Fieldbuses and their influence on dependability

Laurent Cauffriez, Blaise Conrard, Jean-Marc Thiriet, Mireille Bayart

IMTC 2003 – Instrumentation and Measurement
Technology Conference
Vail, CO, USA, 20-22 May 2003

Fieldbuses and their influence on dependability

Laurent Cauffriez*, Blaise Conrard**, Jean-Marc Thiriet***, *member IEEE*, Mireille Bayart**

*Laboratoire d'Automatique et de Mécanique Industrielles et Humaines (L.A.M.I.H.) - UMR CNRS n° 8530
Université de Valenciennes et du Hainaut-Cambrésis - Le Mont Houy –
59 313 Valenciennes Cedex 9 - France
Laurent.Cauffriez@univ-valenciennes.fr

** Laboratoire d'Automatique et d'Informatique Industrielle de Lille
(LAIL UPRES A CNRS 8021), Université des Sciences et Technologies de Lille
USTL, Cité scientifique, Bât. EUDIL
59 655 Villeneuve d'Ascq Cedex - FRANCE
Blaise.Conrard@eudil.fr, Mireille.Bayart@univ-lille1.fr

*** Centre de Recherche en Automatique de Nancy
(CRAN-CNRS UMR 7039), Université Henri Poincaré Nancy 1
2, rue Jean Lamour, 54 519 VANDOEUVRE les Nancy cedex France
jean-marc.thiriet@esstin.uhp-nancy.fr

Abstract* – The use of fieldbuses combined with intelligent sensors and actuators are opening up new possibilities for building control systems. Due to a reduction and a simplification of wire, they can reduce the cost of systems, which own a relatively great number of instruments, and which therefore offer a wide range of possibilities of task distribution, redundancy and reconfiguration. If fieldbuses seem to be a good solution to improve the dependability, it could be also a trap due to the new possible failures they may introduced. In the paper, these failures and their effects on dependability parameters are studied. Some elements are presented in order to provide designers with means to assess dependability at each design step by integrating field feedback. Assessing dependability is too often limited to an evaluation at the end of the design process, which often involves reselecting previous choices. To sum up, this contribution constitutes a structured overview of fieldbus faults given to help users to select the most suitable fieldbus for their applications, both in control and measurement.

Keywords: Fieldbus, Reliability analysis, Safety analysis, Automatic process control, Communications systems, Distributed Measurement.

I. INTRODUCTION

The rapid expansion of digital technology offers new possibilities of control and measurement system architecture with a favorable price ratio for computer components while improving reliability. Technological progress had a particularly significant impact on sensors and actuators, which evolved into intelligent devices communicating by the means of fieldbuses. From this point of view, a control system, which becomes a distributed system, is composed of devices that contain many functions and both interchange and share data [1]. Its particularity relates to data exchange between the devices via a communication medium supposed to be a network or a fieldbus. This medium constitutes a new element to be taken into account in the dependability studies.

This article is based on the reflection work of the working group on dependability of the CIAME-SEE (Constituants Intelligents pour l'Automatisation et la Mesure - Société des Electriciens et Electroniciens / Intelligent Components for Automation and Measurement - Electricity and Electronics Society). Industrialists, research workers and users working on fieldbuses, intelligent/smart sensors and actuators take part in the work of this group.

This paper provides an overview of the constraints related to fieldbuses and presents the results of the dependability study of the "communicating" function related to fieldbuses.

II. FIELDBUS COMPONENT

The presence of a network has introduced an additional functionality, namely "communication", which was implicit with pin stripe wiring. From this point of view, the functional decomposition of these two architectures is given by Figure 1, which shows that the "communication" function constitutes a component of the system. It can be placed at the same level than the other components and consequently its dependability (and its different failure modes) must be studied with the same methods: the problem is to prove that the dependability of a distributed architecture is greater than or equal to that of a centralized architecture [2].

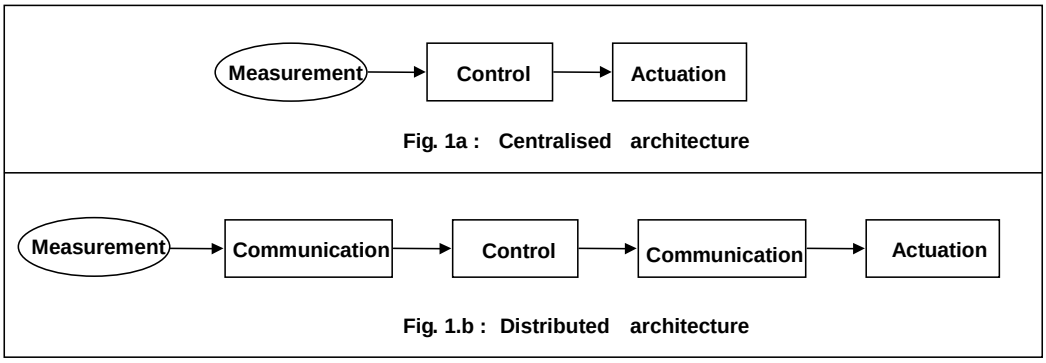

Fig 1: "Communication" function in a distributed architecture

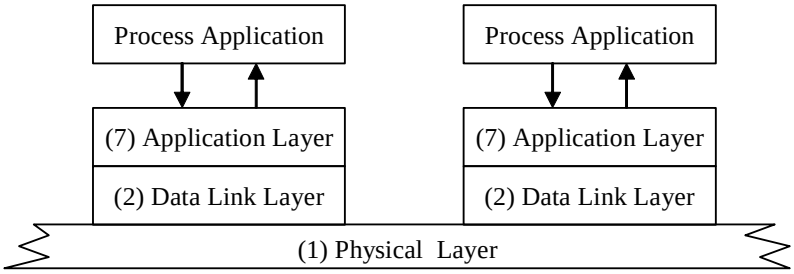

Fig. 2. Three-layer model for time constraint fieldbus system

III. FIELDBUSES AND DEPENDABILITY

The type of production environment determines largely the usable fieldbuses. Thereby, some fieldbuses are dedicated to specific areas such as home networking (EIB, Batibus, …), aviation (ARINC, …), continuous process (HART, Profibus PA, Fieldbus), machine safety (Sibus, Safety Bus, …) or embedded applications in the field of transport (CAN, VAN, …) [3]. Other important criteria include cost, confidentiality, and compatibility with equipment. According to these criteria, the designer has to choose a material architecture, and particularly a fieldbus system what also depends on factors such as application size, data throughput, and integration of time constraints.

The choice of a fieldbus and the retained architecture must be based on the means of dependability in order to predict, to combat, to eliminate or to tolerate the faults identified during the design phase.

The dependability is a complex concept, which can not be studied with a single point of view. It is thanks to the availability, the reliability, the maintainability and the safety that the dependability can be characterized in case of product systems [4].

The general measures to be applied to achieve this objective are presented from the reduced ISO/OSI model (Open System Interconnection) model (Physical layer, Data Connection layer, Application layer), according to the category claimed by the application using a fieldbus type communication system. The OSI model is normally composed of 7 layers [5]. These 7 layers are reduced to 3 layers for time constraints fieldbus systems:

- the physical layer which codes and transmits bits on the medium,
- the data link layer that manages frames and controls access to the medium,
- the application layer, which includes all the services available to a user application.

Figure 2 shows the three-layer communication system for a time constraint fieldbus system. The protocol for this triple-layer-reduced architecture is described in European standard EN 60870 "Safety systems for remote control".

To identify the failure modes of the "communication" function, the causes, and the effects on the control system, an inductive approach based on a FMECA analysis (Failure Mode, Effects and Criticality Analysis) is carried out [6].

The FMECA analysis of the failure modes of these three parts and their possible causes (internal or external causes) aims at leading to a better understanding of the "communication" function.

With this in mind, our study aims at establishing the relationship between a given failure mode and the layer of the

OSI model. The means of detection being located in another layer as shall be seen further. It should be borne in mind that a failure mode of a component is defined as the effect allowing observation of the failure of this component.

IV. THE PHYSICAL LAYER

By its passive nature a serial electrical bus has a very low failure rate. Nevertheless, the failures that can occur with the medium are fatal for the communication system: impedance mismatch or breakage circuit. The medium is therefore a solid point of the system. Two failure modes can be identified:

1) The non-reception of signals by one or several sites leads to a loss of information for the control system. It can be caused by:

- disruption of transmission on the medium causing a partially or totally illegible frame,
- external aggression such as nipping, cuts, deformation, shocks, climatic conditions, senescence, impedance mismatch, line termination loss, etc…
- the non-connection of a subscriber meant to be connected to the network,
- a subscriber connected to the network but in short-circuit condition.

2) A continuous emission on the network (excessive dialogue) due to infinite repetitions of transmission attempts, to an internal failure of a component or to an avalanche of events can lead to overloading the network and to a sudden degradation in the system performance [7].

To make the medium safe in relation to these faults, it is necessary to choose a transmission support compatible with environmental conditions. More often than not, the sheathed twisted pair is sufficient to protect transmissions from electromagnetic disturbance. Redundancy of the transmission medium in fieldbuses is a particularly delicate point. Networks openly demonstrate that operating safety has been taken into account during their design, as they have redundancy of the medium. However, whereas field networks for critical applications have a redundant medium intended to increase the reliability and availability attributes of the communication system, this redundancy, such as it is managed in the majority of cases, contributes nothing to the safety attribute. The contradiction between safety attribute and availability attribute again comes into its own.

With error detection in mind, the redundant medium (as in the case of the previous complex communication system) must not serve as an emergency medium but must be meant to ensure redundancy of the information transmitted at the physical layer level. The aim is to detect an error either on wire or on the redundant structures (if redundancy of the medium is accompanied by redundancy of the upper layers) by means of reciprocal comparison of their behavior. Such a configuration leads to further weakening of this solid point of the communication system: cataleptic failure of one or the other of the two mediums leading to complete failure of the communication system.

V. THE DATA LINK LAYER

The arrival of an erroneous frame at the Data Link Layer (of note is that this frame is necessarily complete, in other words not truncated as, according to the OSI principle, the physical layer would not be transmitted to the data link layer) leads to non-valid information for the control system.

The efficiency of an error detector code employed at data link layer level must take into accounts the flow rate and criticality of the information transmitted as well as environmental disturbances.

The detection capability of the code must guarantee a low probability of the occurrence of an undetected fault. The other detection mechanisms that can accompany the error detection code are not in question (various redundancies: medium, information, and transmission redundancy). The authors have intentionally excluded specifying an acceptable quantitative limit for the efficiency of the error detection code (e.g., an error not detected within 20 years as laid down in standard EN 50170 [8]), as the problem is complex and depends on numerous criteria.

The data link layer is sometimes equipped with an error recovery mechanism following error detection. It should be noted that this recovery must only be employed if the system allows it temporally and if the integrity of the information is not reduced by this recovery.

For an application favoring the safety attribute, the recovery mechanism must not lead to a degraded state of the system (e.g. an error on a medium must not be recovered by pursuit on a redundant medium). For this reason, the new state following a transmission error that cannot be recovered otherwise, is a shutdown state. This state is a default state that must inexorably lead to shutdown of the dangerous system protected by the safety device. This default state is acceptable to the system insofar as it does not lead to a dangerous situation.

VI. THE APPLICATION LAYER

The more the communication system is responsible for controlling the time assigned to its communication, the more consideration should be given to the information transmission aspect. This paper is limited in scope to communication systems termed remote input/output networks or networks of sensors/controllers that have the advantage of comprising a limited or at least a defined number of stations. The arrival of temporally erroneous information at the application layer leads to temporally invalid information. Non-respect of

production deadlines and/or non-respect of transmission deadlines can be listed among the possible causes.

Besides the hardware aspect linked to internal failures or to external environmental failures, the integrity of the information transmitted and its temporal validity are fundamental to making the transmission safe in relation to certain faults.

In addition, the integrity of the information transmitted depends on the nature of the information carried. The context of our work leads us to distinguishing two types of information:

- information termed safety such as: state and fault information, and information relative to safe-state control (shutdown orders).
- general operating information.

The recommendations of this study apply only to transmissions of safety information: a safe fieldbus can have recourse to two protocols, each dedicated to two types of information. The communication system, despite its higher complexity, will be both safe (for the safety information) and efficient (for the general operating information). It is also possible to distinguish information stemming from direct safety critical functions whose malfunction has an immediate adverse effect from that stemming from indirect safety functions whose failure engenders no immediate risk but does lower the safety level.

VII. FIELDBUS MANAGEMENT

Fieldbus management is highly dependent on the network studied:

- in certain protocols, it appears as a vertical layer grafted on to the OSI model (See figure 3),
- in others, management is carried out at application layer level.

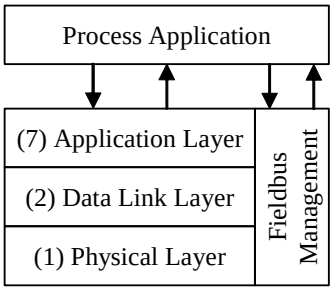

Figure 3: Fieldbus management in certain protocols

Fieldbus management raises the problems of the "non-detection of the disappearance of a station" or "non-detection of the appearance of a station" which can be catastrophic if the station concerned manages access to the network. In this case, the effect for the control system is an interruption of access to the medium.

In ASI, the master possesses the list of active stations and updates it. In CANopen, the disappearance of a station is detected at application layer level by a Node Guarding function. It should be noted that a failure at the network management layer level could stem from a design fault or an operational fault. An example of this is the case of two stations assigned the same address during the design phase or following a maintenance operation.

VIII. EVALUATION OF THE DEPENDABILITY OF THE OPERATIONAL ARCHITECTURE

A. Communication approach

The communication approach presented in this paper aims at focusing on the communication function and is the first step for the evaluation of the operational architecture. As it is mentioned before, this function is the core of the distributed architecture or system. The methodology purpose is to validate the criticality characteristics of the fieldbus network, both its whole real-time capacities and its ability or not to ensure the arrival of a high-criticality and high-priority information within a restricted temporal window.

For a fieldbus based system, evaluation of the dependability can be viewed with quantitative, semi-quantitative or only qualitative point of view [9]. This valuation is very difficult because of the diversity of the applications and the great number of failure possibilities. Several approaches exist for the dependability valuation; but in the case of system design, the chosen method has to allow several solutions to be compared and so several reliability and maintainability levels to be envisaged. The final aim in such an approach is to find the best ratio availability/safety/cost by acting upon reliability and maintainability according to the dependency of the dependability parameters shown in figure 4.

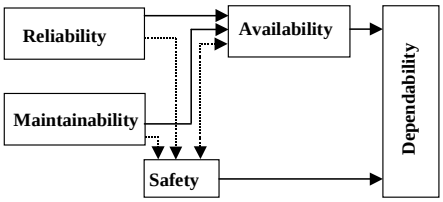

Figure 4: Dependency between the 4 dependability parameters

Field feedback provides a number of results about the behavior of automation components and allows quantification of the probability of failure. This data allow to a quantitative study to be performed. But they are often difficult to obtain and the environment has a great impact on these values. Nevertheless a qualitative or semi-qualitative study can be made more easily. It consists in identifying the weak points, in classifying them and in determining the means to avoid them.

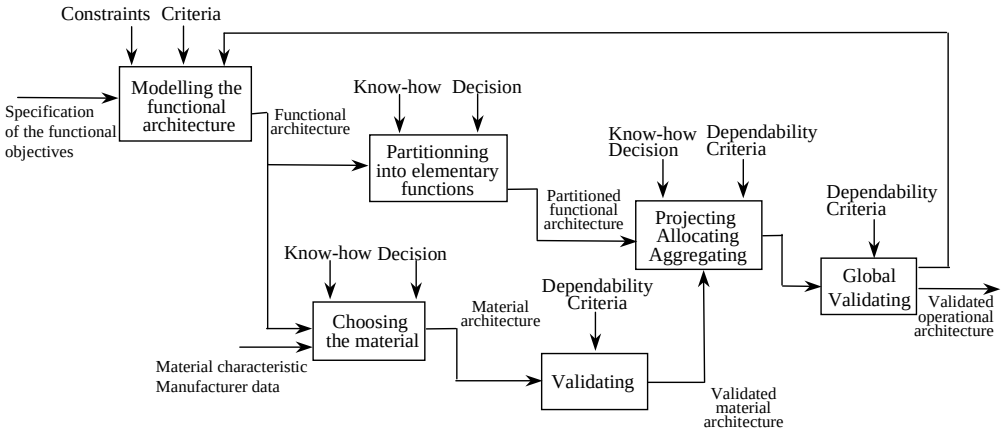

Fig 5: A design method for intelligent distributed control systems

B. Systemic or application approach

The next step of the evaluation of the operational architecture is a systemic approach or application approach to which the validation needs to take into account the whole lifecycle of the system.

In a first way to proceed, the functional partitioning presented in figure 5 proposes a way to determine the operational architecture according to dependability criteria. The overall dependability valuation of the operational architecture can then be obtained by aggregating each elementary function (the aggregation of these elementary functions leads to the notion of functions and missions of the system), while dependability parameters for each elementary function are obtained from the ones of the material component that performs it.

Reference should be made to other studies into functional partitioning including those of [10].

However this valuation requires a complete specification for each function and sub-function, including the quantified performance objective, in terms of response-time and dependability.

A second way to proceed [11] is based on the information: in order to evaluate the dependability characteristics of a distributed control system, it is proposed to study the lifecycle of the information within the running system, in order to determine the critical elements of the architecture, and so to get some parameters for the evaluation of the whole architecture.

This method is based upon the evaluation of the needed credibility of the information as a function of the required criticity of the system, versus the obtained credibility of the information as a function of the actual reliability characteristics of the components. These are approaches to enrich the methodology proposed in this paper. The development of these further works is presently on the way.

IX. CONCLUSIONS

In this paper, the results of the dependability study of the 'communication' function are presented in detail with the identification of the failure modes and causes and effects for each level of the fieldbus. This FMECA leads to present a number of means of prevention to avoid or to minimize the damaging consequences of the occurrence of failure modes.

This paper has shown some important characteristics to take into account for the design of distributed control or measurement architecture.

This point is huge, particularly if the measurement has to be sent to a receiver in a limited temporal window, and so the temporal characteristics of the measurement is very critical.

These data are useful in designing automation systems and in selecting the control system architecture and the suitable fieldbus, and allow achieving the planned dependability objectives. Some future works will be to take account also of the particularities of the wireless networks [12].

ACKNOWLEDGMENTS

The authors would like to thank the other persons which regularly participate to the workgroup:

Eric BENOIT (LAMII, Université de Savoie), Guy BENOIT (CEA), André CHOVIN (CROUZET Automatismes), Joseph CICCOTELLI (INRS), Eric FAE (INERIS), Denis GENON-CATALOT (IUT Valence), J.C. HENRY (Thomson CSF Communications), Martine WAHL (INRETS)

REFERENCES

[1] M. Choi, N. Park, F. J. Meyer, F. Lombardi, "Performance analysis of fault tolerant multistage interconnection networked parallel instrumentation with concurrent testing and diagnosis", *18th IEEE/IMTC Instrumentation and Measurement Technology Conference*, Anchorage, Alaska, USA, 21-23 May 2002.

[2] Z. Mammeri Z. and J.P. Thomesse, *Réseaux Locaux Industriels FIP et MAP dans les systèmes automatisés*, collection réseaux et systèmes, Editions Eyrolles, Paris, 1993.

[3] Ciame, *Réseaux de terrain: Description et critères de choix*, 203 p., Editions Hermes, Paris, 1999.

[4] A. Villemeur, *Methods and Techniques, Volume 1, Reliability, Availability*, 1988.

[5] ISO/IEC 7498-1, *Information Processing Systems - Open Systems Interconnection - Basic Reference Model*, International Standards 7498-1, International Standards Organization (ISO), Genève, 1984.

[6] X60-510, *Technics of reliability systems analysis - Procedures for Failure Mode, Effects and Criticality Analysis* (in French), December 1986.

[7] H. Kopetz, *Real-time systems design principles for distributed embedded applications*, Kluwer Academics Publishers, 1997.

[8] CENELEC, *General Purpose Field Communication System*. EN 50170, Vol. 1/3 (P-NET), Vol. 2/3 (PROFIBUS), Vol. 3/3 (FIP), Cenelec, 1996.

[9] B. Conrard, *Contribution à l'évaluation quantitative de la sûreté de fonctionnement des systèmes d'automatisation en phase de conception*, Phd. Thesis, Université Henri Poincaré, Nancy 1, Septembre 1999.

[10] M. Staroswiecki, M. Bayart, J. Akaichi, "Distribution of intelligent automated production - a clustering approach". In *integrated systems engineering*, IFAC, Baden Baden Germany, pp. 377-382, 1994.

[11] F. Jumel., J.-M. Thiriet, J.-F. Aubry, O. Malassé, "Towards an information-based approach for the dependability evaluation of distributed control systems", to be published in *20th IEEE Instrumentation and Measurement Technology Conference (IEEE/IMTC2003)*, Vail (Colorado, United States), 20-22nd May 2003.

[12] G. Bucci, I. Caschera, E. Fiorucci, C. Landi, G. Ocera, "The use of wireless network for distributed measurement applications", *18th IEEE/IMTC Instrumentation and Measurement Technology Conference*, Anchorage, Alaska, USA, 21-23 May 2002.