

The IEC 60880:2006 Nuclear power plants – (phase 8) governs how software aspects for computer based systems performing the most safety-critical (Category A) functions are verified.

Section 14.2 “Selection of tools” defines the qualification criteria for “verification & validation tools”.

CANTATA

CANTATA HYBRID
Certification Engine for Google Tests

QAMISRA

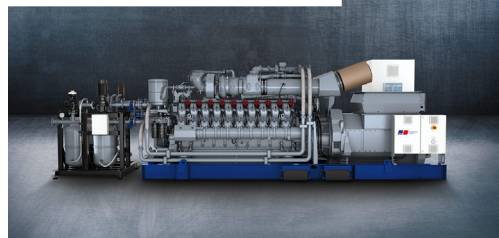


Cantata (including Cantata Hybrid) and QA-MISRA have been certified by SGS-TÜV Saar GmbH against IEC 60880 sections 14.2 & 14.3 as suitable for the verification of safety-related software up to the highest level (Category A).

Tool Certification kits for each are available free of charge.

Energy applications

QA Systems software verification tools are used accross all energy domains.



Cantata was used by MTU Friedrichshafen on their SafeDEC diesel engine project for Category A nuclear power stations and along with WindRiver Diab compiler on PPC architecture successfully qualified to IEC 60880. “Cantata delivered testing automation on target, easy MC/DC code coverage analysis and regression testing for the project.”

Project Lead,
MTU.

The project involved the construction of a Dynamic Test System for a Primary Reactor Protection System. This work had been carried out in C++, using a development process guided by IEC 60880. Cantata played a crucial role at various levels: the static analysis metrics helped OSyS engineers identify the modules requiring special attention, and coverage analysis of the system tests allowed them to complete the work to a high level of confidence.



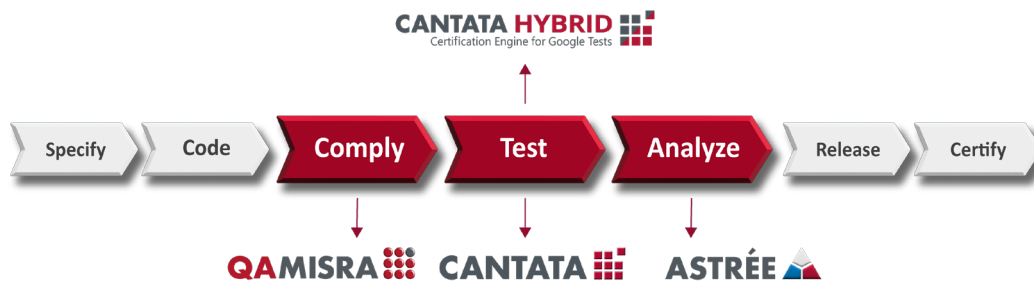
“Without this [Cantata wrapping], difficult external conditions not directly influenced by our code, such as memory allocation errors, may have been difficult to simulate”.

Primary Reactor Protection System Project Lead, OSyS

Standard Compliant Verification

Energy
Customers include:

QA Systems static analysis & software testing tools support standard compliant verification in linear flow as below:



QA Systems tools can be used for standard compliant verification to the energy sector safety standards (below) and to coding standards: MISRA, CERT and CWE.

Nuclear Energy: IEC 61226, IEC 62138 & IEC 60880

IEC 61226:2020 “Nuclear power plants – Instrumentation and control important to safety – Classification of instrumentation and control functions”, is the standard which classifies functions into categories A, B or C.

IEC 62138:2018 covers category B or C functions only, while IEC 60880:2006 covers the most stringent category A functions. The verification and validation techniques defined within both standards are highly reliant on automation tools qualified or certified as suitable for use (as QA Systems tools are).

QA Systems tools Cantata (for unit and integration testing) and QA-MISRA (for coding standards compliant static analysis) address IEC 60880 section 8 “Software verification”, and Annex E “Software verification and testing”. The Cantata IEC 60880 Standard briefing and QA-MISRA Safety Manual detail how these QA Systems tools can satisfy the objectives of this most stringent standard.

Non-Nuclear Energy: IEC 61508

IEC 16508:2010 “Functional Safety of Electrical / Electronic / Programmable Electronic Safety-related systems”, is applicable to cases where non-nuclear power programmable devices in the energy sector are used to control systems with safety considerations. IEC 61508, Part 3 section 7.4.4 recommends that software tools are certified (QA Systems tools are certified as class T2 off-line support tools suitable for use up to SIL 4). Cantata & QA-MISRA address IEC 61508 Part 3 Software Requirements Sections 6 and 7 plus Annexes A & B. The Cantata IEC 61508 Standard briefing and QA-MISRA Safety Manual detail how these QA Systems tools can satisfy the verification requirements of this standard.



QA Systems Group
sales@qa-systems.com | www.qa-systems.com
Stuttgart, Germany | Bath, UK | Milan, Italy
Boston, US | Da Nang, Vietnam | Bengaluru, India

QA-MISRA® and Cantata® are registered trademarks of QA Systems GmbH. © Copyright QA Systems GmbH 2024.
Astrée® is a registered trademark of AbsInt Angewandte Informatik GmbH, developed under license from the CNRS/ENS
Google, GoogleTest, GTest, GoogleMock and GMock are registered Trademarks of Google LLC.



Brunel

CGI

eltwin
powering your impact

**FORSEE
POWER**



GUTOR


sensitron



 **TELEDYNE**
OLDHAM SIMTRONICS
Everywhere you look™


n.e.t.
innovative gas sensing

Read the full success stories
in our resources library:
qa-systems.com/resources