ICIC Express Letters
Part B: Applications
Volume **7**, Number **10**, October **2016**

 ISSN 2185-2766
pp. **2247–2251**

RELIABILITY MODELING OF EMERGENCY SHUTDOWN FUNCTION FOR HEAT RECOVERY STEAM GENERATOR CONTROL

Chaichan Chairuan, Amphawan Julsereewong and Teerawat Thepmanee

Faculty of Engineering
King Mongkut's Institute of Technology Ladkrabang
Chalongkrung Rd., Ladkrabang, Bangkok 10520, Thailand
chaichan4246@gmail.com; { amphawan.ju; teerawat.th }@kmitl.ac.th

Received March 2016; accepted June 2016

Abstract. *This paper presents a method for evaluating reliability and unreliability of emergency shutdown function for a control system of heat recovery steam generator (HRSG), which is operated with active redundant for providing safety and protection. The studied triple-pressure HRSG for driving the steam turbine in a power plant consists of three sections: high pressure section, intermediate pressure section, and low pressure section. A safety shutdown is based on level and pressure sensing system with three pressure transmitters and three level transmitters in each section for implementing a voting algorithm in order to tolerate the failure of one sensor. Fault tree analysis (FTA) is employed as a tool for analyzing probability functions of success and failure for three possible voting algorithm configurations. Based on the obtained modeling, complex data of the studied system are transformed to accurate prediction of its reliability and unreliability.*
Keywords: Modeling, Reliability, Unreliability, Emergency shutdown, Fault tree analysis, Safety, Voting algorithm

1. **Introduction.** Generally, if automatic control systems cannot maintain control strategies, independent alarms indicate a problem. Plant operators can then supervise manual. If human intervention cannot make the specified corrections for critical situations, the last line of defense like emergency shutdown should automatically function to minimize the risk of harming people, environment, property, and so on. There are two ways for implementing safety and protection systems: safety provided by a basic process control system (BPCS) and safety provided by safety-instrumented system (SIS). The latter provides higher level of safety, because it is specially designed to shut down hazardous loops in the event where such a process problem is detected [1]. Instruments and controllers for realizing SIS are usually certified and approved by independent test institutes. On the other hand, the safety provided by the BPCS like distributed control system (DCS) uses regular field instruments and controllers that lack safety approval. In order to be detected reliably for process problems, the instrumentation and control must function properly. Therefore, reliability analysis of safety and protection systems is required to concern [2-8]. For system reliability evaluation, interesting methods based on probabilistic reliability assessment and physical and operational margins [2], based on fuzzy theory [3], or based on fault tree analysis [4,5] have been introduced. In addition, applications of reliability theory for evaluating safety integrity level of SIS have been proposed [6,7]. Alternatively, a practical technique for investigating into nuisance tripping caused the unscheduled plant shutdown as well as its mitigation has been suggested [8]. However, none of them focuses on evaluating reliability of voting algorithm for instrument signal failures.

This paper aims to introduce a reliability modeling of the BPCS-based safety shutdown for controlling heat recovery steam generator (HRSG) used in a power plant in Thailand.

The proposed modeling can be useful to evaluate reliability of shutdown conditions created by voting algorithm configurations. The unreliability evaluation of the studied system can be also obtained, since it is one's complement of the reliability function.

2. Studied Control System.

2.1. **Triple-pressure HRSG control.** The function of the combined-cycle HRSG system is to provide a method to extract sensible heat from the combustion turbine exhaust gas stream. The HRSG recovers the waste heat available in the combustion turbine exhaust gas. The recovered heat is used to generate steam at high pressure and high temperature, and the steam is then used to generate power in the steam turbine generator. The studied HRSG has three sections to generate steam at three different pressure levels for use in a steam turbine generator set and for power augmentation of the combustion turbine. The pressure levels of steam output are high pressure (HP), intermediate pressure (IP), and low pressure (LP). The studied HRSG is controlled by the open and closed loop controllers, which keep the process within the defined limits. If the controller or component deviates from its intended function, a process value may exceed the defined limits, causing a possibility of damage. Therefore, the automatic safety system, independent of the control system, must operate with the following tasks: to indicate to the operator when a limit is exceeded, to stop the process from further exceeding a limit, and to activate the emergency shutdown or trip function.

2.2. **HRSG shutdown configuration.** In the proposed modeling, the HRGS failure is identified as a system failure event to cause the process to be shut down. Figure 1 shows the fault tree construction for logical even relationships to identify the failure event. The process-problem shutdown of the studied triple-pressure HRSG is based on measuring level and pressure of three stream drums used. In order to implement a voting algorithm based on k-out-of-n system for tolerating the failure of one sensor, three level transmitters and three pressure transmitters are installed at a stream drum in each section (HP DRUM, IP DRUM, or LP DRUM). Thus, there are three possible cases for configuring the voting algorithm of level and pressure measurements: one out of three (1oo3), two out of three (2oo3), and three out of three (3oo3). For example, the 2oo3 system for measuring level of the stream drum means that this system requires at least two of three level transmitters to be operated successfully. If two or three level transmitters fail, the system will fail. The k-out-of-n system is an effective form of redundancy.

A fault tree can be used as a quantitative probability analysis tool. Probabilities are assigned to basic faults and trigger events. Reliability, $R(t)$, is a measure of success whereas unreliability, $F(t)$, is a measure of failure. $R(t)$ is defined as "the probability that a device will be successful during the operating time interval, t", while $F(t)$ is defined as "the probability that a device will fail during the operating time interval, t". For the

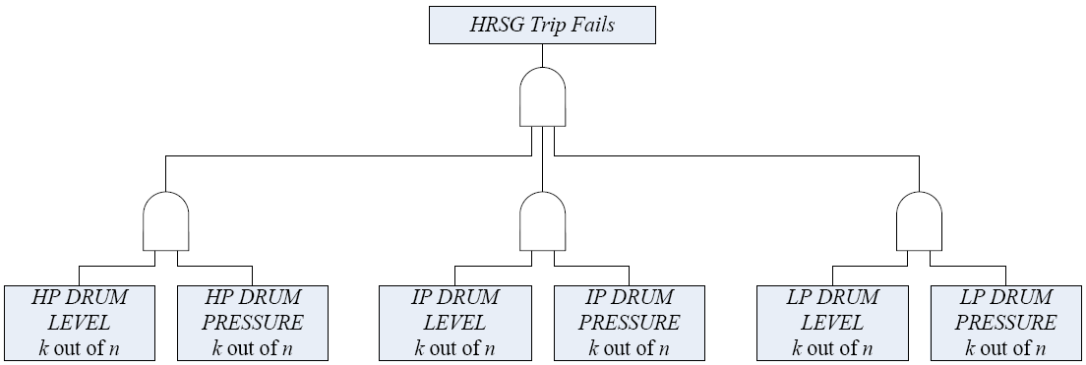

FIGURE 1. Fault tree construction for configuring shutdown conditions

analytical evaluation of the unreliability $F(t)$, or reliability $R(t)$ for the system, all the devices used are supposed to be not repairable, and the probability distributions of time to failure random variables are assumed to be exponential. Since any device must be either successful or failed, then

$$F(t) = 1 - e^{-\lambda t} = 1 - R(t) \tag{1}$$

where λ = failure rate (failures per hours) and t = time interval (hours).

When the failure rate of a component is known, the probability of failure for a given time interval can be calculated by multiplying the failure rate by the time interval.

3. **Reliability and Unreliability Models [9,10].** From Figure 1, the unreliability of the emergency shutdown function (F_{HRSG}) can be given by

$$F_{HRSG} = F_{HP\ DRUM} \times F_{IP\ DRUM} \times F_{LP\ DRUM} \tag{2}$$

where $F_{HP\ DRUM}$, $F_{IP\ DRUM}$, and $F_{LP\ DRUM}$ are the unreliability of high pressure drum, intermediate pressure drum, and low pressure drum, respectively, which can be stated as

$$F_{HP\ DRUM} = F_{LT(HP)} \times F_{PT(HP)} \tag{3}$$

$$F_{IP\ DRUM} = F_{LT(IP)} \times F_{PT(IP)} \tag{4}$$

$$F_{LP\ DRUM} = F_{LT(LP)} \times F_{PT(LP)} \tag{5}$$

where $F_{LT(HP)}$, $F_{LT(IP)}$, and $F_{LT(LP)}$ denote the unreliability of the level transmitters installed in high pressure drum, intermediate pressure, and low pressure drum, respectively, while $F_{PT(HP)}$, $F_{PT(IP)}$, and $F_{PT(LP)}$ are the unreliability of the pressure transmitters used in high pressure drum, intermediate pressure, and low pressure drum, respectively.

The level and pressure measurements of the studied HRSG are based on the k-out-of-n system, where k can be either 1, 2, or 3, and $n = 3$. The level (or pressure) measurement is successful, if k or more level (or pressure) transmitters are successful. The number of combinations can be written as

$$\begin{pmatrix} n \\ k \end{pmatrix} = \frac{n!}{k!(n-k)!} \tag{6}$$

The generic expression of reliability for the k-out-of-n system composed of identical and independent components can be expressed by

$$R(t)_{k/n} = \sum_{i=k}^{n} \begin{pmatrix} n \\ i \end{pmatrix} R(t)^i (1 - R(t))^{n-i} \tag{7}$$

Substituting (6) into (7), then the probalities of success for realizing combination of 1oo3, 2oo3, and 3oo3 configuraitons can be stated as

$$R(t)_{1\text{oo}3} = 3R(t) - 3R^2(t) + R^3(t) \tag{8}$$

$$R(t)_{2\text{oo}3} = 3R^2(t) - 2R^3(t) \tag{9}$$

$$R(t)_{3\text{oo}3} = R^3(t) \tag{10}$$

From (1) and (8)-(10), if the failure distribution is exponential, the unreliability $F(t)_{(i,j),k/n}$ of level (or pressure) measurement in each section (HP DRUM, IP DRUM, or LP DRUM) of the studied HRSG for 1oo3, 2oo3, and 3oo3 voting algorithms can be written as

For configuration with $k = 1$ and $n = 3$

$$F(t)_{(i,j)1\text{oo}3} = 1 - R(t)_{1\text{oo}3} = 1 - \left(3e^{-\lambda t} - 3e^{-2\lambda t} + e^{-3\lambda t}\right) \quad \forall i \in I,\ j \in J \tag{11}$$

For configuration with $k = 2$ and $n = 3$

$$F(t)_{(i,j)2\text{oo}3} = 1 - R(t)_{2\text{oo}3} = 1 - \left(3e^{-2\lambda t} - 2e^{-3\lambda t}\right) \quad \forall i \in I,\ j \in J \tag{12}$$

For configuration with $k = 3$ and $n = 3$

$$F(t)_{(i,j)3\text{oo}3} = 1 - R(t)_{3\text{oo}3} = 1 - e^{-3\lambda t} \quad \forall i \in I,\ j \in J \tag{13}$$

where i = set of generated steam in the section (HP DRUM, IP DRUM, or LP DRUM), and j = set of device used in the measurement (level or pressure transmitter).

From (3)-(5), and (11)-(13), the unreliability $F(t)_{(i,j)}$ for measuring level and pressure in three stream drums used in the studied HRSG can be stated as

$$F_{(i,j)} = \left(F(t)_{(i,j),k/n}\right)^j \tag{14}$$

Substituting (14) into (2), the unreliability $F(t)_{(HRSG)}$ for activating the emergency trip of the studied triple-pressure HRSG can be expressed by

$$F(t)_{(HRSG)} = \left(F(t)_{(i,j)}\right)^i \tag{15}$$

4. **Numerical Illustration.** For reliability analysis, the devices used in instrumentation and control of the studied HRSG are supposed to be not repairable, and the probability distribution of mean time to failure (MTTF = 17,520 hours or 2 years) is assumed to be exponential. For level (or pressure) measurement in each stream drum of HP DRUM, IP DRUM, or LP DRUM, the exponential distributions of the unreliability $F(t)_{(i,j),k/n}$ as given by (11)-(13) and the reliability $R(t)_{(i,j),k/n}$, can be illustrated in Figure 2. Figure 3 shows the exponential distributions of the unreliability $F(t)_{(i,j)}$ stated as (14) and the reliability $R(t)_{(i,j)}$ for measuring level and pressure in three stream drums, while Figure 4 shows the exponential distributions of the unreliability $F(t)_{(HRSG)}$ from (15) and the

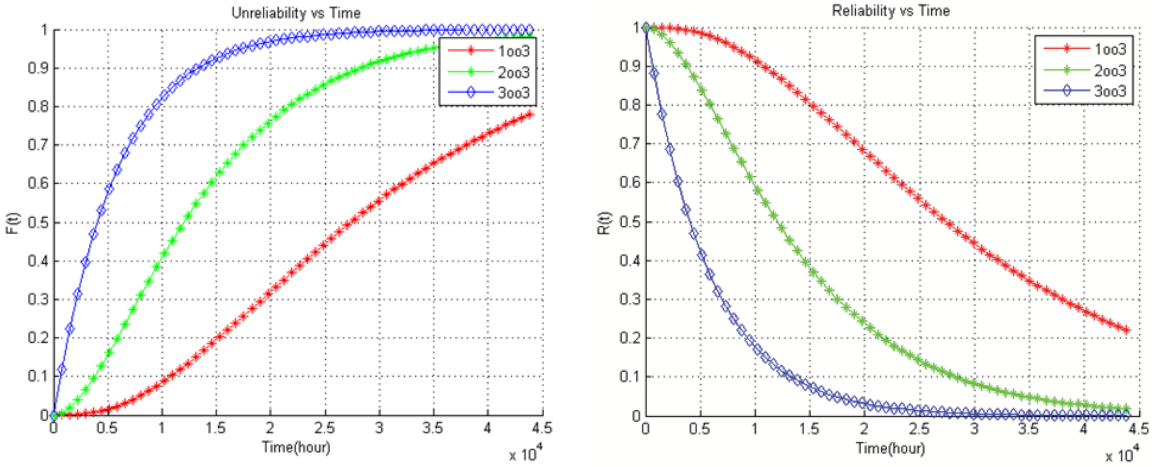

FIGURE 2. $F(t)_{(i,j),k/n}$ and $R(t)_{(i,j),k/n}$ for measuring the level (or pressure) in each stream drum

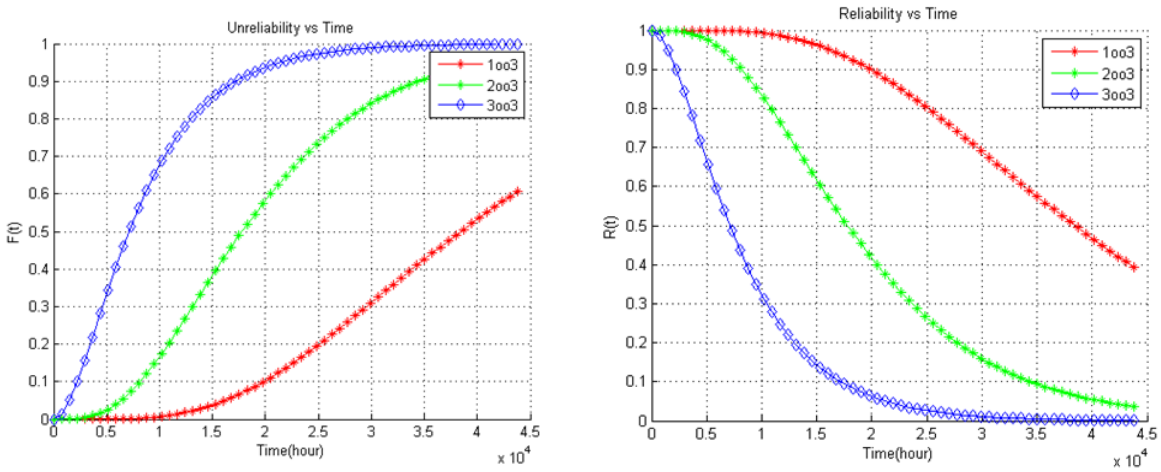

FIGURE 3. $F(t)_{(i,j)}$ and $R(t)_{(i,j)}$ for measuring level and pressure in three steam drums

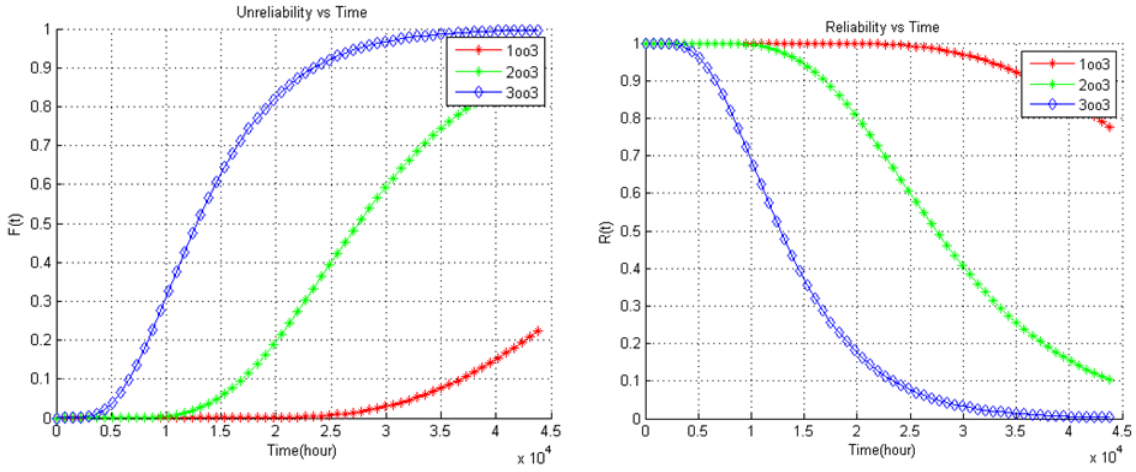

FIGURE 4. $F(t)_{(HRSG)}$ and $R(t)_{(HRSG)}$ for activating the emergency trip of the studied HRSG

reliability $R(t)_{(HRSG)}$ for activating the emergency trip when the studied HRSG control is failed.

5. **Conclusions.** The reliability modeling of the emergency trip for the triple-pressure HRSG control has been described in this paper. The process-problem shutdown is based on measuring two key parameters in the stream drum with k-out-of-n redundant configurations. The fault tree is used for describing how the studied HRSG is supposed to operate under various fault conditions and for analyzing the probability functions of both reliability and unreliability. The obtained modeling can be useful as a guideline during engineering design to select the voting algorithm configurations suitable for users' requirement. It should be recommended that the installation of measuring devices used for voting schemes must be paid careful attention. In addition, the reliability as well as unreliability of common cause failures in voting algorithm configurations will be examined in the future work.

REFERENCES

[1] P. Gruhn and H. L. Cheddie, *Safety Instrumented Systems: Design, Analysis and Justification*, ISA, USA, 2006.

[2] J. Park, W. Liang, J. Choi and J. Cha, A probabilistic reliability evaluation of Korea power system, *Proc. of International Conference on Innovative Computing, Information and Control*, pp.1-4, 2008.

[3] J. Zhou, L. Li, Z. Li and Q. Zhao, A new method of system reliability evaluation based on the fuzzy theory, *Proc. of International Conference on Innovative Computing, Information and Control*, pp.1005-1008, 2009.

[4] J. Che, M. Lv, Z. Yang, Z. Wang and F. Xu, Equipment systems reliability analysis based on FTA, *Proc. of Internaitonal Conference on Quality, Reliability, Risk, Maintenance, and Safety Engineering*, pp.293-296, 2012.

[5] M. Takahashi and R. Nanba, A proposal of fault tree analysis for control programs, *Proc. of SICE Annual Conference*, pp.1719-1724, 2014.

[6] Y. Lee, J. Kim, J. Kim and I. Moon, A verification of fault tree for safety integrity level evaluation, *Proc. of ICROS-SICE International Joint Conference*, pp.5548-5551, 2009.

[7] T. Thepmanee and S. Junlee, Investigation into nuisance tripping of stream turbine generator due to increase of shaft vibration amplitudes, *ICIC Express Letters, Part B: Applications*, vol.5, no.1, pp.243-250, 2014.

[8] T. Thepmanee and P. Khamkoon, SIL assessment and implementation case study: A safety instrumented function for overpressure protection in a two-phase gas-liquid separator, *ICIC Express Letters, Part B: Applications*, vol.5, no.1, pp.45-50, 2014.

[9] R. Manzini, A. Regattieri and H. P. E. Ferrari, *Maintenance for Industrial Systems*, Springer, 2010.

[10] W. M. Goble, *Control Systems Safety Evaluation and Reliability*, ISA, USA, 2010.