THE ITER INTERLOCK SYSTEM

A. Vergara-Fernández[1], J.L. Fernández-Hernando[1], C. Fernández-Robles[1], A. Marqueta[2], I. Prieto-Díaz[3], R. Pedica[4], M. Savouillan[5], S. Sayas[6], A. Wallander[1], I. Yonekawa[1]

[1]ITER Organization, route de Vinon sur Verdon, 13115 St. Paul lez Durance, France
[2]IFMIF/EVEDA Project Team, Rokkasho, Japan
[3]Iberdrola Ingeniería y Construcción, Av. Manoteras 20, 28050 Madrid, Spain
[4]Vitrociset, via Tiburtina 1020, 00156 Roma, Italy
[5]Assystem, 70 boulevard de Courcelles, 75017 Paris, France
[6]Arkadia, 298 avenue du club Hippique, 13090 Aix-en-Provence, France

Abstract

ITER is formed by systems which shall be pushed to their performance limits in order to successfully achieve the scientific goals. The scientists in charge of exploiting the tokamak will require enough operational flexibility to explore as many plasma scenarios as possible while being sure that the integrity of the machine and safety of the environment and personnel are not compromised. The I&C Systems of ITER have been divided in three separate tiers: the conventional I&C, the safety system and the interlock system. This paper focuses on the latter. The design of the ITER interlocks has to take into account the intrinsic diversity of ITER systems, which implies a diversity of risks to be mitigated and hence the impossibility to implement a unique solution for the whole machine. This paper presents the chosen interlock solutions based on PLC, FPGA, and hardwired technologies. It also describes how experience from existing tokamaks has been applied to the design of the ITER interlocks, as well as the ITER particularities that have forced the designers to evaluate some technical choices which historically have been considered as non-suitable for implementing interlock functions.

THE ITER RISKS AND ITS INTERLOCK CHALLENGES

The scientific nature of the ITER Project imposes an engineering design of the tokamak that provides to the experimentalists enough operational space and flexibility to investigate as many plasma scenarios as possible. This involves diagnostic equipment and plasma actuators with tuneable operational parameters and a control system (CODAC) capable of managing them in a reliable and efficient manner [1]. In contrast with other large scientific machines like high energy physics particle accelerators or astronomy telescopes, where the device is *just* an instrument to observe Nature, the ITER machine is the object under investigation (or at least a big part of it) and the way that it is operated may vary significantly along the years and even within a single operational shift.

On the other hand, The ITER tokamak is a one-in-a-kind machine that will run long plasma discharges under very demanding and sometimes difficult to predict conditions. This makes necessary an independent system which takes care only of protecting the investment while reducing as much as possible the impact of its task on the whole machine availability.

The ITER interlock is a highly dependable system in charge of mitigating the risks that can endanger the ITER equipment and operation.

The main sources of risk to the ITER investment are (not necessarily by order of importance): the superconducting magnet system and its associated equipment, the plasma itself, the plasma heating and fuelling equipment (e.g. neutral beams and electro/ion cyclotrons), and the vacuum, cryogenic and water cooling systems.

The ITER interlocks are in charge of detecting, or if possible preventing, any combination of states that may set the machine in a dangerous scenario for one or several of its components. The interlocks are also responsible of performing the required sequence of protective actions to bring back the machine to a safe state while minimising the time to resume operations.

While interlock technologies have been used extensively in scientific projects for decades, some of the particular characteristics of the ITER machine make the design, implementation and commissioning of its interlock system specially challenging.

CHASING PROTECTION FUNCTIONS

The first challenge that engineers found when the design of the ITER interlocks started was the fact that nearly all the equipment that this protection system was supposed to protect were still under design. Moreover, the global strategy under which ITER would be operated was still in a very early phase of its definition.

All the different standards and common practices used for the design and implementation of automatic protection and safety systems clearly state that the first thing to do is to elaborate a risk analysis of the systems to protect, in order to identify all the risks and their mitigation strategy. This obviously represented a challenge when most of the plant systems forming ITER were still going through intermediary design reviews.

ISBN 978-3-95450-139-7

The strategy adopted by the controls division at ITER was to start a round of joint analysis with the technical responsible of each plant system in order to identify the risks of the equipment under their responsibility and prepare a first list of potential machine protection functions critical enough to be implemented by the interlocks instead of the conventional control systems.

In order to simplify and modularise the design, the protection functions for each plant system were divided in two types: local and central. The first ones are the protection functions implemented autonomously by one plant system without requiring intervention of other ITER equipment. In other words, local functions are those in which the sensors, actuators, and interlock logic are implemented by one ITER system. In contrast, the central interlock functions are those protection functions for which the event is detected by one (or several) plant systems and the protection action carried out by another one. The controls division focused their efforts on the identification and analysis of the central interlock function, the most complex as they required the coordination of several actors, while the responsible officers of each plant system are in charge of identifying the local interlocks. At the time this paper is written already 130 central interlock functions have been identified involving 24 different plant systems and a similar number is expected for the local ones.

Despite this segregation between local and central, it is important to keep in mind that the ITER interlocks will work as a unique system. Once all pieces are put together during the integrated commissioning, all functions, local and central, shall be managed, implemented, and operated in perfect coordination. In order to strengthen this last point and to avoid having one project-wide architecture working in parallel with a bunch of isolated local interlocks, the following integration methods and tools have been proposed.

i. A global ITER investment protection policy that sets the rules to follow for the identification of interlock functions and assignment of their integrity level.
ii. A set of templates to standardise the way as the interlock risks and functions are documented independently of the system under analysis.
iii. Five technical documents that elaborate and standardise the guidelines and rules for the design, construction, and operation of the interlock system for each plant system.

These tools have allowed the team in charge of developing the interlock system in the controls division to delegate an important part of the work on the plant system responsible, while ensuring the future correct integration of all the pieces of the puzzle.

AN ECLECTIC COLLECTION OF ACTIONS

It was easy to notice after the first interlock functions of the project were identified that different interlock events are followed by protection actions of very different sorts. The nature of the risks to be mitigated also changes completely between plant systems. For instance, while some events like the neutral beam shine-through (i.e. wrong absorption of the neutral beam energy by a plasma with wrong density that may compromised the integrity of the inner vessel components) required interlock actions in the order of few milliseconds, others like a problem with the cold compressors of the cryogenic system allowed reaction times in the order of minutes.

Diversity between functions arises not only from the very different time performance requirement but also from the complexity of the protection and detection procedures. For instance, while the detection of a local overheating in the inner wall of the tokamak can be followed by a simple injection of impurity gasses into the tokamak to immediately stop the on-going plasma discharge, more complex events, like an unbalanced distribution of mechanical forces across the tokamak structure, are rather complicated to detect and even more difficult to mitigate given the number of complex actuators involved (e.g. magnet power converters, plasma heating equipment, etc.)

This added level of complexity has been reflected in the solution adopted for the preliminary design of the ITER interlock control system. The system is divided in four almost-independent architectures: 1. The slow interlocks, implementing interlock functions with logic slower than 300 ms using PLCs; 2. The fast interlocks, which are in charge of implementing functions between 10 ms and 300 ms with FPGA technology; 3. The hardwired interlocks used for executing very simple but especially critical functions such as the protection of the superconducting magnets after a resistive transition of their components (quench); and finally, 4. The most complex solution (still to be named) that will take care of implementing complex protection functions which usually are taken care by the conventional control systems. This latter architecture has the particularity that it shall be always backed-up by a function performed by one of the other three. Its main usage is to minimise the impact on the machine availability caused by the activation of a *standard* interlock function.

THE NOT-SO-SAFE FAIL SAFE STATES

The second ITER characteristic, from a machine protection point of view, that was rapidly spotted is the fact that the identification of the safe states, in which the interlock system shall set the actuators in case of loss of control of the dangerous parameters (e.g. plasma current or position, superconducting coil current or temperature, deposited energy by the plasma heating systems, etc.) or simply after a detected degradation of the machine protection system components (e.g. loss of electrical powering, loss of plasma control system, etc.) is not always obvious. In some cases it is simply impossible to define a 'default' action to be performed by the actuators to bring the machine to a safe state without implying a considerable recovery time after the event.

ISBN 978-3-95450-139-7

For instance, in case of a quench in the toroidal superconducting circuit (which is the circuit with the largest stored magnetic energy, 40 GJ), a fast discharge of the current of the coils has to be initiated while gas is massively injected in the vessel to mitigate the effect that the sudden disappearance of the plasma current (i.e. disruption) would cause. While these actions are completely necessary if a quench happens in order not to damage the machine, the long recovery time that they involve (i.e. weeks to months) forces the interlock system to trigger these actions only when absolutely necessary. The interlock system shall be designed such that internal failures are detected soon enough to allow a controlled sequence of actions (sometimes performed in close collaboration with the conventional control systems). Setting the interlock outputs in their fail-safe states is therefore the last option to be taken (e.g. full loss of interlock controllers).

A system based on redundant controllers, networks, hardwired loops, and I/O modules is being implemented for the slow, fast, and hardwired architectures. Continuous self-diagnostics are able to detect internal malfunctions or degradation of the system redundancy allowing conventional plasma pulse terminations with very limited impact of the machine availability.

WHEN THE CURE IS WORSE THAN THE DISEASE

The activation of some essential interlock actuators of ITER will not only have the cost of long machine downtime explained above, but it will also impact on the total lifetime of some tokamak equipment. Simulations and real experiments have shown that components like the superconducting magnets can only go through a limited number of fast discharges. Likewise, the number of mitigated and non-mitigated plasma disruptions, which most likely will be produced after some *hard* interlock actions, that the machine can bear is also limited.

This constraint on the interlock operation reinforces the use of self-diagnostic redundant solutions mentioned above and also forces the interlock system to use alternative actions before activating the most radical protection measures like the fast discharge of coils, sudden interruption of plasma heating systems or massive gas injection for plasma termination.

These less drastic actions are often too complex to be implemented by the interlock system alone. In such cases the interlock works in collaboration with the conventional, less dependable systems such as the plasma control system. This creates a functional interface between the conventional control tier and the interlock one that breaks the rule of having three independent control systems of ITER (i.e. CODAC, interlock and safety). However, the final interlock can always trigger its own actuators in case that the conventional systems fail to perform an interlock request, hence the machine integrity is never compromised and the interlock dependability requirements are kept.

An example of this combined protection functions is the detection of an internal problem in the neutral beam injector (e.g. internal vacuum loss) which requires a quick stop of the device. Since a sudden stop of a heating system may cause an important disruption, the interlocks would have to trigger the disruption mitigation system (i.e. massive gas injection) in parallel with the order to shutdown the neutral beam. Instead, the interlock system, after detection of the event, shall first send a request to the plasma control system to stop the neutral beam power in a coordinated way with the other plasma actuators, such that the disruption is not produced. Only if after a certain time the problem persists and the injector is still working, the interlock system directly cuts the neutral beam high voltage source and, if required, triggers the disruption mitigation system.

A similar strategy is used if the interlock detects a dangerous combination of currents in the superconducting coils or some external failure that may lead to a quench: an order to smoothly interrupt the plasma pulse and bring current in the coils to zero is sent to the plasma control system and only if after a certain time the problem persists the interlocks activates the fast discharge units in charge of passively and quickly removing the energy from the coils, while the disruption mitigation system is triggered.

SAFETY AND INTERLOCK SEGREGATION

The segregation of the ITER I&C systems in three tiers follows important managerial, functional, technical, and regulatory goals. We have seen already that for the conventional and interlock tiers the borders are not fully impermeable and some functional and consequently physical connections exist. This is not the case for the boundaries with safety.

The main reason to separate the ITER interlock and safety systems is the fact that the latter shall follow the strict rules imposed by the nuclear standards and go through the licensing process. The separation gives freedom and broader range of technological solutions to the interlock designers, simplifies the safety systems, reduces the amount of equipment under regulator's supervision, and ensures that machine protection actions do not disturb the correct performance of the safety components.

Said this, it is not possible to ignore the many similarities existing between the two systems: technologies, standards, terminology and even the profiles and background of the experts. This has many advantages (e.g. team synergies, shared experience on prototypes and R&D projects, etc.) but can lead to dangerous overlapping between the systems if borders are not correctly set from the beginning. The main measures taken by the control division, which is in charge of designing and implementing both systems at ITER, to ensure the correct segregation are:

ISBN 978-3-95450-139-7

i. Managerial: systems are developed by two independent teams led by different responsible officers.
ii. Technical: the hardware and software used by the interlock is never shared with the safety systems. Networks, electronic components and even the cubicles are completely separated. While some resources in the control room of ITER will be used for managing both interlocks and conventional data, this will not be the case for the safety system. No action on the interlock system can be performed from the safety desks and vice versa
iii. Methodological: while standards like the IEC-61508 or IEC-61511 are used by both systems, each has been independently adopted and adapted to the different characteristics of each one.

Finally, and in order to minimise the risk of misunderstanding by ITER staff, partners in our domestic agencies and contractors, the frequently used term SIL (Safety Integrity Level), has been removed from all interlock documentation at ITER and replaced by the equivalent ITER Interlock Integrity Level or 3IL.

TAKING MOST OF THE PAIN

The Central Interlock System is the part of the ITER interlocks in charge of coordinating the tokamak plant systems involved in central interlock functions. It went through its preliminary design review at the end of 2012 and will complete its final design in December 2015. Since the final design of some ITER systems is still on going and some interlock functions will not be frozen until well advanced plasma operation, it has been decided to develop a central interlock flexible and reliable enough to cope with future requirements.

The machine protection functions of ITER are divided in three types depending on the required integrity: 3IL-1, 3IL-2 and 3IL-3. ITER has decided to implement the first ones by the conventional systems, while 3IL-2 and 3IL-3 functions are considered interlocks. The integrity level of an interlock chain is given by the sum of all its elements. Hence in order to meet the required 3IL, all the components involved in the protection action need to be developed towards that goal. The problem found during the design of the central system is that it is not easy to assess at this stage of design which is the level of integrity that the interlock of each plant system must and can achieve.

In order to minimise future risks, and despite most interlock functions are only 3IL-2 (equivalent to SIL2 according to IEC-61508), it has been decided to develop a 3IL-3 central interlock system (equivalent to SIL3).

Simulations and detailed reliability studies of the selected solutions for the slow central interlock system (based on SIL3 certified redundant PLC) show that the target availability (99.9%) is largely reached, with less than 11 minutes of downtime for 20 years of operation. The mean time to first failure (MTTF) is around 200 times larger than the expected time mission. These figures leave enough room (around 88% of the integrity requirements) to the other components within the interlock chain to ensure the 3IL-3 performance from sensor to actuator.

CONCLUSIONS

The ITER interlock system is in charge of protecting the tokamak against component failures or dangerous machine operation. Because of the unprecedented technical and managerial complexity of the ITER Project, the traditional simplicity of the interlock systems for scientific experiments has been replaced by a more complex approach in which new performance requirements, usually out of machine protection systems, are being targeted, while trying to keep the high level of robustness and integrity inherent to interlock systems.

This will most likely be the first machine protection system built with most of its components provided in-kind from up to 36 different countries. A strong effort is being put in place to ensure that all actors involved across the globe design, build, and configure the parts of the puzzle under their responsibility such that these can connect properly to the central system, while keeping the global reliability figures above the targeted requirements.

Standardisation of hardware, software and methods are essential to build an interlock system with such procurement strategy. The experience acquired during the design of a much larger control system like ITER CODAC is extremely valuable. However, the criticality of the interlocks together with its tight dependability requirements makes even more compulsory a close collaboration between all the partners involved.

REFERENCES

[1] A Wallander et al., “Approaching Final Design of ITER Control System”, Proc. of ICALEPCS 2013, San Francisco, http://jacow.org

The views and opinions expressed herein do not necessarily reflect those of the ITER Organization.

ISBN 978-3-95450-139-7