Network of Excellence

IST-004527 ARTIST2:
Embedded Systems Design

Activity Progress Report for Year 1

JPRA-Cluster Integration:

Diagnosis in Distributed Hard Real-Time Systems

Cluster:

Hard Real-Time

Activity Leader:

Hermann Kopetz, Philipp Peti (TU Vienna)

The primary purpose of diagnostic systems is to trace failures back to the field replaceable units of the system and to decide whether the unit needs replacement (i.e. permanent fault) or can remain in the system (i.e. transient fault).

This activity will investigate to which extent methods and techniques from architecture design, statistics, contract-based design and formal methods can be combined to improve the accuracy of diagnostic mechanisms. The expected results are important from both a theoretical point of view, and also for industry which is currently facing substantial maintenance problems that result in high warranty costs and loss of customer's satisfaction. The exchange of research results of the different groups involved in this JPRA allows the exploitation of existing knowledge of different domains for solving problems in the context of diagnosis.

Table of Contents

1. Introduction

1.1 Activity Leader

Team Leader: Hermann Kopetz and Philipp Peti (TU Vienna)
Areas of their team's expertise: Time-triggered architecture, fault-tolerance, architecture design

1.2 Clusters

Hard Real-time

1.3 Policy Objective

The primary purpose of diagnostic systems is to trace failures back to the field replaceable units of the system and to decide whether the unit needs replacement (i.e. permanent fault) or can remain in the system (i.e. transient fault).

This activity will investigate to which extent methods and techniques from architecture design, statistics, contract-based design and formal methods can be combined to improve the accuracy of diagnostic mechanisms. The expected results are important from both a theoretical point of view, and also for industry which is currently facing substantial maintenance problems that result in high warranty costs and loss of customer's satisfaction. The exchange of research results of the different groups involved in this JPRA allows the exploitation of existing knowledge of different domains for solving problems in the context of diagnosis.

1.4 Industrial Sectors

Improving state-of-the-art techniques for diagnosis to achieve a better accuracy in order to reduce unnecessary component replacements is important for

- Automotive industry
- Avionics
- Rail transport

2. Overview of the Activity

2.1 Artist Participants and roles

Team Leader: Hermann Kopetz (TU Vienna)
Areas of his team's expertise: inventor of the TTA concept.

Team Leader: Alberto Ferrari (PARADES)
Areas of his team's expertise: strong interaction with automotive and hardware industries, contract-based design for diagnosis.

Team Leader: Albert Benveniste (INRIA)
Areas of his team's expertise: synchronous languages, control and statistical techniques in fault detection and diagnosis.

Team Leader: Stavros Tripakis (VERIMAG)
Areas of his team's expertise: formal methods.

2.2 Affiliated partners and Roles

Team Leader: Neeraj Suri (TU Darmstadt)
Areas of his team's expertise: diagnostic algorithms.

Team Leader: Andrea Bondavalli (University of Florence)
Areas of his team's expertise: statistical methods for diagnosis.

Team Leader: Miroslaw Malek (Humboldt-University of Berlin)
Areas of his team's expertise: diagnostic algorithms.

2.3 Starting date, and expected ending date

Starting date: September 1st, 2004

Expected ending date: December 31st, 2005

2.4 Baseline

There is a significant trend in the automotive and avionics industry to increase the number of electronic devices in order to provide a functionality that goes beyond common mechanic/hydraulic systems. The reduction of cost, increased safety and reliability, reduced complexity, and enhanced quality of control are among the primary objectives of replacing conventional subsystems with electronic ones. However, despite all the benefits it is important to state that with the increasing use of electronic devices in transportation systems the likelihood of malfunctions and thus the numbers of defective electronic components will also increase.

For example in the automotive domain on-board diagnostic solutions have originally been developed to provide simple open/short circuit and abnormal voltage level detection mechanisms. Today electronic diagnosis evolved into an integral part of every automobile. All modern cars are equipped with On-Board Diagnosis (OBD) systems (OBD-II in USA or EOBD

in Europe). OBD, originally developed to continuously monitor the emissions of a car, provides now almost complete engine diagnosis and also monitors parts of the chassis, body electronics, and the control network of the vehicle. However, the development of effective diagnostic systems has stayed behind the recent increase of electronic systems in modern cars.

One reason for the diagnostic deficiencies of modern OBD systems is the fact that diagnosis is often treated as add-on to communication systems rather than an integral part of the architecture. Consequently, the problem of the identification of faulty Electronic Control Units (ECUs) is one of the predominant challenges that need to be solved. Though the breakdown logs of the ECUs inform the service technician about detected errors within the system, they do not assist the technician adequately in the identification process. Thus, fully functional units are replaced, or even worse, faulty ECUs remain unchanged in the system. These diagnostic deficiencies will become more and more obvious when X-by-wire solutions will be subject to mass production. Since a mechanic at a service station is no specialist in automobile electronics, the diagnostic system of the car must provide all necessary information that allows maintenance of faulty components. For this reason it must be possible in modern automotive electronic architectures to trace an entry in a breakdown log back to its source. If this is not possible, as a consequence, fully operational units will be replaced by mistake.

Many deployed OBD systems analyze the internal state of a component (e.g., plausibility checks) by applying embedded assertions in the application software in order to identify component errors. Assertions are a powerful and accepted mechanism in helping in the detection of application errors. However, such assertions operate in general only on the internal state of components. The inability to trace correlated failures of the nodes of a distributed system makes diagnosis prone to misjudgement about transient faults affecting the system. These so-called cannot duplicate failures frequently result in the replacement of operational Field Replaceable Units (FRUs). As a consequence, these spurious failures have a lasting effect on the customer's trust in the product and the reputation of the manufacturer.

2.5 Technical Description

Currently, node-local diagnosis is prevalent. This diagnostic strategy, however, has the significant drawback that global information is not included into the analysis process to improve the quality of the result. Furthermore, diagnosis has not been considered as a core design driver for many of the deployed communication systems. Also in the application development process diagnosis is not always of primary concern but rather treated as an addendum. These call for:

- Architecture design that facilitates diagnosis
- Improved statistical methods to effectively discriminate between permanent and transient faults
- Formal methods for the specification and analysis of diagnostic algorithms

2.6 Organization of the report

The rest of the report is organized as follows.

Section 3 provides the activity report. The added value of having ARTIST2 with this activity is explained in this section. The funding of the reported activity is mainly ARTIST2, except that a few travels may have in some cases been supported by other sources.

Section 4 summarizes ongoing activities at the partners. This section reports ongoing research which is not funded by ARTIST2 and provided for reference.

3. Activity Progress Report

3.1 Work achieved in the first 6 months

The first meeting on diagnosis was held in Vienna and hosted by TU Vienna (December 2005). The primary motivation was to review diagnostic strategies and techniques by the various partners. In addition, an industrial advisor from TTTech was invited and contributed to the discussions. The meeting was organized in the following way:

- Detailed minutes were recorded, discussed and approved at the meeting, and enriched with additional material from some partners after the meeting. This resulted in detailed minutes that have acted as a baseline for future steps. The minutes begin with an *executive summary* that collects the main findings from this meeting.
- A number of long and detailed technical presentations were given by the academic participants. Some of the presentations gave rise to extended and intensive discussions between participants.

We collect here what we consider to be the major findings as collected in the above mentioned executive summary. ARTIST2-HRT and this JPRA must be credited for these findings.

3.1.1 Summary of research suggestions

- An important research topic is to look at diagnosis in the context of integrated architectures, since integrated architectures, as already partly deployed in avionics (Integrated Modular Avionics (IMA)), promise massive cost savings due to the multiplexing of hardware resources among different application subsystems. Furthermore, the resulting reduction of wiring and connectors results in dependability improvements. For this reason, integrated architectures are gaining more and more momentum also in the automotive domain (AUTOSAR consortium) in order to resolve the pending “one function - one control unit” problem. As part of the design of integrated system architecture, a diagnostic framework needs to be devised that in contrast to many addendum solutions deployed today allows evolving beyond “best guess maintenance”. Such a framework should support both *systemic* and *application-specific* diagnosis. While systemic diagnosis focuses on the assessment of the health status of the underlying platform (e.g., physical components, connectors), application-specific diagnosis aims at revealing application inherent faults such as software and actuator/sensor faults. By precisely defining the interface state of the applications, applications diagnosis can be handled in a generic manner outside the application functionality, as required by today’s industrial demand for intellectual property protection (i.e. no modification of the application source code). This way only the application inherent complexity must be dealt with during application development but no additional complexity is introduced by the diagnostic subsystem.
- In the control community the concerns with respect to diagnosis are mainly set on actuators, sensors. Therefore, the knowledge from the control community is complementary to the research performed by the other partners.

- Another important research topic is the use of formal techniques for improving the diagnostic capabilities of today's systems. Especially, the use of automata theory (both timed and untimed) is very promising and also linked with the issue of testing of real-time systems. In the context of real-time systems the notion of physical real-time is very important, and thus must not be neglected. Another promising research topic is the automatic synthesis of on-line diagnosers.
- In computer science threshold-based algorithms are frequently used in order to discriminate between transients and intermittent faults. A particular interesting threshold-based algorithm is the so-called α-count mechanism. The rationale for the α-count mechanism is to decide on the point in time when keeping a system component on-line is no longer beneficial. The algorithm is partly based on the observation that intermittent (transient internal) faults exhibit a relatively high occurrence rate after their first appearance. The α-count is a threshold-based fault classification mechanism designed to identify permanent faulty components from components affected by external transient faults. The main idea of the algorithm is to keep track of every fault occurrence in each component. When the α-counter value exceeds a given threshold value, the component is diagnosed as affected by a permanent/intermittent fault. Depending on the expected frequency of permanent, intermittent and transient faults the values assigned to the parameters of the algorithm are set. Naturally, all threshold-based algorithms depend on the setting on the parameters (e.g. penalty values, thresholds). The exact values of these parameters are application specific and depend on the application field, field data, and experience of the system designer.

3.1.2 Future plans

It was decided that the next meeting should address discrete event diagnosis techniques for diagnosis of platform diagnosis and investigate to which extent existing statistical techniques used in control can be used to improve the accuracy of the analysis process w.r.t. transients. In particular to which extent statistical techniques from quality control can be applied in the context of threshold-based techniques.

3.2 Work achieved in months 6-12

The second meeting was held in Grenoble and hosted by VERIMAG (May 2005). The primary purpose of this meeting was to discuss to how the findings of the first meeting have influenced the research of the partners. The meeting was organized in the following way:

- Detailed minutes were recorded, discussed and approved at the meeting. The minutes begin with an *executive summary* that collects the main findings from this meeting.
- A number of long and detailed technical presentations on preliminary results were presented. In particular, the application of newly devised methods originating from discussions during the first meeting has gained a lot of great interest among the participants.

We collect here what we consider to be the most important findings that must be credited to ARTIST2-HRT and this JPRA.

3.2.1 Updating the findings from Vienna meeting

- As direct results of the first diagnosis meeting in Vienna, the use of timed automata for the specification of diagnostic checks and analysis algorithms in the DECOS architecture has been deeply investigated. Since the DECOS architecture is built on top

of a time-triggered core network, the underlying sparse time base allows a precise definition of the execution semantics of these timed automata. So called out-of-norm assertions that combine information from the interface state of the nodes and respective applications to assess the system health state on a global level. This way, the functional and physical structure serves as an important source of information to increase the accuracy of the diagnostic services of the architecture.

- A key aspect of diagnosis is the detection of unspecified behavior and to provide sufficient information to support the identification process of the fault source, since this illegal behavior can originate form the plant, platform or the application. A promising solution is to decompose the diagnosis problem into a set of unambiguous assumptions/assertions, expressing non-functional and/or functional properties of components, to be validated at run-time. By capturing the assumptions/assertions using the Logic of Constraints (LOC) formal language, ideas from the design-by-contract methodology are applied in the context of system diagnosis. An important finding is that LOC and timed automata can express set of properties that overlap but do not coincide. Timed automata allow to model behaviour over time, hence verifying temporal properties. LOC allows expressing properties on sequences of events, whose attributes can provide information on both functional and non-functional aspects (value, time, power, etc).

- Based on the discussions of the previous meeting, it was found that the known threshold-based methods could be cast into the well-known family of statistical Page-Hinkley Tests used in statistics and quality control for years. This way the frequently heuristically settings of the parameters can be replaced by a mathematical techniques and extensions of the method can be envisioned.

3.3 Milestones

We see the executive summaries of these two meetings as providing new avenues for research. And we regard these findings as the essential contribution of this ARTIST2 cluster. In particular, the discussions have lead to the following ARTIST2 results:

- In order to improve diagnosis to tackle prevalent problems, techniques from different domains need to be combined. In particular, knowledge from architecture design, formal methods, and statistics are needed to improve current solutions. Furthermore, diagnosis needs to be included into the development process from the beginning and not treated as an addendum at the end of the design flow.

- In the context of integrated architectures such as DECOS, IMA in avionics, and AUTOSAR in the automotive domain, new possibilities for diagnosis emerge. By exploiting knowledge about the functional and physical structure of the system the accuracy can be significantly improved. In particular, by exploiting the error containment properties of time-triggered architectures (e.g. TTP, FlexRay) for diagnosis and by operating on the distributed state induced by a sparse time base, a global wide view on the health state of the distributed system can be established. Since integrated architectures overcome the “1 Function – 1 ECU” limitations by integrating multiple applications within a system component, also the detection and analysis of software faults is subject to intensive research.

- The introduction of formal methods into the field of diagnosis is considered as a very relevant and promising research topic. Of particular interest is the use of automata

theory, both in the timed and untimed case, for diagnostic purposes. The main idea is the automatic synthesis of monitors to detect faults in a given model of a real-time system. For the system model timed automata are used. In particular, in case of a distributed system a set of decentralized monitors needs to be automatically synthesized.

- By using contract-based software design for diagnosis, a reduction in the design time, design errors and possibly of application source code is expected due to elimination of manual coding of diagnostic checkers. The key idea is to separate assertions, properties that must be guaranteed by the system (component), from assumptions, properties guaranteed by the environment (interacting components). The separation between assumption/assertion allows diagnosing, during run-time, the cause of errors. The designer refines the functional behaviour of the system (component), guaranteeing the promised assertions based on the given assumptions. By applying the contract-based method, the assumptions and assertions are defined using a declarative formal language, called logic of constraints (LOC), allowing to express both performance and functional constraints and to automatically synthesize run-time checkers. The proposed contract-based design method applied at component level provides additional information to isolate, run-time, faulty components, therefore fulfilling industrial needs for system diagnosis.

- During and between meeting discussions, it was found that the known threshold-based methods (e.g., alpha-counter algorithm) could be cast into the well-known family of statistical *Page-Hinkley Tests* used in quality control for years. These tests are based on a solid mathematical foundation and not based on heuristics that are typically applied in case of threshold-based analysis techniques.

3.4 Main Funding

Here we do not refer to the support needed to cover research activities that are ongoing at partners, but only to the support needed to perform the activities reported above. Corresponding main sources of funding are ARTIST2-HRT and other cluster's funds to support for participation to the various meetings and inviting affiliate partners.

Other funds than just travel used by partners correspond to the meeting preparation, contribution to the meeting minutes, and preparation of the material presented at the meetings.

In this JPRA we had a specific problem with the support of affiliate partners, which was considered by them not sufficient and inconvenient. Given the NoE rules, we were not able to set the problem and this had an impact on the involvement of these affiliate partners.

3.5 Indicators for Integration

We see the above results as a clear proof of team work. We think that:

- *The above results could not have been obtained by just standard interaction by attending conferences*. Face to face discussions in conferences and other usual meetings are typically much thinner in focus and less structured regarding dissemination effect.
- *The above results are different from the ones obtained in research projects, including other types of EU projects*. We do not see, e.g., STREPS or IPs spending such a large percentage of their effort in seeking for new research directions.

3.6 Evolution

The reader is referred to the next 18-month work plan for this point.

3.7 Interaction, Building Excellence between Partners

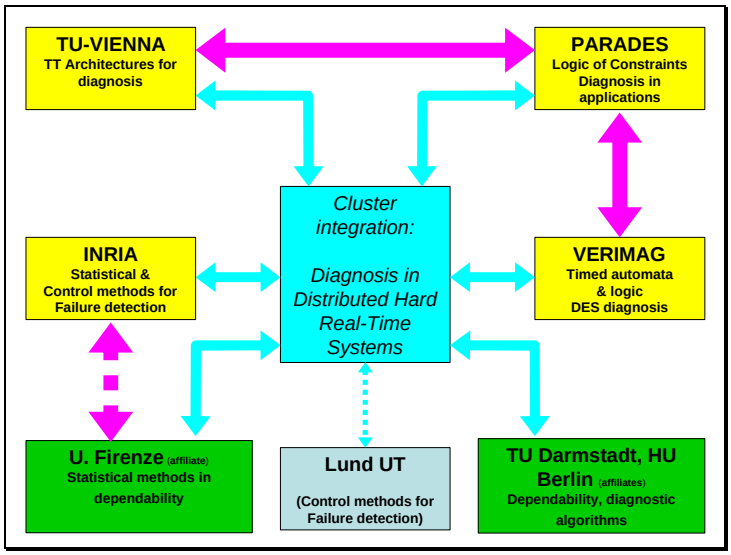
Two meetings have been held gathering industrials and academics, one in Vienna (December 2004) and Grenoble (May 2005) which have allowed discussing needs and possible solutions.

The 1st meeting in Vienna helped discovering and setting the landscape. For the 2nd meeting in Grenoble, Alberto Ferrari (PARADES) and Stavros Tripakis (Verimag) tightly coordinated for preparing their presentations. Qinghua Zhang (INRIA) submitted for reactions and comments its slides to Andrea Bondavalli, who found the discovery of the link between threshold-based methods and Page-Hinkley tests intriguing.

The exchange of information on diagnostic solutions from the groups with different backgrounds (e.g. statistics, architecture design, formal methods) has resulted in a better understanding of the main diagnostic problems that need to be solved. The industrial contacts of the respective partners have significantly contributed to ensure that not only scientific but also topics of industrial relevance are addressed within this work package.

Furthermore, synergies between the partners could be identified and cooperation on important research areas established. The close information exchange between the DECOS IP and ARTIST2 NoE has lead to improvement of the quality of the work in both projects.

The interaction between partners is summarized in the following figure:



In this figure, we indicate the special skills of the different partners, in the way they contributed to the cluster integration (in cyan). The magenta arrows indicate the new point-to-point interactions that resulted from the JPRA's activity – Lund University, from the Control cluster attended the 1st meeting in Vienna. The dashed magenta arrow indicates the interaction that suffered from the funding problem with affiliates.

We cannot mention any joint paper, for the following reasons: the subject for interaction within this JPRA was completely new to the participants. Therefore, the 18 month period of time would not have been enough for any joint paper to be prepared.

3.8 Spreading Excellence

The tight cooperation between academic and industrial partners allows solutions to quickly spread toward end-users via the industrial marketing services. This is the case of Verimag and Esterel, PARADES and ETAS, as well as TU Vienna and TTTech. In addition, the results have been presented in the course of other projects (both on European and national level) to other industrial partners such as AUDI, Fiat, and Airbus.

The cluster activity has been presented by PARADES to ETAS and Magneti Marelli S.p.A, respectively a tool supplier and a tier 1 supplier for automotive, COMAU, a supplier of industrial automation systems, OTIS and Chubb Securite', companies suppling systems for building automation, and STMicroelectronics, a supplier of silicon and system-on-chip.

The following affiliate partners have been supported by ARTIST2 mobility money for their participation to the JPRA meetings:

- TTTech Computertechnik AG: James Sippl (control eng., architectures & TT)
- University of Firenze: Andrea Bondavalli (fault tolerance, modeling & evaluation)
- Humboldt-University Berlin: Miroslaw Malek (dependable distributed/embedded systems)
- TU Darmstadt: Neeraj Suri (distributed systems & protocols, fault tolerance)

4. Detailed Technical View

In this section we gather general remarks on the topic. The below mentioned research cannot be acknowledged to ARTIST2 and is entirely funded by other means.

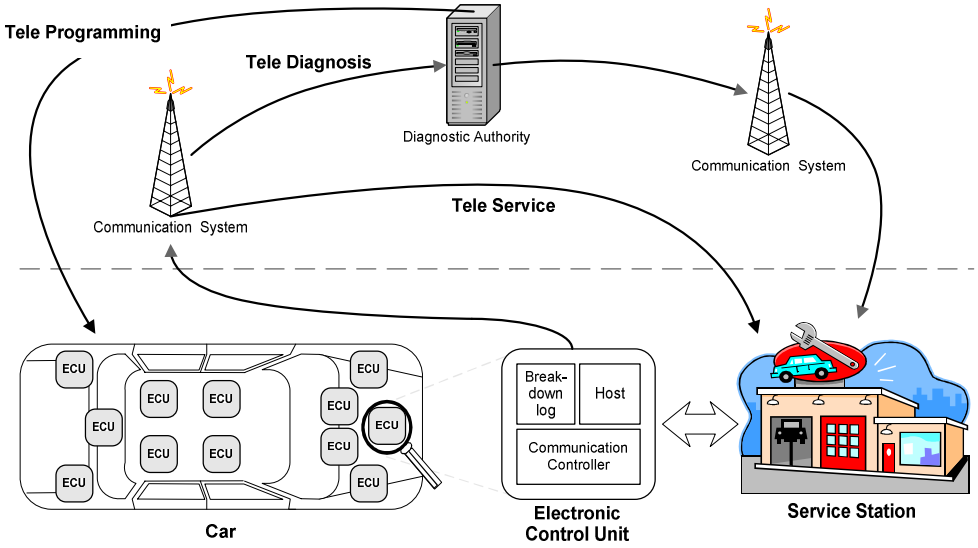
4.1 Brief State of the Art

In the following we provide a short overview on automotive and avionic diagnosis and maintenance strategies.

4.1.1 Automotive Diagnosis and Maintenance

Figure 4-1 shows the diagnostic infrastructure of today. Each ECU deployed in a car typically has a diagnostic subsystem that analyzes the functionality of the constituting parts (e.g., via Built-In Self Test (BIST)) or performs application specific plausibility checks, i.e. assertions, to detect errors.

Once the OBD system of the car detects a violation of the specification of an ECU, a breakdown log entry is written, and in case of a high severity, the driver is informed via the Malfunction Indicator Light (MIL). In case of an error, current diagnostic systems provide a so called freeze frame function that records the condition of the vehicle when a failure occurs. The freeze frame provides important information for the failure cause analysis. The breakdown-log typically stores data on the type of fault, the state of the system, the priority, the environmental conditions, a timestamp, and information on the mileage of the car. Depending on the type of inspection (e.g., garage, factory inspection, development) different parts of the breakdown log entry are analyzed.



information on the failure, for example an 8 bit value describing prevalent faults. Based on this information the mechanic must be able to decide which part of the system caused the failure and needs to be replaced to restore full functionality.

The dashed line in Figure 4-1 indicates the cut between current available technology and advanced services that are subject of current research. Future trends like tele-diagnosis, tele-service and tele-programming offer new possibilities in the collection of diagnostic information and customer service. The ultimate goal is to shorten the delay between the occurrence of a failure and the definition of corrective action.

Tele-service is used to automatically inform the dealer about wearout and tear of the car via a telephone network (GSM, UMTS). The service call is then inspected by the service advisor who supervises the needed services, checks the availability of the parts to be replaced and makes the necessary appointments. The vision of tele-diagnosis is to send detailed diagnostic information of the car to a diagnostic authority that processes and analyzes the collected data. Thus not only malfunctions of components are reported (like OBD) but also valuable information of data from vehicles on the road can be collected and analyzed in order to enhance diagnostic procedures. However, data privacy issues have to be clarified by the legislator.

Role of Diagnosis

Three related diagnostic tasks can be identified in advanced automotive system, namely fault detection, identification of faulty Fault Containment Regions (FCRs) and fault identification within a FCR, which will be discussed in the following.

Failure Detection. Failure detection is the identification of a deviation of the provided service from the intended specification of a component of the system. Failure detection is the minimal function that any OBD system of a vehicle must perform. One of the most important parameters in the design of failure detection is the sensitivity of the analysis algorithms. By designing the algorithms too sensitive the likelihood of faulty classification of operational components will increase significantly. Unnecessary MIL activations will have a lasting effect on the user's trust into his car. For this reason setting the scope of the analysis parameters is a trade-off between the frequency of faulty detection and detection of faulty nodes. During the factory inspection process the situation is different. The required level of diagnosis is far more sensitive than the diagnostics functions adopted for market conditions.

Identification of faulty FCRs. This service of a diagnostic system provides a determination of the exact location of the fault within the system, i.e. which FCR deviates from its intended function. Recent studies provide some interesting numbers that underpin the current problems of diagnostic services in automotive communication systems. In more than 20% of MIL activations, the OBD did not provide sufficient data to identify a root cause and were dismissed as No Fault Found (NFF). Furthermore Original Equipment Manufacturer (OEM) studies show alarmingly high rates of incorrect initial diagnosis of electrical problems, in some cases exceeding 50%. This figure points out the lack of current communication systems to provide assistance in the fault isolation process. As a consequence the car repairman chooses the simplest solution and changes all components that can be responsible for the malfunction. This procedure of throwing away operational components dramatically increases the costs of a car either for the user (costs of ownership) or the manufacturer (warranty repair costs).

Fault Identification within the FCR. After the faulty FCR within the system has been identified, the fault identification process classifies the fault and determines the root cause. Fault identification is mostly an offline activity due to high complexity and effort required. In automotive applications fault identification is typically applied to returned parts or for warranty analysis by the OEM. Studies of the ECUs used in automotive applications underpin the so-called Pareto-principle, i.e. a phenomenon that can have many theoretical causes has in reality

only a few. Recent studies show that the components with the highest failure rate are Printed Circuit Boards (PCBs) and micro-controllers followed by analog ICs and ASICs (the higher the integration, the more likely the component is subject to fail). Resistors, transistors and diodes have the lowest failure rates.

4.1.2 Avionic Diagnosis and Maintenance

In order to reduce “best guess, shotgun maintenance” in avionics, aircraft manufacturers provide on-board maintenance solutions following the design guidelines of documents like ARINC 624. According to recent studies approximately 50% of all equipment removals are reported as NFF, i.e. electronic equipment removed from an aircraft during maintenance troubleshooting, which, when returned to the manufacturer, is tested and found to work correctly.

ARINC 624

As for any diagnosis and maintenance system, ARINC 624 emphasizes that unreliable diagnosis is worse than no diagnosis. ARINC 624 provides design guidelines for an Onboard-Maintenance System (OMS) for state-of-the-art aircrafts. Thereby, the main objectives of an OMS are to serve as the tool for consolidation and correlation of all Built-In Test Equipment (BITE) results for centralized access and display:

- Cost-effective and user friendly means of airplane maintenance
- Reduction of shotgun maintenance
- Simplification of maintenance procedures
- Elimination/reduction of ground support equipment
- Provision of an Airplane Condition Monitoring System (ACMS) for the monitoring of performance trends

A key aspect of ARINC 624 is the reduction of efforts required by maintenance personal by automating ground tests and minimizing the need for operator interactions. To ease maintenance, the OMS should also provide an overview about the installed Line Replaceable Units (LRUs) onboard the aircraft. Furthermore, the OMS allows ground personal to correlate reported system anomalies by the aircraft crew with BITE records in the system. For this reason, for each entry in the database contextual information is stored, such as

- Failure indication or flight deck effect, if any
- Flight phase and flight leg
- Time and date
- Flight number and city pair or route number
- Airplane identification
- Airplane flight parameters to support the pilot report and/or troubleshooting, e.g., altitude, airspeed etc.

Since airlines typically require large amounts of maintenance documentation, the OMS should provide an interface to allow accessing an electronic library system. This way the maintenance engineer has access to relevant information for maintenance activities for each deployed LRU onboard an aircraft.

Airplane Condition Monitoring System (ACMS). As part of the OMS, the Airplane Condition Monitoring System (ACMS) monitors and records selected airplane data related to aircraft maintenance, performance, and troubleshooting. The main goal of the ACMS is the detection and analysis of potential malfunctions (cf. CBM) in order to allow timely maintenance actions resulting in quick turn-around of the aircraft.

The ACMS is required to collect data over a specified period of time referenced to a specific event. This way trend reports can be generated for either engineering feedback or anomaly analysis. Another fundamental function of the ACMS is also providing access to the current health status of fault-tolerant subsystems (e.g., the fly-by-wire system) of the aircraft. This way the redundancy status can be assessed by the service technicians, and maintenance activities scheduled before the minimum redundancy level is reached.

Scrubbing Techniques. Since fly-by-wire applications require ultra-high dependability fault-tolerant strategies need to be utilized that enable the continued operation of the system in the presence of component failures. So-called “scrubbing-techniques” are used to validate the functionality of fault-tolerance mechanisms in specified time intervals. Figure 4-2 illustrates the basic concept of this approach. The reliability of electronics components decreases with time. At time t_0 the component is assumed to be fully functional. At time t_1 the proper function of fault-tolerance mechanisms is validated again and therefore the component is supposed to have the same reliability as at instant t_0. The likelihood of undetected components that are stuck at-good-failure, i.e. the component works as specified as long as no failure occurs, depends on the time interval $?_s$. Scrubbing is closely related to CBM techniques. However, the system is tested in a special maintenance mode and never in operational mode. Intentionally generated faults are used to examine the specified behavior of all components in the case of a malfunction.

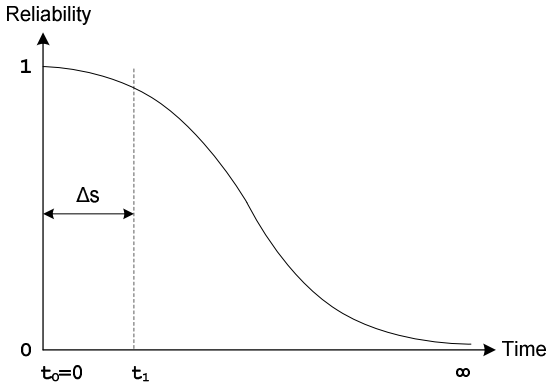


Figure 4-2: Scrubbing Techniques

4.2 Industrial Needs and Experience

What is required by industry in distributed embedded systems is a diagnostic subsystem with detection mechanisms focussing on transient failures. In particular, from a maintenance perspective, the most important diagnostic objective is the discrimination between transient failures induced from external and internal faults to put an end to unnecessary component replacements.

- **Improved Accuracy of Diagnosis**: Currently, industry has significant problems detecting and identifying electronic devices that cause system failures in electronic systems. This so called Trouble Not Identified (TNI) phenomenon is an increasing problem in automotive and avionic electronics with major economic implications. The lack of information provided by currently deployed OBD systems often results in unnecessary replacements of working components.
- **Advanced Maintenance Strategies**: In both avionics and in the automotive domain manufacturers envisage a shift from traditional corrective to preventive maintenance strategies to reduce costs and to provide optimal availability of the systems. As a prerequisite for the realization of preventive maintenance strategies, diagnostic mechanism are needed to judge about the health status of each replaceable part of the system. In order to adopt CBM for electronic systems suitable indicators for degradation or wearout must be identified and analyzed to detect deviations from sound operation.
- **Service Technician Assistance**: Diagnostic deficiencies of deployed architectures complicate the job of the service technician to remove only those components that are causing the system malfunction. Since a mechanic at a service station is no specialist in electronics, the diagnostic system must provide all necessary information that allows maintenance of faulty components.
- **Assessment of Fault-Tolerance Mechanisms:** Fault-tolerance mechanisms are required to achieve the necessary degree of dependability for the deployment of electronic systems in safety-critical environments. Consequently, architectural diagnostic services need to monitor the health state of the fault-tolerance mechanisms. Furthermore, the diagnostic subsystem must provide means to support the inspection of fault-tolerance mechanisms – also known as scrubbing techniques – to validate the functionality of fault-tolerance mechanisms in specified time intervals.

4.3 Ongoing Work in the Partner Institutions

- At INRIA statistical methods for intermittent fault monitoring are investigated. Based on the interactions with affiliate A. Bondavalli on threshold algorithms, similarities between well-known threshold algorithms and statistical tests have been discovered. The main observation is that intermittent faults have random behavior and therefore the change searched for is a change on statistical behavior, not the occurrence of a deterministic property. Ongoing research on this topic has revealed that a version of the alpha-count algorithms using two thresholds is known in the statistical community under the name of the Page-Hinkley test. INRIA focuses on how statistical methods can improve the discrimination between transient and intermittent faults.
- Verimag has a strong background in formal methods and investigates to what extent formal methods can be applied to improve the capabilities of today's diagnostic systems. Of particular interest is the use of automata theory, both in the timed and untimed case, for diagnostic purposes. The main idea is the automatic synthesis of monitors to detect faults in a given model of a real-time system. For the system model timed automata are used. In particular, in case of a distributed system a set of decentralized monitors needs to be automatically synthesized. In addition, Vermiag's relationship with Airbus strongly influences the work package. Therefore, at Verimag research on diagnosis for loosely time-triggered architectures is ongoing work.
- PARADES as a strong interest in rigorous design methodologies for real-time distributed embedded systems. The definition of system (component) properties with formal methods (e.g. logic of constraints) allows to unambiguously define aspects of the *expected* behaviour of the system (component) and its environment (other

components). These properties can be separated in assumptions, guarateed by the environment (other components) and typically exploited during the design, and assertions, guaranteed by the system (components) if the related assumptions hold. By checking assumptions and assertions separately at run-time, the cause of error can be diagnosed during system operation. The checked the properties can refere to functional and non-functional aspects of the system, The investigated logic of constraints (LoC) allows to express properties involving both functional and performance aspects. The on going research activities aim at investigating formal models and languages to express properties on both functional and non functional aspects, proving the effectiveness of the proposed methods in the automotive (in relation to AUTOSAR) and industrial automation domain, evaluating standard constraint languages for properties specification and extending the methods to diagnose hardware components. The logic of constraints (LoC) is one of the candidates among the possible formal languages and is the subject of the current on going work.

- TU Vienna looks at diagnosis in the context of integrated architectures such as IMA in avionics and AUTOSAR in the automotive domain. In particular, TU Vienna investigates the benefits of using a time-triggered core architecture with respect to diagnosis and maintenance. Thereby, the error containment properties of time-triggered architectures (e.g. TTP, FlexRay) allow for an improvement of the accuracy of the diagnostic algorithms. By operating on the distributed state induced by a sparse time base, a global wide view on the health state of the distributed system can be established. Since integrated architectures overcome the “1 Function – 1 ECU” limitations by integrating multiple applications within a system component, also the detection and analysis of software faults is subject to intensive research. Together with TU Darmstadt as, as an affiliate to ARTIST2, emphasis is set to provide architectural services for the detection, dissemination and analysis of diagnostic information within the integrated time-triggered DECOS architecture.

4.4 Main Funding (not ARTIST2)

Main sources of funding include (the list below is not comprehensive):

- DECOS IP
- Austrian Advanced Automotive Technology Project
- In-house INRIA funding (team resources, no specific funding)