

Challenges for application of IEC61508 to systems for investment protection containing FPGA Off-the-Shelf components: the ITER Interlock System Fast Architecture use case

Monday, 5 July 2021 14:10 (10 minutes)

The ITER Interlock Control System (ICS) requires the application of the IEC61508 standard for all mission-critical (known as investment protection) control functions. Such functions at nuclear fusion facilities present a unique challenge where events from integrated physics processes need to be detected and distributed to actuators with hard real-time constraints in the order of single-digit milliseconds - sometimes microseconds.

Systems that can achieve these kinds of requirements are often bespoke FPGA-based solutions, which are a well-known challenge to IEC61508 processes. However, to minimize the variety of components and simplify the procurement process for an international supplier-base, ITER decided to standardize the use of off-the-shelf devices. This is where a third challenge arises, to provide the required level of assurance that an COTS device is of good quality, fit-for-purpose and can be integrated adequately into an investment protection control loop with the necessary level of systematic capability over the development process.

The COTS devices chosen by ITER for the realisation of hard real-time interlock functions, require the use of a high-level language, and the associated integrated development tools to develop the FPGA functionality. This supposes a fourth challenge, as IEC61508 processes are still oriented to Hardware Description Language-based developments rather than high-level languages, such as, OpenCL, HLS, Mathworks-Simulink or LabVIEW-FPGA being increasingly used every day.

This paper explores the method ITER use to meet these four challenges with reference to a case-study system architecture with fast, hard real-time requirements. The paper also presents successes and limitations in attempting to apply rigor throughout the system realization process with COTS devices and high-level languages.

Member State or IGO

ITER Organization

Speaker's Affiliation

IO - ITER Organization, Route de Vinon-sur-Verdon, CS 90 046, 13067 St. Paul Lez Durance Cedex, France

Primary authors: KARKINSKY, Damien (ITER Organization); ESQUEMBRI, Sergio (Universidad Politécnica de Madrid); CARPEÑO, Antonio (Universidad Politécnica de Madrid); BARRERA, Eduardo (Universidad Politécnica de Madrid); MARQUETA, Alvaro (ITER Organization); PRIETO DIAZ, Ignacio (ITER Organization)

Presenter: KARKINSKY, Damien (ITER Organization)

Session Classification: Machine Control 1

Track Classification: Machine Control, Monitoring, Safety and Remote Manipulation