

RAMI analysis of the ITER Central Safety System



Sin-iti Kitazawa^{a,*}, Katsumi Okayama^{b,1}, Yuzuru Neyatani^a,
Francois Sagot^b, Didier van Houtte^{b,2}

^a ITER Project Unit, Japan Atomic Energy Agency (JAEA), Naka, 311-0193 Ibaraki, Japan

^b ITER Organization, Route de Vinon sur Verdon, 13115 Saint Paul Lez Durance, France

HIGHLIGHTS

- We performed the functional analysis of the ITER CSS.
- We performed a failure mode analysis of the ITER CSS.
- We estimated the reliability and availability of the ITER CSS.
- The ITER RAMI approach was applied to the ITER CSS for technical risk control in the design phase.

ARTICLE INFO

Article history:

Received 19 December 2013

Received in revised form 11 April 2014

Accepted 7 May 2014

Available online 8 June 2014

Keywords:

RAMI
Availability
Nuclear fusion
ITER
Safety
CSS

ABSTRACT

ITER is the first worldwide international project aiming to design a facility to produce nuclear fusion energy. The technical requirements of its plant systems have been established in the ITER Project Baseline. In the project, the Reliability, Availability, Maintainability and Inspectability (RAMI) approach has been adopted for technical risk control to help aid the design of the components in preparation for operation and maintenance. A RAMI analysis was performed on the conceptual design of the ITER Central Safety System (CSS). A functional breakdown was prepared in a bottom-up approach, resulting in the system being divided into 2 main functions and 20 sub-functions. These functions were described using the IDEF0 method. Reliability block diagrams were prepared to estimate the reliability and availability of each function under the stipulated operating conditions. Initial and expected scenarios were analyzed to define risk-mitigation actions. The inherent availability of the ITER CSS expected after implementation of mitigation actions was calculated to be 99.80% over 2 years, which is the typical interval of the scheduled maintenance cycles. This is consistent with the project required value of $99.9 \pm 0.1\%$. A Failure Modes, Effects and Criticality Analysis was performed with criticality charts highlighting the risk level of the different failure modes with regard to their probability of occurrence and their effects on the availability of the plasma operation. This analysis defined when risk mitigation actions were required in terms of design, testing, operation procedures and/or maintenance to reduce the risk levels and increase the availability of the main functions.

© 2014 Elsevier B.V. All rights reserved.

1. Introduction

ITER is an international experimental nuclear fusion facility whose technology is challenging and its technical risk control is extremely crucial. The RAMI approach (Reliability: continuity

of correct operation; Availability: readiness for correct operation; Maintainability: ability to undergo repairs and modifications; Inspectability: ability to undergo visits and controls) should be applied to all ITER components during their design phase to reduce potential technical risks impacting machine operation [1]. In the ITER project there are 3 design phases: conceptual, preliminary, and final design. RAMI analysis is done for a functional analysis and preliminary risk assessment in the conceptual design phase and is updated in the preliminary and final design phases. The RAMI analysis is based on a bottom-up approach using the latest designs of each component. A functional analysis is applied to define a complete functional breakdown description of the system in question from its main functions to basic functions and components. Failure

* Corresponding author. Tel.: +81 292707767.

E-mail address: kitazawa.siniti@jaea.go.jp (S.-i. Kitazawa).

¹ Present address: PricewaterhouseCoopers LLP, 2-1-1 Nishi-Shinjuku, Shinjuku-ku, Tokyo, Japan.

² Present address: Project Office, CEA-Cadarache, DSM/IRFM, 13108 St Paul lez Durance Cedex, France.

Modes, Effects and Criticality Analysis (FMECA) establishes a list of functional failures, causes and effects, and the probability of failure modes against the severity of the consequences (major, medium, or minor risk) by using a criticality chart. Reliability Block Diagrams (RBD) were prepared to estimate the reliability and availability of each function under the stipulated operating conditions. Risk mitigation actions are applied to both FMECA and RBD to initiate actions in terms of design, tests, operation and maintenance to reduce the risk levels.

The ITER Instrumentation and Control (I&C) system is divided into 3 vertical tiers with 2 horizontal layers; the 3 vertical tiers CODAC (Control, Data Access and Communication), interlock systems, and safety systems, and the 2 horizontal layers central and plant [2]. It is worth noting that the terms “interlock” and “safety” indicate “machine protection” and “human and environmental protection”, respectively in the ITER project. For the ITER I&C system, separate RAMI approaches were prepared for each central system (CODAC, CIS and CSS) in their conceptual design phase. RAMI analyses of plant I&C systems are prepared within their respective plant system. Previous reports were done for CODAC [3] and the CIS [4]. The details for the CSS was reported in [5] and is summarized in this paper.

2. Functional analysis of the ITER CSS

The functional breakdown of the CSS is divided into 2 main functions which are prepared to execute the central safety function for nuclear risks and conventional risks. Each function should be executed by having the request designated as an automatic or manual safety command. Furthermore, the command should be provided to the machine operators and CODAC and all of the data should be archived in the CSS. The ITER CSS system is well-integrated with other I&C systems, and have substitute functions with each other. In this functional analysis, these supplementary functions are not taken into account, and the inherent functions were considered. The entire functional breakdown structure is summarized in Table 1 where each node corresponds to 1 function. Node indexes were attached for IDEF0 analysis. There are 2 main functions, 10 sub-functions and several deep functions. The main functions are “To coordinate the individual protection provided by the intervention of locally distributed safety systems for nuclear Risks” (A1) and “To coordinate the individual protection provided by the intervention of locally distributed safety systems for conventional Risks” (A2). Nuclear risks occur in systems which have potential radiological impact, such as those located in Tokamak building, Tritium plant building, Hot Cell buildings and other low-level Radwaste buildings. In a former design, the first level had 3 functions; the third one was “To prevent personnel access from entering dangerous areas”, which has been included in Conventional Risks.

Fig. 1 shows the top IDEF0 diagram of the CSS. The logical input of the CSS is “Hazardous Conditions” of the ITER system, and the output is “Safety Conditions” of the ITER system. For input, the power supply also exists in addition to the logical input. The “Safety Conditions” is executed by actuators in plant systems via the Plant Safety System (PSS). The safety events are detected by the PSS and transmitted via the plant safety network (PSN) and the central safety network (CSN) to the CSS. The control is based on “nuclear risks” and “conventional risks”. The mechanism includes PSS, CODAC system and operator’s safety desk, and the analysis was performed under conditions that their specifications are not well decided.

Fig. 2 shows the parent diagram of A0 of the CSS. There are 2 main functions, “nuclear safety” and “conventional safety”. A hazardous condition is detected by a sensor in PSS and the safety condition will be performed by an actuator in PSS.

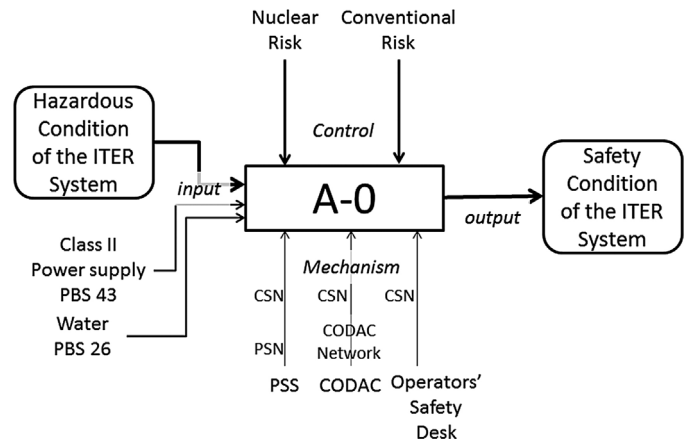


Fig. 1. Top IDEF0 diagram of the ITER CSS. PBS is the ITER Plant Breakdown Structure which was defined to enable identification of the root of all ITER systems, subsystems, assemblies and subsequently, their components. And to also support engineering data structure and configuration management of the ITER project.

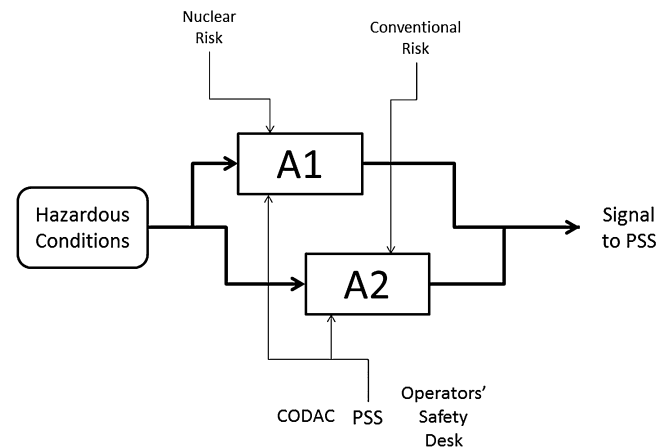


Fig. 2. Parent IDEF0 diagrams of the ITER CSS.

Fig. 3 shows the diagram of A1: Nuclear Risks. In the upper current of data flow, there are 2 functions, automatic safety commands A11 and manual safety commands A12. Automatic safety commands A11 is controlled by safety functions. Manual safety commands A12 is controlled by safety functions and manual safety

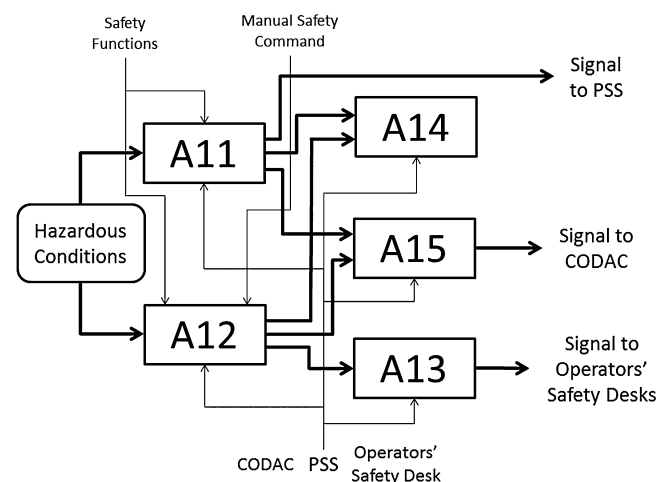


Fig. 3. IDEF0 diagram of A1: To coordinate the individual protection provided by the intervention of locally distributed safety systems for Nuclear Risks.

Table 1
Functional break down of the ITER CSS for the RAMI analysis.

A-0 To provide protection of people and the environment for the entire ITER site
A1 To coordinate the individual protection provided by the intervention of locally distributed safety systems for Nuclear Risks
A11 To request automatic safety commands based on combinations of safety inputs and predefined conditions
A111 To generate automatic safety commands for Confinement systems in the Tokamak building
A112 To generate automatic safety commands for Confinement systems in the Tritium plant building
A113 To generate automatic safety commands for Confinement systems in the Hot Cell/Low-Level Radwaste building
A114 To generate automatic safety commands for Fusion power shutdown system
A115 To generate automatic safety commands for Magnets
A12 To request manual safety commands from the Operator's Safety Desks
A121 To generate manual safety commands for Confinement systems in the Tokamak building
A122 To generate manual safety commands for Confinement systems in the Tritium plant building
A123 To generate manual safety commands for Confinement systems in the Hot Cell/Low-Level Radwaste building
A124 To generate manual safety commands for Fusion power shutdown system
A125 To generate manual safety commands for Magnets
A13 To present the safety systems data for the operator at the Operator's Safety Desks
A14 To archive or export all safety data in a database for off-line analysis
A15 To signal the internal and external status to CODAC for additional monitoring, display and archiving from the main control room
A2 To coordinate the individual protection provided by the intervention of locally distributed safety systems for Conventional Risks
A21 To request automatic safety commands based on combinations of safety inputs and predefined conditions
A22 To request manual safety commands from the Operator's Safety Desks
A23 To present the safety systems data for the operator at the Operator's Safety Desks
A24 To archive or export all safety data in a database for off-line analysis
A25 To signal the internal and external status to CODAC for additional monitoring, display and archiving from the main control room

commands. Both of the outputs are archived by A14 and signaled to CODAC A15. Automatic safety commands A11 signals to PSS directly and manual safety commands A12 signals directly to the operator's safety desk.

Fig. 4 shows the diagram of A2: Conventional Risks. In the upper current of data flow, there are 2 functions, automatic safety commands A21 and manual safety commands A22. Automatic safety commands A21 is controlled by safety functions. Manual safety commands A22 is controlled by safety functions and manual safety commands. Both of the outputs are archived by A24 and signaled to CODAC A25. Automatic safety commands A21 signals to PSS directly and manual safety commands A22 signals directly to the operator's safety desk. This architecture is very similar to that of Nuclear Risks.

Fig. 5 shows the diagram of A11: To request automatic safety commands based on combinations of safety inputs and predefined conditions. The automatic safety commands are generated in Tokamak building A111, Tritium building A112, Hot Cell/Low-Level Radwaste building A113, Fusion power shutdown system A114 and Magnets A115. The inputs are safety functions in each function, and the mechanism to execute this function is PSS. The outputs signal to PSS, Archive, and CODAC.

Fig. 6 shows the diagram of A12: To request manual safety commands from the Operators' Safety Desks. The manual safety commands are generated in Tokamak building A121, Tritium building A122, Hot Cell/Low-Level Radwaste building A123, Fusion power shutdown system A124 and Magnets A125. The inputs' mechanism and outputs are the same as A11 in Fig. 5. The architecture is similar to A11, though the control and one of the outputs are different.

3. FMECA of the ITER CSS

A failure mode analysis of the CSS was applied to the results of the functional analysis. A critical list of all the possible function failure modes was established, and their causes and effects in terms of the basic functions themselves were identified. The criticality (C) level of each function failure mode was derived from the ITER method for quantifying the Severity (S) of the effects, the

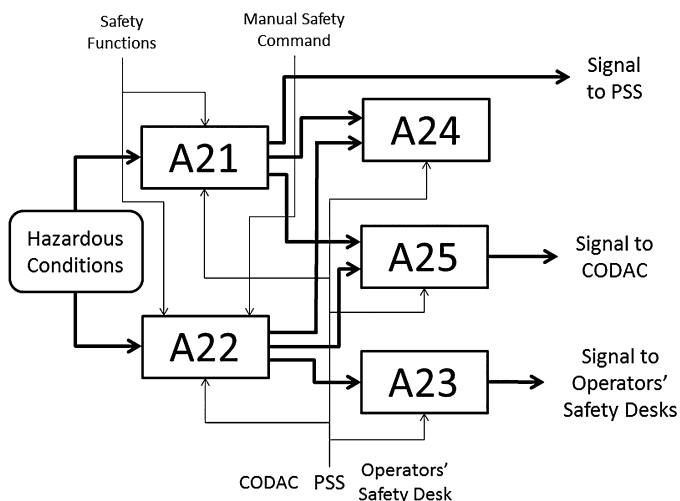


Fig. 4. IDEFO diagram of A2: To coordinate the individual protection provided by the intervention of locally distributed safety systems for Conventional Risks.

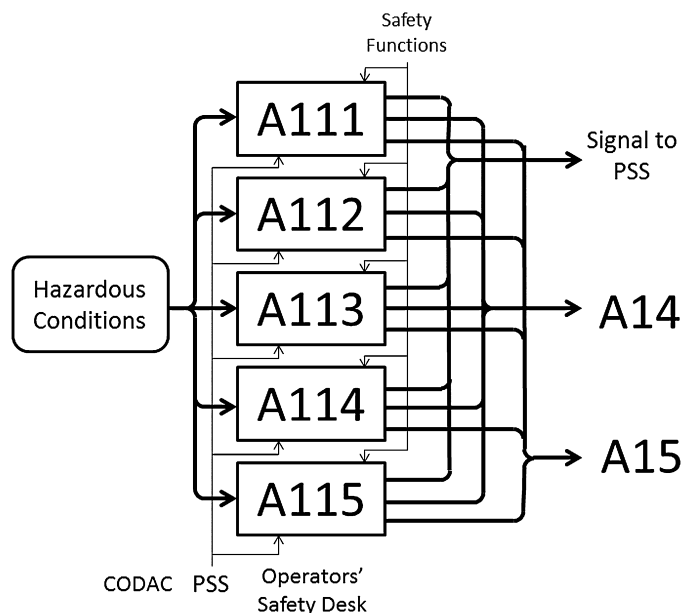


Fig. 5. IDEFO diagram of A11: To request automatic safety commands based on combinations of safety inputs and predefined conditions.

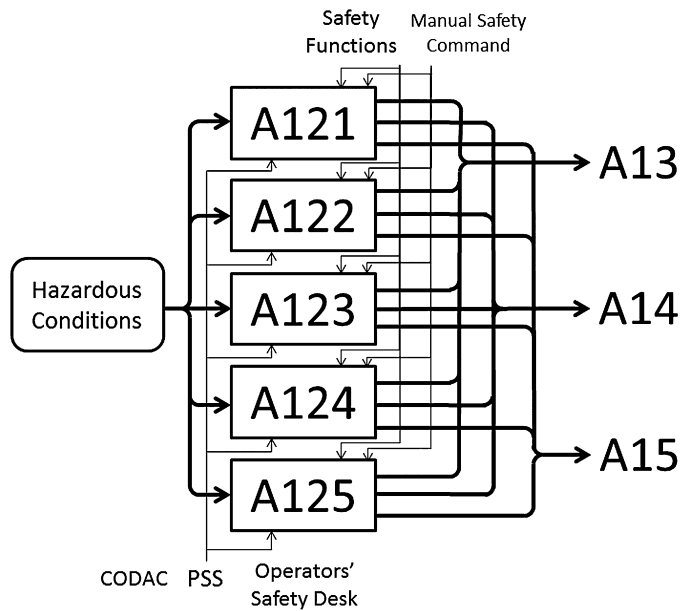


Fig. 6. IDEFO diagram of A12: To request manual safety commands from the Operator's Safety Desk.

Occurrence (O) of the causes in terms of the following formula: Criticality $C = S \times O$. The ITER RAMI severity S and occurrence O rating criteria are summarized in Table 2.

In the RAMI approach, criticality C is used to evaluate the magnitude of each risk. According to its level, the criticality is divided into 3 zones: red, yellow, and green representing major, medium, and minor risks. Criticality over 13 is considered to be a major risk and mandatory mitigation provisions must be implemented. Criticality between 7 and 13 is categorized as a medium risk and mitigation actions are recommended and for criticality less than 7 mitigation actions are optional.

Fig. 7(a) shows the initial criticality matrix with 57 failures. Fig. 7(b) shows the expected criticality matrix which displays the expected results after implementation of the advocated risk-reducing actions and mitigating provisions. There are no risks in the red zone, and the criticality can be reduced by taking proper actions. In the initial criticality matrix in Fig. 7(a), the maximum criticality $C = 12$, where $S = 3$ and $O = 4$, are mainly due to software failures and cable disconnections. Typical major failure modes of

Table 2
ITER rating scale for severity S and occurrence O [1,3].

S value	Description	Machine unavailability
1	Weak < 1 h	Less than 1 h
2	Moderate < 1 d	Between 1 h and 1 day
3	Serious < 1 w	Between 1 day and 1 week
4	Severe < 2 m	Between 1 week and 2 months
5	Critical < 1 yr	Between 2 months and 1 year
6	Catastrophic > 1 yr	More than 1 year
O value	Description	Failure rate
1	Very low	$\lambda < 5 \times 10^{-4}/\text{yr}$ (less than once in 2000 years)
2	Low	$5 \times 10^{-4}/\text{yr} < \lambda < 5 \times 10^{-3}/\text{yr}$ (less than once in 200 years)
3	Moderate	$5 \times 10^{-3}/\text{yr} < \lambda < 5 \times 10^{-2}/\text{yr}$ (less than once in 20 years)
4	High	$5 \times 10^{-2}/\text{yr} < \lambda < 5 \times 10^{-1}/\text{yr}$ (less than once in 2 years)
5	Very high	$5 \times 10^{-1}/\text{yr} < \lambda < 5/\text{yr}$ (less than five times per year)
6	Frequent	$\lambda > 5/\text{yr}$ (more than five times per year)

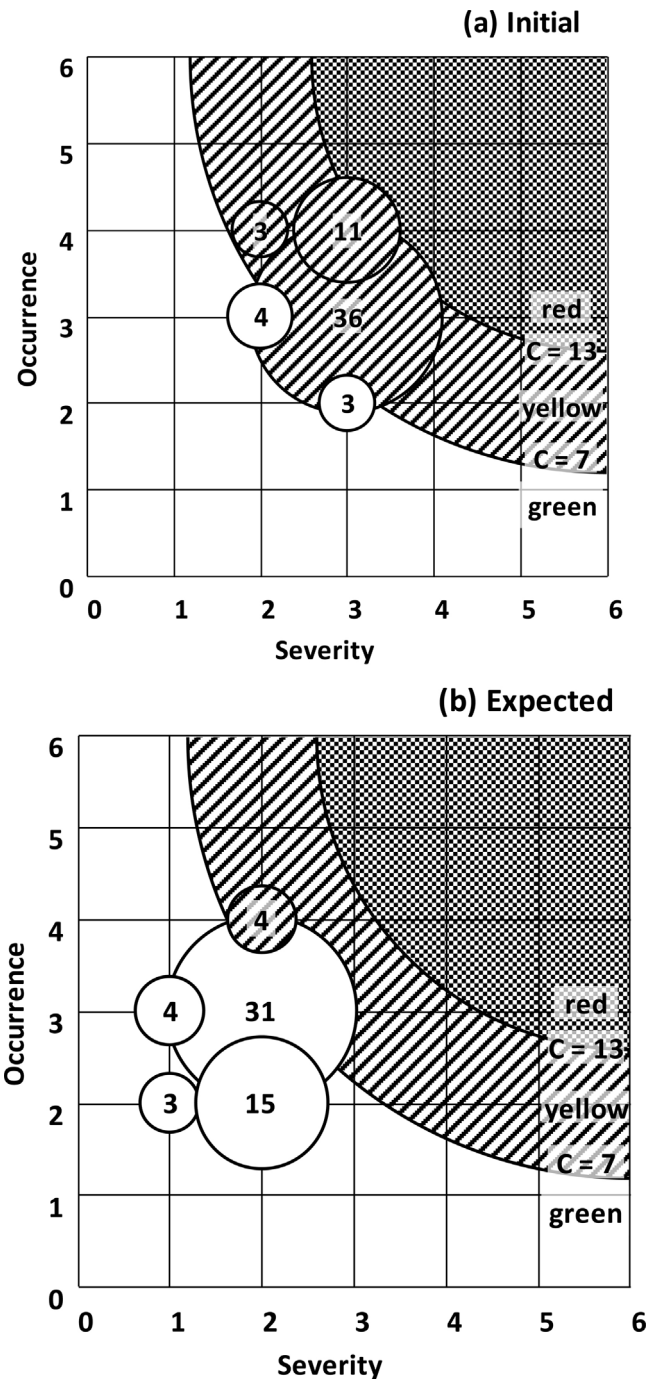


Fig. 7. Criticality matrixes of the ITER CSS in initial (a) and expected (b).

the CSS are expected to originate in hardware cables, programmable logic controllers (PLCs), transmission, server and software [2]. The CSS mainly uses only highly reliable PLCs. The occurrence of some software failures can be reduced by continuous maintenance, but they are very hard to eliminate statistically. This assumption is based on years of experience with JT-60 at JAEA. The severity can be reduced from $S = 3$ to 2 by preparing a spare component. Cable disconnections can originate from connector failure, cable failure, or physical disconnection. Their occurrence can be reduced by relentless testing, and the severity can also be reduced by preparing spares. Fig. 7(b) shows that only 4 failure modes are medium risks in the yellow zone after risk-reducing actions & mitigating provisions to reduce their criticality with the associated costs and spares.

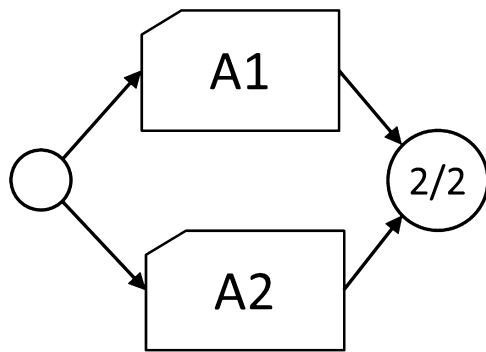


Fig. 8. RBD of the major functions of the ITER CSS. Each pentagonal box stands for a major function, and the circles stand for logical blocks. “2/2” means 2-out-of-2 configuration.

4. RBD analysis of the ITER CSS

The RBD analysis was prepared to estimate the reliability and availability of each function under the stipulated operating conditions. The first attempt to evaluate reliability and availability of each main function in the CSS used the software BlockSim7 [6].

The RBD analysis of the CSS was performed using the functional breakdown structures that were prepared in the former analysis in IDEF0. The RBDs were drawn as a diagram consisting of nodes of system components for each function. The RBDs of the top functions are shown in Fig. 8. For a detailed analysis, the nodes should be system, sub-system, unit, device, and parts. Nevertheless, in the case of the ITER CSS, the details for devices are not yet decided and therefore only some fundamental units can be used (software, server power supply, server, cables, hub, storage, and display). There are many minute parts or components that are not described in the RBD drawings in this manuscript. The main components which affect failure rate and reliability are extensive, meaning that a cable is not only a cable but includes transportation units and other minute parts.

The main functions of the CSS, Nuclear Risks (A1) and Conventional Risks (A2) are different in function but quite similar in their structures. In a former design, the risk for Personnel Access entering dangerous areas was independent, but it was incorporated into conventional risks.

The RBD of A1 is shown in Fig. 9 and the RBD of A2 also has the same structure. The function of Automatic safety (A11) has redundancy thanks in part to compensation with Manual Safety (A12 + A13). Extra attention is paid to data archiving, exporting, and processing since they are nuclear safety instruments.

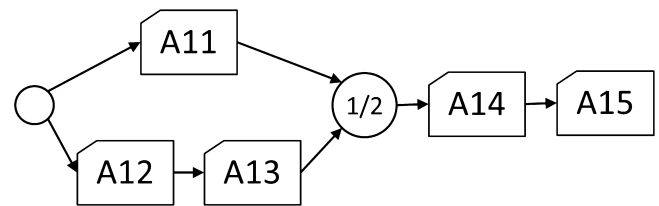


Fig. 9. RBD of A1 function of the ITER CSS. The configurations of A11 and A12 + A13 are 1-out-of-2.

The architecture of both the top A1 and A2 has the same hierarchical system. The RBD of these systems are shown in Fig. 10. This system stems from the CODAC hatch system which transports data from PSS and its processing system. There are 25 CODAC hatches to transmit data from PSS for the entire ITER system to achieve high reliability. All of the hatches should work simultaneously and the RBD has a 25-out-of-25 configuration. Any additional redundancies, such as control chain, are not taken into account for the inherent architecture. This data processing system should have the same set of devices both in the main server room and in the backup server room to secure high redundancy.

These systems of network cubicles are shown in Fig. 11. Electric fans are very vulnerable since they are moving parts and therefore should have a redundancy to compensate for their weaknesses. For this reason, fans are not treated as the most critical.

These systems of system cubicles are shown in Fig. 12. For system cubicles, 3 different architectures of the CSS are implemented: Slow High Integrity Architecture is based on PLCs, Fast High Integrity Architecture is based on fast controllers, and Hardwired High Integrity Architecture is based on hardwired loops between plant systems. The candidates for PLCs were selected by commercial products. Failure rate of the components was estimated by appropriate devices [5,7].

The failure rates of the interface module for hardwire is 0.0081 and that of the system PLC is 0.0290 per year. Failure rates of the ethernet switch and archiving server are 0.0207 and 0.0153, respectively. Those of other components are much more reliable. Electric fans for air circulation show a high failure rate but this can be reduced by using multiple devices.

Both the inherent availability and reliability of the main functions of the CSS are summarized in Table 3. The simulation end time is 17,520 h = 730 days = 2 years for availability, and 264 h = 11 days for reliability. Eleven days is consistent with a single ITER plasma operation cycle. The numbers of simulations is fixed at 100,000. For availability, the values of “Expected” are larger than those of “Initial”. It is expected that the availability naturally increases when there are spares.

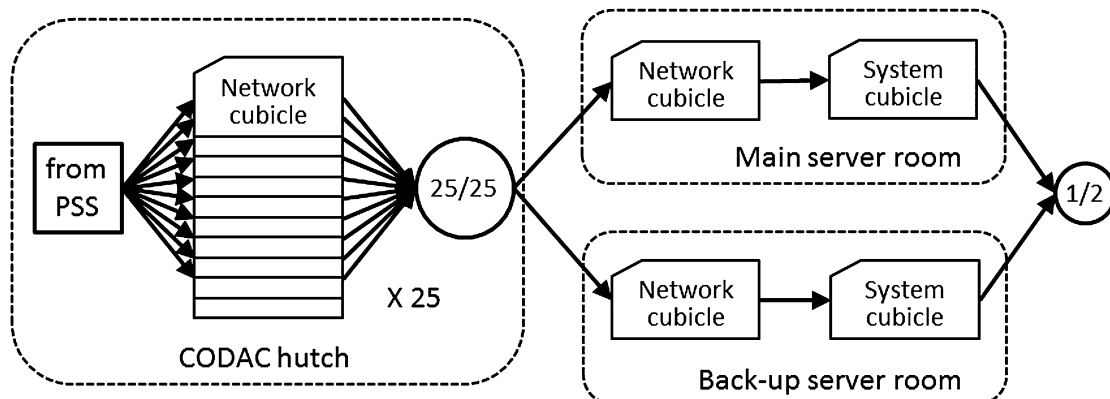


Fig. 10. RBD of a typical function of the ITER CSS. The network cubicles in CODAC hatch should work simultaneously; therefore it has 25-out-of-25 configuration. Both the network cubicle and system cubicle pair in either the main server room or back-up server room can work; therefore it is 1-out-of-2 configuration.

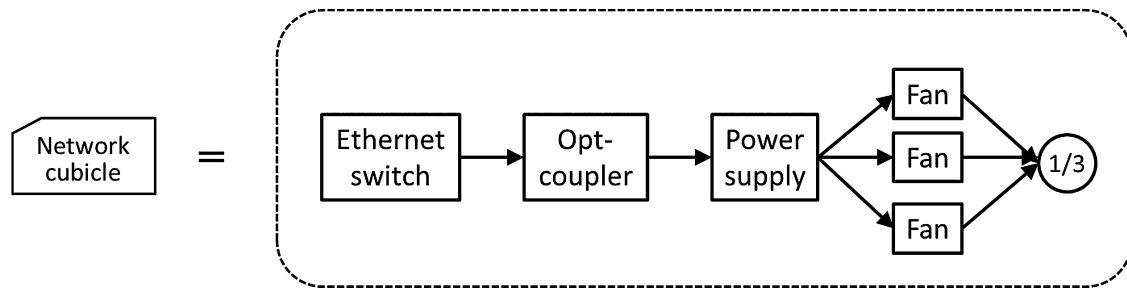


Fig. 11. System for RBD of devices in a network cubicle of the ITER CSS.

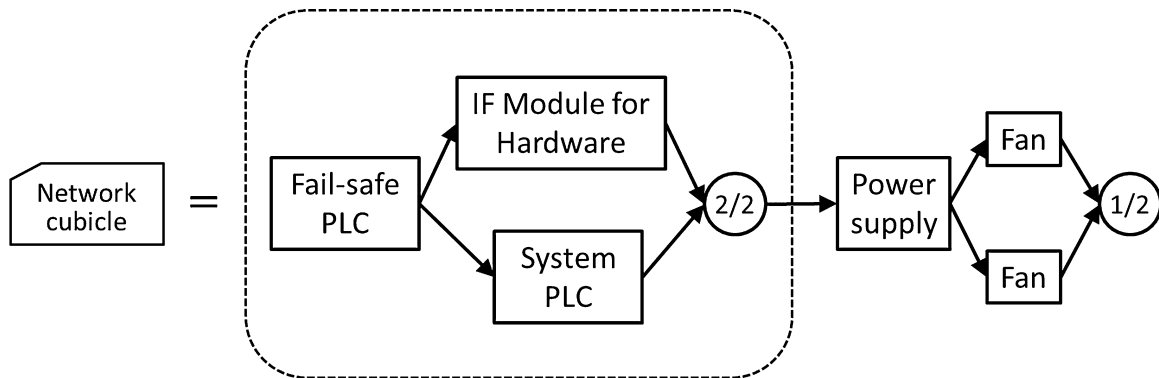


Fig. 12. System for RBD of devices in a system cubicle of the ITER CSS.

Table 3

Inherent availability and reliability of main functions of the ITER CSS.

Function	Inherent availability (%)		Reliability (%)	
	Initial	Expected	Initial	Expected
A0	97.24	99.80	86.97	86.89
A1	98.60	99.90	93.17	93.24
A2	98.60	99.90	93.17	93.24

The availability for all functions of the ITER CSS is 97.24% without spares and 99.80% with spares over 2 years. It is quite reasonable that this could be consistent with the project required value of $99.9 \pm 0.1\%$ not by changing the design, but preparing spare parts [8].

5. Conclusion

The RAMI approach was applied to the CSS for technical risk control in the design phase. A functional breakdown was performed to unveil the CSS which commands safety for nuclear and conventional risks. Simulations of functional breakdown were performed to recognize failure modes for the CSS. In this process, the analyses were mainly focused on identifying the data flow and data processing of information systems. IDEF0 analysis was applied to show diagrams of the processes for each function in the system and define the relationships among sub-functions. FMECA analysis was performed to evaluate severity and occurrence of failure modes within the system on which the criticality matrix is based. The occurrence is very difficult to reduce, whereas the severity of the risk can be reduced by preparing spares on-site. RBD analysis was applied to failure modes, the failure ratio, and availability for the device block for each function in initial and expected conditions. The availability of the CSS in the expected condition was calculated as 99.80%, a level which fulfills the project requirement of

$99.9 \pm 0.1\%$. Many significant tips to proceed forward regarding the preliminary operation and maintenance plan for the system were prepared on the basis of these results. Proposals for risk reductions were prepared to enhance the reliability of devices and include preparing spares and implementing standardization. The results of these works were archived in the ITER database to assist with ITER construction and operation.

Acknowledgments

Work was performed in the framework of RAMI analysis for the ITER CSS task agreement (C70TD06FJ). The authors acknowledge the fruitful discussions about JT-60 research with S. Sakata, M. Kuriyama, T. Yamamoto and other JAEA colleagues including N. Duncan for his help with the English manuscript. The authors also thank J.M. Fourneron, I. Yonekawa, A. Wallander and other IO control system division colleagues.

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

References

- [1] D. van Houtte, K. Okayama, F. Sagot, RAMI approach for ITER, *Fusion Eng. Des.* 85 (2010) 1220–1224.
- [2] L. Scibile, J.-Y. Journeaux, W.-D. Klotz, I. Yonekawa, A. Wallander, The ITER safety control systems – status and plans, *Fusion Eng. Des.* 85 (2010) 540–544.
- [3] S. Kitazawa, K. Okayama, Y. Neyatani, F. Sagot, D. van Houtte, L. Abadie, et al., RAMI analysis of ITER CODAC, *Fusion Eng. Des.* 87 (2012) 1510–1513.
- [4] S. Kitazawa, K. Okayama, Y. Neyatani, F. Sagot, D. van Houtte, RAMI analysis of the ITER CIS, *Fusion Eng. Des.* 89 (2014) 88–93.
- [5] S. Kitazawa, Summary report of RAMI analysis of CSS, ITER.D.4A6K8F v1.0, 2011.
- [6] <http://www.reliasoft.com/BlockSim/>
- [7] L.C. Cadwallader, Selected component failure rate values from fusion safety assessment tasks, INEEL/EXT-98-00892, 1998.
- [8] D. van Houtte, K. Okayama, F. Sagot, ITER operational availability and fluence objectives, *Fusion Eng. Des.* 86 (2011) 680–683.