relative cost of devices used in a SAS with 40 bays for example. Generally, users of SAS, i.e. electric power utilities, require Availability higher than 99.98% for the SAS. All cases in Table 5 satisfy this criterion. The cost increases for devices used in the SAS are reasonable even for Case 4.

Table 5 Availability calculation and relative cost

Case	System configuration	Power supply of Ethernet switch	Availability (%)	Relative cost of devices used in 40-bay SAS
Case 1	Basic configuration (Fig. 2)	Single	99.9820	100%
Case 2	Basic configuration (Fig. 2)	Redundant	99.9880	104%
Case 3	Redundant configuration (Fig. 5)	Single	99.9918	113%
Case 4	Redundant configuration (Fig. 5)	Redundant	99.9948	119%

6 Dependability Consideration

6.1 Redundant system configuration

It is important to conduct an FMEA for critical systems such as SAS. The basic system configuration has a risk that one failure in the system may affect the whole system from the FMEA point of view. Therefore it is preferable to configure a redundant system for important or large substations. Ethernet switches have to be highly reliable because they are

the key components that make up the LAN. Thus we have to select a switch which is compliant to the relevant IEC standards and is applicable in the harsh environment that is encountered in substations. Furthermore, when the Ethernet switch is common to several pieces of equipment, it is effective to have a redundant power supply unit in the switch in order to increase dependability, i.e. the MTTF of the switch itself. As for a port failure in Ethernet switches, the MTTR can be shortened, i.e. Availability can be improved by preparing spare ports in the switch.

From the view point of FMEA, other redundant measures can be possible, such as the use of a redundant LAN or distributed Ethernet switches, for example additional switches for every Voltage level or individual switches for protection devices and control devices etc. However these redundant measures may increase system cost, maintenance cost or may decrease system capacity. For example, the cost of devices used in a SAS having 40 bays will increase by approximately 30% if each BCU has an individual switch. Therefore it is not a simple decision. The redundancy level of the system should be considered and decided based on the overall consideration with respect to power system utilities' policy on SAS, importance and size of the substation, etc.

The SAS configuration shown in Fig. 5 is one of the optimum solutions achieving a good balance between redundancy and its benefit because it has a sufficient level of redundancy with a cost increase of less than 20% for the devices used in the system having 40 bays for example as shown in Table 5.

6.2 Fail-safe and fool-proof design

Needless to say the use of high reliable devises, it is also other measures to improve dependability in wider sense to use redundancy explained already, to use distributed system, to simplify system and/or functions, to adopt fail-safe and fool-proof design etc.

As described earlier, control and protection are the main functions of a SAS. For control functions, measures that prevent improper operation caused by human error with equipment such as circuit breakers and measures that will avoid unnecessary output are the most important in order to improve dependability. Fool-proof design is effective for avoiding improper commands to equipment and fail-safe design is helpful in avoiding unnecessary output. These measures need to be considered in designing equipment or a system.

6.2.1 Fail-safe design

Avoiding unnecessary outputs or commands to equipment is one of the most important features even when one failure occurs in one device or communication path in the system. Various methods have been proposed and implemented in SAS so far. But maximizing the effect of this feature and at the same time minimizing the complexity or cost of the system is still an issue of concern.

To achieve this feature with less complexity, our solution is to have the following design as shown in Fig. 8;

(a) SBO (Select Before Operation) control
SBO control consists of selection followed by control and is applied both in command protocol between station server and BCU, and in the communication procedures.

(b) Encoding of information
Representing information such as command data using multiple bits by using an encoding technique is effective in avoiding misinterpretation of command data and helps to avoid unnecessary operation or output.

(c) Redundant output from BCU
In parallel with (a) above, we have implemented an "AND" connection of two independent binary outputs from the BCU, i.e. device selection output and close/open command output in order to avoid unnecessary operation or output when one failure occurs in BCU hardware.

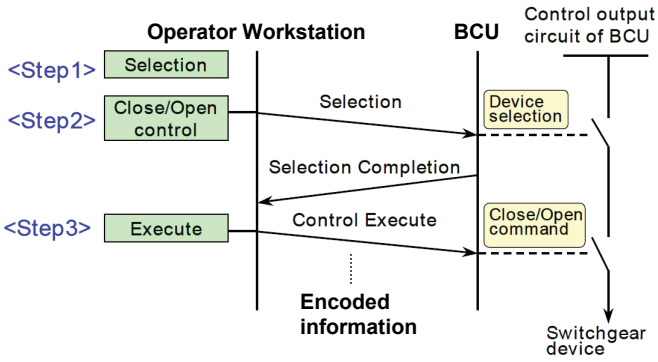


Fig. 8 SBO (Select Before Operation) control

6.2.2 Fool-proof design

To maximize the actual dependability of the SAS when in operation, we have to consider the dependability of SAS with respect to operator human error rate as well as the dependability of the system itself. This is because there is little difference in terms of results between the failure of SAS hardware /

software and unnecessary operation caused by operator human error.

It is therefore very important to adopt a fool-proof design in order to prevent improper operation caused by human error for equipment such as circuit breakers. Around the world, there have been several examples of unnecessary operations caused by human error. One typical example is that selection of the wrong bay may result in unnecessary operation of equipment which may cause an unwanted fault on the power network or even a fatal accident.

Based on our experience, information and requirements from electric power utilities, we have developed and implemented various fool-proof designs and features. The followings are such examples;

(a) Three step control operation after selection of bay

In order to prevent the human error of selecting the wrong equipment in the substation as far as possible, we have implemented the following steps for controlling equipment within the substation;

1) Selection of the bay to be controlled in a one line diagram displaying multiple bays (see Fig. 9)
2) Selection of equipment in the diagram of the selected bay (see Fig. 9)
3) Selection of close or open control
4) Execution of the control

(b) Test mode

SAS is required to have a test function for the addition of bays etc. since there may be system expansion in the future after the substation has gone into operation. One of the redundant operator workstations and BCUs under test can be set to "Test Mode" and transmit data with a "Test Flag". Having this mechanism, data transmission and being able to receive it with a "Test Flag" can only be done between devices when in the "Test Mode". This ensures that there will be no effect to non-"Test Mode" devices for normal operation of the SAS, even if there are problems within the new BCUs that have been added etc. or a human error occurred during the test procedures.

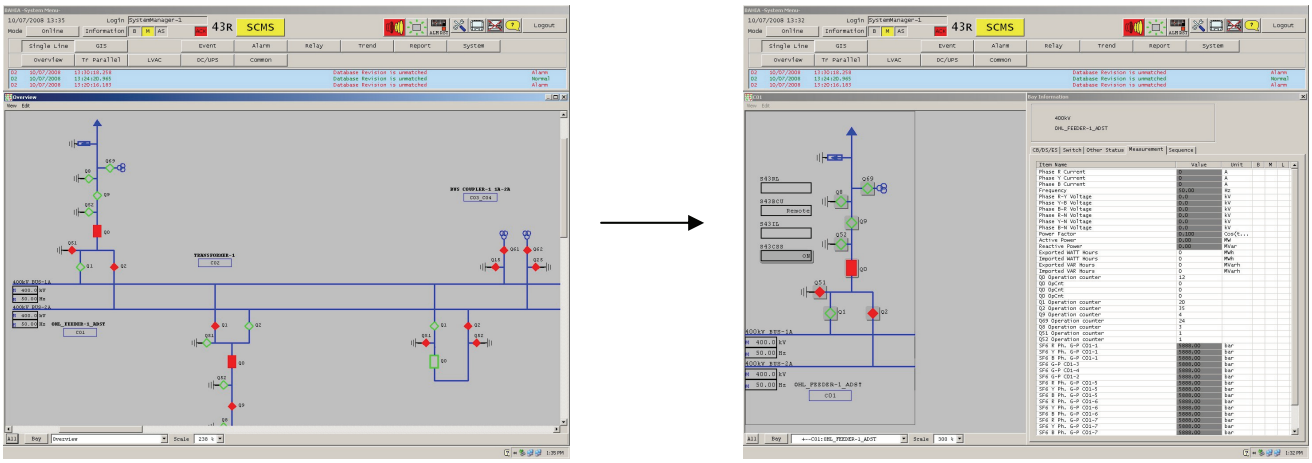


Fig. 9 Bay selections in one line diagram and display of selected bay

7 Conclusion

In this paper, we have explained the followings;

(a) We have described the configuration policy for a SAS applying IEC 61850, the system configuration and the redundant configuration to improve dependability. Station-level LAN, Bay-level LAN, the LAN for protection relay maintenance, and the time distribution network have often been implemented separately, frequently with different protocols in the past and are still being applied in the majority of the SASs around the world. But by applying improved SNTP technology which enables 1ms resolution over an Ethernet LAN, and by adopting the IEC 61850 standard, we have been successful in integrating these networks into one Ethernet LAN and have also simplified the system.

(b) Also, we have explained some of the new functions that we have developed which are not currently covered by the IEC 61850 standard in order to improve usability and availability. These new functions are implemented using dedicated new GGIO logical nodes. Having these new logical nodes contributes in reducing the MTTR and increasing the dependability of the system

whilst maintaining the high level of interoperability which the IEC 61850 standard is aiming at.

(c) We then presented a dependability evaluation for MTTF, availability, and FMEA for these configurations of SAS described in (a) and (b) above based on the dependability requirements for SAS. Generally, users of SAS, i.e. electric power utilities, require availability figures higher than 99.98% for SAS. We evaluated the availability of four cases in this paper, i.e. 2 cases for a basic system configuration and a redundant system and 2 cases with and without redundant power supplies for the Ethernet switch for each system. All four cases of SAS configurations satisfied this criterion.

(d) Further, we explained the necessity of choosing the appropriate redundancy for the SAS to be applied in an actual substation from the view point of FMEA. It is important to apply devices which have a high enough dependability, such as Ethernet switches having redundant power supply circuits.

(e) Also we raised the importance of adopting a fail-safe and fool-proof design to improve dependability of the SAS in the broadest sense. Within the control functions of the SAS, measures that will prevent improper operation due to human error for equipment such as circuit breakers and measures that will avoid unnecessary output caused by device failure etc. are the most important in order to improve dependability. Fool-proof design is effective for avoiding improper commands to equipment and fail-safe design is helpful in avoiding unnecessary outputs. These measures must be considered in designing any equipment or a system. In this paper we have explained several examples of fail-safe and fool-proof designs of SAS which we developed and implemented. These designs helped greatly in improving the dependability of SASs by avoiding improper operation or unnecessary outputs.

A substation automation system configured in accordance with the redundant system architecture described in this paper is scheduled for commercial installation in an EHV (Extra High Voltage) substation early 2009. We will propose this type of SAS system to various electric power utilities.

References:

[1] Klaus-Peter Brand, et al., *Substation Automation Handbook*, Utility Automation Consulting Lohmann, 2003

[2] T. Mitani, T. Sato and K. Nara, A Novel Optimal Power Flow for On-line Analysis, *WSEAS Transactions on Power Systems*, Issue 8, Vol.1, Aug. 2006

[3] M. Marmiroli, et al., Congestion Transmission Network Management Algorithm for Wholesale Spot Market, *WSEAS Transactions on Power Systems*, Issue 8, Vol.1, Aug. 2006

[4] J. Pedro, et al., IEEE Standard 519-1992 Application in Industrial power Distribution Network with a New Monitoring Approach, *WSEAS Transactions on Power Systems*, Issue 8, Vol.1, Aug. 2006

[5] Keiichi Kaneda, Koji Igarashi, Koichi Hamamatsu and Shigekazu Morita, Modern Substation Control and Monitoring System, *ICEE*, Hong Kong, 1999.

[6] N. Kusano, New Trends in Protection Relays & Substation Automation Systems in Japan, *IEEE/PES T&D Asia Pacific Conference*, Japan, 2002

[7] *IEC 61850 "Communication Networks and Systems in Substations"* 2002-2005 (www.iec.ch)

[8] Lars Andersson, Christoph Brunner and Fred Engler, Substation Automation based on IEC 61850 with new process-close Technologies, *IEEE Bologna Power Tech Conference*, Italy, June, 2003.

[9] Klaus-Peter Brand, The Standard IEC 61850 as Prerequisite for Intelligent Applications in Substations, *IEEE/PES General Meeting*, USA, 2004

[10] Masayuki Kosakada, Hiroshi Watanabe, Tokuo Ito, Yoshito Sameda, Yuji Minami, Minoru Saito and Shiro Maruyama, Integrated substation systems – harmonizing primary equipment with control and protection systems –, *IEEE/PES T&D Asia Pacific*, Japan, 2002.

[11] M. Saitoh, T. Kimura, Y. Minami, N. Yamanaka, S. Maruyama, T. Nakajima and M. Kosakada, Electronic Instrument Transformers for Integrated Substation Systems, *IEEE/PES T&D Asia Pacific*, Japan, 2002.

[12] Y. Minami, et al., Substation architecture with protective relays using digital instrument transformers and digital interface technology, *IEE/DPSP,* 2004

[13] Klaus-Peter Brand, Martin Ostertag and Wolfgang Wimmer, Safety related, distributed functions in substations and the standard IEC 61850, *IEEE Bologna Power Tech Conference*, Italy, June, 2003.

[14] Bogdan Kasztenny, James Whatley, Eric A. Udren, John Burger, Dale Finney and Mark Adamiak, Unanswered Questions about IEC 61850, What needs to happen to realize the vision?, *32nd Annual Western Protective Relay Conference*, USA, Oct., 2005.

[15] Lars Andersson, Klaus-Peter Brand, Christoph Brunner and Wolfgang Wimmer, Reliability investigations for SA communication architectures based on IEC 61850, *IEEE PowerTech*, Russia, 2005.

[16] Hachidai Ito, Keiichi Kaneda, Koichi Hamamatsu, Tatsuji Tanaka and Koichi Nara, Dependability Evaluation of Substation Automation System with Redundancy, *12th WSEAS International Conference on Systems*, Greece, July, 2008

[17] Martin L. Shooman, *Reliability of Computer Systems and Networks – Fault Tolerance, Analysis, and Design* -, John Wiley & Sons, 2002.

[18] Jan Pukite and Paul Pukite, *Medeling for Reliability Analysis - Markov Modeling Reliability, Maintenability, Safty, and Supportability Analyses of Complex Computer Sytsems*, IEEE Press, 1988.