

**Résumés des présentations du Colloque AAAF:**

**AAAF FIRST INTERNATIONAL  
CS2E CONFERENCE:  
Complex and Safe Systems Engineering**

**Arcachon 21-22 juin 2004**



**ASSOCIATION AERONAUTIQUE ET ASTRONAUTIQUE DE FRANCE**

**Secrétariat exécutif**  
61, avenue du Château  
78480 VERNEUIL-sur-SEINE  
Tél.:33 (0) 1 39 79 75 15  
Fax.:33 (0) 1 39 79 75 27  
E-mail : [secre.exec@aaaf.asso.fr](mailto:secre.exec@aaaf.asso.fr)  
Web : [www.aaaf.asso.fr](http://www.aaaf.asso.fr)

# OPENING SESSION



**CHAIRMEN :** C. CAVAILLER CEA/DAM  
D. CABANEL EADS ST

ITER: a Key Experiment to Meet the Challenges of Magnetic Fusion  
J. JACQUINOT, CEA Cadarache

Deep Water Sub-sea Oil Field Development Project  
B. FAURE, A. MARION, TECHNIP

Risks and Opportunities Management on Laser Megajoule Project:  
The Development of a new Knowledge !  
H. DELAFOSSE –LE BER, CEA/DAM

ITER: A KEY EXPERIMENT TO MEET THE CHALLENGES  
OF MAGNETIC FUSION

J. JACQUINOT, CEA Cadarache

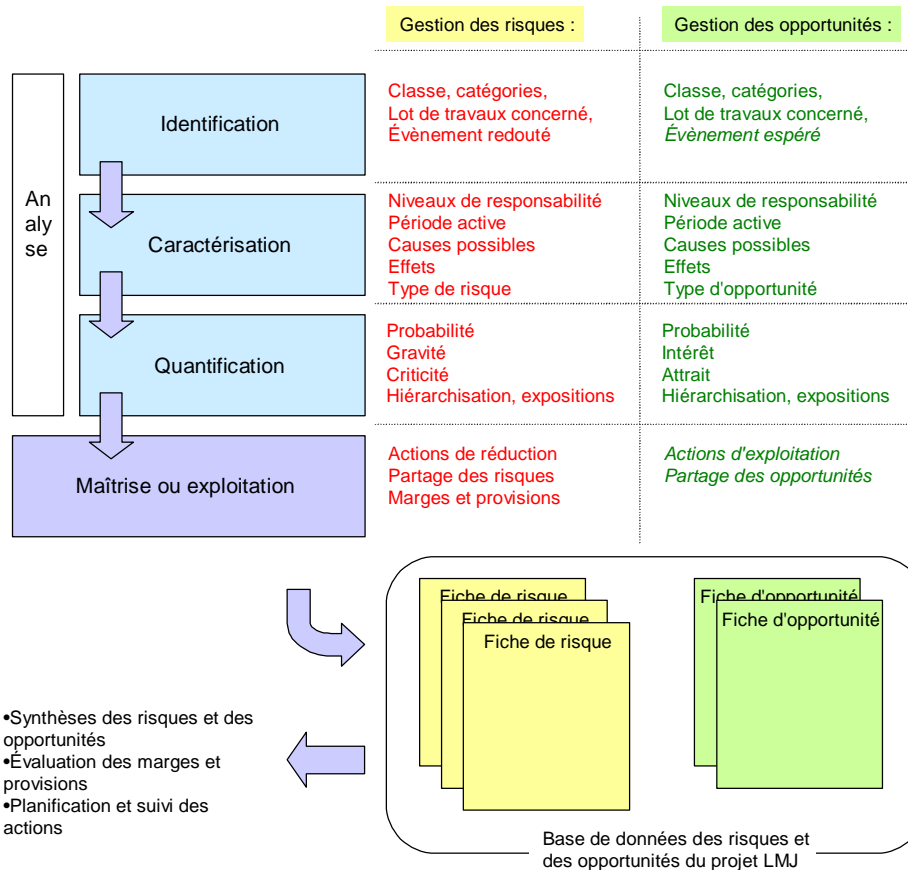
*Abstract not available*

DEEP WATER SUB-SEA OIL FIELD DEVELOPMENT  
PROJECT

B. FAURE, A. MARION, TECHNIP

# RISKS AND OPPORTUNITIES MANAGEMENT ON THE MEGAJOULE LASER PROJECT: EVOLUTION OF A CULTURE !

H. DELAFOSSE-Le BER, CEA-DAM



The interest of these six years spent to build the management through the Risks and the Opportunities (R&O) approach on the project Megajoule Laser as well did not hold with the practical application of a method as to the installation of a formal culture and to its evolution in time. This culture, it had to be progressively founded within a mainly technical project team.

More qualitative with most quantitative aspects, the putting into practice of the R&O approach on project LMJ knew all the degrees of evolution and precision.

The starting of the project saw being born the first analysis of its "Project Risk" with a series of interviews, carried out by the Quality Manager at the time. This analysis took the shape of a technical item lists, which are identified in an empirical way.

Then, some brainstorming meeting were led under the responsibility of the Technical Coordinator (which is the Project Manager assistant) in order to identify and to evaluate the "Project Risk" on a qualitative way, but always keeping a strong technical connotation.

The methodological reference of the "Project Risk" was outlined taking into account the DGA AQ 923 without directly interaction with the other project processes (for example, the cost, the deadlines and the performance management).

Initially, the project developed an Access database, which allows the storing of the risk files. Unfortunately, this database is isolated from the other project management data processing tools.

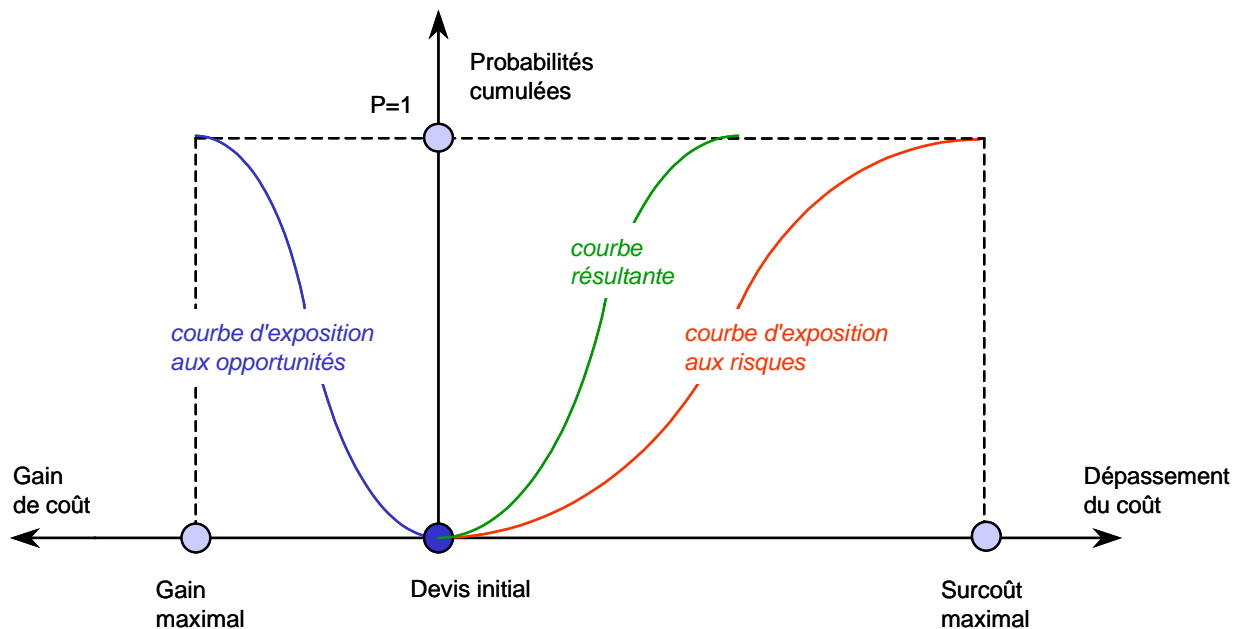
In the second time, the project decided to obtain a dedicated organisation, hierarchically independent from the technical managers but however integrated into the project and attached to the assistant of the Control Project Manager. This organisation being called “Risks & Opportunities Team”, when the management of the opportunities supplemented the R&O approach. This team combines today the individual interviews and the Working Groups in order to identify and to evaluate the effects of the R&O on the project in a quantitative way. These effects could have a technique, a contractual, a legal, a lawful, a political, a social or an organisational aspect.

The “Risks & Opportunities Team” carries out the management of the portfolio of the project risks and opportunities according the DGA AQ 924 reference, helps each operational level of responsibility to refine its analyses and to prepare its reporting near the Project Manager.

The R&O process is integrated into the costs, the deadlines and the performance management. It allows the leading of the System Engineering, feeds and exploits the experience feedback, works in interface with the Integrated Logistical Support / Reliability Availability Maintainability (ILS/ RAM) team, with the safety, with the quality and with the management configuration aspects. A data-processing tool (which is a multi-user accesses and interfaces exploitation database) assists this methodology. This tool is, firstly connected, to the OPX2 planning software for the action planning and the simulation of deadline impacts; and secondly to the database of annual financial estimation and cost management with project termination in order to establish the risk and opportunities margins.

More than the risks and opportunities portfolio traceability aims, this tool allows:

- Monte-Carlo simulations in order to evaluate financial or calendar margins (exposure curves which combined risks and opportunities),
- edition of indicators file-index with file (for example, safety risk table; evolution of the global safety risk in time; comparison between the before action additional cost and the a priori after additional cost action cumulated to the cost of the action plan itself; concept of return on investment),
- edition of dashboards of follow-up of portfolio,
- etc.



|  |
|--|
| <p style="text-align: center;"><b>SESSION N° 1</b><br/><b>PROJECT MANAGEMENT 1</b></p> |
|--|

**CHAIRMEN :** R. MARCILLAT, CNIM  
M. FREUCHET, EADS ST

Schedule Risk Assessment  
G. SMITH, JACOB SVERDRUP

LMJ, Equipments Chamber and Integration:  
A Complex Project within a Complex Program  
R. DURANTON, CNIM

Presentation of all Permitting Subjects in Management of Complex  
And Technological Projects  
JP LANGUY, N. NOEL, TECHNIP

Criticality Management Organisation in the Alpha Incinerator  
C. THIEBAUT, M. HUIN, D. DEVILLARD, J.Y. POINSO, CEA

# SCHEDULE RISK MANAGEMENT

## G. SMITH, JACOBS SVERDRUP

The intended audience for this presentation includes project managers, business managers, project control professionals, senior engineers or engineering managers, and other who are interested in methods and techniques for establishing and maintaining a valid foundation for cost and schedule reserve requests or justifications.

This paper has been presented to the International Council on Systems Engineering (INCOSE), the project Management Institute (PMI), and is part of NASA's project Planning and Control (PP&C) curriculum at the Marshall Space Flight Center (MSFC).

Probabilistic Schedule risk assessment is a valuable management tool that has been around for some time but is not yet in wide spread use. This is an unfortunate circumstance, as the schedule risk assessment process can be a valuable one for project managers to use in order to determine the likelihood of completing a project on time and within budget constraints.

Schedule risk assessment bridges the gap left between traditional CPM scheduling techniques and the project manager's need to know the most likely completion date and cost for a project to a specified level of probability.

The results of this type of assessment can be used to establish or evaluate a baseline. Once established, subsequent changes to the project plan, reflected in the project schedule, can be further analysed and their schedule and cost impacts assessed. In addition, it is possible to examine multiple scenarios with multiple outcomes using schedule risk assessment methods.

The value of any given schedule risk assessment is dictated by several factors. Each of these factors will be discussed in the presentation. The presentation will begin with some reasons why it is prudent to conduct a schedule risk assessment and proceed into a flow chart illustrating the basic process. Subsequent slides will break each flow chart element down into discrete topics for discussion.

These are five distinct categories of schedule risk assessments. Each of these will be discussed. There are two different mathematical assessment techniques. These will also be discussed.

The attendees for this presentation will be familiarized with the schedule risk assessment process and the methods of conducting such an assessment, including the strengths and weaknesses of each.

# ECI : A COMPLEX PROJECT WITHIN A COMPLEX PROGRAM

R. DURANTON, CNIM

The Laser Megajoule program covers the design and construction of a large laboratory facility to conduct nuclear fusion ignition experimentations in controlled conditions, using the technology of high power laser compression.

The construction of this large installation is split into a number of complementary projects relating to the production of all its constituents.

The ECI Project (“Equipements de Chambre et Intégration” = target area integration) covers the design, production and installation of the equipments, housed in the target area hall where all the laser beams are driven to the target. This project includes the development of 5 000 tons of cutting edge technology instrumentation and ancillary equipment, to be integrated into a 35 000 m<sup>3</sup> confined and clean volume.

This instrumentation has to meet very demanding operational specifications such as location accuracy, positioning stability, pointing precision, cleanliness, operational accessibility and maintainability, etc...

It also has to sustain very specific operational environmental conditions : experimentation itself : nuclear radiations, contamination, electromagnetic effects, etc...

The technologies and knowledge expertise involved in this project are extended on an exceptionally wide spectrum : laser conditioning, positioning optics, sub micronic mechanics, stable vibration free mechanical and concrete structures, high precision metrology, vacuum management, radiations protection, multi-level command control supervision, etc...

This project has to be managed in a specific and stringent concurrent engineering context, in order to comply with the overall program planning and to meet a large number of milestones related to interfaces management with the other projects, accurate integration sequences, and co activities on the erection site.

All these features qualify the ECI project as particularly complex in many respects, on the technical and organizational sides and required to setup very specific organization and management procedures. The project structure as well as a range of specific design and risk management tools have been tailored to these particular features.

PRESENTATION OF ALL PERMITTING SUBJECTS IN  
MANAGEMENT OF COMPLEX AND TECHNOLOGICAL  
PROJECTS  
JP LANGUY, N. NOEL, TECHNIP

*Abstract not available*

# CRITICALITY MANAGEMENT ORGANISATION IN THE ALPHA INCINERATOR

C. THIEBAUT, M. HUIN, D. DEVILLARD, JY POINSO, CEA

The operation of the facilities at the VALDUC centre generates alpha-contaminated wastes. So an incineration plant has been built to treat them. The result of the process is a reduction in volume and weight. On average, the reduction factor is more than 15. It depends very strongly on the composition of the waste incinerated. The produced ash is suitable for in-line vitrification or plutonium recovery by argentic dissolution.

The criticality issue is being conducted very carefully step by step. The risk prevention is based on mass limitation of active material undergoing treatment in the facility. A balance is compiled continuously by calculating the difference between the mass of active material entering the facility and the masse leaving it. These masses are evaluated by the activity measurements performed on qualified measurements circuits.

Due to measurement uncertainty, the absence of hold up in the different part of the incinerator must be checked regularly.

The referential consists mainly in : the safety report (RS), the exploitation general rules (RGE), the Technical Prescription (PT), the criticality application (CSC), the ruling document (DP) which describes precisely the way that the technicians operate the incinerator.

The Nuclear Material measurements that are used are :

- gamma spectrometer for the wastes before entering the process,
- gamma spectrometer for the ashes at the end of the process,
- gamma spectrometer and passive neutron spectrometer for the hold up measurement at the end of a criticality run. The operator has first conducted tests with calibrated radioactive sources to qualify the systems for measuring hold up from outside of the glove boxes. These sources have been put at different locations in the process so as to determine the hold up in the most difficult parts. Most of the time, gamma spectrometer is sufficient to determine the value of the retention. But when the thickness of the ovens is too large, this technique is no more sufficient and we have to use passive neutron counting. The instruments used are mobile, since non continuous hold measurement is carried out. So the same spectrometers are used to evaluate the hold up at different locations.

The results of the hold up measurements will be presented. They will be compared with the evaluation of the calculated hold up determined by the balance between the amount of plutonium which has been put into the process and the amount of plutonium retained in the ashes.

|   |
|---|
| <p style="text-align: center;"><b>SESSION N° 2</b><br/><b>SIMULATION - MODELISATION</b></p> |
|---|

**CHAIRMEN :**                    B. SACHET, TECHNICATOME  
    H. PIGANEAU, SETEC-TPI

Architecture Patterns for safe Design  
C. KEHREN, P. BIEBER, C. CASTEL, C. SEGUIN, ONERA  
C. BOUGNOL, J.P. HECKERMANN, S. METGE, AIRBUS FRANCE

Finite Element Calculation for Updating of existing Structures  
(Shock Between Two Adjacent Buildings)  
X. CESPEDES, SETEC-TPI

Using the Concepts of Configuration Management for Designing a Virtual  
Mock-Up Associated to a PDM in a Concurrent Engineering Process, for the  
LMJ Project  
J.-M. JAEGER, SETEC-TPI

# ARCHITECTURE PATTERNS FOR SAFE DESIGN

C. KEHREN, P. BIEBER, C. CASTEL, C. SEGUIN, ONERA  
C. BOUGNOL, J.P. HECKERMANN, S. METGE, AIRBUS FRANCE

Recently, AIRBUS France and ONERA-CERT have launched an R&T study on architecture patterns to enhance safe design activities. The purpose of this study is to provide methods and computer based tools to assist the modelling and the assessment of safety architectures of all kinds of complex systems (e.g. software, mechanical). The basic idea is to encode experts' know-how into formal model libraries of typical safety micro-architectures.

Those micro-architectures models exhibit elements of interest for a safer design: structural features (e.g. redundancy), good use conditions and induced safety properties. They are indeed abstract views of the system safety elements and will be called safety Architecture Patterns (SAP). Sets of SAP are identified both in literature and in Airbus Practice. This language was developed at Bordeaux University and is supported by toolsets including simulation, fault tree generation and model-checking capabilities. We have been inspired by computer science studies where design patterns have been introduced to ease software development process by allowing the reuse of mature application templates. As for design patterns, attributes are associated with each SAP. As shown in figure 1, some attributes are informal ; for instance, the problem attribute is a text describing the issue that this SAP solves. Other attributes are described with formal notations. For instance, the architecture attribute is an AltaRica model that defines the SAP components and interfaces. Another important attribute is the pre-proved property attribute. It is a temporal logic formula that states safety requirements enforced by the SAP.

SAP have been used, as an experiment, to model Airbus electrical and hydraulic generation and distribution systems. A first benefit of SAP is rapid prototyping of system models. Indeed, using an SAP library has shown that the design of system architectures is made easily and quickly. This allows the creation of several prototypes. The system designer can compare those competitive solutions of architecture in terms of feasibility or cost for instance (figure 2). Moreover, safety requirements are automatically assessed thanks to the available verification technologies. We used Cecilia OCAS ( developed by Dassault Aviation) graphical simulation and fault tree generation toll coupled with SMV model-checker. Next step in the design process is to shift from a SAP based model to a more concrete one. Pre-proved properties of the SAP can be used to make easier the safety requirements allocation from high-level system safety objectives. Furthermore we are studying a refinement relation between detailed and SAP models that should guide and limit the assessment task of the detailed architecture.

As a conclusion, these first experiments showed that SAP based models enable capitalization of the experts' know-how and the possibility to reuse validated patterns in new architectures. They also provide a more concise view of the whole system and ease the exhibition of the satisfied properties. As a benefit, we expert this approach will offer a better and wider understanding of system safety and will save time during the preliminary assessment phase.

## SEISMIC INTERACTION BETWEEN 2 EDIFICES

### X. CESPEDES, SETEC TPI

Seismic interaction between 2 adjacent concrete structures was investigated as part of a global safety assessment of a large industrial plant. The expected impacts, located on the edifice's top floor, were feared to create large crack propagation. Specific attention was paid to one of the edifices, in which are stored highly toxic products, with possible environmental contamination if opened cracks were to be expected after earthquake.

Investigations were conducted by 2 different approaches respectively for global and local behaviour:

- Yield line analysis was used for global behaviour. The comparison between the building's kinetic energy just before impact and the energy dissipated by creating series of large cracks in the building lead to a first global safety coefficient. Conventional yield line analysis had to be improved to take into account fundamental dynamic relations.
- Non linear time dependent finite element calculation, with contact elements and a precise modelling of the interaction area lead to an accurate simulation of the local behaviour close to the impact points.

Both calculations gave complementary results, showing a good behaviour of the edifice, and a rather small contribution of the interaction effects.

Approaches using yield line analysis, which are not commonly used by structural Engineers, could be helpful for analysis of highly non linear structural behaviours, during impacts or explosions.

USING THE CONCEPTS OF CONFIGURATION  
MANAGEMENT FOR DESIGNING A VIRTUAL MOCK-UP  
ASSOCIATED TO A PDM IN A CONCURRENT  
ENGINEERING PROCESS,  
FOR THE LASER MEGA JOULE PROJECT  
JM. OLLIVIER, TECHNICATOME

The use of a virtual mock-up is now very common when associated with the design and engineering of complex systems. Technicatome in the nineties has suppressed the usual scale 1 wood mock-ups of its nuclear power engines by introducing virtual reality.

In 1998 Technicatome has been involved in the Laser mega joule project, with a mission that included the design of the virtual mock-up of the most dense zones of the plant, in a concurrent engineering process where we had to assembly parts from various actors and partners.

One of the main problems was to keep up to date the mock-up !

So we made a parallelism between the configuration management and a mock-up management. The latter being used to help illustrate the former, a link was to be established.

The guideline has been the RG Aero 40 and RG aero 023 specifications.

Two main notions have been extrapolated : the Development Component Baseline (drawing tree), and the choice of Configuration Items (leaves).

The usual baseline is a tree structure, but it will only describe the items with no difference between their cases of use. In a bill of materials a car has 5 identical wheels, I need to describe only one of them. The baseline for a mock-up is functional, and each instance of an item must be described : my car has only one left front wheel witch has a geographical position relative to it's father. And a functional name different from it's identity name. so for our mock-up, we built a topo-functional tree.

Because a big mock-up may consist of many thousands of items, a configuration management must limit its watch to some specific items : the configuration items. We call them mock-up items and they are treated as unique entities. Even if the item has its own tree structure, it will be represented by one mock-up object : that is the leaf on the tree. Creating a mock-up object consists in creating a simplified representation of a CAD design.

Managing the configuration of the entire mock-up essentially consists in changing the leaves : changing the revision, or changing the item.

To day, the current mock-up is made of more than 50 000 objects, and to keep it coherent we use a PDM, with some customizations : each time a CAD part is stored or updated, a program will create the equivalent mock-up object, and keep the tree structure in an Oracle relational database. The guarantee required before distributing the mock-up to the various partners on the project is brought by the PDM.

All this will be demonstrated by a virtual visit through the mock-up of Laser Mega Joule, from the 240 lasers to the one millimetre target, when in the real world the concrete is still drying.

**FINITE ELEMENT CALCULATION FOR SEISMIC  
DIMENSIONING OF NEW NUCLEAR STRUCTURE  
CEA LMJ PROJECT  
JM JEAGER, SETEC-TPI**

With its 240 beams, the megajoule laser system should deliver in 2010, a luminous energy of 1.8 million joules. The laser beams converge toward the heart of the AEC center of CESTA : the Experimentation Hall. The BOUYGUES Group which is developing this structure conferred to the SETEC TPI design & engineering department the detailed execution studies of the Experimentation Hall and the task of developing a finite elements computational model.

The Experimentation Hall is a monolithic reinforced concrete block with in-plane dimensions of 75.4 m x 72.5 m and a height of 43.5 m based on a 2.5 m thick frame. The heart of the experimentation chamber consists of a reinforced concrete cylinder having a thickness of 1 m and a diameter of 33 m, which houses a sphere having a diameter of 11 m. The foundation floor is made of a clay/sand base and the floor/structure interaction was taken into account in the structural analysis in the form of impedance functions.

The finite element computational model has 90 000 nodes and uses shell elements. This model accurately reflects all the structure elements and integrates all the "hoppers" greater than 1 m. The acceptance of these 2500 hoppers at their exact position was one of the major problems in the development of the geometric model.

400 cases of static loads related to the actions of permanent loads, equipment and operating loads were applied to the model, as well as the cases of loads specific to seismic actions. A special computational code for the reinforced concrete material was developed by SETEC TPI in post-processing of the ANSYS computational software to carry out the thousands of regulatory combinations in the Civil Engineering field and to determine the concrete reinforcements to be applied.

SETEC TPI thus developed a series of computer assisted computational/design tools such as AUTOCAD, ADFER as well as others, to allow totally justifying that this complete structure will behaved correctly in all of its operating phases.

**SESSION N° 3**  
**SAFETY, RELIABILITY AND AVAILABILITY**  
**APPROACH 1**

**CHAIRMEN :**                    **B. SACHET, TECHNICATOME**  
   **H. PIGANEAU, SETEC-TPI**

A Reliability Process Applied to Designing & Manufacturing Nuclear  
Weapons  
JL LABASTE, CEA/CESTA

An Integrated Approach to Risk Analysis and Risk Management of Complex  
and Innovative Systems  
F. VUILLE, GESTE Engineering

From the Project to the Field for Meteor Metro Line (a pragmatic Approach  
for Configuration Management and Integrated Logistic Support)  
H. DE LARQUIER, AXILYA

Theoretical & practical RAMS Application to Launch Vehicle System  
E. VIVET, EADS ST  
O. ROCHER, EADS APSYS

# A RELIABILITY PROCESS APPLIED TO DESIGNING AND MANUFACTURING NUCLEAR WEAPONS

J.L. LABASTE, CEA/CESTA

Implementing a specific reliability approach is required now that nuclear tests have been banned but also due to the very characteristics of nuclear weapons as well as hardly achievable objectives given the utmost complexity of the latest systems.

This methodology rests on three basic points:

- A thorough qualitative process in order to ensure that none of the basic parameters was left out and identify the sizing parameters relating to reliability.
- A quantitative process modelling and evaluating the behavior of the parameters.
- Feedback, when applicable, which takes account of weaponry expertise and will help adjust treatment of points 1 and 2 above.

Each point will break down into the following:

- Qualitative modelling which is based on three analytical models:
  - A functional model, i.e. how it works,
  - An organic model, i.e. what is made up of,
  - A structural model, i.e. how the various element interact.
- Quantitative modelling which is based on three types of models:
  - An operating model (operational margin versus specifications),
  - A behavior model (resulting from the previous one and taking account of all constraints related to the concept implementation),
  - An implementation model (including all defects related to manufacturing, assembly and acceptance).
- The feedback process comprises three phases:
  - What about the technology being used ?
  - A methodological approach (analysis, technical data processing).

Compared to former reliability studies performed on previous weaponry systems, our methodology provides a well-structured understanding as well as a very consistent reliability approach to the warhead as a whole, thus increasing the confidence level in data acquisition.

This process is similar to the one developed within the framework of nuclear warhead functioning guarantee, thus proving to be both homogeneous and consistent and confirming our expertise in designing and manufacturing nuclear weapons capable of fulfilling their mission now that tests have been definitively banned.

# AN INTEGRATED APPROACH TO RISK ANALYSIS AND RISK MANAGEMENT OF COMPLEX AND INNOVATIVE PROJECTS

F. VUILLE, GESTE Engineering

Complex and innovative projects necessitate some specific approach to dependability demonstration that has to be both systemic and exploratory. Current methodologies often fail at tackling jointly all the RAMS aspects and are not all designed to integrate risk factors other than technical. Furthermore, it is well known that, for maximum efficiency, a risk analysis should start at an early development stage of a project, but should then be able to accompany this project all along its evolution until the operational start-up.

The approach presented here is based on the elaboration of a hierarchical and computational FMECA (Failure Mode Effect and Criticality Analysis) model of the system and on the creation of an evolutionary core data providing a permanent up-to-date view of the project development. Compared to a classical FMECA analysis, the methodology has been enriched to enable, on the one hand, to consider simultaneously the technical, human and environmental hazards, and on the other hand to optimize jointly the global safety and availability performances of the system (risk management).

This approach has been successfully applied for the risk analysis of the new Alpine railway lines of the Gotthard and Loetschberg (both lines are operated with the innovative ETCS-2 signaling system and encompass very long tunnels), as well as for the solar plane of Bertrand Piccard & Brian Jones (Solar Impulse project).

FROM THE PROJECT TO THE FIELD FOR METEOR METRO  
LINE  
(A PRAGMATIC APPROACH FOR CONFIGURATION  
MANAGEMENT AND INTEGRATED LOGISTIC SUPPORT)  
H. de LARQUIER, TECHNICATOME

RATP built a new line under Paris: METEOR. Major investment of these last years and extensive use of new technologies are the main characteristics of METEOR Automated Train Operating System (ATOS).

As far as RATP maintenance strategy is to do it by itself ; maintain and redesign if required from the D day till the end of life cycle become a real challenge.

To face this challenge a Technical Information Management Plan has to be defined and implemented. Covering a combined approach of Configuration Management (CM) and Integrated Logistic Support (ILS), this plan allows to transfer adequate information from the project structure to the maintenance structure.

This presentation shows how CM and ILS have been pragmatically implemented using software tools from the market.

Steps and results are described, strength and weakness are explained, lessons for the future are detailed.

# THEORETICAL & PRACTICAL RAMS APPLICATION TO LAUNCH VEHICLE SYSTEM

E. VIVET, EADS SPACE Transportation

O. ROCHER, EADS APSYS

The main topic of this paper is to present the main steps and rules of the practical RAMS rationale in the frame of a launch vehicle system associated to drastic reliability and safety requirements, covering all phases from manufacturing to operational life.

Starting from reliability, availability, maintainability and safety requirements at system level, the RAMS rationale of such a complex systems consists in:

- allocating the system level requirements towards the sub-systems / components to be designed with respect to these declined,
- designing the sub-systems / components by taking into account RAMS requirements from the preliminary concept to the detailed definition,
- guaranteeing that the manufacturing and maintenance processes of the sub-systems / components allow to reach and maintain the RAMS performances through operational life,
- consolidating the sub-system / component level performances to provide the system performance assessment with reliable data,
- managing the risks at interfaces and the discrepancies / non-compliances between requirements and demonstrated / achieved performances,
- maintaining the required level of RAMS performance through operational life (up to 40 years) and implementing the necessary organisation.

After defining the technical and industrial risk, this paper details a practical RAMS method so called Design Features Hierarchisation (DFH) (in French HCD = Hiérarchisation de Caractéristiques de Définition) that aims at classifying the design features according to their impacts on safety or mission success in order to focus the attention and energy of the manufacturing and maintenance process managers on the relevant design features (weakest points).

|   |
|---|
| <p style="text-align: center;"><b>SESSION N° 4</b><br/><b>NEW TECHNOLOGIES INTEGRATIONS 1</b></p> |
|---|

**CHAIRMEN :**                    J.-P. BORSOI, TECHNICATOME  
   G.-G. LEGRAND, THALES

Technical Risk Management Approach Applied to the Development of a  
New Transport System : The GATEWAY  
B. PONSOT, CNIM

Deck Reconstruction of Jacques Cartier Bridge Using Precast Prestressed  
High Performance Concret Panels  
A. ZAKI, SNC – Lavalin Inc

ECORAIL : A Step Toward Safe Railway Controlling  
Systems Based on Satellite Positioning  
V. THEVENOT, TECHNICATOME – T. BRUCKMUELLER, ALCATEL  
C. DOEDERLEIN, STERN & HAFFERL – R. SARFATI, SYSTRA  
P. MATTOS, ST MICROELECTRONICS – E. WASLE, TELECONSULT  
M. TOSSAINT, ESA

Concrete Structures Design for an Extended life Span  
J.-P. PERSON, COYNE ET BELIER  
B. TAINE, TECHNICATOME

# MANAGEMENT DES RISQUES APPLIQUE AU DEVELOPPEMENT DU TROTTOIR RAPIDE : LE GATEWAY B. PONSOT, CNIM

L'objectif de cette conférence est de présenter la démarche adoptée pour développer un nouveau moyen de transport en mettant en évidence les aspects liés à la gestion des risques inhérents à la sécurité des personnes d'une part et des risques relatifs à la fiabilité du produit d'autre part.

Le trottoir rapide est un système développé en partenariat avec la RATP, qui répond au besoin de transport public sur des distances intermédiaires de l'ordre de 200 à 500 m. Les cibles visées sont les liaisons entre terminaux dans les aéroports, les correspondances entre gares des réseaux ferrés et plus généralement entre les centres de vie à l'intérieur des grandes métropoles tels que les zones parking, les zones commerciales, les quartiers d'affaires,...

La première application est un trottoir de correspondance d'une longueur de 186 m, installé à la station Montparnasse dans le réseau RATP.

La mise en place d'un nouveau système de transport dans le domaine public nécessite une approche spécifique sur le plan de la sécurité des personnes. La démarche adoptée s'appuie sur :

- La création d'une commission de sécurité sous l'égide du ministère de tutelle,
- La mise en place d'un référentiel normatif,
- Une analyse des risques liés à l'utilisation du produit,
- Une pré-validation sur maquettes et une validation in-situ,
- Une autorisation d'exploitation du produit par les Organismes de Tutelle de la RATP (la Direction Régionale de l'Équipement d'Ile-de-France DREIF et le Syndicat des Transports d'Ile-de-France STIF).

Par ailleurs, les contraintes d'exploitation nécessitent une gestion des risques techniques pour répondre à un impératif de disponibilité du produit vis à vis des usagers. Une démarche d'analyse lors de la conception et de validation expérimentale est prise en compte pour le développement du produit.

L'ensemble de ces travaux est concrétisé par l'installation et la mise en service du premier Trottoir Rapide à la station Montparnasse de RATP en octobre 2002 pour une période d'observation d'un an.

Depuis 2004, les Organismes de Tutelle autorisent l'exploitation du produit permettant d'envisager une commercialisation du Trottoir Rapide dans les réseaux des transports des grandes métropoles internationales.

Des projets d'implantation sont actuellement en cours d'analyse, notamment en Amérique du Nord et en Asie du Sud-Est.

**DECK RECONSTRUCTION OF JACQUES CARTIER BRIDGE  
USING PRESTRESSED HIGH PERFORMANCE  
CONCRETE PANELS  
A. ZAKI, SNC – Lavalin Inc**

In 2001 and 2002, the Jacques Cartier Bridge in Montreal, one of Canada's busiest and historically important bridges underwent a total reconstruction of its 70-year-old deck. Involving more than 60,000 m<sup>2</sup> (645,800 sq ft) of deck to be replaced, this project represents the biggest bridge rehabilitation project ever undertaken in Canada under a single contract. Driven by the need to replace the existing deteriorated reinforced concrete deck by a new and highly durable deck without disrupting normal rush-hour traffic, a precast, prestressed, high performance concrete (HPC) deck replacement system was implemented requiring the installation of 1680 deck panels which were post-tensioned together in both longitudinal and transversal directions once placed on the bridge's existing steel support members. Design features, durability issues, fabrication and construction techniques, which included the erection and operation of a temporary precast plant built specifically for the project, are presented. The benefits of using an HPC precast deck replacement method to successfully restore this important and historical urban bridge are also discussed.

This project recently won the award for Best Rehabilitated Bridge in the PCI's 2003 Design Awards Program.

# ECORAIL: A STEP TOWARDS SAFE RAILWAY CONTROLLING SYSTEMS BASED ON SATELLITE POSITIONING

V.THEVENOT, TECHNICATOME - T.BRUCKMUELLER, ALCATEL  
C.DOEDERLEIN, STERN & HAFFERL - P.MATTOS - ST  
MICROELECTRONICS  
R.SARFATI, SYSTRA - E. WASLE, TELECONSULT - M.TOSSAINT,  
ESA

## Generic topics/application areas:

This paper is related to the following generic topic/applications area:

- Safety, Reliability and Availability approach
- Dependable Transportation Networks
- Safe and secured Command & Control



Today, a European satellite navigation system is on the move: EGNOS raises the hope of an unique world-wide network, the Global Navigation Satellite System.

EGNOS is entering in a real life experimentation phase. This opportunity to have an accurate and more reliable localization system smoothes the way for a concrete railway application which proves satellite navigation an attractive part in this field.

The objective of the ECORAIL project is to demonstrate that railways now have the means to cope with a new challenge by introducing satellite navigation in safety critical railway applications.

But a satellite positioning system, even with EGNOS functionalities, does not provide on its own the safety integrity level required by many railway applications. This integrity level can be achieved by applying data fusion and map matching algorithms on measurement from satellites, odometers, acceleration sensor, gyros etc...

The project is mainly aimed at providing a new technological and technical solution: an on-board module which is able to localize a train on the track, ensuring a adequate safety level. The second aim is to demonstrate the efficiency of satellite-based localization by comparing it with existing conventional equipment.

In doing so it should be possible to convince railway operators that satellite navigation can be a qualified element of safety critical railway applications. The project concentrates on the definition and demonstration of a fail-safe railway control system, but only marginally addresses to the standardisation and certification issues.

To demonstrate the efficiency of the localisation, the system will perform an automatic level crossing control.

A train of a local railway company (an Electric Multiple Unit: EMU) in Upper Austria will be equipped with the proposed on-board system.

To examine the quality of localization the activation of a level crossing will be simulated and compared with the data derived from the conventional equipment. In addition to that a time-optimised activation, based on the current speed of the EMU will be tested. Therefore, the objective is to demonstrate that the satellite navigation is not only an equivalent alternative to conventional track-side equipment but it has to be considered as a more efficient solution. This demonstration will start early 2004 and last for about 6 months.

The main advantages of the ECORAIL system are :

- reduction of investment and operation costs,
- performance improvement with an equivalent safety level as existing systems : for example, in the prototype application (level-crossing commanding),
- the capability to integrate additional functions based on satellite navigation data.
- the system is based on existing technologies and equipment which will be adapted for this application. No new developments are planned.

The project is founded by ESA and developed by the following partners:

- Alcatel Austria - Transport Automation Solutions (Austria)
- Teleconsult Austria (Austria)
- Stern Haferl (Austria)
- St Microelectronics (Italia)
- Systra (France)
- Technicatome (France)

# CONCRETE STRUCTURES DESIGN FOR AN EXTENDED LIFE SPAN

J.-P. PERSON, COYNE ET BELIER  
B. TAINE, TECHNICATOME

Today, service life span to be guaranteed for great infrastructures reaches or exceeds 100 years. Issue for such objectives in case of reinforced concrete structures requires design rules and criteria adapted to these durations.

Design of durable concrete structures relates thus more particularly to:

- *the analysis of the factors of liability towards deterioration of the concrete,*
- *the predicted behaviour of concrete with time under the operating conditions of the structures,*
- *the evaluation of precise loading for the structural dimensioning,*
- *the composition of the reinforced concrete in order to limit the external aggression,*
- *choices of the reinforcement patterns to minimise cracking.*

Specific recommendations for concrete structures erection are proposed which are beyond the current standards.

A program of monitoring is included at the design stage so as to allow safety evaluation throughout the life of the facility.

The know-how feedback acquired from survey of great existing structures since about thirty years (nuclear containments, bridges) makes it possible to validate some of the design rules and provides a canvas of reference for the performance of long service life span concrete facilities.

**SESSION N° 5**  
**SAFETY, RELIABILITY AND AVAILABILITY**  
**APPROACH 2**

**CHAIRMEN :**                    J.-P. BORSOI, TECHNICATOME  
   G.-G. LEGRAND, THALES

Safety Reassessment and Upgrading Program for a Building  
M. HUIN, D. DEVILLAR, C. THIEBAUT, CEA-Valduc

Passive Safety System Reliability Evaluation and Integration of this System  
in Nuclear Power Plant PSA  
V. LA LUMIA, S. MERCIER, TECHNICATOME  
M. MARQUES, JF. PIGNATEL, CEA-Cadarache

RAMS Engineering Process in Highly Complex System :  
Applications to EGNOS  
M. OBERLE, THALES Engineering Consul.

SEVESO II Directive and its Applications in Industrial Fields  
S. PAGNON, D. BECT, Groupe SECHAUD

# SAFETY REASSESSMENT AND UPGRADING PROGRAM FOR A BUILDING

M. HUIN, D. DEVILLARD, C. THIEBAUT, CEA

The activity of a building dedicated to radioactive material such as plutonium, uranium or tritium is defined as production, refining, scraps treatment and waste treatment. It has a total surface area of about several 1000 m<sup>2</sup> and has hot cells containing glove boxes.

Most of these buildings have been built in the years between 1958 and 1965 and the nuclear activity has begun just afterwards. It happens that these buildings have expansions which have different configurations due to the evolution of the law and the decrees that are imposed to the nuclear buildings.

About every ten years, the regulator ask for a reassessment which is made in collaboration with the exploiting people. This reassessment is based on the current laws and decrees which can be summarised as :

- the 10/08/84 decree concerning the quality and its management in the nuclear industry,
- the Security Safety (RFS) describing the seismic risk, the fire protection, ...

The regulator asks most of the time several requests, especially those concerning the analysis due to earthquake.

The decision is then made to perform studies for :

- evaluation of the building state after earthquake,
- evaluation of radiological consequences in case of building collapses,
- evaluation of 30 years extending life accounting the earthquake resistance of the building. This 30 years extending is generally very expensive, risky and requires a long outage time.

Depending on the result of the comparison of the extending cost and that of a new building, the upgrading program varies widely. The main topics of the reassessment are :

- fire protection (replacement of the automatic fire detection system, extending of the fire detection in glove boxes, upgrading cells in fire sectors, ...)
- radiological protection and criticality (neutronic shielding, replacement of the in cell contamination detection system, ...)
- fluid distribution,
- electrical distribution,
- ventilation,
- seismic risk which must be declined in two topic : glove boxes and the building itself (stack, walls).

Results concerning several topics will be presented.

# PASSIVE SAFETY SYSTEM RELIABILITY EVALUATION AND INTEGRATION OF THIS SYSTEM IN NUCLEAR POWER PLANT PSA

V. La LUMIA, S. MERCIER, TECHNICATOME  
M. MARQUES, J.F. PIGNATEL, CEA/DEN

Innovative nuclear reactor concepts could lead to use passive safety features in combination with active safety systems. A passive system does not need external input (especially energy) to operate. It is expected that passive systems combine the advantages of simplicity, reduction of the need for human interaction, avoidance of external electrical power or signals. These advantages are very attractive for safety nuclear plant improvements and economic competitiveness. But lack of data on some physical phenomena, missing operating experience and smaller driving forces - compared to active safety systems - must be taken into account (especially applicable to passive systems relying on natural forces, such as natural convection). In this context, the European Commission (EC) decided to start the RMPS (Reliability Methods for Passive Safety functions) program. As part of the RMPS program, TECHNICATOME and CEA has:

- Realized a quantitative reliability evaluation of the BOHR/RP2 (Base Operation Passive Heat Removal strategy applied to the Residual Passive heat Removal system on the Primary circuit, thereafter called **RP2 system**) passive system reliability,
- Introduced this evaluation in a simplified PSA (Probabilistic Safety Assessment).

The scope is to get out experience, for any passive system, in terms of:

- Definition of characteristic parameters for the evaluation of reliability,
- Analysis of PSA results (safety improvements verification),
- Credibility of calculated reliability results,
- Difficulties encountered for the validation of a passive system (safety passive system efficiency demonstration to power plant designers and safety authorities),
- Identification of the tasks to perform, after this RMPS project, to define a validated methodology for reliability evaluation of passive system.

The integration of passive systems in the PSA requires to take into account failures of its components (e.g. pipes, valves) but also failures of the physical process involved (e.g. natural circulation). The difficulty remains in the large number of physical parameters with their associated uncertainties and in the physical model limitations. A methodology is implemented to evaluate the physical process failure risk. To test this methodology, a fictive PWR nuclear power plant is defined: it would be, in a hypothetical way, equipped with 2 passive safety systems, both on the primary circuit: the new RP2 system for removing the residual power and an usual safety injection system with accumulators for maintaining pressure. The simplified PSA is carried out for the total loss of power supplies initiating event leading to a core fusion. The accident sequences are defined using event trees. The occurrence probabilities of physical process failure have been assessed through uncertainty analyses based on supposed probability density functions for the characteristic parameters of the RP2 system. From these probability density functions, the physical process failure probabilities have been calculated by Monte Carlo simulation coupled to the CATHARE thermal-hydraulic code. The yearly frequency of the core fusion is evaluated for each accident sequence. This analysis has identified the influence of the passive system and propose a re-dimensioning of the RP2 system for achieving the safety probabilistic objectives.

# RAMS ENGINEERING PROCESS IN HIGHLY COMPLEX SYSTEM : APPLICATION TO EGNOS

M. OBERLE, THALES Engineering & Consulting

The aim of this paper is to present the RAM and Safety process developed for EGNOS Ground Segment program, from the early design phase to the integration and validation phase.

The EGNOS AOC system (European Geostationary Navigation Overlay Service – Advanced Operational Capability) is the European contribution to the Global Navigation Satellite System (GNSS-1). It will provide and guarantee navigation signals for aeronautical, maritime and land-mobile trans-European network applications such as not limited to positioning.

The EGNOS AOC system is called an “augmentation” to GPS And GLONASS in the sense that it drastically improves and completes their basic performances of precision, continuity and integrity. In their context, the EGNOS system is designed to provide and meet the expected most stringent performances requirements, which are those for landing aircraft.

Due to this intrinsic nature, RAMS performance, i.e. safety (continuity and integrity) and dependability performances (availability) are the main drivers for design, development and testing activities of EGNOS system.

Algorithm performances, geometric considerations and items failures have to be considered for apportionment, design trade-off and assessment of these performances. Hence, ALCATEL SPACE as the prime contractor supported by THALES Engineering & Consulting as responsible for the RAMS activities implemented from the very beginning of the programme an engineering process based on integrated RAMS and design/development activities. The aim was to permanently control the main area of risks identified so far for the project but also to cope with the quantified integrity, continuity as well as availability performances as part of the navigation performances.

The presentation will extensively describe the RAM and Safety Engineering process implemented on the EGNOS ground segment program including the results obtained so far from an architectural and operational point of view and will highlight the main issue and problems encountered with the associated recovery actions.

# L'APPLICATION DE LA DIRECTIVE SEVESO II PAR UN BUREAU D'ETUDE DANS DES APPLICATIONS INDUSTRIELLES

S. PAGNON – D. BECT, Groupe SECHAUD

La Directive Européenne 96/82/CE du 9 Décembre 1996, dite " Directive SEVESO II " a pour objet la prévention des accidents majeurs impliquant des substances dangereuses et la limitation de leurs conséquences pour l'homme et l'environnement. Elle s'applique aux établissements où des substances dangereuses sont présentes en quantité importante.

Les principales exigences de l'arrêté du 10 Mai 2000 (transposition en droit français) demandent aux industriels l'application de méthodologies de détermination des dangers et la mise en place d'actions.

Les sociétés industrielles font souvent appel à des bureaux d'études spécialisés et reconnus par les autorités pour ces études et surtout la détermination des actions de prévention et de précaution. Les grandes étapes de l'études sont :

- L'étude de danger; il s'agit d'exposer d'une part les dangers que peut présenter l'installation en cas d'accident, en présentant une description des accidents susceptibles d'intervenir, que leur cause soit d'origine interne ou externe, et en décrivant la nature et l'extension des conséquences que peut avoir un accident éventuel. Elle justifie les mesures propres à réduire la probabilité et les effets d'un accident, déterminées sous la responsabilité du demandeur.
- Politique de Prévention des Accidents Majeurs (PPAM) : il s'agit de la politique mise en place par l'exploitant sur la base des accidents envisagés dans l'étude de dangers en vue de prévenir les accidents majeurs et de limiter leurs conséquences pour l'homme et l'environnement.
- Système de gestion de la sécurité (SGS) : l'exploitant met en place dans l'établissement un système de gestion de la sécurité applicable à toutes les installations susceptibles de générer des accidents majeurs. Le système de gestion de la sécurité définit l'organisation, les fonctions des personnels, les procédures et les ressources qui permettent de déterminer et de mettre en oeuvre la PPAM.

**SESSION N° 6**  
**NEW TECHNOLOGIES INTEGRATIONS 2**

**CHAIRMEN :**                    M. DUMOND, SGN  
    JF CAZES, TECHNIP

HABOG, a New Started Nuclear Multi Purpose Storage Facility  
B. TIGOULET, M. CHIGUER, SGN  
C. KALVERBOER, EA. BACH, COVRA

Engineering and Validation on Space Transportation Avionics Systems  
JC MOREY, G. ABOUT, EADS ST

Risks Management in the Construction of a New Technology Based  
Aluminium Smelter in South Africa  
L. BERTRAND, ALUMINIUM Pechiney

Development of Large Concrete Structures for Offshore or Coastal Facilities  
F. SEDILLOT, DORIS Engineering

# HABOG, A NEW MULTI-PURPOSE STORAGE FACILITY IS READY TO START-UP

C. KALVERBOER, E.A. BACH, COVRA  
B. TIGOULET, M. CHIGUER, SGN

In the Netherlands, COVRA is in charge of radioactive waste management. COVRA currently operates a facility in Borsele in the South West of the country including a low level waste treatment facility (AVG) and a low level waste storage facility (LOG).

For the purpose of Spent Fuel and High and Intermediate Level Waste the storage, including vitrification waste, COVRA started at the end of the eighties to select the process for the HABOG facility. Several concepts were studied and finally in 1993, designing contractors were selected via European qualification procedure. Two contractors were selected :

- HBKC is a consortium composed of two companies in the HBG Group, a world-wide civil contracting company, HBM and HBW; this contractor is in charge of architectural and civil design and execution works.
- SGN, a company of the AREVA Group, is a major engineering contractor in the nuclear field. SGN is in charge of design, implementation of mechanical, electrical and specific nuclear equipment and commissioning.

After a reminder of the project main basic data and of the resulting safety and design criteria, the paper aims at :

- setting out the major project issues and the resulting design and construction
- identifying the various project steps from design to commissioning through basic design, safety analyses, detail design, construction and erection and inactive blank test
- analysing the first experience feedback and defining the lessons to be drawn to provide the methodology and procedure for the design and construction of the future projects.

**ENGINEERING AND VALIDATION ON  
SPACE TRANSPORTATION AVIONICS SYSTEMS  
G. ABOUT - EADS-ST COMPETENCE CENTER  
J.C. MOREY - EADS-ST DEFENCE B.L.**

Avionics systems on board space transportation vehicles concentrate many technical requirements, high level of safety and reliability in-flight and in pre-flight ground operations and tests. Computer and software technology have made possible to take into account more and more functional complexity. Compared to ground-control & command systems, the specific challenges in space avionics are mainly in the level of precision required to succeed a space mission, in the short reaction time of automatic processes needed by the instability of the vehicles and, regarding the development process, in the very late stabilization of the vehicle design.

EADS-ST as prime contractor of ARIANE5 launcher, Automated Transfer Vehicle (ATV) and ballistic Missile systems, has to manage, on avionic systems, the overall process from the initial design up to the in-flight qualification. Avionics teams are particularly in charge of functional and electronic architecture, equipment requirements, flight software requirements (real time algorithm), design and development. At avionic system level, teams are also in charge of all the validation & qualification facilities and tests with respect to scheduling and target costs.

To tackle all these technical constraints, very soon in the development rigorous method and process are laid out to formalize the detailed requirements related to system performances and build a complete validation logic. As much as possible, digital models and simulation are used in the verification phase, but experience and limited know-how on the new technologies used in each space programme required final integration tests on specific benches mixing real time simulation and hardware-in-the-loop simulation and sometimes directly on the vehicle itself. The choices result from of difficult technical and programmatic risks analysis.

Operating for a long time on ballistic missile systems, improvements of the process on functionally complex and redundant avionics architectures, are now demonstrated on ARIANE 5 launcher and put in place on ATV (flight expected in the middle of 2005).

# RISKS MANAGEMENT IN THE CONSTRUCTION OF A NEW TECHNOLOGY BASED – ALUMINIUM SMELTER IN SOUTH AFRICA L. BERTRAND, ALUMINIUM Pechiney

The Coega Aluminium Smelter project concerns the construction of a new plant in South Africa and is innovative in many ways. First of all, this new plant will use the AP50 technology, operating at 500.000 amperes, for the first time. Moreover, the design of the plant will mark a change with the traditional method of smelter construction. This complete change in technology as well as in construction mode requires a thorough analysis of the project's risks.

The risks are multiform. The choice of a location in South Africa generates political and social risks very specific to this country. The social analysis, especially concerning the AIDS pandemic, forces us to work on the implementation of prevention plans for the workers and their families, and to cope with HIV-positive employees.

Concerning the political risk, it is impossible for us to interfere with local politics, so, to protect us against riots, civil commotion or expropriation for example, we must work with major insurance groups to find the appropriate solutions to cope with potential troubles.

Except these business unit environment risks, the major points to manage are, as said above, the technological and construction risks. Risk analyses were thus organized with technology and construction experts.

These risk analyses incorporated historical knowledge on smelter construction, commissioning and operations, or imagined, considering the absence of prior experience with the AP50 technology.

A complete risk universe resulted from these analyses, that materialized in four categories of risks:

- Business unit environment (Economics, sanitary, political...)
- Pre-completion activities (availabilities of equipment, construction activities, commissioning and ramp-up...)
- Business unit liability and undertakings (product liability, contract undertakings...)
- Operations (Raw material supply, health, safety, industrial risks...)

These four categories are divided in 500 risk cards, with around 800 action plans to mitigate the most important risks.

To succeed in the execution of these action plans, it is very important to appoint a sponsor responsible for their follow-up of the risk cards. Only a good management of experts can assure the risk mitigation achievement.

Another key to success is to plan the action plans correctly on the critical path. For example it is very important to first of all ensure a good exchange rate for the funding in a context of low dollar, before knowing how to manage the expropriation risk.

Finally, to prevent any troubles concerning bodily injury or equipment destruction, we work with a company specialised in the prevention of fire, explosion and natural hazards. This partner issued recommendations for the design of the plant so as to avoid future troubles. Moreover, the implementation of these recommendations should allow a HPR (Highly Protected Risk) certification that in turn should lead to reduced insurance premiums.

# DEVELOPMENT OF LARGE CONCRETE STRUCTURES FOR OFFSHORE OR COASTAL FACILITIES

F. SEDILLOT, DORIS Engineering

Over the 40 last years, the structures and systems developed for the offshore oil industry have offered a remarkable field of application for many project management, engineering and construction disciplines. To answer to the need of industrial facilities in the oceans, designers have conceived a variety of support structures: fixed, compliant or floating platforms, made of steel or concrete.

Over the thousands of offshore platforms installed in all the globe oceans, only slightly more than 40 of them were built with concrete. Concrete platforms are often associated to very large field developments. The parameters leading to the choice of a concrete gravity platform rather than a conventional steel structure will be analysed in the presentation.

Doris has been involved in 17 of these projects: always in the engineering activities (conception and basic design, detailed construction engineering) and, often, in the project management and the construction, in association with international civil contractors and local construction companies.

The reputation of Doris in this domain has been established with the concrete gravity platform world premiere, the Ekofisk tank in the North Sea, for which Doris has been awarded the ECPI contract in 1970. Since, Doris has been able to maintain its leadership, as demonstrated with the recent projects of the Hibernia platform, offshore Newfoundland, resisting to the impact of huge icebergs, or the 352 m long floating breakwater of the Condamine harbour, in Monaco.

These two projects will be used as supports to highlight the complex engineering process of a floating or gravity offshore concrete structures. This process is mainly governed by two series of consideration:

- The engineering must combine the requirements from many different disciplines: structural modelling; structural dynamics; reinforced and prestressed concrete calculations; geotechnical analysis; hydrodynamics; naval architecture and weight control; piping and equipment (oil and gas process, mechanical, electrical, control-command, safety, etc).
- The structural design must incorporate the constraints imposed by the construction scenario: this one always includes an afloat construction sequence which often leads to governing load cases.

The attached photographs show some steps of the construction of both the Hibernia platform and the Monaco floating breakwater, which can give an idea of the complexity of the associated engineering.

**SESSION N° 7**  
**PROJECT MANAGEMENT 2**

**CHAIRMEN :** R. MARCILLAT, CNIM  
C. FRANCILLON, EADS ST

Phebus PF Project  
F. SUCHET, J.L. BECH, SETEC-PLANITEC

Knowledge Transfer Between Engineering and Operators  
R. RONDET, SGN

How to Conduct Pre-contract Risk Assessment and Create Value  
A. MALKHASSIAN, SNC-Lavalin Inc.

# PHEBUS FP PROGRAM

## PROJECT MANAGEMENT IN A NUCLEAR CONTEXT

F. SUCHET, JL. BECH, SETEC-PLANITEC

### Contracting part : IRSN

The Institute for Radiological protection and Nuclear Safety (IRSN) was created by decree on February 22, 2002.

The IRSN carries out research and analysis within the fields of nuclear safety, protection against ionising rays, the control and protection of nuclear materials.

The IRSN uses the nuclear reactor Phebus, based in CEA Cadarache research centre, to realize some experiments on severe nuclear accidents.

### **Phebus FP Program**

The experimental setup is a small-scale replica of a pressured water reactor. The plant has undergone considerable change since the end of 1980's to ensure the efficiency and safety. In particular, its building was reinforced to withstand the severest earthquakes liable to occur on the site.

The Phebus FP Program has an international dimension, it is conducted by IRSN in association with EDF, the European commission and American, Canadian, Japanese, Korean, Swiss nuclear safety organizations.

The program includes experiments to reproduce all the phenomena involved during a core meltdown accident and contributing to the release of radioactive products.

6 experiments are scheduled between 1990 and 2005. 4 tests have been successfully completed.

Each experiment is prepared with meticulous care, making extensive use of predictive calculations and lasts about 3 years.

### **Project management**

The main characteristics of the program:

- A complex environment with a plant belonging to the CEA and the tests under the responsibility of IRSN (two independent organizations: one project oriented, the other one workload oriented)
- The Safety constraints: the purpose of the test is to create a nuclear accident and to study its consequences without taking any radiations risk.
- Overall duration (15 years) and the consequences of a test slippage on the following ones.
- The work to be done between two tests (decontamination, modifications,...)
- The funding issues

Force Planitec to set-up rigorous and detailed project management processes:

- A multi-level schedule (Synthetic Program schedule for all the 6 experiments, "level2" schedules for all activities to be done in a 2 years period, weekly-monthly-quarterly schedules for the plant activities,...).
- Interface management between numerous competence centres.
- Ressources management
- Risk management focused on the schedule issues.

# TRANSFER OF EXPERTISE BETWEEN THE ENGINEERING AND THE OPERATOR

P. RONDET, SGN

The Engineering is generally involved through various steps from the feasibility or design of an item of equipment or process up to their delivery to the operator.

## Gathering of Knowledge by the Engineering

Thanks to these different steps, the Engineering will acquire a cumulated knowledge and therefore the proficiency to help the future operator.

### « WHY » : the theoretical knowledge

The design phase gives the Engineering the opportunity to define the operating conditions of its facility ( theoretical knowledge, understanding of the physical, chemical and mechanical phenomena , the nominal operating conditions, the operating limits and the identification of safety and security risks ).

When necessary, the development and qualification phases will help to increase this theoretical and/or practical knowledge (validation or definition of the operating principle)

### « HOW » : the implementation

The construction follow-up phase provides the knowledge of the equipment and of the different interfaces layout within the plant .

The shop tests and the on-site test phases provide a detailed knowledge of the facility, of the operating modes (normal, incidental conditions) and of the maintenance operations.

The knowledge gathered by the Engineering in the various specialties (safety, process, general arrangement, control...) is significant and should therefore be transmitted to the operator.

## Transmission of the knowledge to the Operator

This knowledge can be transmitted via the following means :

### Training

To involve the Operator from the beginning of the shop and on-site tests.

To train the Operator to the process control.

To consolidate the Operator training with theoretical sessions, platform tests ( learning the automatic cycles and associated controls) and through teaming up.

To train the Operator to the analysis of results (To identify the most important parameters to be monitored)

### Technical assistance

To help the Operator during the switching to industrial rate.

To record, analyze and make a synthesis of the facility events and failures.

To Identify the potential deviations of the operating parameters.

To propose and optimize the operating sequences to enable the increase of the production rate and to ensure the reliability of the facility.

To optimize and validate the operating and maintenance procedures.

To be the interface between the Operator and the Engineering so as to identify any modifications to the production tool which may be necessary to reach the targets.

### Drawing up an experience feedback file

Through this assistance to the Operator the Engineering acquires a significant experience feedback which is essential for its new projects or for the modifications to the existing production tool (This should result in a better understanding of the Client's technical and economical requirements with respect to cost and deadlines for instance).

**HOW TO CONDUCT PRE-CONTRACT RISK ASSESSMENT  
AND CREATE VALUE**

**A. MALKHASSIAN, SNC-Lavalin Inc.**

**SESSION N° 8**  
**NEW TECHNOLOGIES INTEGRATIONS 3**

**CHAIRMEN :**                   D. DUMOND, SGN  
  JF. CAZES, TECHNIP

Hall of Experience of the “Ligne d’intégration Laser”  
T. CHARGY, CEA/CESTA

Co-Mining Technology : New generation of Command Control Systems  
M. NAILLON

Qualification of Complex Systems  
M. BOZIO, C. LALANNE, CEA

HALL OF EXPERIENCE OF THE  
“LIGNE D’INTEGRATION LASER”  
T. CHARGY, CEA/CESTA

*Abstract not available*

# CO-MINING TECHNOLOGY NEW GENERATION OF COMMAND AND CONTROL SYSTEMS M. NAILLON

## Activity :

---

The mission of CO-MINING<sup>®</sup> TECHNOLOGY is to design and publish the new-generation decisional systems based on the world wide patented Co-Mining<sup>®</sup> technology, which is a radical **technological breakthrough**. Those systems analyse, model, and industrialize decision-making strategies used by numerous operators (eg: financial community, military intelligence, who are faced with a multitude of data and decision support tools as it is in trading rooms, military command centres, or management committees).

Cognitive Invariance<sup>®</sup> mechanism is apply to design the product named a “Co-decider” which controls a decisional processes. This mechanism has the ability of decoding the invisible bias introduced by the human subjectivity of the decision makers when they are under the pressure of continuous, contradictory and global information flows. Dialoging with such “Co-deciders”, the users early collectively detect those bias and construct a more objective and transparent reality

## Prior applications :

---

Intelligence service officers, more than never in the current international terrorist atmosphere and global investment banking corporations in the current investor’s confidence crisis have both a crucial need of controlling the subjective interpretations and decisions of their operators. That’s why, referring first to the hunch decision principle of military community recently referred by the US DOD and secondly to Behavioral Finance approach recently awarded by the 2002 Economy Nobel prize, the company decided to develop in parallel those two urgent applications

## History and perspectives :

---

Coming from 20 years industrial R&D, civil and military, lead by Dr Martine Naillon, particularly in electronics and aerospace industries, the Co-Mining<sup>®</sup> radical innovation results from a long term alternative multidisciplinary technological vision, in advanced Artificial Intelligence based on Mathematics, Biology, Neuroscience, Cognitive psychology and Phenomenology. As the inventor of the technology, the founder decides 7 years ago, to lead to maturation her vision and patented it. The result is a technological gap corresponding to a new emerging market for co-decision systems. Nowadays, perspectives are multiple : Finance, Defense, 3G Telecom, satellite driven navigation (Galileo project), future generation Business Intelligence, Biotechnology (Artificial Genome), judicial inquiries, corporate management. With a global client in Finance and offers from national and European Defense in military and anti-terrorism surveillance, the company starts to be profitable in 2004 with a value growth with a 20 factor  
The “Cognitive anticipation” for an unstable world

---

Irrationality, blindness, enclosure drive our perception, introducing cognitive bias. If not, how to explain the markets believes obvious lies, that intelligence services don’t anticipate some terrorism actions, that a team in a company don’t see what is necessary to colleges to be efficient and profitable to the company,...

Irrational is the market because bad memories could be kept a long time, blind could be the policies because too much concentrated on a given line, enclosed on her/himself can

be a person regarding another one in a company because too much concerned by her/his history

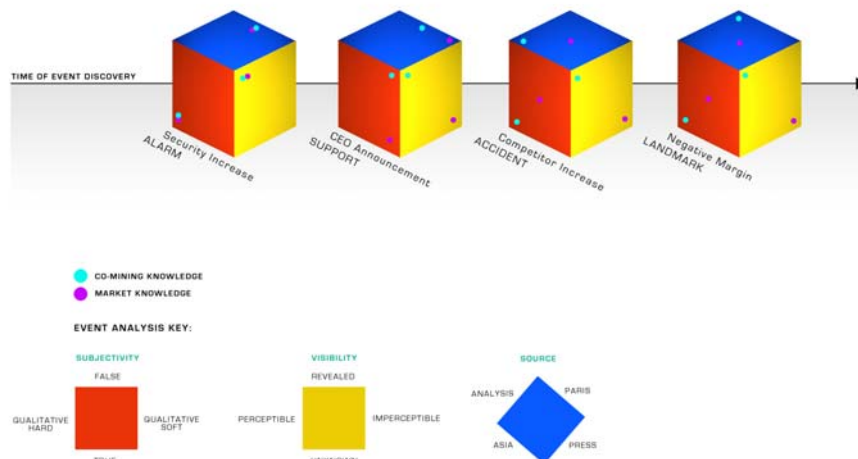
“Cognitive anticipation” as introduced by CO-MINING<sup>®</sup> TECHNOLOGY is the ability (i) to make key and early links between information (ii) to turn around the information to consider it’s different subjective interpretation faces (iii) to compute the propagation time for an information to be revealed (see figures). Doing so, the financial market players users of a global bank can keep control on their collective decisions; the military, policy, judiciary users can make early secret decisions anticipating attacks and revealing inquiry truth ; the corporate manager users can early decode their own and collaborator’s behaviors before the atmosphere being spoiled and act with a concord governance

## Moulinex defining events...

After 2 years in bad shape, the Moulinex stock started to increase. The **STOCK INCREASED SIGNIFICANTLY** after a **CEO DECLARATION** was made, announcing strong Moulinex sales. However, due to **INTENSE COMPETITION**, Moulinex only increased sales by operating with a **NEGATIVE MARGIN** which was known by very few people and eventually led to its downfall.



## Co-Mining<sup>®</sup> Technologies Cube Model Showing Event Analysis (Track 1):



The product : A Co-Decider and it's revolutionary MMI (Man Machine Interface)

The user learns to his/her machine how he/she thinks and decides. The core of the Co-Mining® innovative process relates to the way decisions are coded : Decisions are modelled in the form of micro-decision strings which create semantic links between key information objects, referred to as "Portable Distributed Objects®"

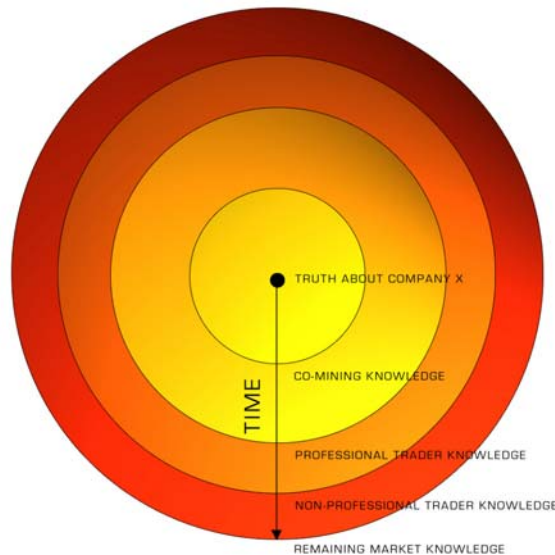
The machine is able to mimic the user reasoning, creating key links between information that usually the user has neither enough time and mental availability neither enough honest human relationship to consider them.

The user is immersed in a Virtual Reality (VR) room or cabin, with colors, enabling him/her to quickly perceive his/her own or college irrationality, blindness or enclosure. The users can touch their MMIs to feel the market, the terrorists, their colleges, the political trends,...

Experiment in immersion VR rooms are organized for convergence dual applications : Military C2I simulation, urbanism, financial markets, judiciary instruction in civil or financial affairs

## Co-Mining® Technologies

### Cognitive Anticipation



# QUALIFICATION OF COMPLEX SYSTEMS

C. LALANNE, M. BOZIO, CEA

"Extreme response spectra (ERS) and fatigue damage spectra (FDS) used for the severity comparison of several vibrations and for writing test specifications can be calculated directly from the time history signal or from its power spectral density (PSD) when the vibration is random, stationary and Gaussian. The sampling rate given by the Shannon's theorem is enough for ERS and FDS calculation starting from the PSD. It is shown that it is necessary to sample the signal with a very higher frequency to be able to deduce directly these spectra from it with the same precision."

# PLENARY SESSION

**CHAIRMEN :** D. CABANEL, EADS ST  
JF. CAZES, TECHNIP

The Safety Influence in the Development of the Swissmetro project  
M. MOSSI, GESTE Engineering

Risk Mitigation for ISS (International Space Station)  
S. CLANTON, JACOBS SVERDRUP  
J.M. HOLT, NASA

Complex Engineering: The Example of the Space Transportation Systems  
T. LEVEUGLE, EADS ST

# THE SAFETY INFLUENCE IN THE DEVELOPMENT OF THE SWISSMETRO PROJECT

M. MOSSI, GESTE Engineering

The continuous growth of people mobility and freight transport observed in many countries has resulted in a saturation of the infrastructures for air, sea and land transportation. During the last few years, different approaches have appeared to counterbalance the negative impact of this global rise in mobility. In this context, the development of new environmental friendly, economical and ecological high-performance transport systems is vital. The Swissmetro Maglev occupies a leading position in this movement. The Swissmetro concept is that of a vehicle travelling at high speed in a mono-directional underground tunnel maintained under a partial air vacuum at the same pressure level as met by the supersonic civil aviation (corresponding to an altitude of 15'000 m). The infrastructure contains two parallel tunnels, one for each direction, connected to the stations of the surface transport networks. The Swissmetro passenger transport system is based on advanced technologies – such as linear electric motor and magnetic levitation – which allow it to reach speeds of over 500 km/h, guaranteeing economical energy consumption and minimum maintenance, whilst ensuring maximum passenger safety and comfort.

The article will present the development status of the Swissmetro project whilst pointing out the safety aspects and their influence on the different development stages, namely:

- integration of the safety considerations from the early development stages;
- Impact of safety in the choice of the project reference values;
- Impact of safety aspects in the future development phases.

Since the Swissmetro is meant to transport passengers in an underground vehicle moving in a tunnel under partial air vacuum, the demonstration that all safety issues are fully under control is in fact a key point in the project development and in the different processes of the dependability demonstration and project acceptance.

# CASE STUDY OF RISK MITIGATION BASED ON HARDWARE/SOFTWARE INTEGRATION (HSI) TESTING FOR THE INTERNATIONAL SPACE STATION

J.M. HOLT, NASA

S.E. CLANTON, JACOBS ENGINEERING SVERDRUP

Within the pressurized elements of the International Space Station (ISS), requirements exist to ensure a safe, habitable environment for the crew. In order to provide this environment, thermal control components work in conjunction with software controls to provide heat rejection for subsystem avionics equipment, for the environmental control system and for experiment payloads. It is essential to ISS operations, mission success and crew safety that necessary testing incorporates the extreme conditions to ensure proper performance. This paper provides a general description and methodology applied to thermal related Hardware/Software Integration (HSI) tests for the ISS Node 2 module. A detailed test plan was developed and implemented with two objectives : the first was for risk mitigation of the thermal control algorithms and software qualification, and the second was for data collection which will substantiate thermal/hydraulic models of the Internal Active Thermal Control Systems (IATCS). Analytical models are utilized to determine on-orbit performance for conditions and scenarios where the simulation of actual on-orbit system performance is limited by test configuration constraints. Node 2 IATCS HSI activities were performed at the Alenia Spazio facility in Torino, Italy with participation from the National Aeronautics and Space Administration (NASA), Alenia Spazio, Jacobs Engineering Sverdrup (JE Sverdrup) and Boeing

COMPLEX ENGINEERING :  
THE EXEMPLE OF THE SPACE TRANSPORTATION  
SYSTEMS

T. LEVEUGLE, EADS SPACE Transportation

*Abstract not available*

**SESSION N° 9**  
**PROJECT MANAGEMENT 3**

**CHAIRMEN :** M. INVERNIZZI, CEA/DAM  
T. LEVEUGLE, EADS ST

Risk Management in Foundation Treatment Design  
N. IBRAHIM, Hydro-Plan Associates

Managing State Reform  
G. GRAS, THALES Engineering Consul.

# RISK MANAGEMENT IN FOUNDATION TREATMENT DESIGN

N. IBRAHIM, Sabke Dam Project, Katsina State, Nigeria.

The Sabke Dam Project is one of the numerous dam projects embarked upon by the Federal Government of Nigeria with the aim of alleviating the problem of water shortage for utilitarian and irrigation use. The dam is located about 550km north of Abuja (the nation's capital), 12m high, crest length of 682m and composed of about 450,000 cubic meters of fill materials. Other structures include a spillway, raw water pump and power stations, intake tower and a valve chamber immediately downstream of the dam.

The dam is constructed across the Sabke River near the border town with the Republic of Niger. Bedrock mapped within the core trench consists of partly weathered sedimentary rock to fresh basement.

To reduce or eliminate the flow of water through the dam foundation and to reduce the risk associated with the stability of the structure due to the unfavorable underlying sub surface formations, the dam designer proposed a corrective operation of foundation grouting. It is a process where open joints or spaces are filled with grout that is usually composed of a mixture of cement and water. The effectiveness of the grouting operation depends on the conduct and result of a flawless sub surface investigation and subsequent design of the grout mix. Any deviation from this correct practice results in the risk of high seepage and dam instability. The initial grout volume proposed for incorporation into this dam was 35 tonnes while after a complimentary sub surface investigation adopting the High Resolution Seismic Reflection technique, the grout volume increased to 3450 tonnes. For this kind of increase (about 100 fold) the indication is that the sub surface investigation carried out at the time of tender was unreliable.

One of the challenges to the construction industry in Nigeria in general and to a complex and high-risk structure such as a dam in particular is the risk associated to faulty designs due to evolving and emerging conditions through the project lifecycle and the environment. To avoid construction projects failures and optimize deliverables, there is the need for effective and deliberate approach to risk management.

This paper introduces the concept of risk management in dam foundation design and the effects during and after construction and concludes by proffering systematic approach to risk management for sound engineering works.

The author is a Partner of Hydro-Plan Associates, a consulting engineering outfit based in Kaduna, Northern Nigeria. A Civil Engineer by training and profession and has been in practice since 1990 upon graduation.

## MANAGING STATE REFORM

### D. GRAS, THALES Engineering Consulting

For almost half a century, governments have been investing in a system of international organisations known as donors: World Bank, Regional Development Banks, Agencies of the European Commission and the United Nations) which fund reform in developing countries.

What is habitually called “the fall of the Berlin wall” – in fact the collapse of planned economies, i.e. those not run in accordance with market rules – introduced a sustainable change on this market in 1992; the scale of this change only appeared at a later date, and it has a considerable effect on the current orientation of development consulting.

To begin with, the donors quickly opened up lines of credit as emergency measures to shore up what very few (actually none) of the political masters of the planet had anticipated, with the aim of avoiding any aggravation of the situation in the countries of Eastern Europe and the former Soviet Union, as this would generate worldwide economic disorders and social problems that would be difficult to control. These funds were used to train civil servants and engineers, to support private farmers and social services, to requalify surplus army officers and to increase security for nuclear power plants, and to reform government organisation, and these were followed by the preparation of the first privatisations and backup for burgeoning SMEs.

This movement was gradually organised during the second half of the 1990s. On the one hand, the donors arranged their programmes around the broad conventional fields of public action: education, employment, environment, transport and energy. On the other hand, a set of projects emerged that concentrated on the reorganisation of structures allowing the States to carry out their basic functions: drafting legislation and ensuring its application, levying income tax, regulating the economy, controlling the development of the country and defining the role and status of its agents. This was dubbed “State Reform”. We then endeavoured to develop systematic action on this segment, based on our previous experience in the transfer of know-how and on expertise – a new departure for our firm – reposing chiefly on the administrations and top institutions in European countries. This action involves the development of a large number of partnerships with these administrations and public institutions (Cooperation Agencies in the Ministries, Schools of Administration and Universities).

The problems to be tackled are complex and interacting: application of the rules of the World Trade Organisation, for instance, presupposes changes in economic legislation, which will influence both the organisation of the legal system and the economic development of the regions, and this obviously requires State coordination and control of financial instruments. This work is carried out both systemically and in depth necessitating diversified expertise, involving projects that are larger, more costly and more complicated to manage. This entails the use of complex management which must take into account top-level expertise of various origins (in particular experts who are not used to the consultant approach), open-ended customer demand and strict administrative and financial constraints.

**SESSION N° 10**  
**INDUSTRIALISATION, TEST AND**  
**QUALIFICATION**

**CHAIRMEN :**           D. SALASCA, THALES  
                              G. ROUSSEAU, SETEC-  
PLANITEC

CAEPE : the Mastery of Complex SRM Testing  
S. SAUVAGE, CAEPE

Static Verification of Embedded Critical Software  
A. DEUTSCH, POLYSPACE Technologies

Risk of Evaluation of the FAL A380 Project  
C. ETCHEVERRY, AIRBUS France  
P. GATARD, EADS APSYS

CAEPE: THE MASTERY OF COMPLEX SRM TESTING  
S. SAUVAGE, CAEPE

*Abstract not available*

# STATIC VERIFICATION OF EMBEDDED CRITICAL SOFTWARE

## A. DEUTSCH, POLYSPACE TECHNOLOGY

We present the principles and applications of static verification of dynamic properties to the development verification and validation of embedded applications and corresponding industrial tools which originated in the automated verification of the Ariane 502 flight program. The topic covered include : what static verification of dynamic properties is, how it works, how it can help in verification, how our technology brings unique benefits and validation activities and how it synergistically integrates with existing standards such as CMM, Ticklt, MISRA, DO-178B or SPICE.

We present an industrial tool for the automatic detection of run-time errors. The most salient and distinguishing properties of our approach :

- 1- detection of 100% of buffer overflow, array indexing, arithmetic overflow, divide by zero, shared variables, ...
- 2- only the source code is necessary, no annotations, assertions or test cases are required
- 3- it operates on Ada 83/95, Java, C, and C++ codes. No adaptation of the tool to specific codes is necessary

This tool has been developed with the support of CNES/DLA and is the industrial descendant of a prototype first tested on the Ariane 502 Flight program with EADS LV in 1997; Our technology is now used by Lockheed Martin, BMW, NASA, Honeywell, Thales Avionics, Bosch, IRSN, Valeo and by more than a hundred other customers in Europe, America and Asia in embedded systems in aerospace , defence, automotive, medical equipment, telecom, ground transportation and power plant.

# RISK EVALUATION OF THE FAI A380 PROJECT

C. ETCHEVERRY, AIRBUS France

P. GATARD, EADS APSYS

Considering the requirements of the November the 5<sup>th</sup>, 2002 law : compulsory drawing up of the single document, and the greatness of the project : the plane is 80 meters long and 80 meters wingspan, the main factory building will be 250 m wide and 500 m long; the department of risks prevention at AIRBUS has decided to integrate the human factor as soon as possible into the design of the A380 final assembly factory, a mission given to EADS APSYS.

The methodology to carry out this a priori evaluation is based on the existing system : an up to date list of risks and a matrix of evaluation. Today this system serves for piloting the safety policy. We add to this a posteriori system, an a priori vision in order to follow the progress of the project. The A380 FAL is organised according to the concurrent engineering method.

An example of analysis of post and its follow up : the A380 half wing

Its characteristics,

The means and the foreseen processes

The hypotheses of future activity

The inventory of the risks

The evaluation

The solutions

The integration of the solutions into the design of the post

In order to have a global vision of this analysis it is necessary to draw up a board. It helps to pilot the FAL by indicating the potential hard points and to guide on the actions to be led in order to conceive a sure manufacturing tool.

A second example of security studies made in Toulouse concerns the outside areas of final tests and preparation of the first flight.

The needs and constraints of the post

The activities

The methods : - exhaustive inventory by type of flow  
- inventory of the risks

The decision : trade-off

The chosen solution

A last example of the work made for the A380 FAL is the writing of a post security handbook. The AIRBUS department of prevention had the idea to use all the professional risks analysis to compile a security handbook for every workstation. It describes entirely the post, its functioning, the main risks generated by the activities and the way to protect oneself from them. It also contains a large number of information directly linked to human security.

The description of each activity, inferred risks, record of safety in touch with this risks, collective protections to be operated, individual protections to be carried, organisation and means.

## Conclusion

The dimension of the project about which we spoke in introduction and which motivates this analysis “a priori” exists really today. The first elements of planes are already made and I would like to show you now some sight. From the work sharing of the main elements and their transport in all Europe to Toulouse where they will be assembled. Secondary some views of the assembly and integration workstation, the 3 test locations and finally the outside places of final test and preparation for the flight.

