REBECCA : a dependable communication support system for for a distributed monitoring and safety system, pp.261-268,

Jean-Paul Blanquart, Karama Kanoun, Jean-Claude Laprie, M. Rodrogues dos Santos

REBECCA: A DEPENDABLE COMMUNICATION SUPPORT SYSTEM FOR A DISTRIBUTED MONITORING AND SAFETY SYSTEM

J. P. Blanquart, K. Kanoun, J. C. Laprie and M. Rodrigues Dos Santos

Laboratoire d'Automatique et d'Analyse des Systèmes du C.N.R.S.,
7 avenue du Colonel Roche, 31400 Toulouse, France

ABSTRACT: This paper presents a dependable communication support system for a distributed monitoring and safety system (protection system). It must cater for steadily generated background information and bursts of high priority information when an incident occurs. For the application to the protection system of Extra-High Voltage substations of the French electricity distribution network, the resulting system consists of a reconfigurable optical counter-rotating double loop. Each loop is independently accessed in an asynchronous way using the register insertion technique.

KEYWORDS: Dependability, Local area networks, Loop architecture, Register insertion technique.

INTRODUCTION

The results reported here concern the second part of a study devoted to the protection system of an Extra-High Voltage (EHV) substation[1]. This system is made up of monitoring equipments interconnected by a communication support system (CSS).
The first part of the study was concerned with the dependability of the whole protection system: for more details, see (Medhaffer, 1980; Laprie and Medhaffer, 1982).

This paper is devoted to the definition of a dependable CSS for this protection system. It summarizes the results of (Blanquart, Kanoun and Laprie, 1981; Kanoun and Rodrigues, 1982; Blanquart, 1983).
The paper is split into five parts : (I) statement of the aims, the environment, and the requirements, (II) methodology followed, and definition of the meaningful criteria, (III) preselection of suitable solutions (qualitative study), (IV) refinement and selection (quantitative study), (V) detailed description of the resulting system.

GENERAL STATEMENTS

Description

The protection system of an EHV substation is aimed at preventing propagation of the effects of an incident occurring in the electrical network. This needs isolation of the part in which an incident has occurred, but isolation of the minimal part, because of the resulting extra load on the network. This function is realized by each substation in an autonomous way. The protection system of each substation is also distributed.

Figure 1 gives a schematic representation of an EHV substation. It consists of two or more sets of triple bus-bars (one for each phase), coupled by circuit-breakers (CB); each bus-bar is connected to N sets of EHV lines via line CB's.

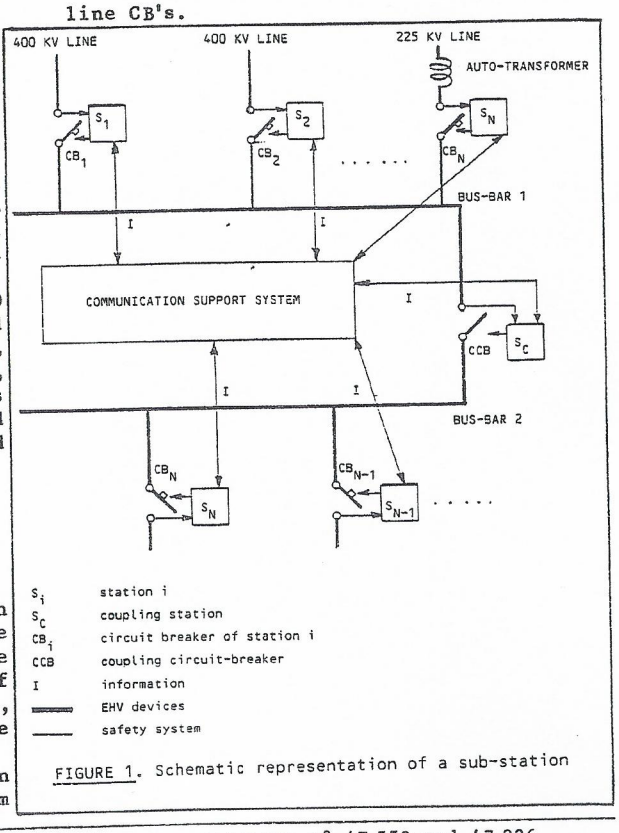


FIGURE 1. Schematic representation of a sub-station

1) This work has been sponsored by Electricité de France, contracts n° 47.559 and 47.836.

The protection system is made up of the monitoring equipments, associated with each three-phase CB. These equipments are able to detect an incident, and to determine in which direction (that is, on which side of the CB) it occurred. Each equipment must get and proceed direction information from the others, in order to localize the incident, and determine whether it has to open its CB. This implies the existence of the CSS, enabling information exchange between the equipments. This CSS must be dependable enough, in order to ensure correct elimination of incidents (by opening all the involved CB and only those).

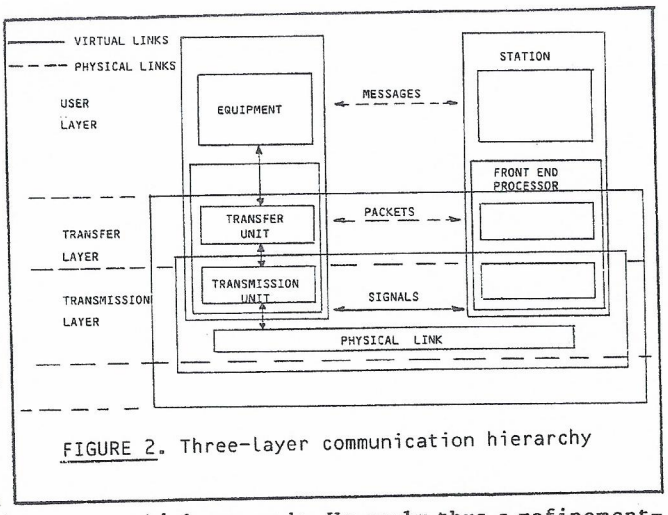


FIGURE 2. Three-layer communication hierarchy

Requirement Specifications

Functional requirements: The CSS must supply a dependable means to exchange information about incident occurrence within a maximum delay time. There may be up to seven incident messages which must be delivered in less than three milliseconds. The CSS is also used for exchanging service information, but there are no time constraints for the corresponding service messages.

Technological requirements: Because of electromagnetic interference due to the environment, it is necessary to use optical fiber technology for realizing the transmission channels.
Moreover, due to the difficulty of protecting the electrical parts against interference, and especially high frequency ones, internal signal rates should not exceed 3 to 4 MHz. This implies the same limitation on the transmission speed.

DESIGN METHODOLOGY

General Considerations

In order to handle the complexity of the system, we shall decompose it into several layers, derived from the OSI reference model of ISO. However, in the same way as in (Powell, 1981), we shall retain only three layers, which fit better the purpose of this study (a local area network) than the seven-layer model of ISO. Figure 2 gives these three layers and the terminology associated:

- the **user layer**, where informations are exchanged between users by means of messages,
- the **transfer layer**, where messages are transformed into packets exchanged between stations,
- the **transmission layer**, where packets are materialized by physical signals.

In fact, only the transfer and the transmission layers are considered. The user layer refers to the system, not studied here, which uses the CSS.

In order to obtain confidence in the results of the study, we must validate the choices which are made. We apply thus a refinement-based approach to the design of the system, which allows us to be aware of all the choices and their consequences. So, choices at each step are motivated and possible inconsistencies induced by choices at preceding steps may be discovered and resolved.

However, as the system is decomposed into layers, it can be seen that at each step, design refinement must be processed in all the layers; interactions, and possible inconsistencies, of the choices in each layer and between layers must be studied and resolved before processing the next step.

This implies special care in the choice of the criteria translating the general requirements in specifications for each layer and each step, in order to avoid as far as possible such inconsistencies.

Choice of criteria

Theoretically, we must evaluate the ability of the CSS to process a burst of seven messages in less than 3 ms. However, such an evaluation requires much detailed information about the system, which makes it of little use at least for the first design steps.

In order to find more useful design guides, we can classify the different kinds of failures which can affect the behavior of the system, by considering two operational modes for the CSS (an obvious decomposition for such an application):

working mode: this mode aggregates the nominal state and all the states of non-negligible probability. We must thus verify that in these states, the CSS can deliver a burst in time.

failed mode: this mode aggregates the states where time for delivering a burst may exceed 3 ms. We must thus verify that their probability is sufficiently low.

We thus have two criteria, one related to functional performance and the other to dependability.

The latter is obviously the more important, as far as for the former we are only concerned with an upper bound and not an exact value.

In the last steps, the CSS dependability can be evaluated by using Markov process. According to the fact that without any communication between stations, incidents are eliminated in a degraded mode, as if they were worst-case incidents, we shall evaluate the CSS dependability according to the degree of its mission achievement . Two levels can be defined for the quantitative evaluation of the CSS dependability :

- nominal dependability: probability of correct elimination of an incident,
- degraded dependability: probability of elimination of an incident with the opening of no more than one extra circuit-breaker.

For the first steps, in each layer, we must use more qualitative criteria:

- simplicity, in order to decrease fault occurrence, and minimize presence of design faults,
- use of standard components (hardware and software), in order to use well-tested components and to increase flexibility,
- decentralization (no single point of failure) in order to minimize the effects of faults,
- minimum latency, in order to minimize the presence of latent faults when an incident occurs (due to the dormant feature of the system: less than one incident per month, processed in a few milliseconds).

These criteria have been used in the design of the CSS. The three major steps and the main results of this approach are reported in the following sections.

PRELIMINARY STUDY

Transmission Layer

For this first step, in the transmission layer, we are mainly concerned with the architectural aspects of the CSS.

We can envisage architectures with multipoint (bus) or point-to-point transmission channels. A multipoint channel using optical fiber technology must have a star structure with a passive optical coupler, because of the current lack of good quality optical derivation components for a linear optical bus.

Differents kinds of architectures with point-to-point transmission channels can be studied. Qualitative criteria can be used for selecting suitables ones. Fully-meshed structure appears to be too expensive and not enough flexible; active star structure is too much vulnerable, and regular or irregular networks imply a priori complex routing procedures, except for the loop structure.

We are thus led, in a first attempt, to retain only the loop architecture, and the bus with a passive star structure.

In both cases, redundant transmission channels can be used to improve the architecture dependability, but the cost of this improvement must be taken into account.

Obviously, a simple loop is much too vulnerable : after any single failure, the complete CSS is lost (high quality optical by-pass mechanisms are not yet available). Thus, we must use redundancy techniques on such an architecture.

On the contrary, failures on a bus are not so catastrophic insofar as we suppose that the coupler failure rate can be neglected. Thus, the dependability improvement of a double bus cannot justify its cost increase.

Figure 3 gives the main structural characteristics of the two preselected solutions: the main conclusion of this comparison is that the double loop is far from being a more expensive solution than the simple bus, as the former needs fewer and cheaper components than the latter (due to the high signal attenuation on a bus).

ARCHITECTURE		BUS	DOUBLE LOOP
CONNECTORS	Number	4 x N	4 x N
	Quality	0.5 to 1 dB	less than 3 dB
FIBER	Length(m)	500 x 2 x N	200 x 2 x N
	Quality	4 dB/km	10 dB/km
TRANSCEIVER	Price	very expensive	low
	Quality	good technology	classical technology
SNR (signal to noise ratio)		bad	good
COUPLER (star)		40 link pairs	-
FURTHER EXTENSION		good-limited	worse unlimited

N = number of stations { Bus : 500 m between stations and coupler. Loop: 200 m between neighboring stations.

FIGURE 3. Structural characteristics of the bus and the double loop

This firt choice can appear to be very restrictive. Obviously, it is just an attempt which can only be validated if the following steps succeed in defining a suitable solution. If not, we should have to proceed again this step and the following ones with some other possible solutions.

Transfer Layer

Qualitative dependability criteria lead us to reject, at least for incident messages, all

centralized and synchronous procedures, that is essentially: polling and token-based access methods (with virtual or real token).

The two classes of solutions are thus:
- bus: competition access ("contention"), with decentralized and asynchronous resolution of eventual conflicts,
- loop: asynchronous access by the register insertion technique (Liu, 1978), with message extraction by the sender.

Obviously, incident messages must not be split into several packets. We shall thus use a synchronous transmission mode with, for instance, an HDLC-like frame, which allows use of some already existant integrated circuits.
This synchronization, though it is not a very strong one with such a short packet length (about ten octets), must be balanced by the use of a self-synchronous code: e.g., the "Manchester biphase" code, or the NRZI code which is self-synchronous if used in association with the HDLC frame.

At this stage, the competition access method for the bus and the asynchronous access method for the double loop both appear to be suitable solutions, according to our qualitative criteria. Both methods allow messages to be sent to groups of stations (broadcast messages). However, the double loop with asynchronous access seems to be more suitable for a bursty generation of messages than the contention bus; moreover, it provides for an automatic acknowledgement procedure (limited to the transmission layer) since messages are returned back to the sender after having gone through all the other stations.

REFINEMENT AND SELECTION

Transmission Layer Refinement

Possible solutions: We have to refine the structure of the interface or "Front End Processor" (FEP), between the equipments and the CSS.

We can assume that each FEP is equipped with a watch-dog timer that monitors the transmission duration and inhibits the faulty station in the event of a maximum duration being exceeded.
In this case, we see that if for the two architectures the FEP has a simplex structure, the double-loop architecture is much too vulnerable (any fault affecting the interface leads to the loss of communication on both loops).

We have thus considered two possibilities for the interface of this architecture: access to the two loops is managed by one Access Unit (AU) in the FEP (a simplex or fault-tolerant one) or each loop is managed by its own AU.

However, whatever the structure of the loop interface, a common mode failure or a failure affecting the both AU's of the same FEP implies that communication is no longer possible. In order to avoid such cases we must use counter-rotating loops together with reconfiguration procedures like in (Ihara and Mori, 1982). The alternate signal path is shown in figure 4.

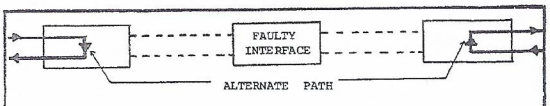


FIGURE 4. Reconfiguration in the double loop

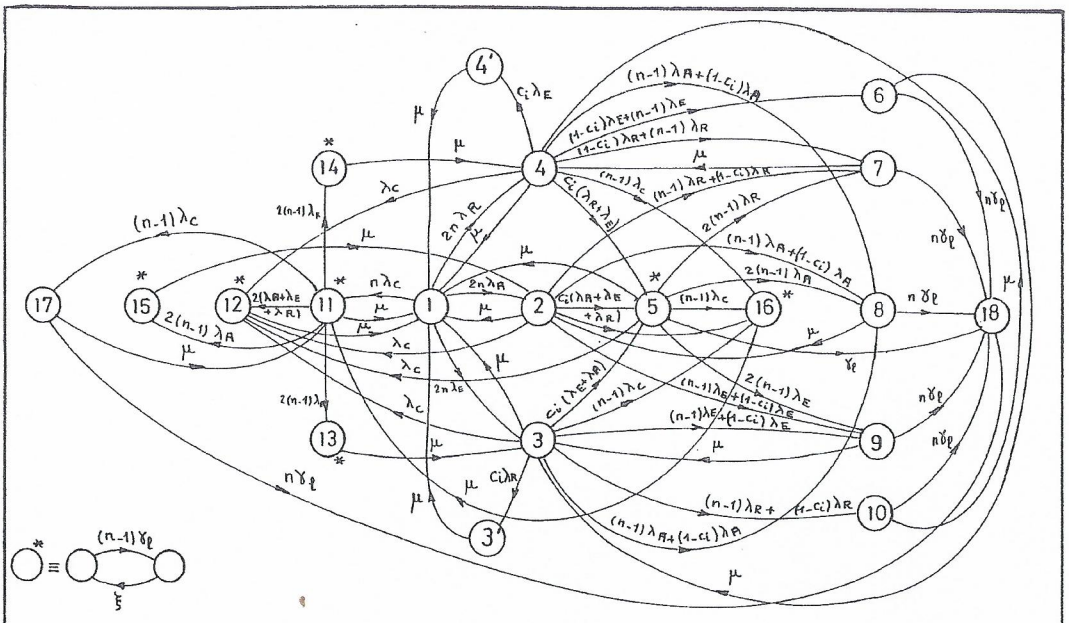
For the same reasons as in the preceding step, it is not worthwhile considering the bus architecture with fault-tolerant FEP's.

Dependability evaluation: In order to obtain measures of the two dependability levels previously defined, we assume that all the random variables associated with the process acting on the CSS are exponentially distributed, i.e. constant rates are associated with these variables. This assumption enables us to evaluate dependability levels by time-homogeneous Markov techniques.

We thus have to make, for each selected architecture, models of the substation protection system with respect to the events which can affect its ability to give the required service. These events are the incidents on the electrical network (which are to be processed), and the failures of the CSS which can affect the mission of the protection system.
As an example, we give in figure 5 the model corresponding to the double loop managed by two AU's, where λ_A is the failure rate of one AU, λ_E (λ_R) the failure rate of a transmitter (receiver), λ_C the common mode failure rate, μ the maintenance rate, γ_ℓ the incident occurrence rate, ξ the incident elimination rate, and c_i the coverage factor defined as the probability that faulty elements have been correctly isolated given that one or more faults affect these elements.

Figure 6 gives an example of the comparative curves obtained with the "SURF" dependability program developed at LAAS (Costes and co-authors, 1981). These curves lead to the following main conclusions:
- a bus and a double loop with simplex FEP are equivalent from the dependability viewpoint,
- a double loop with two AU's in each FEP or with a fault-tolerant FEP bring about a significative improvement on other solutions. The latter is the best solution if the coverage factor of the fault-tolerant FEP is more than 0.9 for the nominal dependability (about 0.85 for the degraded dependability), which is not unfeasible but difficult to guarantee.

It could be concluded at this stage that the double loop architecture with two AU's in each FEP is the best solution, but we must before take into account the possible interactions with the transfer layer, and thus refine the design in it.



(1) all elements are fault-free

(2), (3), (4) loss of one loop due to the failure of : (2) an access unit

(3) a transmitter

(4) a receiver

(5) loss of a station - with success of reconfiguration

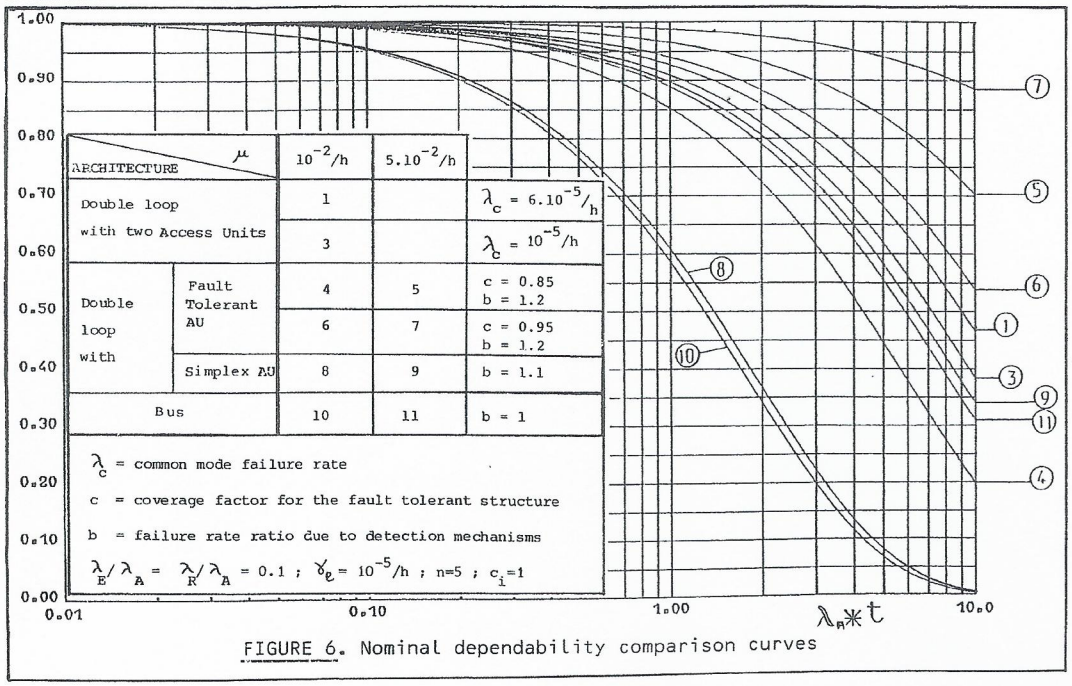
(6) to (10) loss of communication due to the failure of more one station

(11) to (17) states with a common mode failure (x* opening of one more circuit-breaker)

(18) opening of all circuit-breakers of the bus-bar

(3'), (4') covered failures of the receiver and the transmitter of the same station on both loops. The communication is reconfigured with isolation of these two elements, no station loss

FIGURE 5. Model of the double loop with two AU's



ARCHITECTURE \ μ		10^{-2}/h	5.10^{-2}/h	
Double loop with two Access Units		1		$\lambda_c = 6.10^{-5}$/h
		3		$\lambda_c = 10^{-5}$/h
Double loop with	Fault Tolerant AU	4	5	c = 0.85 b = 1.2
		6	7	c = 0.95 b = 1.2
	Simplex AU	8	9	b = 1.1
Bus		10	11	b = 1

λ_c = common mode failure rate

c = coverage factor for the fault tolerant structure

b = failure rate ratio due to detection mechanisms

$\lambda_E/\lambda_A = \lambda_R/\lambda_A = 0.1$; $\gamma_\ell = 10^{-5}$/h ; n=5 ; c_i=1

FIGURE 6. Nominal dependability comparison curves

Reconfiguration: Reconfiguration is carried out in three steps: error detection, fault location and identification, and recovery.

Error detection must be achieved in a continuous way in order to reduce latency; it is carried out at different levels: (a) "is transmission code correct?", (b) "is the CRC correct?", (c) "is the return-packet identical to the one previously sent by the source?", and (d) "are both packets corresponding to the same message received on each loop identical?".

When a persistent fault is detected (faults which resist to retry), the involved station activates the localization procedures.
If the fault affects only one loop, or two different stations on both loops, these procedures are used as an aid to maintenance; otherwise they are used for reconfiguration and maintenance.

Localization is achieved by means of minor loop checks: each station sends a specific message to its neighbor, which must return it. All diagnosis messages are memorized by all the stations in order to make a distributed diagnosis. The results of this diagnosis are broadcast on both loops, which enables every station to make a vote.

Reconfiguration is carried out only by the adjacent stations which change the signal route; the other stations continue to work normally.

Details of these procedures are given in (Kanoun and Rodrigues, 1982).

Management Protocol

This section is devoted to the communication procedure for REBECCA. We shall first consider the normal case before examining the events which can affect this normal mode, and how this procedure can handle them.

Background: In a first attempt, we adopt the first solution selected at the end of the preceding step: incident and service packets are sent exactly in the same way; there is neither a token, nor a second register reserved for incident packets. We thus have to evaluate the required transmission speed.

Packets are sent by the register insertion technique independently on each loop.
With this solution, each AU can store received signals in a memory before sending them again around the loop. This memory can be seen as a shift register which initially contains the locally generated packet. Transmission can be carried out, after reception of the end of another transmitted packet, by cutting the loop and shifting signals out of the register and into the transmitter; signals which arrive at the receiver are then shifted into the register.

Packets are extracted by the stations which have sent them.

A station can thus detect transmission errors on its packet, and try to send it again.
Another advantage is the fact that AU's which must decide whether or not they retransmit received signals are those which have their register inserted; so, they have enough time to make the decision, without it being necessary to delay signals in the AU's.
The time required for deciding whether or not to insert a packet is obtained by ensuring a sufficient space between successive packets.

The following assumptions are used:

Bit duration = B μs
Inter-packet space = 10.B
Time spent in each AU = B
Packet duration = 92.B (10 octets with HDLC bit-stuffing)
Time between stations = 1 μs

If both loops are available, a burst of 7 messages is delivered in less than T_T given by:

$$T_T = 4727.B + 45 \text{ microsecondes}$$

Thus, a transmission speed of 1.5 Mbit/s is sufficient.
With a more realistic value for the maximum number of stations which want simultaneously to transmit, for instance only 15 stations, this transmission speed is also sufficient even if only one loop is available.

As this solution does not lead to unacceptable values for the transmission speed, it seems better than the twin protocol (token access for service packets) and than the double-register technique, because of its simplicity and its robustness. Moreover, the incident mode procedures appear to be much simpler.

Incident modes: The great advantage of the chosen protocol is that the exceptional procedures are very simple, and that they may be run frequently (in order to decrease fault detection latency).

The essential thing we must foresee is to guarantee that an AU can find a space to insert its register. Thus, we provide stations with mechanisms allowing insertion to be enforced when no space has been detected before a time limit.

Another interesting point concerns the way to use the reconfigured CSS.
As a matter of fact, stations which are not directly involved in the reconfiguration procedure need not know if reconfiguration has occurred and they can continue to send their packets on both loops and extract their registers when filled again with their own packet, just as if the double loop were undamaged.

Thus, there is no need for a special procedure after reconfiguration, except of course for the FEP's that are directly involved which must extract information arriving on one loop and put it on the other.

Transfer Layer Refinement

This refinement is based on evaluation and comparison of the functional performance with the following assumptions:

- in a burst, all incident messages are sent by different stations,
- all the packets have the same maximum length: 100 bits,
- the transmission speed is 0.5 Mbit/s.

Bus protocol: The most suitable solution for this application appears to be non-persistant carrier sense multiple access with collision detection (CSMA-NP/CD) protocol: each station which has a packet ready can send it if the channel is free; deference and conflict resolution are both realized by waiting for a random delay. This delay is uniformly distributed between 0 and a value t_p for incident messages, and between t_p and a higher value t_n for the others.

In fact, the delay time for a burst of 7 messages is not bounded. By simulation (Boussin, 1980), a mean value of 1.7 ms has been found, which shows, as the standard deviation is low (0.12), that the seven messages are very likely to be delivered in less than 3 ms.

The major advantage of this protocol is its great robustness, due to (a) its simplicity, (b) the absence of exception procedures (conflicts are normal events, and all the messages are essentially treated in the same way), and (c) the great autonomy of the subscribers.

The disadvantages (essentially due to the architecture) are (a) the need for an acknowledgement procedure, and (b) the low signal-to-noise ratio which increases the transmission error rate.

Loop protocol: We assume here that only one loop may be available, as this event probability can obviously not be neglected.

With an asynchronous access method using the register insertion technique, an AU which wants to send a packet may theoretically have to wait for its register to be removed from the loop with its last packet. In a system with N stations sending packets of length T_p, a new packet could wait for more than $2.N.T_p$ before being delivered to each station; this leads to excessive delays (about 12 ms with N=30).

There are three solutions to this problem. The first solution is to increase the transmission speed.

The second solution consists of decreasing the number of stations which can transmit simultaneously, by using a twin access protocol: incident packets can be sent as soon as the channel is free (or between two packets already on the loop); service packets can only be sent when the AU's receive a specific signal (token). This solution has been thoroughly studied in (Blanquart, Kanoun, and Laprie, 1981) and has been showed to be a suitable one, despite some difficulties about the token management. The maximum delay time for a burst of seven messages is 1.9 ms.

The third solution consists of increasing the capacity of the registers so as to allow each AU to send an incident packet even if it has already sent a service packet that has not yet been extracted. This is not quite sufficient for a burst to be delivered in time. It may still be an interesting solution, because the values chosen for T_p and the transmission speed are pessimistic values.

It is thus possible to select the double loop with two AU's, as (a) it presents the best dependability characteristics and (b) it can be provided with a protocol presenting good dependability and functional characteristics. We are thus led to REBECCA, which is a French acronym meaning "Counter-rotating loop subnetwork for control system monitoring". The last section is devoted to a more detailed description of this solution.

REBECCA

Fault-Tolerance Techniques

Fault-tolerance is achieved via redundancy brought about by the double loop architecture in order to tolerate faults affecting only one loop, and reconfiguration procedures in order to tolerate common mode failures and double faults affecting the same station.

Redundancy utilization: Obviously, as we have two independent AU's, we can use the two loops for sending each packet on both loops independently, which increases the probability of correct transmission and lowers the maximum delay time.

In fact this method has been chosen essentially for safety purposes. As a matter of fact, one can see that it is only during transmission that any station can become dangerous to the whole communication mission; when it is not transmitting, signals go directly through the FEP, i.e. a minimal set of elements with independent elements on each loop.
Thus, it is essential to prevent single faults on a station from affecting both transmitting parts. This can be achieved with this method since the transmitting part of a station that is common to both loops may be no more than a simple branching mechanism that sends packets simultaneously to both transmitters.

The common receiving part is a little more complicated, because it must be able to recognize each pair of packets (by using a message number provided by the transmitter) in order to give only one copy of each message to the user; but faults in this receiving part are not catastrophic to the complete system.

CONCLUSION

In this paper we have presented the methodology and the results concerning the definition of a dependable CSS for the protection system of an EHV sub-station.

We first examined several possible solutions and the final choice was obtained after three steps: a preselection based on qualitative criteria, a selection based on quantitative criteria and lastly, a refinement of the solution obtained in the second step.

This refinement process led us to the final solution: a reconfigurable optical counter-rotating double-loop. Each loop is independently accessed in an asynchronous way using the register insertion technique.

REFERENCES

Blanquart, J.P., K. Kanoun, and J.C. Laprie (1981). Dependability of EHV sub-station monitoring equipment: Definition of the communication support system". EDF contract report, LAAS technical note, n°81.T.25 (in French).

Blanquart, J.P. (1983). Design of a dependable communication subsystem for monitoring and safety systems: REBECCA. Engineer Doctorate Thesis, INP Toulouse, France, n°241 (in French).

Boussin, J.L. (1980). PANDOR project: bus transmission system in an EHV substation. Draft report EDF, Dpt FORCAM, Clamart, France (in French).

Costes, A. , J.E. Doucet, C. Landrault, and J.C. Laprie (1981). SURF: a program for dependability evaluation of complex fault tolerant computing systems. Proceedings of FTCS-11, Portland, Maine, USA, June 24-26 1981, pp.72-78.

Ihara, H. and K. Mori (1982). Highly reliable computer network system based on autonomous decentralization concept. Proceedings of FTCS-12, Santa Monica, CA, USA, June 22-24 1982, pp.187-194.

Kanoun, K. and M. Rodrigues dos Santos (1982). Dependability of EHV sub-station monitoring equipment: Fault-tolerance in REBECCA, the communication support system. EDF contract report, LAAS technical note n°82041 (in French).

Laprie, J.C. and K. Medhaffer-Kanoun (1982). Dependability modeling of safety systems. Microelectronics and Reliability, vol.22 n°5, pp.997-1026.

Liu, M.T. (1978). Distributed loop computer networks. Advances in Computers, vol. 17, Academic Press Inc. pp.163-221.

Medhaffer-Kanoun, K. (1980). Safety system dependability evaluation: Application to the protection of EHV substations. Engineer Doctorate thesis, INP Toulouse, France, n°88 (in French).

Powell, D.R. (1982). Fault-tolerance in distributed computing systems. NATO Workshop on Distributed System Design Methodology, Brussells, Belgium, October 18-22, 1982.