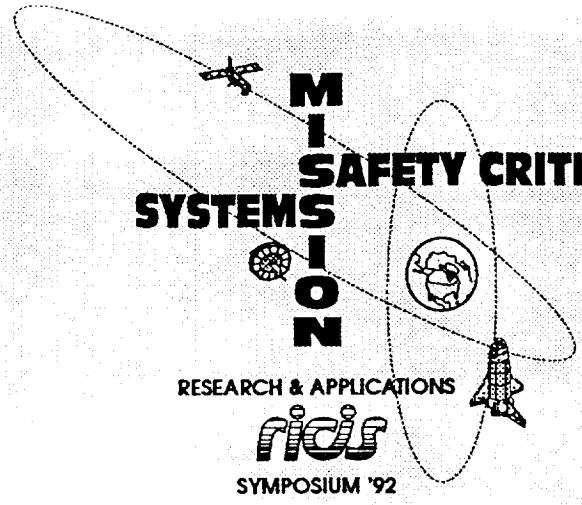


EUROPEAN WORKSHOP INDUSTRIAL COMPUTER SYSTEMS APPROACH TO DESIGN FOR SAFETY

Dr. Janusz Zalewski

ABSTRACT

This contribution presents a set of guidelines on designing systems for safety, developed by the Technical Committee 7 on Reliability and Safety of the European Workshop on Industrial Computer Systems (EWICS). Their focus is on complementing the traditional development process by adding the following four steps: (1) Overall Safety Analysis; (2) Analysis of the Functional Specification; (3) Designing for Safety; (4) Validation of Design; Quantitative assessment of safety is possible by means of a questionnaire composed of a number of modules covering various aspects of all major stages of system development.

BIOGRAPHY

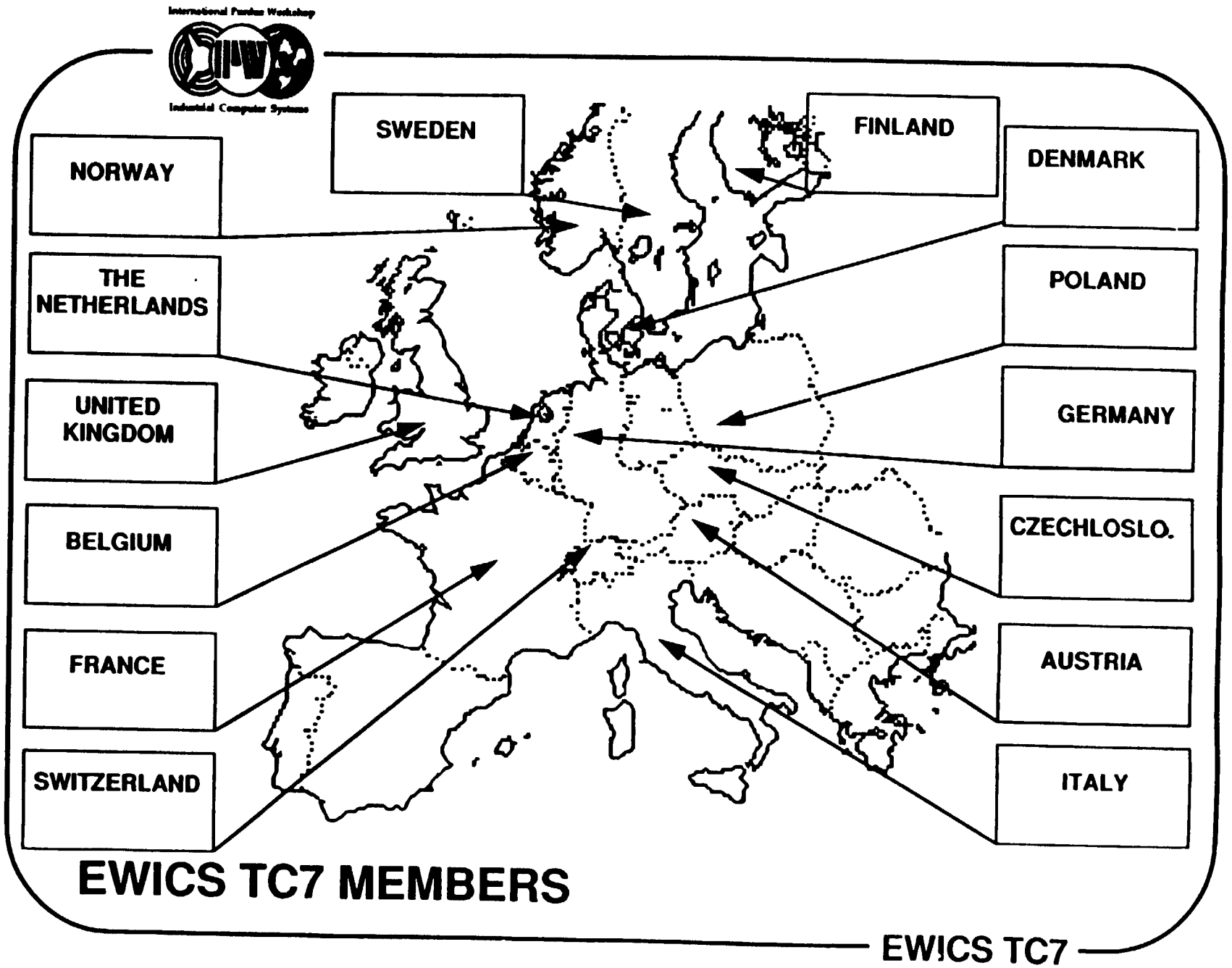
Dr. Zalewski has been working for over 15 years in nuclear research institutes in Europe. As a member of the European Workshop on Industrial Computer Systems he participated in the development of EWICS guidelines for the construction of safety related systems. Most recently he has cooperated with the Data Acquisition Group of the Superconducting Super Collider Lab, in Dallas, working on the real-time kernels and real-time expert systems. Since 1989 he is on faculty at the Dept. of Computer Science, SW Texas State University, where he teaches Real-Time Systems and Software Engineering.

International Purdue Workshop

Industrial Computer Systems

EWICS APPROACH TO DESIGN FOR SAFETY

Janusz Zalewski
Dept. of Computer Science
Southwest Texas State University
San Marcos, TX 78666-4616
JZ01@SWTEXAS.Bitnet


SWEDEN
FINLAND
NORWAY
DENMARK
THE NETHERLANDS
POLAND
UNITED KINGDOM
GERMANY
BELGIUM
CZECHLOSLO.
FRANCE
AUSTRIA
SWITZERLAND
ITALY
EWICS TC7 MEMBERS
EWICS TC7

International Purdue Workshop

MEMBERSHIP (Industries)

- Information Technology
- Nuclear
- Transportation
- Energy
- Chemical
- Telecommunication

PRINCIPLES FOR SAFE DESIGN

- Relate Target Safety Reqs to Plant Safety
- Structure According to Criticality
- Ultra-High Rel. of Safety-Critical Modules
- Design for Safety
- Monitor safety Continuously
- Independence of Safety-Related Activities

FOUR SAFE DESIGN STEPS

- Overall Safety Analysis
- Analysis of the Functional Specification
- Designing of Target System
- Validation of Design

1. OVERALL SAFETY ANALYSIS

- INFORMATION OF THE ENVIRONMENT
- DESCRIPTION OF THE PLANT
- SAFETY CRITERIA
- REGULATIONS AND CONSTRAINTS
- AUXILIARY INFORMATION
- RISK ANALYSIS RESULTS

International Purdue Workshop

Industrial Computer Systems

2. ANALYSIS OF FUNCTIONAL SPEC

- DECOMPOSITION OF THE SPECIFICATION
- CLASSIFICATION OF TARGET SYSTEM RESPONSES
- INVESTIGATION OF TARGET SYSTEMS INFLUENCES
- SAFETY ANALYSIS OF THE FUNCTIONAL SPEC

3. DESIGNING OF TARGET SYSTEM

- PRINCIPLES AND TECHNIQUES FOR SAFE DESIGN
- INTERFACES TO THE PLANT
- SPECIFIC DESIGN CONSTRAINTS
- SPECIFIC FEATURES TO ENHANCE SAFETY
- REVIEWED FUNCTIONAL SPECIFICATION

4. VALIDATION OF DESIGN

- Checking Criteria and Constraints
- Failure Analysis
- Functionality Checks
- Availability/Maintainability Checks
- Integrity/Fault-Tolerance Checks
- External Threat Checks

THE QUESTIONNAIRE

- PROJECT PLANNING AND MANAGEMENT
- SYSTEM REQUIREMENTS SPECIFICATION
- DESIGN
- CODING AND CONSTRUCTION

THE QUESTIONNAIRE (Cont.)

- INTEGRATION OF HARDWARE AND SOFTWARE
- VERIFICATION AND VALIDATION
- QUALIFICATION
- OPERATION AND MAINTENANCE

SAFECOMP Workshops

- 1979 Stuttgart, Germany
- 1982 West Lafayette, IN, USA
- 1983 Cambridge, UK
- 1985 Como, Italy
- 1986 Sarlat, France
- 1988 Fulda, Germany
- 1989 Vienna, Austria
- 1991 Trondheim, Norway
- 1992 Zurich, Switzerland

F. Redmill (Ed.)
Dependability of Critical Computer Syst
Vol. 2, Elsevier, 1989

IEC STD 880, 1986
Software for Computers in the Safety Systems of Nuclear Power Stations

EWICS TC7