COMPLIANCE TO IEC60880 WITH SCADE 6 – DESIGN AND IMPLEMENTATION ASPECTS

(ABSTRACT)

JUL 06, 2009

Table of content

1. INTRODUCTION

1.1. PURPOSE

This document presents means of compliance to IEC 60880 in a process using SCADE Suite 6, regarding design and implementation aspects.
For objectives/activities that are not mentioned in this document, the project is supposed to be based on traditional methods.

1.2. RELATED DOCUMENTS

1.2.1. Norms and Standards

[IEC-60880]

CEI-IEC 60880: second edition 2006-05
Nuclear power plants – Instrumentation and control systems important to safety – Software aspects for computer-based systems performing category A functions
CEI/IEC 60880:2006

[IEC 61508-1]

Functional safety of E/E/PE safety-related systems – part 1
General Requirements
CEI/IEC 61508-1:1998

[IEC 61508-3]

Functional safety of E/E/PE safety-related systems – part 3
Software Requirements
CEI/IEC 61508-3:1998

[IEC 61508-4]

Functional safety of E/E/PE safety-related systems – part 4
Definitions and abbreviations

- CEI/IEC 61508-4:1998

[EN 50128]

Railway applications – Communications, signaling and processing systems
Software for railway control and protection system
EN 50128:2001 E

[EN 50129]

Railway applications – Communications, signaling and processing systems
Safety-related electronic systems for signaling
EN 50128:2003 E

[C-ISO]

Programming languages – C
ISO/IEC 9899:1990

1.2.2. Software Requirements Specifications

[SCADE_RM]
Scade 6.0 Language Reference Manual
KCG-SRS-007
Esterel Technologies

[KCG_TOR]
Tool Operational Requirements
KCG-SRS-006
Esterel Technologies

1.2.3. Project Reports

[KCG_IEC61508]
Compliance analysis to standard IEC 61508
KCG60-TR-004
Esterel Technologies

[KCG_SR]
Safety Risk Analysis Report
KCG60-TR-008
Esterel Technologies

[KCG_SCI]
Software Configuration Index for FQ/R
KCG60-TR-026
Esterel Technologies

1.2.4. SCADE Suite Documents

[SC-TM]
SCADE Suite Technical Manual
Esterel Technologies
SC-TM-61

[SC-UM]
SCADE Suite User Manual
Esterel Technologies
SC-UM-61

1.3. GLOSSARY

1.3.1. Abbreviations

Abbreviation	Definition
ET	Esterel Technologies
HLR	High Level Requirements
incl.	including
KCG	SCADE Qualifiable Code Generator
LLR	Low Level Requirements
MBD	Model Based Development
MC/DC	Modified Condition/Decision
MTC	Model Test Coverage
Mx	Matrix
QA	Quality Assurance
QMTC	Qualified Model Test Coverage
SCADE	Safety Critical Development Environment
SDE	Software Development Environment
SDP	Software Development Plan
SDS	Software Development Standard
SQAP	Software Quality Assurance Plan
SQE	Software Quality Engineer
SRS	Software Requirement Specification
SVP	Software Verification Plan
SW	Software
TOR	Tool Operational Requirements
TQP	Tool Qualification Plan
V&V	Validation and Verification
wrt	with respect to

1.3.2. Terms

1.4. DOCUMENT OVERVIEW

This document is structured as follows:

- Chapter 1 defines the objective of the document, its referenced documents, terms and abbreviations
- Chapter 2 provides the compliance method to IEC 60880 with SCADE regarding design and implementation aspects
- Chapter 3 provides the compliance method to IEC 60880 with SCADE regarding language and translator aspects.

2. COMPLIANCE TO IEC 60880 REQUIREMENTS CONCERNING DESIGN AND IMPLEMENTATION

The following Table has been obtained by exhaustive examination of the IEC-60880 standard in order to identify the objective pertaining to the design phase.
For each objective, the table identifies:

- The support provided by SCADE Suite (ex: automated verification of semantic rules)
- The activities that should be carried out by the user in order to meet the IEC 60880 requirements, in conjunction with the support provided by SCADE Suite.

N°	Section	Page	IEC Requirement	SCADE Support	User Activity
1	1	17	Use top-down design methods	SCADE Suite is well-suited to the application of top-down design	Use mainly a top-down Scade design approach
2	1	17	Use modularity	Scade is a strongly modular notation. The design's modular structure will flow down to the generated code, provided the no-expand option of SCADE Suite KCG is used	Use modularity in Scade designs (e.g. operators with explicit interfaces, packages ...). Use the no-expand option of SCADE Suite KCG so that it flows down to the C code
3	5.4.6	39	When activities of the software development are automated using software tools, the activities automated by the tool shall be documented including the documentation of the inputs and outputs relevant to the phase	SCADE semantic checker automated verification of SCADE semantic rules. The SCADE Reporter tool automatically produces a design report, including full description of the inputs and outputs.	Mention use of SCADE tools and tool certification data in the project documentation.
4	5.6.5	43	It shall be possible to identify the relevant versions of all software documentation associated with each software entity	The SCADE Configuration Management (CM) Gateway allows clearly identifying the versions of a Scade design	Use the SCADE Suite CM Gateway to identify Scade design versions