TU

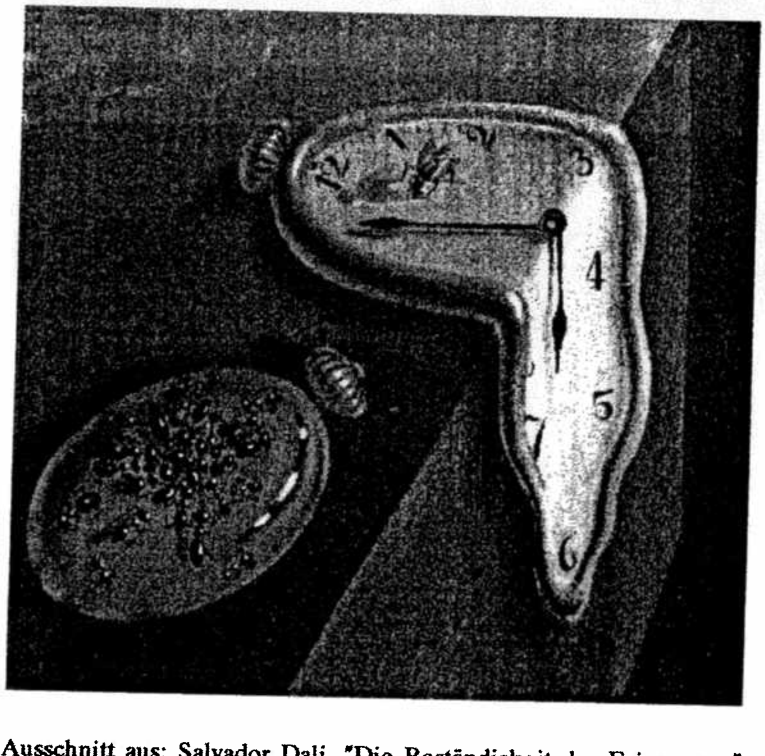
Institut für Automation
Abt. für Automatisierungssysteme

Technische
Universität
Wien

Projektbericht Nr. 183/1-20
Mai 1991

A Proposal of Vital Process Control Using an Expert System

M. Kathofer, G.H. Schildt



Ausschnitt aus: Salvador Dali, "Die Beständigkeit der Erinnerung"

A Proposal Of Vital Process Control Using An Expert System

M. Kathofer and G. H. Schildt (senior member of IEEE)

Technical University Vienna, Institut for Automation,
Treitlstr. 3, A-1040 Vienna

Abstract. After an introduction into safety terms some vital process structures are presented which were used up to now. There may arise a great challenge applying expert systems as a monitoring channel. Therefore a new concept is presented describing a realtime interface between realtime control system and an expert system. Functionality of this system structure will be discussed under dependability aspects.

Keywords: fail-safe, vital process control, hazard detection module, danger and solutions module, resolution searching module, real-time data base, expert system

1. Introduction

In recent years the field of safety engineering has won importance in guideway transit system as well as nuclear and chemical power plants. In these fields devices and control systems relevant to safety are used. Complex system design impacts the use of computer control, although one has to recognize that computer programs of high complexity will never be error-free. Before discussing different vital system structures some safety terms will be defined at first /SCHI 89/.

- <u>System relevant to safety (vital system):</u> Control systems causing no hazard to people or material in case of constructional element failure, environmental influence, or design faults.

- <u>Safety:</u> property of an item to cause no hazard under given conditions during a given time; i. e. avoidance of undue fail conditions. Undue fail conditions may be caused by
  - technical system failures,
  - design faults or
  - malfunction of an electronic device interfered by electromagnetic noise

- o <u>Hazard (acc. to vital control systems):</u> condition of a system that cannot be controlled by given means and may lead to injuries to people.

- o <u>Safe condition of a system:</u> property of a system condition to cause no hazard; i. e. a vital control system has to have a safe system condition (in some systems a safe system condition may be achieved by switching the system off; e. g. in a guideway transit system this may be a 'safe halt conditions', because the kinetic energy is zero, $E_{kin}=0$).

- o <u>Fail safe:</u> technical failures or design faults within a control system may lead to fail conditions of a system ('fail') which, however, have to be safe ('safe'), the safe condition has to be an collective condition for all fail conditions of a system.

2. Vital System Concepts

System design of vital control systems can be done acc. to the following system structures. Basically, these fundamental system structures are valid for hardware as well as for software systems too /FRI 78/.

2.1 Single channel fail-safe control systems

The system reaction of a single channel fail-safe control system may be described by a condition graph together with a temporal diagram in case of failure or if a design fault becomes effective (Fig. 2-1).

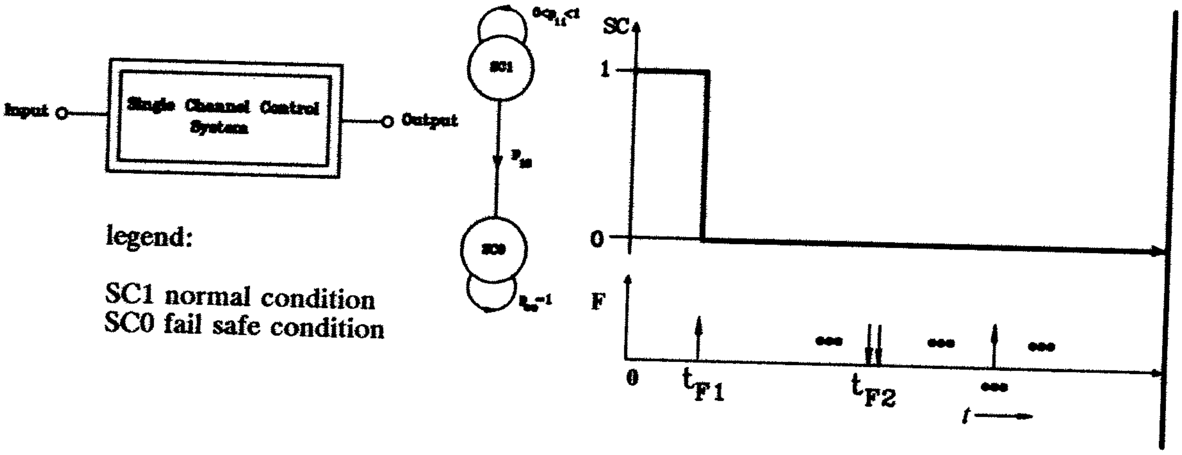


Figure 2-1 Single channel fail-safe control system

If a first failure occurs at t_{F1}, system changes its condition from SC1 to SC0. In case of a second failure at t_{F2} control system will remain in the safe condition SC0. It is an essential feature of a single channel fail-safe control system that transition probability $p_{00}=1$, so that safe system condition cannot be left by itself. A system restart can only be done by an operator after successful system diagnostics and repair. But, because only simple devices may be designed acc. to this system structure, one has to change the design principle: from an intrinsically fail-safe system to a vital control system using special procedures to guarantee a safe system reaction in case of failure or design faults. Thus one has to find other system structures supporting more complexity by special system design.

2.2 Control system with monitoring channel

One approach to realize a vital control system with commercial computers may be done by installing an additional monitor channel checking all input data, intermediate results and output telegrams of the non-intrinsically-safe control system, but operating fail-safe. Monitoring channel has to fulfill the following fundamental tasks:

1. Validating every output telegram acc. to all input as well as intermediate data.

2. Monitoring that output telegrams are generated and validated within time constraints, i. e. directed to process elements on time.

Figure 2-2 illustrates relations between occurence of a critical event, reception of a corresponding signal by computer starting a classified system reaction, which should be terminated within maximum response time.

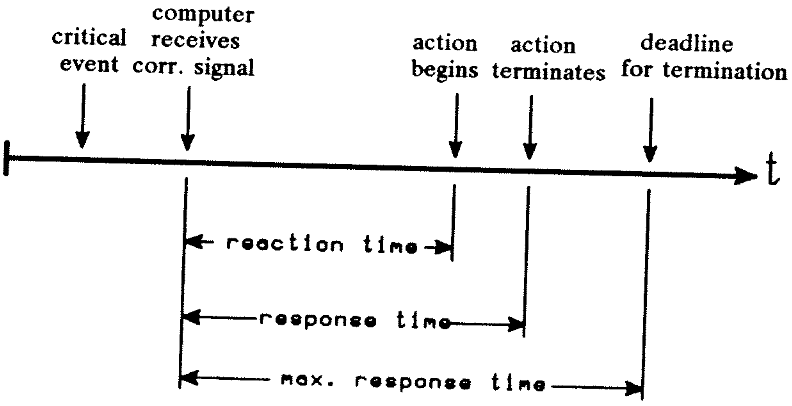
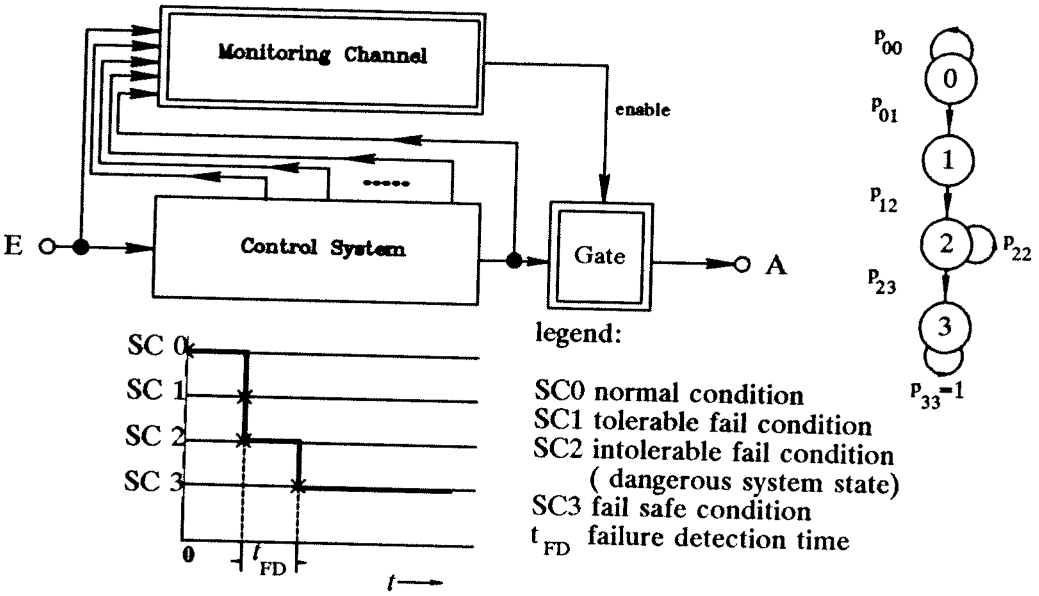


Figure 2-2 Time constraints for system reaction

Fig. 2-3 presents the system structure together with a condition graph and temporal system description. The monitor channel turns out to be a high sophisticated component because it has to prove that telegrams generated by the control system will not cause any hazard within the technical process as well as that command telegrams are on time acc. to the time constraints of the process.



legend:

SC0 normal condition
SC1 tolerable fail condition
SC2 intolerable fail condition
(dangerous system state)
SC3 fail safe condition
t_{FD} failure detection time

Figure 2–3 Control system with monitoring channel

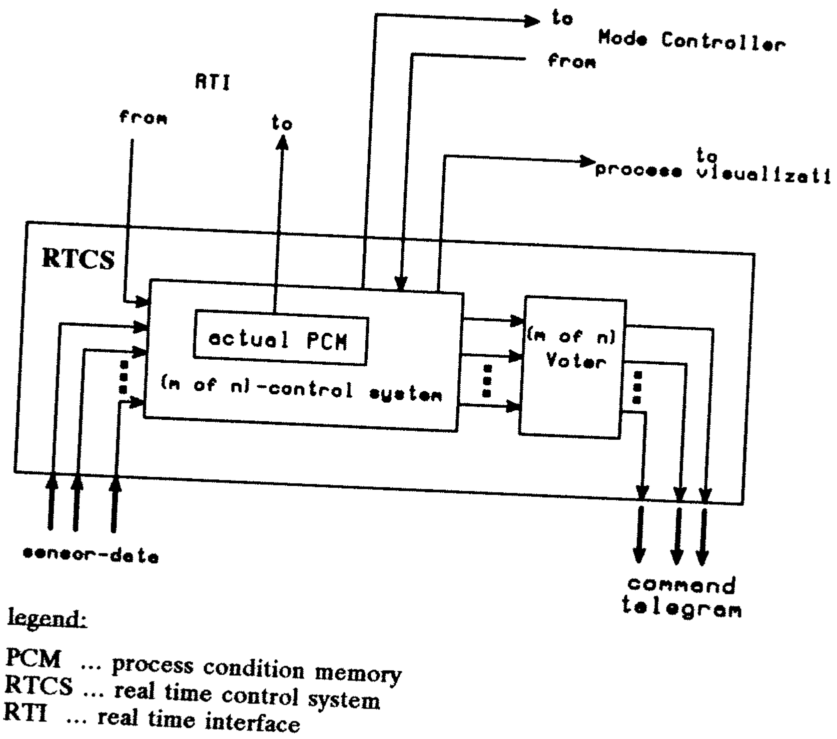
Realtime system starts running in normal condition (SCO). In case of failure or design fault system condition may change over to a dangerous system state (SC2), which means an intolerable fail condition. System condition now has to be changed over to a fail safe condition within a specified failure detection time and should remain there with a transition probability $p_{33}=1$. Because of this high sophisticated functionality such system structures have not been applied so often. Therefore, a possible application of an expert system (XPS) seems to be a great challenge to monitor vital processes. A first implementation may be found as a monitoring channel 'safety bag' /THEU 86/.

Whenever a system concept acc. to Fig. 2–1 pointed out as not to be realized because of high complexity, one tried to substitute the classic fail–safe principle by a new procedure to control the technical process instead of it. In the same way one should use an XPS as a powerful strategy within the monitoring channel (Fig. 2–3).

3. System architecture using an XPS

Acc. to figure 2-3 we should try to specify a system architecture with a monitoring channel using an XPS. Because up to now there has not been done a safety proof of an XPS, we have to design system structure using different levels of degraded modes.

Basically, we start at realtime control system (RTCS) attaching it with a data link to realtime interface (RTI), mode controller, and process visualization (fig. 3-1).



legend:

PCM ... process condition memory
RTCS ... real time control system
RTI ... real time interface

Figure 3-1 System structure of realtime control system with connections to realtime interface, mode controller and process visualization

RTCS may be an n-channelled control system connected with an (m of n)-voter generating command telegrams corresponding to process state report as an usual system control approach. The complete report of all process states may be validated physically and stored in an actual process condition memory (PCM) performing a data link to realtime interface connecting RTCS and XPS (fig 3-2). Functionality of XPS as a first approach should be restricted to hazard forecast without any system diagnostics.

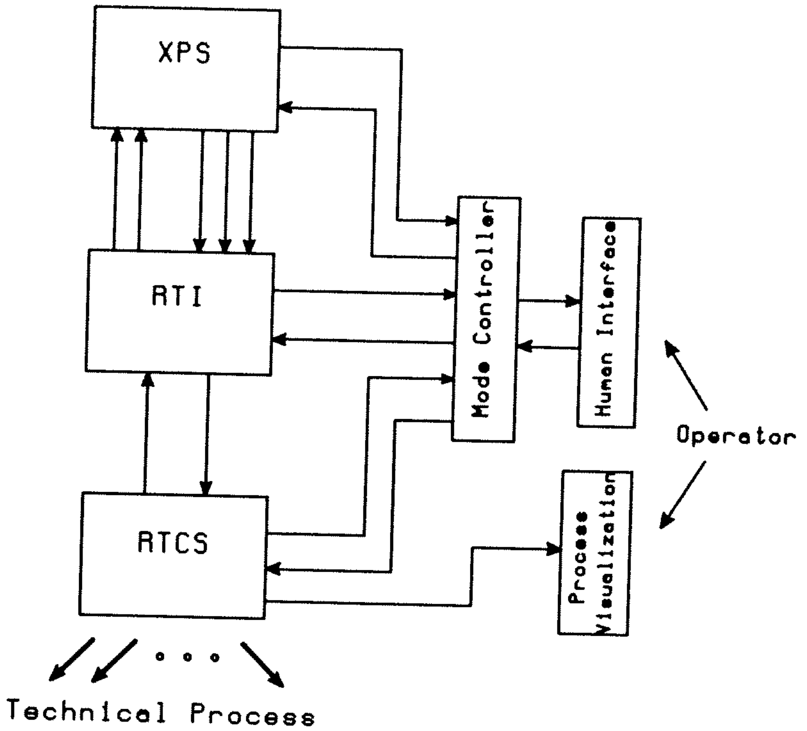


Figure 3–2 System architecture using an XPS monitoring a realtime control system

Because up to now there have not been done safety proofs for an XPS or a computer driven RTI, basic structure should provide several so–called "degraded modes". In case of failures or design faults within XPS or RTI an operator communication should be able by a human interface to change operating mode using a mode controller, so we have to define the following modes:

Normal mode: XPS generates a so–called "hazard forecast" as a computed result via human interface to system operator, who is able to compare hazard forecast with process visualization from RTCS. Human interface provides the following features:

Output: – hazard forecast

Input: – deletion of a pretended hazard reported by XPS, but classified as harmless by system operator,
– contraction or extension of deadlines,
– classification of unknown process situations,

Operator: – in case of any discrepancy between hazard forecast and process visualization switching over to first degraded mode.

First degraded mode: In this mode XPS is disconnected from process control while RTCS, RTI and human interface are still operating.

Output: – RTI generates a compressed form of process visualization containing messages of all changes since last report period on the basis of realtime data base component

Input: – Manual process control by system operator using high level commands, which are passed through processing module as a part of RTI towards RTCS,

Operator: – in case of any discrepancy between both process visualization outputs the operator should change over to second degraded mode

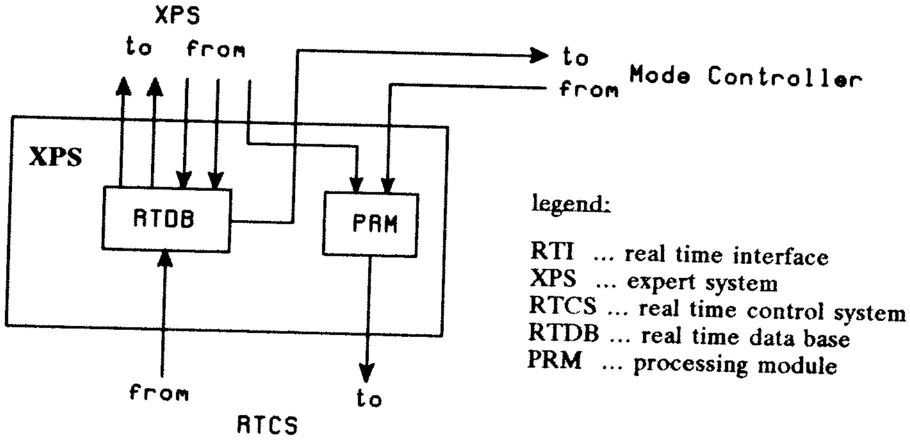
Second degraded mode: XPS and RTI are disconnected from RTCS because of suspicion of incorrect function.

Output: – Contents of actual process condition memory as a part of RTCS,

Input: – Manual process control by system operator using low level commands, which are fed to RTCS directly.

3.1 Real time interface

RTI consists of a realtime data base (RTDB) and a processing module (PRM) (fig. 3-3).



legend:

RTI ... real time interface
XPS ... expert system
RTCS ... real time control system
RTDB ... real time data base
PRM ... processing module

Figure 3-3 Realtime interface

Functionality of both components may be described as follows:

RTDB:

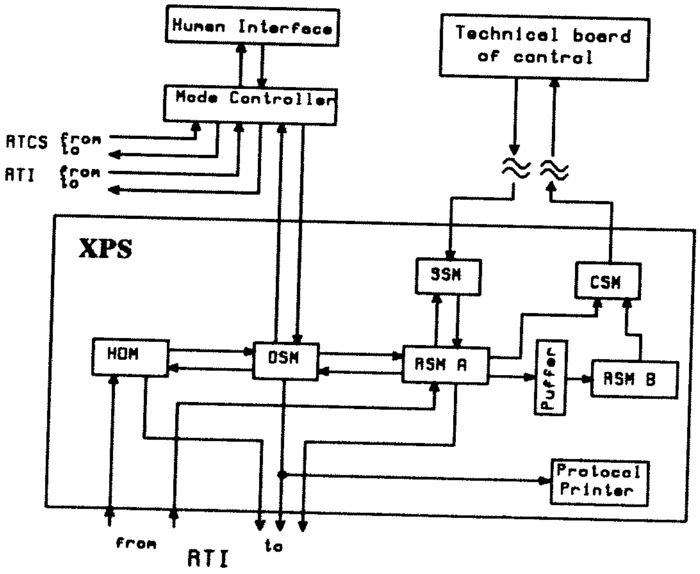
- producing a copy of process condition memory (PRM),
- calculating differences between two successive contents of PCM, deriving an event oriented message to XPS for further calculation,
- generating answers acc. to inquiries from XPS

PRM:

- compilation of high level commands generated from XPS or human interface to low level commands, which are fed to the RTCS directly.

3.2 Expert system

Figure 3-4 presents detailed structure of the used XPS.



legend:
XPS ... expert system
SSM ... standard solutions memory
CSM ... calculated solutions memory
HDM ... hazard detection module
DSM ... danger and solutions module
RSM ... resolution searching module
RTI ... real time interface

Figure 3-4 Detailled structure of XPS

The essential components of XPS are

- hazard detection module (HDM),
- danger and solutions module (DSM),

and

- resolution searching module (RSM).

Functionality of these fundamental components may be described as follows:

Hazard detection module activities: Well-known process situations have been described before real time operation in form of accompanying rules. A transmitted process situation will be checked to see, if it corresponds to one of the defined rules. If there exists a corresponding rule, reactions will be chosen and a corresponding deadline for termination will be specified. If there is no correspondence within the rule base, this process situation has to be classified as unknown and thus as a dangerous one, so that a corresponding message will be sent to DSM.

Danger and solutions module activities: HDM sends hazard messages to DSM, periodically. DSM receives messages and stores them into a kind of hash-table without collision handling; thus only those hazard message will be recognized, which are still valid. Those hazard messages, which do not exist any more, will be transmitted to system operator via human interface, who decides, if these hazard messages could be deleted or not.

The first step of managing an existing and valid hazard message is to define an actual deadline and to specify a standard fail-safe system reaction (may be any standard solution like "energy off", reaching a "safe halt condition" e.t.c). Now time processing will be started decrementing time until deadline will be reached; at the same time a message will be sent to RSM corresponding to that valid hazard to calculate an adequate problem solution. If such a problem solution could not be found within given time constraints, defined standard system reaction will be executed and documentated by a protocol printer registrating process situation, fail-safe system reaction, and execution time.

Resolution module activities: RSM A receives hazard messages from DSM. To offer a corresponding problem solution, RSM A communicates with standard solution memory (SSM) containing a kind of hash-table with validated entries as follows:

hazard ----- problem solution ----- deadline
(adequate system reaction)

Contents of SSM may be changed only by an official technical board of control via an off-line connection. To find adequate problem solutions the following procedures exist:

1. RSM A succeeds in finding an adequate system reaction as problem solution in SSM, so that standard fail-safe reaction chosen by DSM may be replaced by a "smoother" system reaction; additionally, deadline specified by DSM has to be updated. New system reaction will be sent via RTI to RTCS.

2. RSM A is not able to find a corresponding problem solution; therefore RSM A has to start separate calculations to find such a problem solution together with a new deadline.

   2.1. RSM A is able to terminate these calculations before deadline in DSM is reached, results will be written into calculated solutions memory (CSM).

   2.2. RSM A does not succeed in terminating calculations, in-between-results will be sent to an additional buffer, so that RSM B may continue calculating. A calculated problem solution is then written into CSM. The technical board of control is able, to validate additional problem solutions off-line and to update contents of SSM.

Conclusions

This paper offers a first approach on how to design a system structure for realtime applications monitored by an XPS. After introduction into safety terms a system structure with a monitoring channel is presented. The great challenge is to provide monitoring channel with facilities of an expert system. So we have to link RTCS with XPS by a special realtime interface using a realtime data base as well as a processing module. Because up to now there have not been done any safety proofs of XPS or RTI, we had to design a system structure containing additional degraded modes in case of failure or design fault. Procedures how to find problem solutions by RSM-activities are described. Presented system structure may be useful to enrich existing (m of n) - control systems with facilities of expert systems, although this system concept does no diagnostics.

REFERENCES:

/SCHI 89/ G. H. SCHILDT
On diverse programming for vital systems,
IFAC-Workshop Vienna, 1989

/FRI 78/ H. FRICKE,
G. H. SCHILDT
Conception of Safety and Realization Principles, ATRA-Conference
Indianapolis, 1978, USA

/THEU 86/ N. THEURETZBACHER
Using AI-Methods to Improve Software Safety,
IFAC-Workshop SAFECOMP 86,
Paris, p.99-105