Different Methods for Assessing System Failure Criticality in the RAMI Approach

Didier Elbeze, D. van Houtte, E. Delchambre

FUSION SCIENCE AND TECHNOLOGY · VOLUME 75 · 405–411 · JULY 2019

DOI: https://doi.org/10.1080/15361055.2019.1603534

Different Methods for Assessing System Failure Criticality in the RAMI Approach

D. Elbèze,* D. van Houtte, and E. Delchambre

CEA, IRFM, F-13108 Saint Paul Lez Durance, France

Received May 28, 2018
Accepted for Publication April 2, 2019

Abstract — *In the Reliability, Availability, Maintainability, and Inspectability (RAMI) engineering approach used in nuclear fusion research, criticality identifies the failure modes that have the greatest impact on the availability of the studied system. Criticality is expressed as the product of the occurrence level with the severity level of failure modes. The analytical calculation shows that this formulation is equivalent to their availability provided that the duty cycle of basic functions is introduced to adjust the occurrence and the scales of occurrence and severity are homogeneous.*

To consolidate the results obtained with a Reliability Block Diagram analysis, we performed a probabilistic study using an advanced Monte Carlo simulation code: the Primavera® Quantitative Schedule Risk Analysis. This method associates failure modes with conditional activities in a schedule and provides the density distribution of failures and tornado graphs to identify the highest criticality failures.

Statistical tests were performed for two operational systems, and we showed that the criticality evaluated with the RAMI approach was in good agreement with the results of the other methods. Thus, in many cases, the analytical formulas can be used during the Failure Mode, Effects, and Criticality Analysis to quickly assess availability by using a spreadsheet.

Keywords — *Criticality; availability; Reliability, Availability, Maintainability, and Inspectability; Failure Mode, Effects, and Criticality Analysis; Quantitative Schedule Risk Analysis.*

Note — *Some figures may be in color only in the electronic version.*

I. INTRODUCTION

Assessing the criticality of failure modes is a key point for implementing mitigation actions to optimize the availability of operational systems. These mitigation actions can be complex to implement and very costly, so it is essential to prioritize them correctly by determining the right criticality level of each failure mode as well as possible.

The Reliability, Availability, Maintainability, and Inspectability (RAMI) engineering approach used in nuclear fusion research takes place in three steps: functional analysis (FA); Failure Mode, Effects, and Criticality Analysis (FMECA); and Reliability Block Diagram (RBD) analysis. The FA leads to the functional breakdown of the studied system. The FMECA identifies all the failure modes of the components used to carry out the functions; it also evaluates the mode failure rate and the mean time to restore the components. Then, the RBD analysis calculates the availability of the system's functions. If the availability does not meet the acceptance criteria, mitigation actions are then considered, and a new cycle of analyses is performed until an acceptable availability is achieved.[1,2]

Mitigation actions focus on the most significant failure modes according to their criticality, which are calculated during the FMECA. Several questions occur. Is the criticality relevant of most impacting failure modes

*E-mail: didier.elbeze@cea.fr

on the system's availability? How are the criticality thresholds defined? Is the relationship among criticality, occurrence, and severity justified?

In this paper, we compare the FMECA definition of criticality with the analytical formulas of availability for simplified models. Then we assess the criticality through the availability of the failure mode produced by the RBD analysis. Conventional RBD software was benchmarked against an original method based on Primavera® Quantitative Schedule Risk Analysis (QSRA) software. Two previous RAMI analyses illustrated this study: the cask and plug remote handling system (CPRHS) of ITER nuclear maintenance and the WEST tokamak of the infrared thermography diagnostic.

II. DEFINITION AND ANALYTICAL FORMULAS

The operating time t is the time interval during which a system has to be operative or ready for operation. During the time t, the system may either run or fail, up or down (Fig. 1). The mean time to failure (MTTF) is defined as the average of uptimes during the system operation [Table I, Eq. (2)], and the mean time to recovery (MTTR) is defined as the average of downtimes [Eq. (3)]. The availability A of a system is defined as the ratio of the uptime over the operating time [Eq. (4)].

For most components, the failure rate function $\lambda(t)$ has a time profile similar to a bathtub section with three periods: the infant phase (burn-in), the young phase (random failures), and the aging phase (wear-out).[3,4] In general, the operational systems studied are in the second phase, which corresponds to its useful life. Their reliability then has an exponential distribution [Eq. (5)] with an almost constant failure rate λ. In this case, the failure rate is expressed by the inverse of the MTTF [Eq. (6)]. Similarly, the recovery rate μ can be defined as the inverse of the MTTR [Eq. (7)]. Table I gives a synthetic view of these definitions.

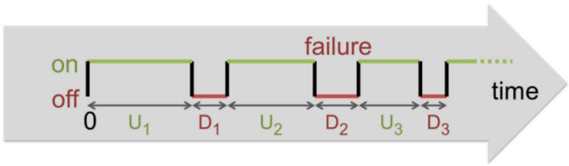

Fig. 1. Running cycle of system. The term U_i is the uptime when the system is operational, and D_i is the downtime when the system is out.

TABLE I

Basic Formulas of Reliability Variables

Operating time	$t = \sum_1^n (U_i + D_i)$ (1)
Mean time to failure	$\text{MTTF} = \frac{1}{n}\sum_1^n U_i$ (2)
Mean time to recovery	$\text{MTTR} = \frac{1}{n}\sum_1^n D_i$ (3)
Availability	$A = \frac{\sum_1^n U_i}{\sum_1^n (U_i + D_i)} = \frac{\text{MTTF}}{\text{MTTF} + \text{MTTR}}$ (4)
Reliability	$R(t) = e^{-\lambda t}$ (5)
Failure rate	$\lambda = \frac{1}{\text{MTTF}}$ (6)
Recovery rate	$\mu = \frac{1}{\text{MTTR}}$ (7)

Complex systems are broken down into subsystems to be analyzed. Since the subsystems may not be used for the entire operating period, the duty cycle (DC) of subsystems is then defined as the ratio of the subsystem operating time to the total operating time [Table II, Eq. (8)]. In this case, we introduced the effective failure rate λ^* for taking into account the DC [Eqs. (9) and (10)].

Assuming that the failure rate is constant and small compared to $1/t$, Table III shows the analytical formulas used to calculate the system availability when subsystems are in series or in parallel.

To simplify the availability formulation [Table III, Eq. (20)], we introduced the normalized expectation of recovery times Er as the expected value of the

TABLE II

Taking into Account the DC of Subsystems

Operating Time, t Time of Use, t_i	Duty Cycle	Reliability	Effective Failure Rate
Subsystem, i	$\text{DC}_i = \frac{t_i}{t}$ (8)	$R_i(t) = e^{-\lambda_i \text{DC}_i t}$ (9)	$\lambda_i^* = \lambda_i \text{DC}_i$ (10)

TABLE III

Formulas of Availability Variables for Various Subsystem Arrangements

λ_i = constant and $\lambda_i t << 1$	Subsystems in Series	Subsystems in Parallel	n Identical Subsystems in Parallel, j Needed, $k = n - j + 1$
Failure rate	$\lambda_s = \sum \lambda_i^*$ (11)	$\lambda_{\parallel} = \sum \mu_i \prod \frac{\lambda_i^*}{\mu_i}$ (14)	$\lambda_{\parallel k/n} = k\binom{n}{k}\frac{\lambda^k}{\mu^{k-1}}$ (17)
Recovery rate	$\mu_s = \frac{\sum \lambda_i^*}{\sum \frac{\lambda_i^*}{\mu_i}}$ (12)	$\mu_{\parallel} = \sum \mu_i$ (15)	$\mu_{\parallel k/n} = k\mu$ (18)
Recovery expectation	$Er_s = \sum \frac{\lambda_i^*}{\mu_i}$ (13)	$Er_{\parallel} = \prod \frac{\lambda_i^*}{\mu_i}$ (16)	$Er_{\parallel k/n} = \binom{n}{k}\frac{\lambda^k}{\mu^k}$ (19)
Availability	$A = \frac{1}{1+\lambda/\mu} = \frac{1}{1+Er}$ (20)		

subsystem's recovery time normalized to the operating time [Eq. (21)]. For subsystems in series, the expected value of recovery times is

$$Er = \frac{1}{t}E(\mathrm{MTTR}) = \frac{1}{t}\sum \left(1 - e^{-\lambda_i t}\right)\mathrm{MTTR}_i \cong \sum \lambda_i \mathrm{MTTR}_i \ . \quad (21)$$

When Er is also small compared to 1, the normalized expectation of recovery times is approximately equal to the unavailability UA:

$$UA = 1 - A \cong E_r \ . \quad (22)$$

Even though $\lambda^* \cdot t$ and Er are not negligible compared to 1, analytically calculated availability remains a good estimate of actual availability. In conclusion, criticality of failure modes can be gauged by the product $\lambda^*_i \cdot \mathrm{MTTR}_i$.

We can also notice that the analytical calculation is a good way to quickly assess the system's availability during the FMECA by using a simple spreadsheet.

III. CRITICALITY AND AVAILABILITY

During the FMECA, failure rates and recovery times are evaluated for each failure mode. The failure rate determines the occurrence level O on a scale from 1, i.e., improbable, to 5, i.e., very frequent. And the recovery time determines the severity level S on a scale from 1, i.e., minor effect failure, to 5 or 6, i.e., catastrophic effect failure. The criticality of failure modes is then defined as the product of the occurrence and severity (or, sometimes, the square of severity):

$$C = O \times S \text{ or } C = O \times S^2 \ . \quad (23)$$

This product is equivalent to the formulation of the normalized expectation of recovery times $\lambda_i \cdot \mathrm{MTTR}_i$, which is another assessment of the criticality of failure modes. The occurrence scale is often logarithmic whereas that of severity is not.[5,6] This is why criticality is sometimes a function of the square of severity. If the occurrence and the severity had an equivalent logarithmic scale, the criticality could be written as the sum of the occurrence and the severity:

$$\left.\begin{aligned} O &= \log(\lambda_i) + \text{const.} \\ S &= \log(\mathrm{MTTR}_i) + \text{const.} \end{aligned}\right\} C = O + S \ . \quad (24)$$

To illustrate this point, we used the RAMI data from a study conducted for ITER nuclear maintenance: the CPRHS (Refs. 5 and 7). In Fig. 2, criticality charts (the occurrence as a function of the severity of failure modes) are compared to the diagram of unavailability as a function of criticality. In Figs. 2a1 and 2b1, as DCs are very different, there are great discrepancies between unavailability and criticality; most failure modes are not well positioned on the chart. Using the effective failure rate λ_i^* [Table II, Eq. (10)], which takes into account the DC, the unavailability is an increasing function of the criticality (Fig. 2a2), and the failure modes on the chart

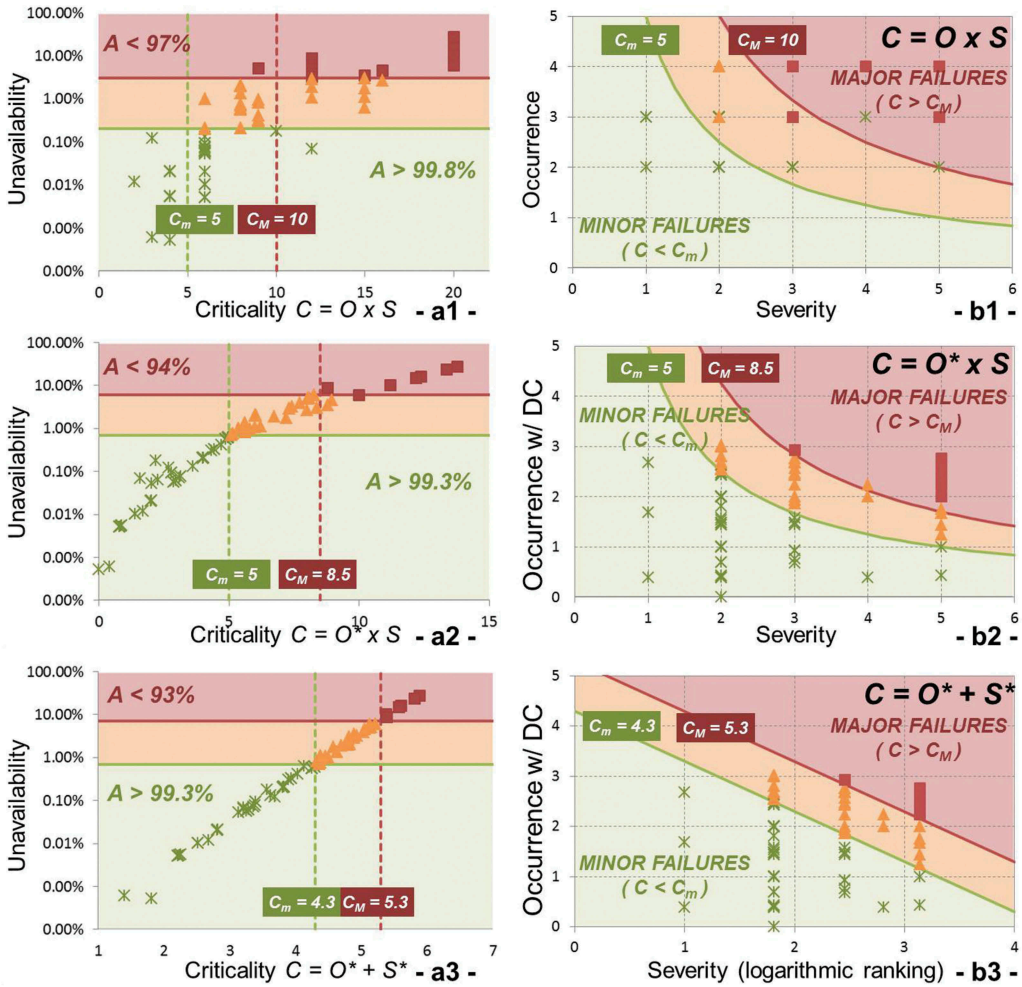

Fig. 2. (a) Unavailability of failure modes versus criticality. (b) Criticality chart. (1) Occurrence level without DC. (2) O*: occurrence level including the DC. (3) S*: severity level with a logarithmic scale. According to their availability, failures are classified into three groups: major, minor, and intermediate.

are in the correct area (Fig. 2b2). In addition, if we change the severity scale for a logarithmic one (this was already the case for the occurrence), the unavailability points are aligned for criticality defined as the sum of occurrence and severity (Fig. 2a3). In this case, the boundaries of failure mode classes are straight lines on the criticality chart (Fig. 2b3).

The limits of failure mode boundaries are determined based on the objective of system availability. This is why these limits depend on the scales of occurrence and severity.

IV. QUANTITATIVE SCHEDULE RISK ANALYSIS

One of the goals of the CPRHS study was to estimate the mean duration of this maintenance operation when the failure risks are taken into account. Without failure, this duration was established as 321 h. The RAMI approach calculated that the mean duration of the operation with failure events increased to 1464 h and, after mitigation actions, to 374 h (Refs. 5 and 7).

Maintenance operations were broken down into sequences that can be included in a time schedule. Therefore, Primavera QSRA was used to calculate the reliability and the availability of CPRHS functions and to compare them to the classical RBD results.

The failure modes of components were identified for each CPRHS sequence. In the schedule, the sequences appear as standard activities with fixed durations, while the failure modes associated with the sequence appear as conditional activities (Fig. 3). The

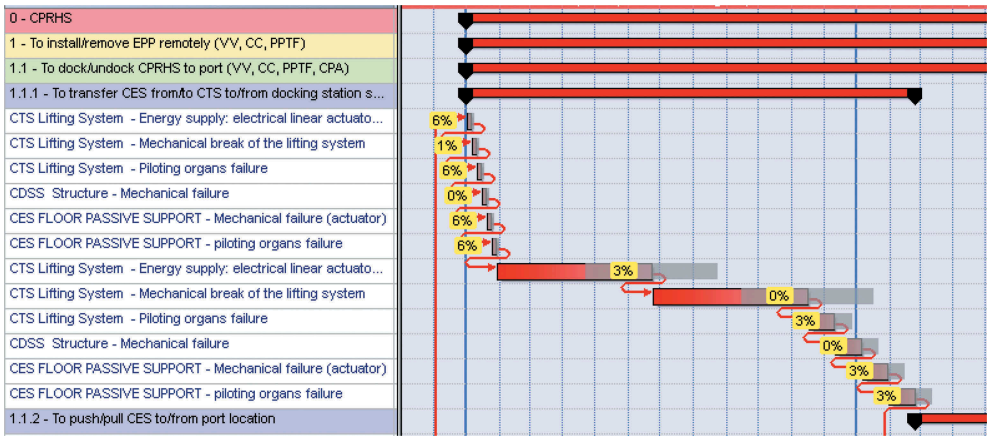

Fig. 3. Gantt chart of failure modes for the CPRHS. Failures are represented by conditional activities whose probability of existence is a function of the failure rate and the DC while its duration is equal to the MTTR.

probability Pr of the activity existence is determined by the reliability of the failure mode FM_i [Eq. (25)], while its duration is equal to the recovery time MTTR_i:

$$Pr(FM_i) = 1 - R_i(\mathrm{DC}_i t) = 1 - e^{-\lambda_i \mathrm{DC}_i t} \ . \qquad (25)$$

Using a Monte Carlo method, the Primavera QSRA provides the duration distribution of downtimes,[5] which allows the calculation of RAMI variables:

1. the failure rate (equal to the probability that no failure will occur)
2. the mean time to recover (equal to the average downtime)
3. the availability (function of the expected value of downtimes).

The Primavera QSRA also provides the duration cruciality of activities that is equivalent to the criticality of failure modes (Fig. 4). The duration cruciality is the correlation between the duration of the activity and the duration of the whole project.

Table IV shows that RAMI variables are in a good agreement for the three methods of calculation: RBD, analytical, and Primavera QSRA.

As a confirmation, we applied the Primavera QSRA method for another RAMI study: the WEST infrared thermography diagnostic. The diagnostic is part of the WEST tokamak protection system, which controls the power load on the plasma-facing components. Mitigation actions led to a design modification that improved system availability.[6] For an operation time of 8 months (5760 h), the Primavera QSRA

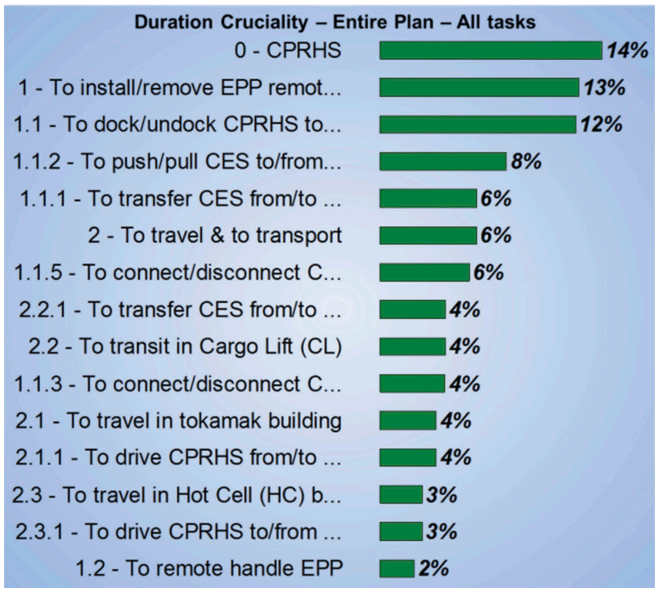

Fig. 4. Tornado graph of the duration cruciality of the main functions of the CPRHS (before mitigation actions).

provides the probability distributions for the two cases: before the mitigation actions and after the mitigation actions (Fig. 5). Here again, the RAMI variables are very similar for the three methods (Table V).

V. CONCLUSION

Using two concrete examples, an ITER maintenance system and a WEST diagnostic, three methods were compared to assess criticality: RBD analysis,

TABLE IV

Comparison of RAMI Variables of CPRHS Resulting from RBD Analysis (Stationary Values), Analytical Calculation, and Primavera QSRA

Duration Without Failure = 321 h	Initial Values			Expected Values		
	RBD	Analytic	Primavera QSRA	RBD	Analytic	Primavera QSRA
Reliability	14.1%	14.0%	14.4%	70.6%	70.6%	70.6%
Availability	21.8%	21.6%	21.9%	85.8%	85.8%	86.0%
Mean time of operation	1471 h	1487 h	1464 h	374 h	374 h	374 h

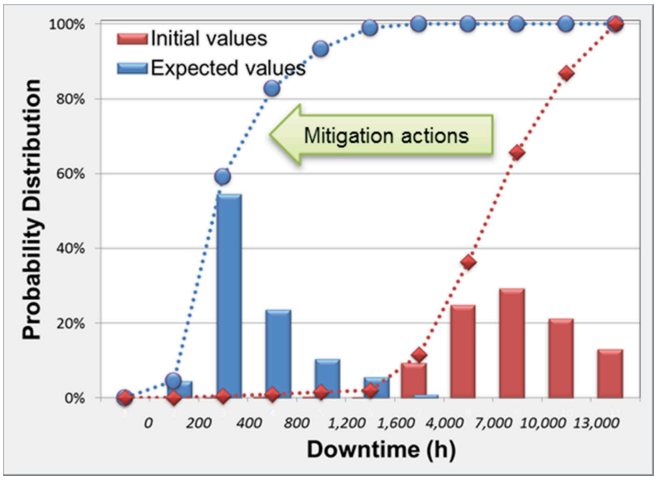

Fig. 5. Probability distribution of downtimes for 8 months of operation (5760 h) obtained by Primavera QSRA for the infrared thermography diagnostic.

Primavera QSRA, and analytical formulas. In all three cases, the results are very similar.

The analytical formulas showed that as a first approximation, the criticality defined by FMECA is the expression of the availability of failure modes. The FMECA criticality is therefore a good measure of the failures that have the greatest impact on the system availability. Furthermore, analytic formulas can also be used to quickly evaluate RAMI variables during the FMECA.

Besides the RBD analysis, the Primavera QSRA is another way of calculating RAMI variables. For this, the failure modes are associated with conditional activities whose probability of existence and duration are determined by the failure rate and the mean time to restore, respectively. The Primavera QSRA is an original method to identify the most critical failure modes and to calculate the availability of functions.

TABLE V

Comparison of the Availability of Infrared Diagnostic Functions Before and After Mitigation Actions Resulting from RBD Analysis, Analytical Calculation, and Primavera QSRA

Function Identifier	Initial Availability			Expected Availability		
	RBD	Analytic	Primavera QSRA	RBD	Analytic	Primavera QSRA
0	41.9%	39.6%	39.6%	91.0%	90.4%	90.3%
1	46.5%	44.0%	43.9%	94.5%	94.9%	94.9%
1.1	62.4%	58.2%	58.2%	98.4%	98.5%	98.5%
1.2	77.5%	72.9%	79.0%	97.9%	97.2%	97.9%
1.3	92.2%	89.3%	92.1%	99.8%	99.7%	99.8%
1.4	94.2%	93.8%	95.3%	99.3%	99.3%	99.4%
2	90.8%	86.7%	90.1%	99.8%	99.7%	99.8%
2.1	95.6%	93.8%	95.5%	99.8%	99.8%	99.8%
2.2	100%	100%	100%	100%	100%	100%
2.3	95.1%	91.9%	94.1%	100%	100%	100%
3	91.5%	91.3%	93.6%	95.4%	95.2%	96.5%
3.1	98.7%	98.7%	99.1%	98.6%	98.7%	99.1%
3.2	96.4%	96.1%	97.2%	98.6%	98.7%	99.1%
3.3	96.4%	96.1%	97.2%	98.4%	98.7%	99.1%

ORCID

D. Elbèze http://orcid.org/0000-0001-6788-6457

References

1. D. VAN HOUTTE, K. OKAYAMA, and F. SAGOT, "RAMI Approach for ITER," *Fusion Eng. Des.*, **85**, 1220 (2010); https://doi.org/10.1016/j.fusengdes.2010.03.007.
2. D. VAN HOUTTE et al., "A Functional Approach for Managing ITER Operations," *Fusion Eng. Des.*, **87**, 652 (2012); https://doi.org/10.1016/j.fusengdes.2012.01.033.
3. P. CHAPOUILLE, "Disponibilité des moyens de production," Techniques de l'ingénieur Fonction stratégique de la maintenance, MT9201 V1; https://www.techniques-ingenieur.fr (current as of Apr. 10, 2009).
4. J. FAUCHER, "Fiabilité. Maintenabilité," Techniques de l'ingénieur Fonction stratégique de la maintenance, T4300 V2, https://www.techniques-ingenieur.fr (current as of Oct. 17, 2016).
5. D. VAN HOUTTE et al., "Dependability Assessment of ITER Cask & Plug Remote Handling System," *Fusion Eng. Des.*, **136**, 1342 (2018); https://doi.org/10.1016/j.fusengdes.2018.05.005.
6. E. DELCHAMBRE et al., "RAMI Approach as Guidance for Optimizing the Design of the WEST Machine Protection System Using IR Thermography Measurements," *Fusion Eng. Des.*, **96–97**, 772 (2015); https://doi.org/10.1016/j.fusengdes.2014.12.037.
7. D. VAN HOUTTE et al., "ITER Framework for RAMI Engineering," presented at Technology of Fusion Energy Topical Meeting (TOFE 2018), Orlando, Florida, November 11–15, 2018.