STSARCES : an European research initiative to harmonize validation methods on safety related complex electronic systems

Philippe Villeneuve de Janti

STSARCES : AN EUROPEAN RESEARCH INITIATIVE TO HARMONIZEVALIDATION METHODS ON SAFETY RELATED COMPLEX ELECTRONIC SYSTEMS

Author

Villeneuve de Janti, Ph. , Institut National de l'Environnement Industriel et des Risques,
Parc Technologique Alata, B.P.n°2, 60550 Verneuil en Halatte, France
Coordinator of Stsarces

Résumé

Dans le cadre de la Directive Machines, des travaux de normalisation du CEN/CENELEC sur les parties des systèmes de commandes de machines liées à la sécurité ont mis en évidence des difficultés pour définir des méthodes harmonisées d'évaluation, aussi bien d'analyse que de test, quand sont mises en oeuvre des technologies électroniques intégrées, en particulier programmables. Aussi plusieurs organismes de recherche et de certification, ainsi que des industriels, se sont regroupés pour lancer une initiative de recherches en soutien à la normalisation, STSARCES, qui a reçu l'appui financier de la Commission Européenne.
Les résultats doivent permettre d'harmoniser les procédures de certification et ainsi de réduire les barrières techniques pouvant freiner le libre-échange au sein de l'Union Européenne.

1. Introduction

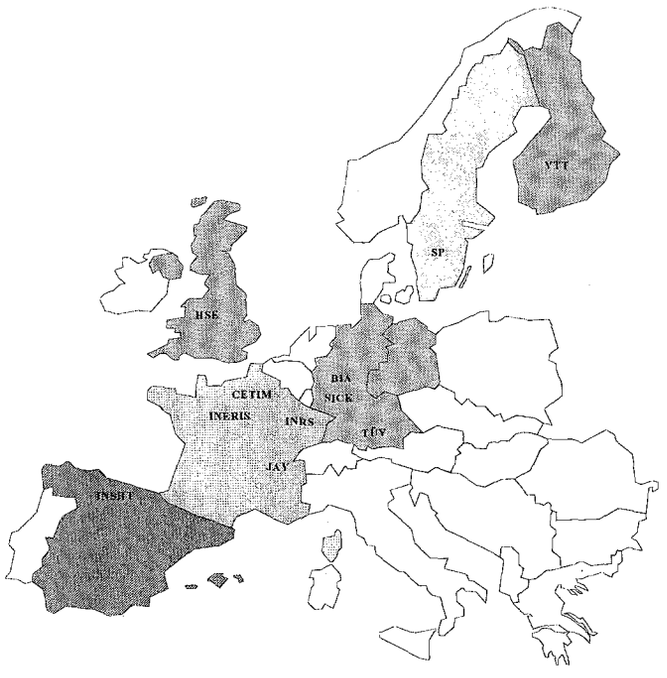
In the new approach to machinery - 89/392/EEC Directive and its amendments- it is intended both to render the machinery necessary for European industry as safe as possible from the design stage onwards and to ensure that the safety features incorporated to achieve this end do not form technical barriers to the commercial exchanges between the member states of the Community.

The essential requirements regarding the safety related parts of control systems are covered by EN 954 part 1 dealing with general principles for design and accepted as European Standard in July 1996. Current work on validation proceeding for the different technologies involved, being the goal of the draft EN 954-2, has demonstrated that no harmonized validation procedures exist for safety related complex electronic systems. A lack of knowledge has proved paramount when facing faults on complex components, which are becoming of a generalized use in the field of machinery safety.

The STSARCES (STandards for Safety Related Complex Electronic Systems) project (1) aims at speeding up the harmonized putting into practice of the EN 954 part 2 by the European Test-Houses as well as by manufacturers of the European Union. Along with research programmes, it faces the problems raised by divergent approaches between the EN 954 and the IEC 61508 Standards, which are strategically valuable to the European economy, since this International Standard, likely to be wholly published during 1999, will be proposed for adoption as an European Standard. The project deals also with innovative technologies and designs, in close relationship with manufacturers, to avoid innovation obstacles.

STSARCES : AN EUROPEAN RESEARCH INITIATIVE TO HARMONIZEVALIDATION METHODS ON SAFETY RELATED COMPLEX ELECTRONIC SYSTEMS

2. The Consortium



The consortium is made of 11 partners from 6 different countries :

- INSHT (Spain)
- CETIM, INERIS, INRS, JAY-Electronique (France)
- BIA, SICK AG, TUV-IQSE (Germany)
- HSE (United-Kingdom)
- SP (Sweden)
- VTT (Finland)

3. Organization of the Work-Programme

The project comprises several steps carefully scheduled in time :

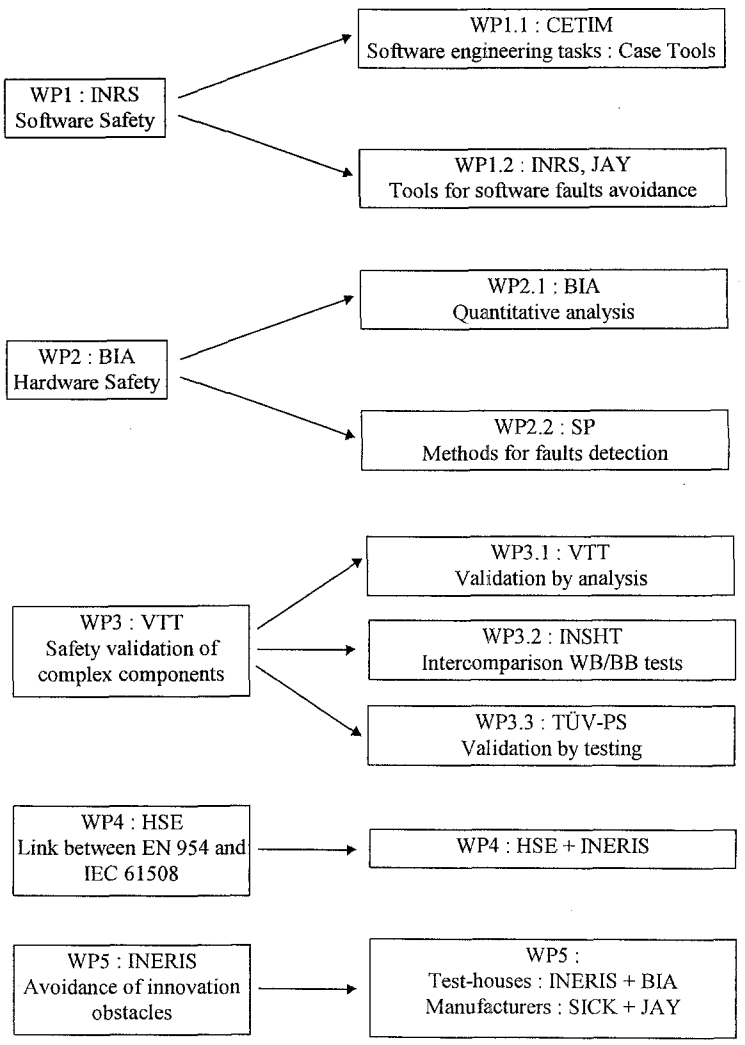
- **STEP 1** : Research studies to fill gaps. Knowledge has to be developed or completed regarding assessment and validation techniques of both hardware and software safety in complex electronic components or systems (**12 months**).

- **STEP 2** : Validation of proposed methods by applying them to different on-the-market systems of graded levels.
This step allows avoidance of discrepancies between research works and practical realistic problems encountered while considering industrial safety products (**6 months**).

STSARCES : AN EUROPEAN RESEARCH INITIATIVE TO HARMONIZEVALIDATION METHODS ON SAFETY RELATED COMPLEX ELECTRONIC SYSTEMS

- **STEP 3** : Integration by a transverse action of results and experience of the other test-houses partners in the project, and also of the participating manufacturers. It allows to reach an European agreement regarding harmonized procedures with a good acceptance by the concerned industry (**5 months**).

- **STEP 4** : Formatting the results so that the proposed harmonized validation methods can be transfered right on time as a technical and application guide to CEN to support the EN 954-2 draft standard (**4 months**).



STSARCES : AN EUROPEAN RESEARCH INITIATIVE TO HARMONIZEVALIDATION METHODS ON SAFETY RELATED COMPLEX ELECTRONIC SYSTEMS

In order to succeed sustaining an efficient level of communications between the partners, the tasks are organized into « clusters » of sub-tasks, and each cluster is managed by a partner being himself a member of the Steering and Management Committee of the project.
It is soundly believed by the Consortium that Software and Hardware aspects cannot be approached completely independently when facing assessment of safety related complex electronic components or systems, which are presently very often programmable ones. The "SYSTEM" approach is therefore enhanced in the course of the project, for instance in individual Work Programmes like "Validation by analysis" where an investigation is led on interconnected components and bus systems safety aspects, and also in a transverse action in STEP 3 which covers all the technical Work Programmes.

4. Progress status and preliminary results

The project was operationally launched in January 1998.
An international Workshop was organized at 'la MAISON de l'EUROPE' in Paris on 6 March 1998.
It was a first CHECK-POINT event in the programme of the STSARCES project and attendants from all parties (twenty-three external experts from 13 countries, including CEN/CENELEC representatives) were invited to give comments on any aspects of the project, and particularly on :

- validity of the technical approach proposed by the STSARCES Consortium
- points that should be reinforced or suggestions to improve the overall value of the project.

The Consortium received many requests from manufacturers and laboratories to establish working relationship in the course of the project, like IVF (Sweden), SCHNEIDER (France), SIEMENS (Germany), BFZ-Arsenal (Austria), the Central Institute for Labour Protection (Poland).The German machine tool builder's association, emphasized the importance of the STSARCES project not only for the manufacturers of safety systems but particularly for machine manufacturers which are the main users of that equipment. In order to ensure that results from the project are well accepted in the market, he asked for an efficient information flow between machine tools manufacturers and STSARCES. Therefore manufacturers will be invited to participate to an International Seminar before the end of the project.
The draft of a report issued by HSE (2) « A STUDY OF THE LINKS AND DIVERGENCES BETWEEN DRAFT IEC 61508 AND EN 954 » received the agreement from the Steering Committee on September 1998 for dissemination outside of the Consortium.This document, also circulated to the JWG 6 CEN/TC 114 & CLC/TC 44X standardization group, is available on request.

All the other intermediate reports issued until the Mid-Term Consortium meeting held on last March 1999 in the premises of the European Commission, DG12, in Brussels, are not yet authorized for external dissemination.

However most of the results are foreseen to be presented by their own authors in their almost definitive form at the MONTREAL INTERNATIONAL CONFERENCE.
The STSARCES Programme includes also a Seminar with manufacturers and the Standardization bodies by the last months of the project, its aim being to validate the putting-into-practice capabilities achieved by the final report under preparation by the Consortium.
It is the hope of the partners in this project that the MONTREAL event, thanks to its large international attendance, might well be an excellent opportunity to hold this Seminar in the presence of the Project Officer of the European Commission.

5. Footnotes

1. European Commission, contract SMT4-CT97-2191.

2. Brown, S.J.; Frost, S.; Health and Safety Executive, Electrical and Control Systems Unit, Technology Division. A study of the links & divergences between draft IEC 61508 and EN 954. WP4 Task1 Report (Ref: STS-WP4-1001) Issue 02, September 1998.