Copyright © 2002 IFAC
15th Triennial World Congress, Barcelona, Spain

FAULT-TOLERANT CONTROL MANAGEMENT - A CONCEPTUAL VIEW -

Dirk van Schrick

Group of Safety Control Engineering (SRM)
Faculty of Safety Engineering (FB 14), University of Wuppertal
D-42097 Wuppertal, Germany, Europe
Vox: ++49 202 439 2019, Fax: ++49 202 439 2586
E-male: schrick@uni-wuppertal.de

Abstract: A draft for a comprehensive conceptual understanding of fault-tolerant control and its management is proposed. This management is considered a part of the technical failure and fault management that comprizes technical and organizational aspects. The latter management is described briefly with respect to its objectives, functions, means, purposes and to faults, fault tolerance and redundancy as well. The fault-tolerant control management is in the centre of the description with a reference to both the three basic aspects plant, control system and controlled system and the two main aspects system accomodation and, in a general sense, control situation.

Keywords: Technical Diagnosis, Fault Recognition, Fault Treatmant, Fault-Tolerant Control, Reconfiguration, Replanning

1. INTRODUCTION

In the last years, ***fault-tolerant control (FTC)*** has been discussed more and more. Often, the discussions concern single realizations of fault-tolerant control systems in an industrial context. In opposition to that, in some publications of recent dates a more general view onto fault-tolerant control has been described. One aspect is the method-oriented state-of-the-art considered in Patton (1997), the other is a more generalizing aspect with some additional notions on the conceptual or terminological description of FTC. This, for example, is documented in Blanke et al. (2000) and Staroswiecki and Gehin (2000).

Up to date, nearly all discussions reveal that, due to different theoretical and practical views onto FTC with technical entities, no unique FTC-terminology exists. Therefore, for the first time some basic terminology-oriented aspects such as fault, fault recognition, fault treatment, redundancy, robustness, adaptivity and fault tolerance have been described in van Schrick (2000a). The above mentioned publications of later date are taken as a basis for the description of a new, more comprehensive conceptual view onto fault-tolerant control. Regarding the contribution to **IFAC World Congress 2002**, this view is directed to some fundamental aspects of the technical failure and fault management (content of section 2) described in subsection 2.1 *Objectives and functions* and subsection 2.2 *Means and purposes*, to the results of a state-oriented study of fault-oriented aspects described in section 3 *Fault and fault tolerance* and finally to the aspect *Fault-tolerant control with a side-glance onto its management* described in detail in section 4 *Fault-tolerant control and its management.*

2. TECHNICAL FAILURE AND FAULT MANAGEMENT

In different contributions such as van Schrick (1998) and van Schrick (1999), a comprehensive *conceptual-system draft (CSD)* for the ***Technical Failure and Fault Management (TFFM)*** has been proposed and outlined from different aspects. The subject of the TFFM consists of both *nondesired technical phenomena (NTP)* such as faults, failures and disturbances occuring in technical systems and the *handling of these phenomena* in sense of a comprehensive management not restricted to a handfull of managers with jurisdiction. The TFFM concerns everybody from the top to the bottom of an enterprise and vice versa. The idea behind this management refers to different subjects: the occurrence of nondesired technical phenomena representing insufficient technical systems, the location of the NTP-occurrence (technical system), the handling of the NTP (technical management), the implementation of the technical management (management system) and the location of the technical management (enterprise).

With regard to the concepts of interest, the complex structuring process first led to a German-language basic draft for the conceptual system based on qualitative definitions (non-metrical) mainly taken from appropriate standards and guidelines. The German-language draft has been considered a foundation for the TFFM-CSD. This English-language version does not only focus on terms and definitions of concepts, it mainly comprises both the concepts of interest and their mutual relations. The TFFM-CSD is overlapping with respect to standards and guidelines to combine different views onto the management of NTP in fields such as control engineering, technical diagnostics and maintenance. The draft is intended as a further step to discuss terminological problems within the *diagnosis community world wide*. Excerpts from this conceptual-system draft are described in van Schrick (2000b) and taken here as a basis for discussion.

2.1 *Objectives and functions*

The TFFM is organized in management sections and management levels. Relevant sections are on one hand-side the *diagnosis management (DM)* and on the other hand-side the *maintenance management (MM)*, the *quality management (QM)*, the *process management (technical, organizational) (PM)* and the *organization management (OM)*. The levels, relevant to a vertical structuring of the TFFM refer, starting from the bottom, to the aspects *operation, tactics, disposition* and *strategy*. In all TFFM-sections and on all TFFM-levels, the activities performed manually and automaticlly have to be in harmony with the objectives of the TFFM. The essential objectives are *safety, dependability, economy* and *ecology*, where the technical interest mainly refers to safety and dependability. To approach the objectives, different types of strategy can be applied, mainly *short-term strategies, median-term strategies* and *long-term strategies*. Each of these types concerns a number of different functions that have to be performed. There are two groups of functions to be distinguished: the ***technical diagnosis (TD)***, necessary to obtain information on the (technical) entity of interest by monitoring, diagnosing and prognosing the entity's state and condition, and the ***technical therapy (TT)***, necessary to process the information obtained for appropriate actions with respect to safety and reliability (at least). Such actions could be: system-fault alarm, power reduction or re-adjustment of controller gains and system reconfiguration, for example. The TFFM-functions and their interrelations are given in Fig. 1 in form of a closed-loop control representation. The control error is the difference between the actual information and the nominal information about the entity (process, controlled system). Technical or organizational (business) interrelations between TD and TT are considered ***supervision*** (at least monitoring and high-level safety actions such as shut-down of technical processes) and ***controlling*** (at least monitoring and control of business processes). Details on the TFFM with respect to objectives and functions are given in van Schrick (1997, 1998). Definitions of concepts relevant to these two aspects of TFFM are stated in van Schrick (2000b) and considered here a basis for understanding as well.

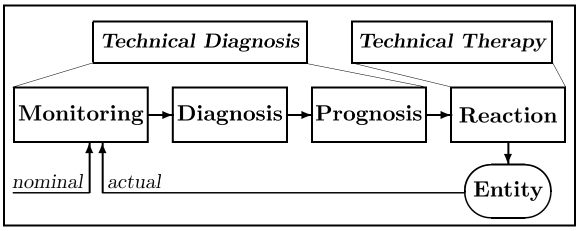

Fig. 1. TFFM-Functions

2.2 *Means and purposes*

For performing the functions, appropriate means have to be provided. The means for technical diagnosis, i. e. the means for realizing the functions *monitoring, diagnosing* and *prognosing* are provided by the TFFM-section *diagnosis management* and, partially, by the TFFM-section *maintenance management*. For example, associated means are plausibility tests for variables, pattern recognition procedures for inspection of entities within the maintenance procedure. The means for technical therapy, i. e. the means for realizing the functions of re(medial-)actions are provided by those management sections that refer to maintenance, quality, process (technical, organizational) and organization. The associated means are *entity maintenance*

(EM), quality control (QC), process control (PC) and *organization replanning (OR)*. These means have to be purposeful, i. e. the application of these means has to make possible the achievement of TFFM-purposes according to its objectives.

The set of essential TFFM-purposes and their interrelations are represented in Fig. 2. With respect to maintenance, aspects marked with "*" refer to both technical diagnosis and technical therapy. Two purposes of fault control are relevant: The main TD-purpose ***fault recognition*** that comprizes the fault-related purposes *detection, diagnosis* and *prognosis* and the informational results from the application of appropriate means for technical diagnosis are represented in Fig. 3. The main TT-purpose ***fault treatment*** that comprizes the fault-related purposes *suppression, bypassing* and *elimination* and the entity-related states after the application of appropriate means for technical therapy are represented in Fig. 4. With respect to the fault-tolerant control management, *fault-cause elimination* is of major importance: It is considered the result of activities for the transition of an entity from a faulty state to a fault-cause-free state. This comprizes on one hand-side the shift of function(alitie)s from the faulty to a fault-free entity that performs the functions completely or with reduced functionality, on the other hand-side it comprizes both the separation of the faulty entity after its localization in sequence of a detected fault and the allocation of an entity that replaces the faulty one. Related aspects are *graceful degradation* and *fail-soft*. In a narrow sense, fault-cause elimination is termed ***reconfiguration***. In a broad sence, reconfiguration is conceptionalized the result of activities for re-assembling or new-assembling of open-loop and closed-loop control systems with respect to their sub-systems, the sub-systems' properties and the relations between the sub-systems (control system's structure). In this broad sense, reconfiguration comprizes the purposes *fault(-effect) suppression* and *fault-cause elimination*!

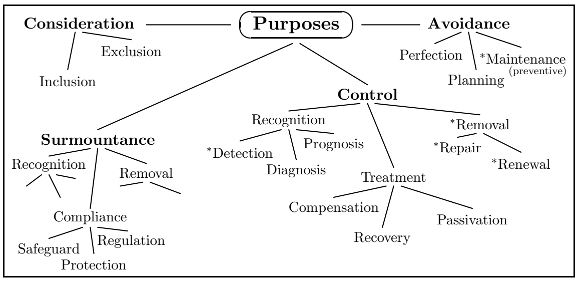

Fig. 2. TFFM-Purposes

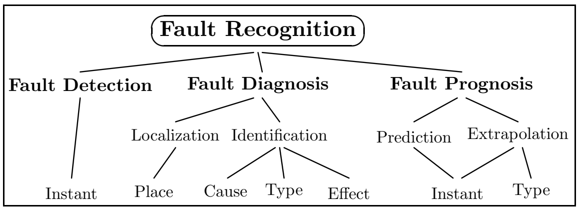

Fig. 3. TD-Purposes and results

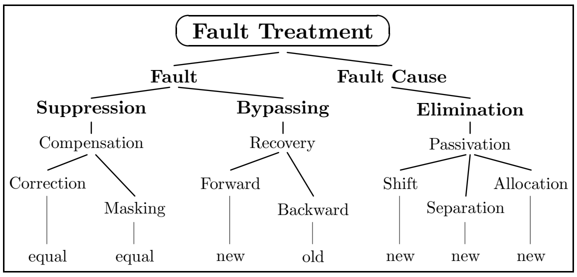

Fig. 4. TT-Purposes and states

3. FAULT AND FAULT TOLERANCE

In the context of the subject regarded here, the most important nondesired technical phenomenon is the fault. A ***fault (F)*** is considered a nonfulfilment of a specified requirement. The state-oriented view onto faults refers to two states a technical entity can take: correct state (C) and incorrect state (I). The state of incorrectness represents the inability to perform the required function. It is a *faulty state* (F_2), a malcondition described (measured) as an error in sense of a discrepancy between a computed, observed or measured value or condition and the true specified or theoretically correct value or condition. This error is considered the *described faulty state* (F_1). Figure 5 represents this state-oriented fault causality, where the unplanned transitions from state C to state I are *failures* (F_r) in sense of events associated to the (undesired termination of the) ability to perform a required function. The unplanned transitions from I to C are *reverse failures* $(\overline{F}_r)$ in sense of events based on physical-chemical processes that happen accidentally. The planned transitions from I to C are desired *restorations* (R_1) in sense of the reclamation of the ability to perform a required function. The dynamics of the state-oriented fault causality mainly refers to the effect *failure* (F_r) and its causes such as *technical and pre-operational human faults* $(F_3$,

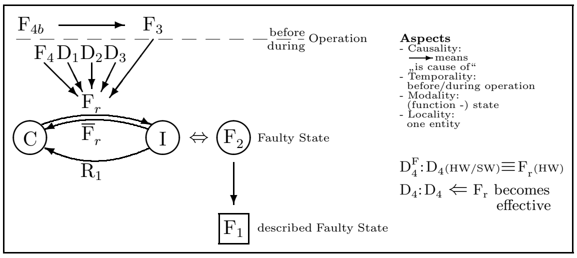

Fig. 5. State-oriented fault causality

F_{4b}) and operational human faults (F_4), internal and external disturbances (D_1, D_2), damages (D_3) and *defaults (D_4, D_4^F)*. With respect to failure F_r only related to hardware-realized entities, a default D_4^F is considered a failure-equivalent event related to entities that are both hardware- and software-realized. In opposition to this, a default D_4 is considered an event that occurs when a failure F_r becomes effective. For more details (on such nondesired technical phenomena NTP) cf. van Schrick (2000b).

With respect to a technical entity structured through the levels *system, group, element*, Fig. 6 represents a level-oriented fault causality. A fault (F), in form of a faulty state F_2, can be a cause (FC) for a fault on the same level (element (E), group (G), system (S)) or on a higher level (G, S).

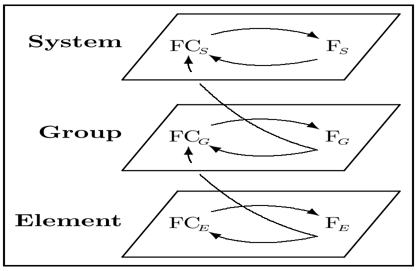

Fig. 6. Level-oriented fault causality

With this background, ***fault tolerance (FT)*** is considered the ability of an entity to perform the required function inspite of incorrect sub-entities. This ability requires appropriate means for the accomplishment of purposes. These purposes (and their sub-purposes) are *fault recognition (detection, diagnosis, prognosis)* and *fault treatment (compensation, recovery, reconfiguration)*. The latter is based on ***redundancy***, i. e. the existence of more than one means for performing a required function, mainly with respect to sub-entities such as system components or parts (structural, functional (logical, analytical), informational). Figure 7 represents a taxonomy of redundancy types, structured with regard to the case of an existing fault. This taxonomy is based on the contribution of an entity to the performance of a function in question. The active-passive dichotomy refers to the activity of additional (sub-)entities (spare-parts, redundant entities) in the no-fault situation, where the dynamic-static dichotomy refers to the situation whether additional (sub-)entities have to be integrated (shifted, separated, allocated by switching) into an entity (technical system) or whether they are already performing their function (masking), i. e. they have not been moved for fault tolerance.

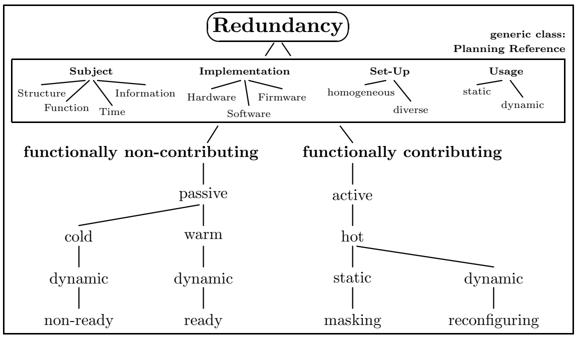

Fig. 7. Redundancy; disturbed performance

4. FAULT-TOLERANT CONTROL AND ITS MANAGEMENT

The type of control considered here has the ability to be fault-tolerant. In non-simple cases such as large production systems, this ability has to be managed, especially when technical and business processes are interconnected. ***Fault-Tolerant Control Management (FTC&M)***, i. e. FTC with a side-glance onto its management, is considered a functional combination of supervision and controlling. This will be described roughly: The entities for consideration are dynamic technical systems. A technical system containing components for the manipulation of physical, chemical or informational properties is a system to be controlled, a *plant*. A technical system containing at least components for measuring (sensors), influencing (actuators) and scheduling/executing (computers) is a *control system (or controller)*. A technical system consisting of the system to be controlled and the control system is a ***controlled system***, sketched in Fig. 8 as a part of a control-loop (cp. Fig. 1) with reference variable $w(t)$ (nominal value), control variable $u(t)$ and measured variable $y(t)$ (actual value).

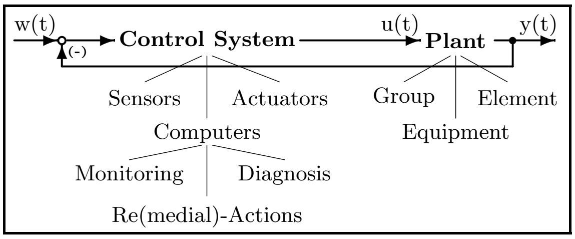

Fig. 8. Controlled system

Regarding this system partitioning, and with respect to the system's state of incorrectness, the main purpose of TD- and TT-activities is ***entity accomodation***, i. e. accomodation of the controlled system to the faulty situation. This can be realized by appropriate control variable values and actions wrt. the system components to achieve the relevant objective, e. g. correct system performance. The main function is ***entity control***, technically and organizationally. Combining both accomodation and control, three sub-aspects of ***accomodation by control*** are relevant:

1) **Controller accomodation by conventional control**, i. e. passive FT: *robust* or *adaptive controllers* for *fault insensitivity* or *controller-parameter adaptation* wrt. the fault (effect).
2) **Controlled-system accomodation by fault-tolerant control**, i. e. active FT:
   a) *controller reparametrization* wrt. the controller parameters directly or indirectly after *controller restructurization* due to a change of the controller type for *fault (effect) suppression* (fault correction or fault masking) or
   b) *controlled-system reconfiguration* wrt. the system's sub-entities (replacement) and their properties (calibration) and relations (controller-plant inputs-outputs) for *fault (cause) elimination* (passivation of the faulty sub-entity);
   Remark: FTC is associated with supervisery/intelligent control, cp. Patton (1997);
3) **Control accomodation by fault-tolerance control**, i. e. *control replanning* based on manual (or automated) decisions concerning the control objective, strategy and tactics, or eventually *control reengineering* concerning the aspects of replanning and additionally, e. g., manual or automated activities, human abilities and responsibilities, both for *fault avoidance and prevention* in the near/far future.

The different situations to be managed are associated with four essential aspects of control, cp. Staroswiecki and Gehin (2000): *objectives* ($g \in G$)*, relations* ($r \in R$)*, parameter values* ($p \in P$)*, control variable values* ($v \in V$) (a small letter symbolizes an element of the relevant set it belongs to, a capital letter symbolizes the set). The relations between the aspects and the types of control determine different underlying ***control situations***, mainly after the reaction to a fault (cases b, c):

a) **Conventional control situation** $\{\mathbf{g}, \mathbf{r}, \mathbf{p}, \mathbf{V}\}$**:**
   Here, in accordance with system's r and p a suitable v has to be determined to achieve g. More realistic, $\{\mathbf{g}, \mathbf{r}, \mathbf{P}, \mathbf{V}\}$ exists, where the parameter values $p \in P$ are unknown, i. e. an uncertain or time-varying system has to be considered. The relevant situations are:
   - *Robust control situation* $\{g, r, P', V\}$, where the fault-insensitivity-guarantying $P' \in P$, instead of a single p, has to be covered by the controller to achieve g.
   - *Adaptive control situation* $\{g, r, \hat{p}, V\}$, where the single p is replaced by the reconstruction $\hat{p} \in P$ to achieve g.

b) **Fault-tolerant control sit.** $\{\mathbf{g}, \mathbf{R}, \mathbf{P}, \mathbf{V}\}$**:**
   This situation is characterized by the occurence of a fault resulting in a faulty state of the controlled system considered. Therefore, at least information on the existence of the (unknown) faulty state is required to react properly by fault-tolerance-based actions. The relevant situations are:
   - *Reparametrized control sit.* $\{g, \hat{r}, \hat{p}/\hat{P}', V\}$, where powerful algorithms for *fault detection and isolation (FDI)*, cf. Patton (1997) for example, could provide the information required of the actual parameters or of a robust parameter set in form of the reconstructions $\hat{r}, \hat{p}$ or $\hat{r}, \hat{P}'$, for example.
   - *Reconfigured control situation* $\{g, \rho, \pi, \Upsilon\}$, where instead of the reconstructions $\hat{r}$, $\hat{p}/\hat{P}'$ for the unknown r, p/P' new, known values $\rho \in \Gamma$, $\pi \in \Pi'$ have to be provided (new situation!). This requires the determination of the sets Γ and Π, Π', and additionally, the set Υ for the control variable values υ. FDI-algorithms are not necessarily required.

c) **Fault-tolerance control sit.** $\{\mathbf{G}, \mathbf{R}, \mathbf{P}, \mathbf{V}\}$**:**
   With respect to the more organizational management aspect *objectives*, the control situation additionally refers to fault-tolerance in the most general sense. The relevant situations are:
   - *Replanned control situation* $\{\gamma, r, p/P', \Upsilon\}$, a generalization of the reparametrized control situation regarding the change of objective (human decision) with the change of control variable values in consequence.
   - *Reengineered control sit.* $\{\gamma, \rho, \pi/\Pi', \Upsilon\}$, a generalization of the reconfigured control situation regarding the change of objective (human decision) with the change of, for example, relations, parameter values and control variable values in consequence.

From a slightly deviating point of view on FT in control, different *control problems* are described in more detail in Staroswiecki and Gehin (2000).

Figure 9 represents a management-level-oriented summary of FTC&M with respect to a unique assignment of management aspects to three TFFM-management levels:

	Management Levels		
Aspect	**Operation**	**Tactics**	**Strategy**
Situation	$\{\mathbf{g}, \mathbf{r}, \mathbf{p}, \mathbf{V}\}$**:** $\{g, r, P', V\}/$ $\{g, r, \hat{p}, V\}$	$\{\mathbf{g}, \mathbf{R}, \mathbf{P}, \mathbf{V}\}$**:** $\{g, \hat{r}, \hat{p}/\hat{P}', V\}/$ $\{g, \rho, \pi, \Upsilon\}$	$\{\mathbf{G}, \mathbf{R}, \mathbf{P}, \mathbf{V}\}$**:** $\{\gamma, r, p/P', \Upsilon\}/$ $\{\gamma, \rho, \pi/\Pi', \Upsilon\}$
Entity of Accomod.	Controller	Controller/ Controlled System	Control
Function	Convent. Control	FT-Control	$\mathrm{FT_C}$-Control
Purpose	F(E)-Insensitivity/ Adaptation	F(E)-Suppression/ F(C)-Elimination	F(C/E)-Avoidance
Means	Parametrization	Reparametrization/ Reconfiguration	Replanning/ Reengineering
Basis	F-Consideration	F-Recognition	F(CE)-Analysis

abbreviations: fault-tolerant (FT), fault-tolerance (FT_c)*, fault (F), cause (C), effect (E)*

Fig. 9. FTC&M-Aspects and levels

- The level *strategy* concerns all areas of strategical (overall objectives, guidelines for sectional objectives, ...) and informational functions necessary for the management of an enterprise or organizational units of it. On this level, the formulation of objectives of the overall enterprise takes place (what should be achieved?).

- The level *tactics* concerns all technical, but also all administrative, logistical or economical functions, e. g. both *higher functions* of production, transport or upper management of business processes and *basic functions* of control or supervision of technical processes. On this level, the provision of operational means for technical or business purposes for the lower levels and the coordination of the application of these means ready for use takes place (which operational means are necessary and how to apply them?).
- The level *operation* concerns all technical operational functions wrt. the influence of technical (and organizational) processes. On this level, the performance by purposeful operational means (machines, transportation systems, ...) takes place (how to perform the function?).

With respect to faults that occur on the operational level, FTC&M by conventional control concerns this level only. In opposition to that, FTC&M by fault-tolerant control and fault-tolerance control concerns additionally the tactical level and the tactical/strategic levels, respectivly. It is important to note, according to the accomodation levels *controller, controlled system, control* the management level *tactics* refers to both accomodation levels: controller, controlled system.

Each basis for the functions to be performed on each management level can be derived from the TFFM-purposes shown in Fig. 2. Fault consideration and fault recognition are mentioned in this figure and refer to the operational and tactical management, respectively, whereas the analysis of fault causes and effects that refer to the strategical level can be considered *fault-oriented consideration* directed to an overall view wrt. management units, levels, sections and space and time (strategy, deadlines for re(medial)-actions, ...) as well.

5. SUMMARY AND OUTLOOK

A draft for a comprehensive conceptual understanding of the FTC&M has been proposed. This management has been considered a part of the TFFM that comprizes technical and organizational aspects. As a basis for understanding, this management has been described with respect to its objectives, functions, means, purposes and to faults, fault tolerance and redundancy as well. The FTC&M, that is in the centre of interest with this contribution to the IFAC World Congress 2002, has been described with a reference to both the three basic aspects *plant, controller* and *controlled system* and the two main aspects *entity accomodation* and, in a general sense, *entity control*. Additionally, the main FTC&M-aspects have been related to three TFFM-levels of the technical failure and fault management. Current work concentrates on a more detailed description including definitions for concepts essential to the FTC&M. Moreover, more theoretically, the reconfiguration process will be analysed with the help of Boole's theory.

REFERENCES

Blanke, M. et al. (2000). What is Fault-Tolerant Control?, in: Edelmayer, A. M. and Bányász, Cs. (Eds.) (2000). *Proc. IFAC Symp. on Fault Detection, Supervision and Safety for Tech. Proc. (SAFEPROCESS 2000)*, Budapest, Hungary, Vol. 2, pp. 40-51.

Patton, R. J. (1997). Fault-Tolerant Control: The 1997 Situation, in: Patton, R. J. and Chen, J. (Eds.) (1997). *Proc. IFAC Symp. on Fault Detection, Supervision and Safety for Tech. Proc. (SAFEPROCESS'97)*, Kingston Upon Hull, England, pp. 1291-1296.

Staroswiecki, M. and Gehin, A.-L. (2000). From Control to Supervision, in: Edelmayer, A. M. and Bányász, Cs. (Eds.) (2000). *Proc. IFAC Sympo. on Fault Detection, Supervision and Safety for Tech. Proc. (SAFEPROCESS 2000)*, Budapest, Hungary, Vol. 2, pp. 312-323.

van Schrick, D. (1997). Technical Fault and Quality Management - Terminology of Functions, Purposes and Means. In: Cho, H. S. (Ed.) (1997). *Prepr. Workshop on Int. Manufact. Systems (IMS'97)*, Seoul, Korea, pp. 127-132.

van Schrick, D. (1998). Technical Failure and Fault Management Terminology. In: Morél, G. and Vernat, F. (Eds.) (1998). *Proc. IFAC Symp. on Inf. Control in Manufact. (INCOM'98)*, Nancy & Metz, France, pp. 247-252.

van Schrick, D. (1999). Redundancy, Functions, Purposes & Concepts and Structures, in: Frank, P. M. (Ed.) (1999). *Proc. Europ. Control Conf. (ECC'99)*, Karlsruhe, Germany, pp. 234-239.

van Schrick, D. (2000a). Fault, Tolerance and Control: A Conceptual System Draft: Relations and Definitions, in: Zheng, Y. (Ed.) (2000). *Proc. 3rd Asian Control Conf. (ASCC 2000)*, Shanghai, PR China, pp. 2795-2800.

van Schrick, D. (2000b). Conceptual System Draft for Safeprocess: Relations and Definitions, in: Edelmayer, A. M. and Bányász, Cs. (Eds.) (2000). *Proc. IFAC Symp. on Fault Detection, Supervision and Safety for Tech. Proc. (SAFEPROCESS 2000)*, Budapest, Hungary, Vol. 2, pp. 792-797.