15th Triennial World Congress, Barcelona, Spain

# MAGIC – IFATIS: EC-Research Projects

**Birgit Köppen-Seliger, Steven X. Ding and Paul M. Frank**

*Gerhard-Mercator Universität Duisburg, Institute for Automatic Control,*
*Bismarckstr. 81 BB, D-47048 Duisburg,*
*koeppen-seliger@uni-duisburg.de*

Abstract: In this contribution two European research projects funded by the European Commission in the framework of the IST programme are introduced. The goal is to present the basic ideas and concepts of the projects " Multi-Agents-based Diagnostic Data Acquisition and Management in Complex Systems (MAGIC)" and "Intelligent Fault Tolerant Control in Integrated Systems (IFATIS)" which both aim at the solution of diagnostic problems but in different respects. While MAGIC is based on a multi-agents-based architecture which integrates all levels in a diagnostic scheme, IFATIS deals with hierarchically structured fault-tolerant control for integrated systems. A wide range of industrial applications is expected for both projects. *Copyright © 2002 IFAC*

Keywords: Fault diagnosis, Fault tolerance, Decision support systems, Complex systems, Intelligent knowledge-based systems, Agents.

## 1. INTRODUCTION

The increasing demands for higher system performance, product quality, productivity and cost efficiency lead to a continuous growth of the complexity and automation degree of technical processes. The rapid development of microsystems, information and communication technologies further makes it possible to integrate more and more sensors, actuators, control loops, computing units and standardised bus systems in the control system. Typical instances of such kind of complex and distributed systems are sophisticated vehicles, civil aircraft, environment treatment processes, large fleets and infrastructures etc. Associated with these development trends, high reliability, availability and safety become an important system requirement which is included in many international standards and regulations.

Besides of enhancing the quality and robustness of process components, using hardware redundancy is a traditional way to improve the process reliability and availability, which has been extended to the use of software redundancy during the last decade. Due to the fixed structure and high demands for hardware and software resources, the application of redundancies strategy is usually limited to some special technical processes or to the part of key system components like the central computing system or the bus system. Evidently more flexible and effective are the fault tolerant (FT) strategies with fault accommodation or system and/or controller reconfiguration. In an FTC system, an early fault detection and isolation (FDI) and an effective fault diagnosis play a key role.

While the complexity of technical systems rapidly increases and the trends show a high integration of different types of sub-systems and various technologies in technical processes, the research of FDI/FTC technologies in the last ten years is marked by the development of methods and tools, which solve FDI and FTC problems for a certain type of systems and are usually developed based on some technology or on the integration of different technologies and schemes to a low degree. To increase FDI/FTC performance and to meet high requirements, individual methods will be continuously improved and optimised, which means in turn that these methods almost reach their limit. It is therefore reasonable to expect that a significant improvement of FDI/FTC system performance can only be achieved when FDI/FTC problems are dealt and solved in a framework of integrated use of different FDI/FTC technologies from the integrated viewpoint of sub-systems and system components.

The need for know-how and competence in different technical disciplines and in dealing with different types of systems on the one side, and the limited research and development funding for such activities at national level on the other side, make the realisation of this idea however much difficult. A joint research by research groups with different scientific and technical backgrounds promises a potential solution for this problem. The European Community has added advanced control technology and fault tolerant control in complex system in its current call of the IST programme to promote such joint research.

In this contribution, we are going to present two EC-research projects in the field of FDI and FTC, Multi-Agents-based Diagnostic Data Acquisition and Management in Complex Systems (MAGIC) and Intelligent Fault Tolerant Control in Integrated Systems (IFATIS). Both of them are funded in the IST programme of the European Community. Although both projects are of evidently different objectives, they are common in a) Europe-wide participation b) participants with different scientific, technical backgrounds and competence c) Development of new FDI/FTC technologies on the basis of an integrated technology and tools from different technical and technologic disciplines.

## 2. MAGIC

### *2.1 Basic concept.*

The overall objective of diagnostic and data management schemes is to increase the performance, reliability, availability and safety of complex systems like industrial processes, sophisticated vehicles and machines, large fleets and infrastructures by providing a real-time architecture which is able to diagnose abnormal and faulty conditions. An architecture based on a multi-agents concept, in which the agents besides the diagnosis task itself perform tasks like data and knowledge acquisition and management, choice of diagnostic tools, decision conflict resolution as well as documentation and operator information, is presented in the following. In this context “agents” are software components, running on the same or separate computer platforms, co-operating with each other, having each a specific task, like acquiring and monitoring data, processing and diagnosing, etc. They form an architecture of functionally, semantically and spatially distributed elements, forming an integrated expandable (modular) whole system (Knapik and Johnson 1998).

Due to increasing demands for higher performance and quality on the one side and more cost efficiency on the other side, the complexity and automation degree of technical processes are continuously growing. Associated with this is an increased demand for more safety, reliability and availability. A traditional way to improve the process safety, reliability and availability is to enhance the quality and robustness of each process component. Nevertheless, it is not possible to guarantee a fault-free process operation. Process monitoring and fault diagnosis are hence becoming an ingredient of a modern automatic control system and are often made mandatory by authorities (Frank 1990, Frank 1991, Isermann 1994, Gertler 1998).

One of the main goals of MAGIC is the on-line detection and diagnosis of incipient or slowly developing faults in complex systems. By detecting faults before they fully develop, the operator can plan his plant operation or the automatic control system can be reconfigured to compensate for the fault. Thereby not only continuation of production can be achieved but also constant product quality can be ensured. The early identification of potentially faulty conditions provides the key information for the application of predictive maintenance regimes. Thus repair or replacement may be scheduled in a convenient production window. As a result, plant downtime is minimised, plant production maintained, and the use of maintenance personnel optimised, thereby maximising plant availability and efficiency (Aström et al. 2000). In this respect the MAGIC tool will be of great use for maintenance and process engineers.

Today's industrial plants are complex and in order to achieve efficient and safe operation modern automatic control schemes are required. The current role of the plant's operator is that of a system supervisor responsible for strategic control decisions to maintain the plant within a safe and efficient operating state. In the event of a developing abnormal situation, the operator is often overwhelmed by a mass of low level information often several stages away from the original source of the faulty component. This information requires rapid assimilation to allow a potentially dangerous plant's state to be diagnosed and the incipient faults to be located. This demonstrates the necessity of an operator support tool to assist him in his data and information interpretation. The aim of MAGIC in this respect is to provide the plant operator with clear, as detailed as necessary and easily comprehensible information about the cause of the abnormal plant condition and to suggest appropriate remedy actions or controller reconfiguration.

### *2.2 MAGIC architecture.*

The planned distributed architecture for MAGIC is based on a Multi-Agents-Multi-Level (MAML) concept as depicted in Fig. 1. The idea is that the task of the complex embedded system's diagnosis and operator support is distributed over a number of intelligent agents which perform their individual tasks nearly autonomously and communicate via the MAGIC architecture.

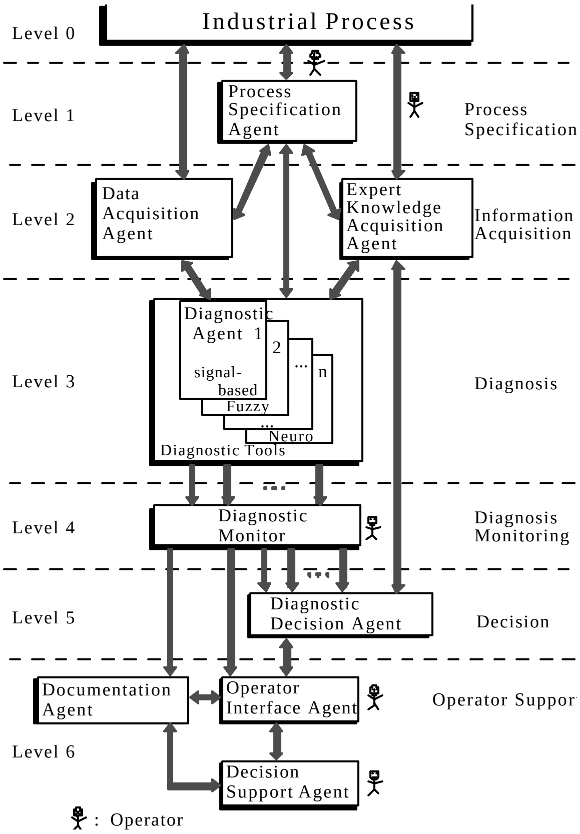


Fig. 1. Multi-Agents-Multi-Layer (MAML) Concept

Referring to the MAML-Concept in Fig. 1 the different agents in MAGIC would have the following tasks:

**Level 1: Process Specification**

*Process Specification Agent:* Communicates with the operator and the industrial process in order to specify the process (or component of the process) as a certain type within a certain class. Triggers data and knowledge acquisition agents to what type of data and expert knowledge may be available and should be collected from the process. Makes decision on the choice of diagnostic tools depending on its process characterisation. Operator involvement is necessary on that level.

**Level 2: Information Acquisition**

*Data Acquisition Agent*: Collects process data relevant for chosen diagnostic tools depending on process specification.

*Expert Knowledge Acquisition Agent*: Collects expert knowledge about the process relevant for chosen diagnostic tools depending on process specification. Operator involvement is necessary here as well.

**Level 3: Diagnosis**

*Diagnostic Agents*: Depending on the process specifications a set of different diagnostic tools implemented as different diagnostic agents will be applied, performing their individual fault diagnosis algorithm. The methods to be employed will be classical signal-based techniques such as statistical methods, knowledge-based techniques such as causal graphs as well as model-based approaches. These will include analytical models (where available) employing identification tools and data-based models employing modern tools such as neural networks, fuzzy logic and genetic algorithms (Köppen-Seliger and Frank 1996, Marcu et al. 1999).

**Level 4: Diagnosis Monitoring**

*Diagnostic Monitor*: Collects and displays all diagnostic information from the different Diagnostic Agents. No evaluation is performed yet. Operator *may* use it for additional information.

**Level 5: Decision**

*Diagnostic Decision Agent*: Evaluates the output of the different Diagnostic Agents with the goal of an as clear as possible decision on the cause of the abnormal or faulty process condition. Resolution of conflicting diagnostic results will be realised (Evsukoff et al. 1999).

**Level 6: Operator Support**

*Documentation Agent*: Documents the Diagnostic Monitor and the suggestions of the Operator Interface Agent as well as the resulting actions of the Decision Support Agent.

*Operator Interface Agent*: Diagnostic decision and alarm display together with causal graph visualisation.

*Decision Support Agent*: Operator supporting suggestions towards recovery or emergency actions, maintenance schedule, automatic or operator driven process/controller reconfiguration or accommo-dation.

In general this MAGIC tool can be applied and implemented in any industrial sector where diagnostic data acquisition and management is necessary to ensure a reliable and safe performance of complex technical processes. Application areas range from steel and automotive industry over chemical plants, nuclear reactors, power plants and mass transports systems, e.g. in the railways, naval and aviation industries. The basic requirement for such an implementation is the availability of adequate historical measurement data as well as analytical and/or expert knowledge to feed the diagnostic tools as described above.

The final goal for a practical prototype implementation is the customisation to a process of a rolling mill plant, which is of high complexity exhibiting slowly developing faulty conditions of multiple causes with costly consequences. These processes therefore represent a challenging application for MAGIC.

### *2.3 MAGIC communication infrastructure and agents.*

All agents to be implemented in MAGIC will have a similar structure. This allows to reuse already developed software components. Each agent will consist of the following parts:

**Communication Interface**: Each agent has to be implemented with the same interface to make it able to communicate with all other agents within the MAGIC infrastructure. It has to be investigated which technology will be most suitable to realise the exchange of information between agents.

**Communication Wrapper**: This software part will be responsible for storing the received data, for following the communication protocol and for pre-processing the information. This part will be unique for all agents.

**Agent Brain**: Depending on the type of the agent, different brains have to be developed to perform the specific tasks like data acquisition, diagnosis or process specification. For a new agent of a different application, a new instance of this brain has to be built.

**Interface to legacy software**: The connection to legacy software components will be realised by this part of the agent. For each legacy software that will be integrated into MAGIC, an interface to the agents brain has to be created.

## 3. IFATIS

### *3.1 Objectives and basic idea*

The objective of IFATIS is to establish a framework of intelligent fault tolerant control (IFTC) technology, to develop a novel methodology and a software tool for designing real time, hierarchically structured multilevel FTC systems, to design and construct a platform (hardware and software) for the implementation of the developed IFTC system and to apply the achieved results to different technical processes. This project will contribute to the overall goal of increasing the system reliability and dependability to meet the high performance, availability and safety requirements on complex control systems, which is of high nonlinearity and uncertainty, and in which numerous control loops, sensors, actuators, computing units are integrated and networked by bus systems.

Due to significantly different functions and working principles, problems related to the reconfiguration of the control system and the platform, on which the control algorithms and further signal and data processing are running, are generally considered in two different contexts and, as a result, different strategies have been developed. From the functional viewpoint, a control system is generally understood as a composition of controllers, sensors as well as actuators together with the controlled system (plant) in an open or a closed-loop structure. The development in this area is focusing on the software redundance based FDI and FTC (Blanke et al. 2000, Noura et al. 2000, Patton 1997, Rauch 1995, Wu and Chen 1996, Wu and Zhou 2000, Zhou 2000).

In a process control system, the platform for the implementation of control algorithms, signal and data processing consists of computers (hardware and software) and bus systems for the data transmission and communications among the different system parts. To achieve fault tolerance, much research attention in this area has been devoted to the design of computer architecture with selected redundancy of components, to the fault tolerance of the software (Halang et al. 2000). In addition, application of artificial intelligence to fault diagnosis and fault tolerance is state of the art in the computer science.

The rapid extension of control systems, from a single control loop implemented on a single microprocessor to distributed control systems with integration of control loops, sensors, actuators on a platform with networked computer systems, reveals the limitation of the existing FTC methods. They have been developed from the viewpoint of single system structure, and FDI as well as FT problems of the control system and its technical platform are considered separately. A new technology for an integrated design of the FTC system together with its implementation platform (hardware, software and bus systems) is desired, both from the practical and theoretical viewpoints.

### *3.2 Outline of major tasks*

One of the main goals of this project is to **design a real time, hierarchically structured FTC system** as depicted in Fig.2, in which integrated FDI and FTC in the control system and its platform are realised.

The basic building block at the 1st level is called fault tolerant control cell. The main components of an FTC cell are - control system, -monitoring system and -reconfiguration system. The control system receives as inputs raw data, and/or reference signals from the upper level, as well as commands regarding reconfiguration. It generates manipulated variables and/or control signals. Its aim is to achieve specified

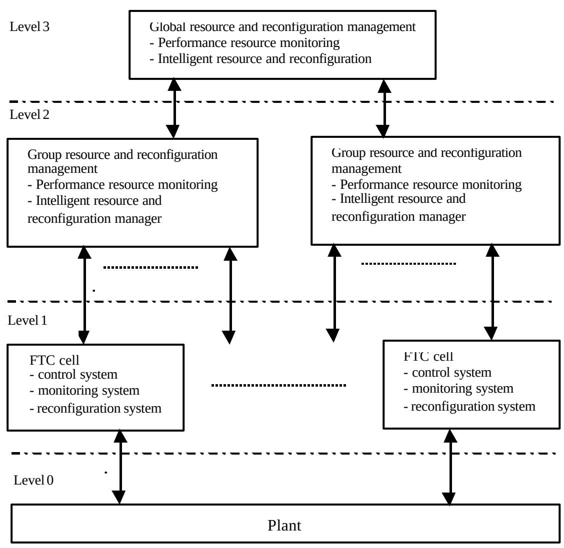


Fig. 2. Hierarchical structure of FTC system

performance objectives in terms of tracking, disturbance rejection, robustness w.r.t. modelling uncertainties, or objectives like average energy consumption or average operating costs etc. The control action can consist of closed-loop feedback or open-loop action.

The monitoring system determines the state of the component or the sub-system it supervises. The diagnostic results and information of the state of the sub-system should indicate the most likely faults and the degree of confidence in the result, as well as possible fault signal estimates and evaluation of the actual system performance. The monitoring system also determines availability of processors on which the control system is running.

When the monitoring systems report the occurrence of faults, the reconfiguration system decides, either to accommodate these faults or to perform controller and/or hardware reconfiguration, which might imply graceful performance degradation, or in case of severe faults to put the concerned component or process in a safe mode. In all cases, reconfiguration results are transmitted to the controllers which are influenced by the reconfiguration action and to the blocks at the higher level. The decision on the type of action taken by the reconfiguration system is based on the evaluation of the actual system performance provided by the monitoring system, and on the need to assure an adequate transient behaviour upon reconfiguration.

At the $2^{nd}$ and the $3^{rd}$ level, group and global resource and reconfiguration management are carried out. Different from the conventional FTC strategies, parts or aggregates of the plant, controllers, sensors and actuators, processing and communication resources including processors, memory, communication bus systems, power supply for these parts are considered as system resources. Occurrence of faults means a loss of a part of system resources and reconfiguration the (re-)allocation of system resources. From this viewpoint, at these two levels, the FDI and FTC problems are reduced to resource monitoring and management.

Each performance and resource monitoring block is associated to a defined range of one or more resources and is responsible for FDI and performance evaluation of its associated resources. As far as resource monitoring is implemented in software, it can possibly run in different modes (e.g. in a degraded mode) and can be treated similar to other functional units, but with some limitations to allocation of a different processing unit. An intelligent group resource manager is responsible for a confined set of FTC cells and thus resources and functional units which can be allocated to each other. For its local group it decides on resource allocation and mode setting of functional units. This information will be sent to FTC cells and to the global resource and reconfiguration management. The necessary reconfiguration actions are controlled by the group resource manager. The intelligent global manager gathers all diagnosis results, information on the process state and reconfiguration commands delivered by the blocks of the group resource and reconfiguration management. It is responsible for mode and resource allocation decisions of the whole system.

In order to design the above-described FTC system, a framework of IFTC technology (IFTCT) should first be established. The core of the IFTC technology is the research on the integrated design of the FTC system and its implementation platform. A strong interaction between the control engineers, the electronic engineers and the computer scientists is required and will be guaranteed through the building of the project consortium from research teams with different backgrounds. In the framework of IFTCT, research will mainly be done in the following fields:

a) Depending on the analysis of requirements on the control objectives, on safety and reliability, performance indices should be defined;
b) Modelling, system analysis, and design of structure of FTC system. On the basis of a structural or functional model of the plant including the effect of faults, one should identify the relations between the different process variables and components and come up with a first proposal for decomposing the plant into a hierarchical structure of subsystems with limited interaction. The model could be of the form of an analytical model, a discrete-event system or a hybrid system depending on the nature of the signals and the process functional components (both hard- and software) involved in the considered subsystem;
c) For hybrid systems, the question of structure determination for monitoring and control will be addressed;
d) Advanced FDI and FTC methods for nonlinear and uncertain systems;
e) A systematic methodology to perform system and/or controller reconfiguration. The determination of the hardware structure should also include the design of the electronics and the micro-controller architecture, as well as the distribution of the control task among the different processors.
f) Resource and configuration management using computational intelligence technologies.

The second goal of this project is to **develop a methodology and further a software tool for an integrated design of the hierarchically structured FTC system** shown in Fig.2. It will be done on the basis of the results achieved in the framework of the IFTCT. The monitoring as well as FDI and FTC systems must be designed in an integrated manner. Besides of the tasks like

a) Design of monitoring and FDI system;
b) Development of intelligent decision system and
c) Development of reconfiguration concepts,

the following issues should be addressed:

a) The interaction between fault detection and isolation on the one hand, and feedback control on the other hand;

b) The choice between fault accommodation (controller re-tuning) and controller reconfiguration based on procedures for fault severity assessment and the given performance indices;
c) The compromise between complexity and real-time requirements;
d) Co-ordination between different levels to achieve an optimal FTC performance.

The design will be carried out in an iterative way, that means once a design is performed, one should verify that the performance objectives are reached and, if they are not, an iteration on the design should be realised. To support the FTC system design, a software tool, called IFATIS tool, will be developed. In order to be applied in any industrial sector where fault tolerance is required, IFATIS tool should be platform independent. It will be constructed in two levels, at the lower level functional modules for the individual FDI/FTC problems are integrated, while at the higher level an iterative design procedure is implemented. The expected (but not limited) application areas range from automotive industry over chemical plants, nuclear reactors, power plants to mass transports systems, e.g. in the railways, naval and aircraft industries.

The final goal for **practical prototype implementation** is the customisation to automotive systems, to a water treatment process and to the construction of an FTC platform for robotic systems.

## 4. CONCLUSIONS

In this contribution the main ideas and objectives of two research projects with European consortia from academia and industry are presented. While the MAGIC diagnostic concept is based on a multi-agents-based architecture which integrates all levels in a diagnostic scheme, IFATIS deals with hierarchically structured fault-tolerant control for integrated systems. Due to their industrial partners both projects have a wide variety of industrial sectors for practical applications.

## ACKNOWLEDGEMENT

This work is supported by the European Commission under EU-IST-2000-30009 MAGIC and EU-IST-2001-32122 IFATIS.

## REFERENCES

Aström, K., Albertos, P., Blanke, M., Isidori, A., Schaufelberger, Sanz, R. (Eds.) (2000). *Control of Complex Systems*, Springer Verlag.

Blanke, M., Frei, C., Kraus, F., Patton, R. J. and Staroswiecki, M. (2000). What is fault-tolerant control? In. *Proc. 4th IFAC Symp. SAFEPROCESS ‘2000,* Budapest.

Chen, J., Frank, P.M., Kinnaert, M., Lunze, J. and Patton, R. J. (2000). Fault detection and isolation, In: *Control of Complex Systems*, (K.J. Astrom, P. Albertos, M. Blanke, A. Isidori, W. Schaufelberger et R. Sanz (Eds.)), Springer, pp 191-208.

Evsukoff, A., Combastel, C., Gentil, S. (1999). Qualitative and neural decision for fault detection and isolation, *IFAC World Congress*, Peking (RPC).

Frank, P. M.(1990). Fault Diagnosis in Dynamic Systems using Analytical and Knowledge-Based Redundancy - A Survey and some New Results; *Automatica*, Vol. 26, No. 3, pp. 459 - 474.

Frank, P. M. (1991). Enhancement of Robustness in Observer-Based Fault Detection; *IFAC/IMACS-Symposium SAFEPROCESS'91*, Baden-Baden, Vol. I, pp. 275 - 287.

Frank, P. M., Ding, S. X., Köppen-Seliger, B. (2000). Current Developments in the Theory of FDI, *Safeprocess 2000*, Budapest, Vol. 1, pp. 16 – 27.

Gertler, J. J. (1998). *Fault Detection and Diagnosis in Engineering Systems*, Marcel Dekker, Inc., NY,484 pages.

Halang W.A., Vogrin P., M. Colnaric (2000). A Safety Licensable PES for SIL~4 Applications. Computer Safety, Reliability and Security, In: *Lecture Notes in Computer Science 1943*, F. Koornneef and M. van der Meulen (Eds.), pp. 141 - 150, Berlin-Heidelberg:Springer-Verlag.

Isermann, R. (1994). Integration of Fault Detection and Diagnosis Methods, *SAFEPROCESS '94*, pp. 597-612, Helsinki.

Knapik, M. and Johnson, J. (1998). *Developing Intelligent Agents for Distributed Systems*, McGraw-Hill, NY.

Köppen-Seliger, B. and Frank, P.M. (1996). Neural Networks in Model-Based Fault Diagnosis; *IFAC'96 World Congress*, San Francisco, pp. 67 - 72, 7f-02 5.

Marcu, T., Ferariu, L., Frank, P. M. (1999). Genetic Evolving of Dynamic Neural Networks with Application to Process Fault Diagnosis; *ECC’99*, Karlsruhe, Germany, Paper ID: F1046-1.

Noura H., Sauter D., Hamelin F., Theilliol D (2000). Fault-tolerant control in dynamic systems: Application to a winding machine. *IEEE Control Systems Magazine*, Vol. 20, N° 1, pp. 33-49.

Patton, R. J. (1997). Fault tolerant control: The 1997 situation, In: *Proc. IFAC SAFEPROCESS ’97*, pp.1033-1055.

Rauch, H.E. (1995). Autonomous control reconfiguration, *IEEE Control Systems Magazine*, pp.37-48.

Wu, N.E. and Chen, T.J. (1996). Feedback design in control reconfigurable systems, *Int. J. of Contr.*, pp.560-570.

Wu, N.E. and Zhou, K. (2000). Reconfigurability in fault tolerant control, In*: Proc. 4th IFAC Symp. SAFEPROCESS ’2000,* Budapest.

Zhou K. (2000). A new controller architecture for high performance, robust, and fault tolerant control, In: *Proc. the 39th IEEE CDC*.