Available online at www.sciencedirect.com

ScienceDirect

Journal of Power Sources 171 (2007) 46–54

JOURNAL OF POWER SOURCES

www.elsevier.com/locate/jpowsour

Reliability analysis and initial requirements for FC systems and stacks

K. Åström[a,*], E. Fontell[a], S. Virtanen[b]

[a] *Wärtsilä Corporation, Tekniikantie 14, FIN-02150 Espoo, Finland*
[b] *Tampere University of Technology, Korkeakoulunkatu 6, FIN-33101 Tampere, Finland*

Received 12 September 2006; accepted 21 November 2006
Available online 5 January 2007

Abstract

In the year 2000 Wärtsilä Corporation started an R&D program to develop SOFC systems for CHP applications. The program aims to bring to the market highly efficient, clean and cost competitive fuel cell systems with rated power output in the range of 50–250 kW for distributed generation and marine applications.

In the program Wärtsilä focuses on system integration and development. System reliability and availability are key issues determining the competitiveness of the SOFC technology. In Wärtsilä, methods have been implemented for analysing the system in respect to reliability and safety as well as for defining reliability requirements for system components. A fault tree representation is used as the basis for reliability prediction analysis. A dynamic simulation technique has been developed to allow for non-static properties in the fault tree logic modelling.

Special emphasis has been placed on reliability analysis of the fuel cell stacks in the system. A method for assessing reliability and critical failure predictability requirements for fuel cell stacks in a system consisting of several stacks has been developed. The method is based on a qualitative model of the stack configuration where each stack can be in a functional, partially failed or critically failed state, each of the states having different failure rates and effects on the system behaviour. The main purpose of the method is to understand the effect of stack reliability, critical failure predictability and operating strategy on the system reliability and availability. An example configuration, consisting of 5 × 5 stacks (series of 5 sets of 5 parallel stacks) is analysed in respect to stack reliability requirements as a function of predictability of critical failures and Weibull shape factor of failure rate distributions.

Keywords: Reliability analysis; Fault tree analysis; SOFC system; Stack reliability

1. Introduction

Increasing customer awareness of reliability and its influence on lifetime costs and safety, together with increasing complexity of industrial plants and equipment has resulted in an escalating need for systematic methods of accounting for reliability in design and manufacturing. Traditionally, the use of such methods has essentially been limited to aviation, space and nuclear applications. More recently these methods have been adapted in several other industry branches. Reliability is expected to become a key competitive factor in applications where safety and availability are important [1].

Since the year 2000, Wärtsilä has developed planar SOFC systems for distributed power generation and marine applications. Wärtsilä focuses on system design and integration, balance of plant (BoP) development, and the interface between the SOFC power unit and the application. The SOFC stack being an integrated part of the FC system, optimal interaction between the stack and the BoP is an essential part of system optimization, which calls for close cooperation between the stack manufacturers and system integrators. Wärtsilä Corporation and Haldor Topsøe A/S, whose fuel cell program is managed by Topsøe Fuel Cell A/S, are running a joint development program within the planar SOFC technology. The program aims to bring highly efficient, clean, reliable and cost-competitive fuel cell products to the market for stationary power generation and marine applications. Within the program, a conceptual study of a 250 kW planar SOFC system for combined heat and power (CHP) applications was presented in 2003 [2], along with strategies to counter-

---

Abbreviations: ac, alternating current; BoP, balance of plant; CHP, combined heat and power; dc, direct current; FMEA, failure mode and effect analysis; FTA, fault tree analysis; HAZOP, Hazard and Operability Analysis; MTBF, mean time between failure; MTTF, mean time to fail; R&D, research and development; SOFC, solid oxide fuel cell; VBA, Visual Basic for Applications; WFC, Wärtsilä fuel cell

[*] Corresponding author. Tel.: +358 10 709 5473; fax: +358 10 709 5440.
E-mail address: kim.astrom@wartsila.com (K. Åström).

0378-7753/$ – see front matter © 2006 Elsevier B.V. All rights reserved.
doi:10.1016/j.jpowsour.2006.11.085

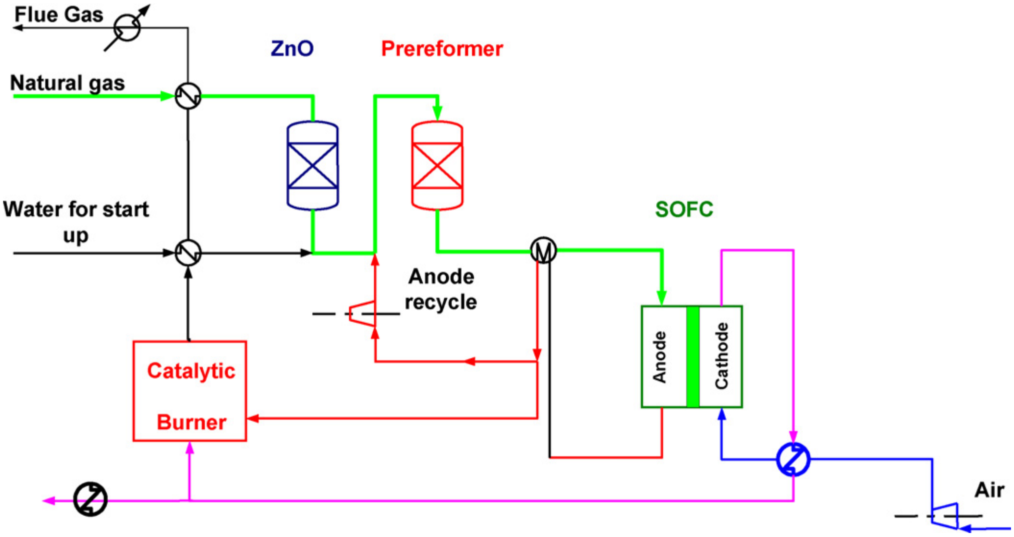

Fig. 1. Basic gas flow pattern of the 20 kW SOFC concept.

act stack ageing [3]. To demonstrate the developed concept a 1–5 kW test system was developed and presented in 2004 and 2006 [4,5]. Currently Wärtsilä is developing an alpha prototype of the WFC20 power unit, an independent SOFC module in the power range of 20 kWe.

During the R&D program Wärtsilä Corporation has developed methodologies and software tools for analysis of the fuel cell system and applications, e.g. [6]. This paper deals with analysing reliability aspects of SOFC systems and stacks through the analysis of a 20 kW SOFC concept. Wärtsilä expects reliability to be crucial for the competitiveness of SOFC power units both in respect to life cycle costs and feasibility in various applications. Due to high operating temperatures system components are subjected to significant thermomechanical stress in relation to thermal cycles which negatively impact performance and lifetime. This calls for systematic methodologies for accounting for and improving reliability throughout the design process.

A customized combination of methodologies, applicable for BoP and stack analysis is presented along with initial results. A dynamic simulation technique is derived for reliability prediction based on a fault tree representation of component dependencies. Based on a set of failure rate assessments the analysis yields a mean time between failures (MTBF) of 4400 h for the 20 kW SOFC concept. A fault tree model for a SOFC stack consisting of three qualitative states is presented and used to analyse the effect of critical failure predictability on the operability of a SOFC system with multiple stacks. The results clearly indicate that good failure predictability is a prerequisite for operating a configuration with multiple stacks having limited lifetime.

2. SOFC system description

The SOFC system developed within the Wärtsilä program is a natural gas fuelled system designed for various stationary and marine applications. Natural gas is supplied to a sulphur removal unit. The sulphur-free fuel is partially reformed by an adiabatic pre-reformer prior to entering the fuel cell stacks. The reformer is a fixed bed steam reformer reactor where all higher hydrocarbons are converted into methane, hydrogen and carbon oxides. In operation the steam is supplied by an anode recirculation blower. During start-up steam is supplied from an external water supply. The cathode air is supplied by a blower and preheated by cathode off-gases prior to entering the fuel cell stacks. The heat-exchanged off gas is divided between a heat recovery unit and a catalytic afterburner. In the catalytic afterburner, the anode off-gases are fully oxidized, which ensures extremely low emission. The basic system flow sheet is presented in Fig. 1.

In the power conversion part, the dc current produced by the fuel cell stacks is converted into a three-phase 400 V ac current by a dc/dc converter followed by a dc/ac inverter. The fuel cell stacks are arranged in series connected groups to obtain a voltage suitable for high-efficiency step-up dc/dc conversion to the dc/ac intermediate voltage level. With a nominal output of 400 V ac, this voltage lies in the range of 650–700 V dc. The dc/ac inverter is capable of both grid-paralleled and grid-independent operation.

In addition to the areas described above the system also includes hard-wired safety and control systems ensuring the safe operation of the power unit under all circumstances.

3. Reliability analysis methodology

3.1. General

Reliability is a measure of the probability of a product to perform certain required functions without failure under stated conditions during a stated period of time. Traditionally, the accounting for the reliability in design process has mostly or solely relied on the experience and attentiveness of the designers. However, increasing customer awareness of reliability together with increasing complexity of products has resulted in an escalating need for systematic approaches to account for reliability as an essential part of design and manufacturing processes. Active accounting for reliability aspects in design, manufacture and maintenance is the key to increasing safety and reducing warranty and lifetime costs of products [1].

A number of mathematical and statistical methods have been developed for quantifying reliability and analysing reliability data. It must be emphasized that the accuracy and credibility of the results obtained with these methods are typically not of the kind that engineers are accustomed to when dealing with most other problems. Due to the high levels of uncertainty in the input parameters, the uncertainty of the results may be up to several magnitudes (see, e.g. [7]). Still, these methods can provide valuable contributions to the reliability analysis provided that the interpreter has appreciated their basic limitations in respect to the credibility of the results.

Common methodologies used within reliability engineering include fault tree analysis (FTA), Petri nets, Markov analysis, failure mode and effect analysis (FMEA) and Hazard and Operability Study (HAZOP) (refer to, e.g. [7]). Broadly, the three former are methods for describing and analysing the failure logic of a system whereas the latter two are used for the identification of failure causes and consequences.

3.2. Objectives and approach

The main objective of the work presented herein was to construct a platform of methodologies for achieving an understanding of the reliability of the 20 kW SOFC system and to identify how different components and system entities affect it.

The reliability analysis was started from a component basis using FMEA for all components or functional entities considered relevant from the reliability point of view. Close to 70 entities were included in the analysis. Special attention was placed on identifying the mechanisms of detection of the identified failure types, based on which the severity of the failures could be assessed. The FMEA served as the basis for constructing the failure logic of the system. A fault tree representation was chosen for describing the logic as the large number of components ruled out the use of more complex representations such as Petri nets or Markov state space. A graphical fault tree analysis tool, ELMAS Analysis, developed at the Tampere University of Technology was used for the construction of the fault tree [8,9].

In FTA, the interrelations between failures and their consequences are expressed using Boolean logic to form a logical tree. The logical tree consists of nodes which can be either in a false (non-failed) or in a true (failed) state. The model distinguishes between two types of nodes: *basic parts* (root causes) and *gates* (consequences). Generally, each basic part in the constructed fault tree represents a physical component place or a functional entity which can fail. The gates represent events or logical groups of events whose occurrence depend of the states of the respective input nodes (=events). The uppermost gate in the hierarchy is called the TOP-gate and represents the state of the whole system.

For the SOFC system, the fault tree was grouped according to functional entities, i.e. air supply, fuel supply, exhaust system, etc. and, depending on the entity, further into sub-entities and down to the component level. For clarity, faults or combinations thereof that were identified as potentially hazardous were linked under a separate branch in the tree. The uppermost level and one sub branch of the failure tree depicted in Fig. 2.

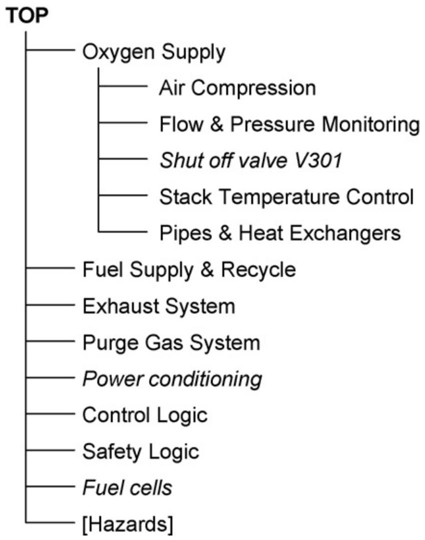

Fig. 2. Main branches in the fault tree for the 20 kW SOFC concept. Basic parts are printed in *cursive*.

3.3. Dynamic simulation

For reliability prediction, the occurrence of events in the fault tree was to be estimated through simulation or calculation based on estimated quantitative reliability and maintainability input parameters for the basic parts. To allow for non-constant failure rates and certain dependencies between the basic parts and the states of the system and other nodes, a time based simulation approach was required. For the purpose, a custom-made algorithm using Weibull distributions to estimate the failure rates of basic parts was implemented.

The starting point in the dynamic simulation is to determine the random failure moment of a component in accordance with its given reliability parameters. The *hazard rate*, $r(t)$ is the conditional probability of failure per unit time, given that there was no failure in the time interval $(0, T]$. The *reliability function* $R(t)$, in turn expresses the probability that there is no failure in the time interval $(0, T]$. The two are related by the so called generalized reliability equation which is valid for all hazard rate distributions [10]:

$$R(T) = \exp\left(\int_0^T r(t)\,\mathrm{d}t\right) \tag{1}$$

From the reliability function, we can further derive the conditional reliability function $R(t_1,t_2)$ [10], which assesses the probability that a component will not fail within the time interval $(t_1,t_2]$, given that the component is functional at t_1. Mathematically this can be expressed as

$$R(t_2) = R(t_1)R(t_1, t_2) \tag{2}$$

from which we get by solving for $R(t_1,t_2)$ and using (1)

$$\begin{aligned} R(t_1,t_2) &= \frac{R(t_2)}{R(t_1)} = \frac{\exp\left(-\int_0^{t_2} r(t)\,\mathrm{d}t\right)}{\exp\left(-\int_0^{t_1} r(t)\,\mathrm{d}t\right)} \\ &= \exp\left(-\int_0^{t_2} r(t)\,\mathrm{d}t + \int_0^{t_1} r(t)\,\mathrm{d}t\right) \\ &= \exp(I(t_1) - I(t_2)) \end{aligned} \tag{3}$$

where we have denoted $I(t)$ as the cumulative failure function [8]

$$I(t) = \int_0^t r(s)\,\mathrm{d}s \tag{4}$$

A direct consequence of the definition of the conditional reliability function is that if t_2 denotes the random variable representing the time of failure in the time interval ($t_2 \in (t_1,\infty)$) then $R(t_1,t_2)$ is uniformly distributed on the interval [0,1) [11]. Taking the natural logarithm of both sides of (3) and arranging terms we have

$$I(t_2) = I(t_1) - \ln(R(t_1,t_2)) \tag{5}$$

Further, if $I(t)$ (cumulative failure function or "information function") and its inverse function $I^{-1}(t)$ are known, a formula for simulating the next moment of failure of a component functional at $t = t_1$ is obtained by solving (5) for t_2

$$t_2 = I^{-1}[I(t_1) - \ln(rnd(1))] \tag{6}$$

where $rnd(1)$ returns a random variable uniformly distributed on the interval [0,1).

In the reliability prediction simulation, Weibull distributions were used for the hazard rates of all components. For the Weibull distribution we have [10]

$$r(t) = \frac{\beta}{\eta}\left(\frac{t-\gamma}{\eta}\right)^{\beta-1} \tag{7}$$

$$R(t) = \exp\left(-\left(\frac{t-\gamma}{\eta}\right)^{\beta}\right) \tag{8}$$

$$\mathrm{MTTF} = \gamma + \eta\Gamma\left(\frac{1}{\beta}+1\right) \tag{9}$$

where $t \geq \gamma$, $\beta > 0$, $\eta > 0$, $\gamma \in (-\infty,\infty)$, β is the shape parameter, η the scale parameter, γ the displacement parameter, and MTTF is the mean time to fail.

The displacement parameter shifts the distribution along the time axis. The shape parameter determines whether the hazard rate is decreasing ($\beta < 1$), constant ($\beta = 1$) or increasing ($\beta > 1$). The effect of the shape parameter on the hazard rate function is shown in Fig. 3.

Substituting (7) into (4) we obtain

$$I(t) = \int_0^t \frac{\beta}{\eta}\left(\frac{s-\gamma}{\eta}\right)^{\beta-1}\mathrm{d}s = \left(\frac{t-\gamma}{\eta}\right)^{\beta} + \left(\frac{\gamma}{\eta}\right)^{\beta} \tag{10}$$

Solving (10) for I^{-1} we have

$$I^{-1}(t) \equiv t(I(t)) = (\eta^{\beta} I(t) + \gamma^{\beta})^{1/\beta} + \gamma \tag{11}$$

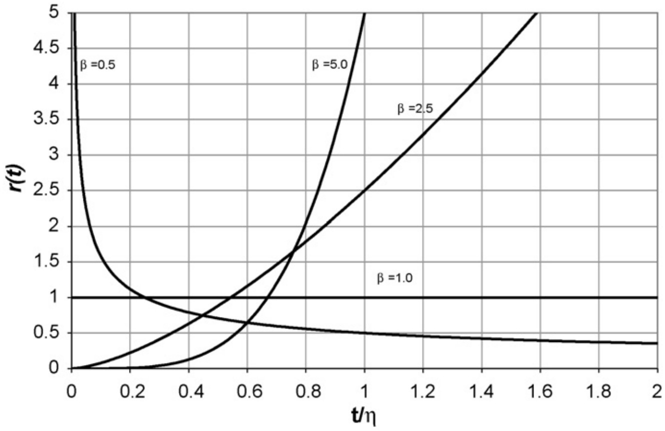

Fig. 3. Effect of the Weibull β-parameter on the hazard rate function $r(t)$ ($\gamma = 0$).

Combining (10), (11) and (6) we get

$$t_2 = \left(\eta^{\beta}\left(\left(\frac{t_1-\gamma}{\eta}\right)^{\beta} - \ln(rnd(1))\right) + \gamma^{\beta}\right)^{1/\beta} + \gamma \tag{12}$$

which, having $\gamma = 0$ simplifies to

$$t_2 = \eta\left(\left(\frac{t_1}{\eta}\right)^{\beta} - \ln(rnd(1))\right)^{1/\beta} \tag{13}$$

In the simulation algorithm, Eq. (13) is applied for each of the components to obtain the moment of its next failure. Upon failure or scheduled overhaul of a component, its effective age (t_1) is updated after which (13) is reapplied. For each of the components, the following attributes are defined:

- Weibull shape and scale factors for the hazard rate.
- Age correction multiplication factor: It describes how overhaul affects the effective age (t_1).
- Preventive/scheduled maintenance interval.
- Overhaul possible when TOP is operating (true/false)? For the components that were serviceable during system operation, a fixed repair time of 72 h was applied.
- Failure detectable condition: A failure can be configured to remain undetected, i.e. not repaired until a set of nodes become true. This feature is used for safety functions.
- Active condition: The component can be configured to be active only when a set of nodes are true. This feature is used for redundant components and to implement certain dynamic features.

Using the listed reliability attributes, the algorithm simulates and records the occurrence for a specified time for a large number of instances after which the results are outputted. Visual Basic for Applications (VBA) in combination with MS-Excel was chosen as the simulation platform as computation speed was not critical. The versatility of MS-Excel provided an efficient means for entering the data and organizing it in an easily manageable structure. A rough presentation of the code execution flow is given in Fig. 4.

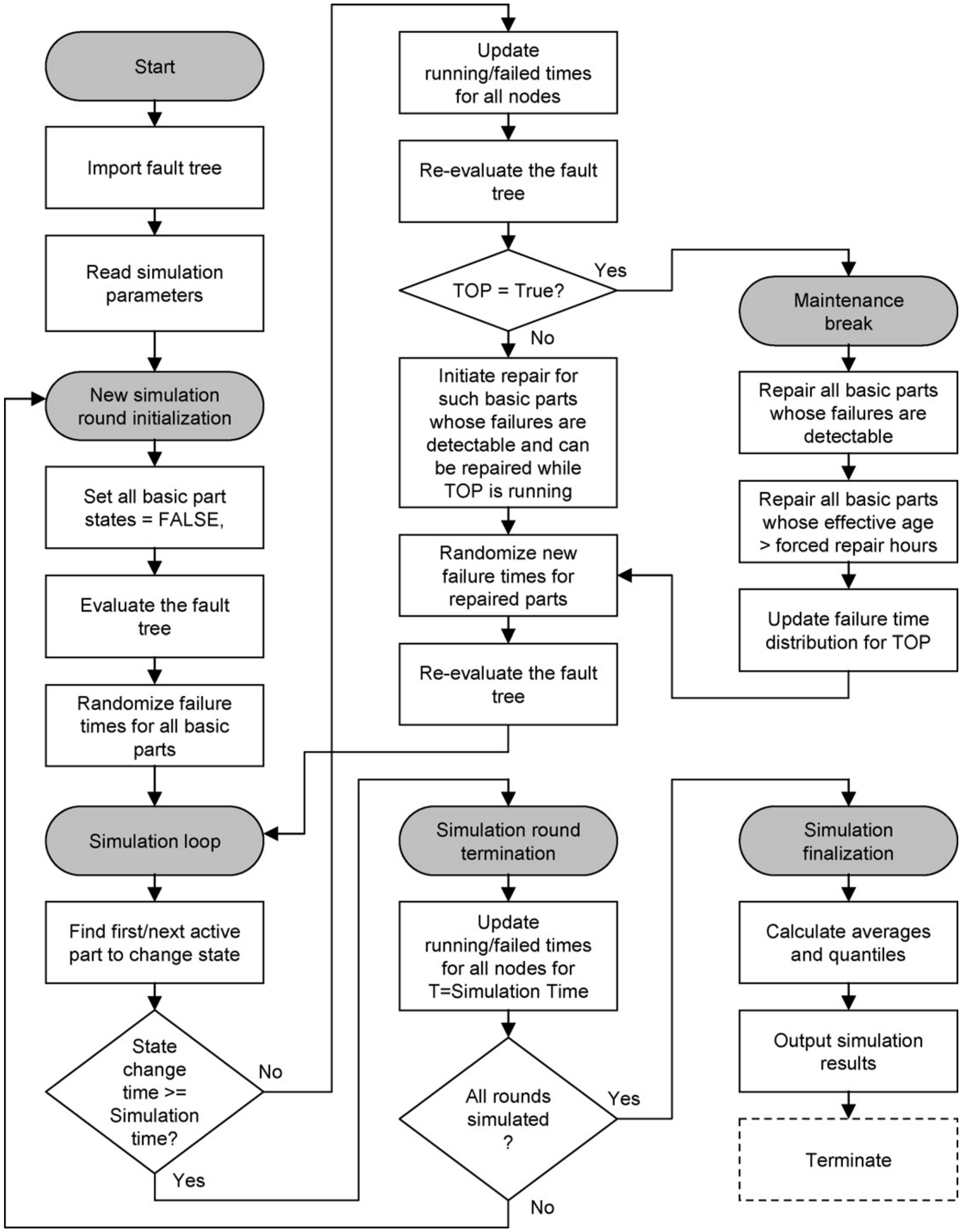

Fig. 4. Flow chart representation of the simulation logic.

The averaged results include the failure count, the time spent in active, non-active and failed states and the number of scheduled maintenance actions for each of the nodes in the fault tree. For the TOP node, a graph representing the average and 5 and 95% quantiles of the cumulative amount of failures as a function of time is outputted.

3.4. Applied assumptions and results

In the previous subsection the methods used for describing and analysing the reliability of a fuel cell system were presented. It should be appreciated that despite all limitations and constraints inherent to the methods, the most significant limitations regarding the credibility and applicability of their results stem from the uncertainty of the applied reliability data. Various reliability data sources based on qualitative studies of the construction, properties, parts and typical stress levels of components (expert judgement) or on statistics are available for component-level reliability prediction purposes. The following data sources were used: SINTEF Reliability Data for Safety Instrumented Systems [12], OREDA Offshore Reliability Data [13], Exida Safety Equipment Reliability Handbook [14] and T-

Table 1
Summary of applied failure rate parameters for BoP components

	MTBF (h)	Weibull shape factor
Blowers and compressors	40,000–100,000	2.75
Control valves	40,000–150,000	1/2.75
Controlling logic	30,000	1
Flow controllers	60,000	1
Flow sensors	120,000	1
Gas indicators	300,000	1
Pressure sensors	500,000	1
Reactors, pipes, heat exchangers	100,000–200,000	2.75
Shut-off valves	600,000	1
Temperature sensors	20,000–100,000	2.75

book Reliability Data of Components in Nordic Nuclear Power Plants [15]. The applicability of the data presented in reliability data sources is, however, in general subject to controversy due to the uncertainty and sensitivity to parameter changes intrinsic to reliability prediction. For some of the system components the operating conditions may differ significantly from the ones that that any statistical data or expert judgement is based on. Thus, using this data to predict the system reliability can be misleading. The use of these data sources was thus limited to components whose characteristics and operating conditions could be considered essentially similar to the typical ones which the statistical data was assumed to be based on. This condition was considered to apply for “standard” parts operating in the cold compartments of the system, particularly sensors and transmitters and to a limited extent valves and electronic equipment. Only critical failures, i.e. failures capable of causing a system trip, were considered. For components whose reliability could not be estimated based on reliability databases or estimates provided by the components suppliers, the failure rates applied in the reliability prediction analyses were assessed as targeted values rather than actual estimates. The choice of targeted values was based on the qualitative FMEA analysis in which the expected failure modes and potential related hazards had been considered. When interpreting the results of the reliability prediction analysis it must thus be kept in mind that these targeted reliabilities may be way in excess of the actual reliabilities of prototypic components.

A Weibull distribution function was considered sufficient to depict the failure rate of each component as infant mortality failures were not taken into account. For components considered not subject to wear a constant failure rate (shape factor = 1) was applied whereas for deteriorating components a shape factor of 2.75 was used. This particular shape factor was chosen to represent an average for mechanical components [7]. For this shape factor the probability of failure before $t = \eta/2$ is 13.8% whereas the probability of failing before $t = \eta$ is 63.2%, where η is the Weibull scale parameter (characteristic life). A rough summary of the failure rates used for BoP components is provided in Table 1. The rates are exclusive of non-critical failures and regular preventive maintenance.

A summary of the failure distribution results obtained from the dynamic simulation is presented in Fig. 5.

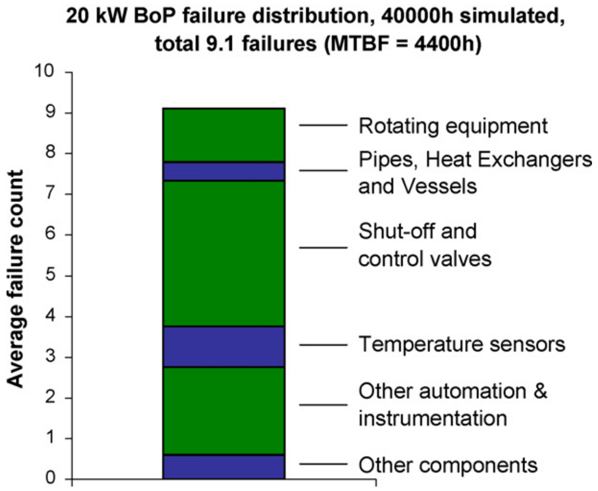

Fig. 5. Summary of the failure distribution results obtained for the BoP system in the 20 kW SOFC concept.

The amount of failures caused by rotating equipment reflects relatively high requirements combined with a low number of devices. The low number of failures in the pipes, heat exchangers and vessels, in turn stem from stringent requirements which have been set based on poor maintainability and unfavourable properties of failures in this category. Reaching the reliability targets listed in Table 1 may, however, prove to be very demanding. The relatively high proportion of failures in the automation and instrumentation equipment and reflects the fact that the prototypic system has a very high number of adjustable process parameters and consequently a high number of failure-prone devices, which can be expected to reduce as the technology matures.

The results must be regarded as highly optimistic for the system prototype as they are based on the assumption that the reliability of all components reaches the relatively high levels listed/allocated in Table 1. Additionally preventive and corrective maintenance, such as temperature sensor recalibration or replacement has been assumed to take place at regular intervals. Still, the results imply that high temperature fuel cell systems show the potential to achieve high reliability once the technology matures. By the addition of redundant devices, which becomes viable particularly in larger systems, reliability can be further improved.

4. Stack reliability

In systems comprising of groups of stacks whose operating conditions cannot be independently controlled, the effects of variance in the characteristics of individual stacks on the system behaviour need to be considered. Variance in the stack characteristics or in the operating conditions of individual stacks may, depending on the design of the system, cause an uneven distribution of load among the stacks which, in turn may have a negative impact on system stability, performance and stack durability. The system must be designed to be stable in respect to expectable variances in the stack characteristics as well as performance deterioration. However, with respect to certain stack failure types, such as significant leakages, redundancy among

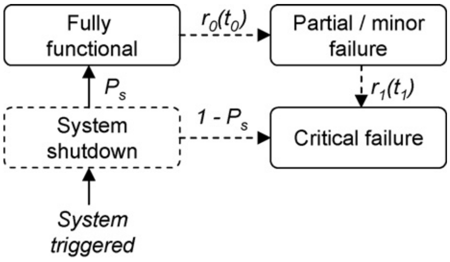

Fig. 6. Qualitative failure model for SOFC stacks.

interacting stacks may not be readily achievable. This implies that increasing the number of stacks subject to common control brings along more stringent stack level reliability requirements in respect to these critical failure types.

In the following, a qualitative approach for assessing initial reliability requirements for stacks in an example system is presented. The assessment is based on a qualitative model dealing with probabilities of different types of failures rather than actual performance variables. In the qualitative model, the input parameters can be reduced to a low number allowing for concrete results without needing to define a large number of underlying performance parameter values and distributions. The failure logic of the stack array is expressed using a fault tree which is analysed using the same dynamic simulation techniques as were used for the analysis of the BoP-section. It distinguishes between two types of failures, minor/partial failures and critical failures. Critical failures are failures that require an immediate system shutdown, whereas minor/partial failures are assumed to be detectable but not alone critical. The minor/partial failure state may, e.g. represent a state where the stack voltages have degraded by a certain amount, or a decrease in voltages or currents caused by any incipient mechanical failure.

The probability of a fully functional stack to develop a minor/partial failure is expressed by a hazard rate function $r_0(t_0)$, where t_0 is the operational age of the stack. When in the partially failed state, the probability of developing a critical failure is expressed by a hazard rate function $r_1(t_1)$, where t_1 is the time spent in the partially failed state. Additionally, the ability of a stack to withstand a thermal cycle is expressed by a fixed probability P_s. The operational states and the corresponding transition probabilities are illustrated in Fig. 6.

Weibull distributions are used for the hazard rate functions, whereby the described model contains a total of 5 degrees of freedom to characterize the failure logic of a stack, when the displacement parameters are omitted for both r_0 and r_1. For convenience, the same shape parameter is applied for both hazard functions. A fault tree representation of the failure logic applicable for dynamic simulation is presented in Fig. 7.

To allow for dynamic analysis using the algorithm described previously, Weibull distributions have been applied for the failure rates of basic parts as indicated by the shape and scale parameters in Fig. 7. For convenience, the same shape parameter has been used for both r_0 and r_1. The desired two-step transition from the fully functional state down to the critical failed state has been accomplished using separate basic parts for r_0 and r_1 where the part representing r_1 has been configured to be active only when r_0 has failed, i.e. when the stack is in the minor failure state. The third basic part is a help part set to fail approximately 1 h after each start-up, whereby the conditional start-up failure gate is evaluated. All three basic parts are set to be repairable only during system shut-downs and have an age correction factor of 0, i.e. their cumulative age is reset upon repair. This corresponds to a maintenance strategy where all partially or critically failed stacks are replaced prior to restarting the system after a shut-down.

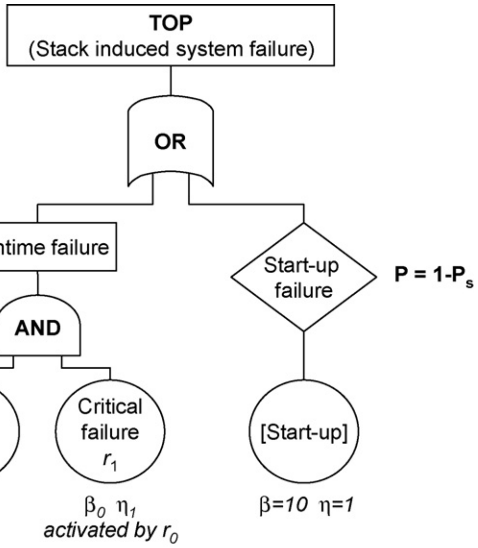

Fig. 7. Fault tree representation of the stack model with relevant parameters for dynamic simulation.

The described stack model has been used to analyse the failure tendency of an example system consisting of 25 stacks, arranged into 5 groups. A system shutdown was defined to occur if any of the stacks develops a critical failure or if at least two out of five stacks in any of the groups are in the partially failed state. For convenience, P_s was set to 1 as the expectable number of start-up failures N_s can be readily approximated from

$$N_s = N_f \frac{1 - (P_s)^A}{(P_s)^A} \tag{14}$$

where N_f is the number of simulated system failures and A is the amount of stacks.

BoP system induced failures were simulated using a basic part having MTBF = 4000 h with constant failure rate. The amount of stack-induced failures obtained from simulation with various scale and shape parameters for the hazard rate functions r_0 and r_1 are displayed in Figs. 8 and 9.

The results in Figs. 8 and 9 highlight the necessity of accounting for stack reliability and demonstrate the effect of stack critical failure predictability on system operability. With the given maintenance strategy, the hazard function r_1 is a direct measure of the ability to forecast and avoid critical failures. With no predictability, i.e. MTTF $r_1 = 0$, high stack reliability is required to bring down the number of failures to an acceptable level, e.g. less than 5 failures 40,000 h^{-1}. As the r_1 MTTF is increased, the requirements on r_0 can be released. Due to the lower variance in failure times, increasing hazard rates are

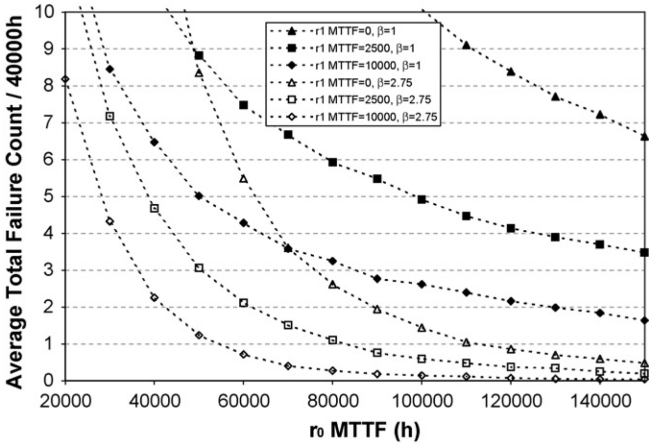

Fig. 8. Total number of stack induced failures for 40,000 h of operation obtained by dynamic simulation of a 25 stack configuration with various shape and scale parameters for the hazard rate functions r_0 and r_1 of the qualitative stack model.

clearly more favourable than constant failure rates for all simulated combinations of r_0 and r_1 whose results lie in a feasible range. For $\beta = 2.75$ and MTTF $r_1 = 10{,}000$ the amount of critical failures can be reduced to below 0.5 failures in 40,000 h even with low relatively low stack lifetimes. It however remains to be validated by experiment and further analysis how this level of predictability is to be achieved.

For the example system consisting of 25 stacks, the effect of less than unity probability P_s of a stack to start up successfully is shown in Fig. 10, where N_f is the number of failures other than stack-induced start-up failures, i.e. number of successful start-ups. Clearly, a P_s very close to unity is a prerequisite for keeping the number of thermal cycles within acceptable bounds in a multiple-stack configuration. If e.g. 10% of the system start-ups are allowed to fail due to a stack failure, a P_s of approximately 0.996 is required.

5. Discussion

Reliability is widely anticipated as a key factor determining the competitiveness of SOFC technology. In this paper, a set of methodologies for analysing certain aspects of reliability of a SOFC system have been presented. A failure mode and effect analysis was used to identify the dependability of all relevant BoP system components. Based on this analysis, a fault tree representation was used to describe the event chains. The fault tree representation together with assumptions regarding the failure characteristics were used as input data for reliability as well as hazard prediction using a customized dynamic simulation tool.

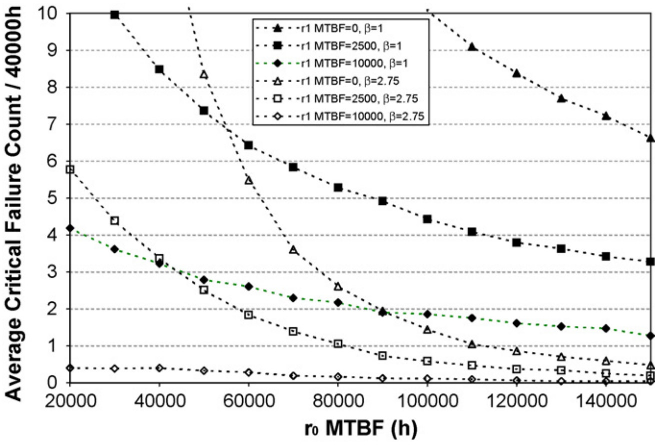

Fig. 9. Simulation results for number of critical stack induced failures for 40,000 h of operation.

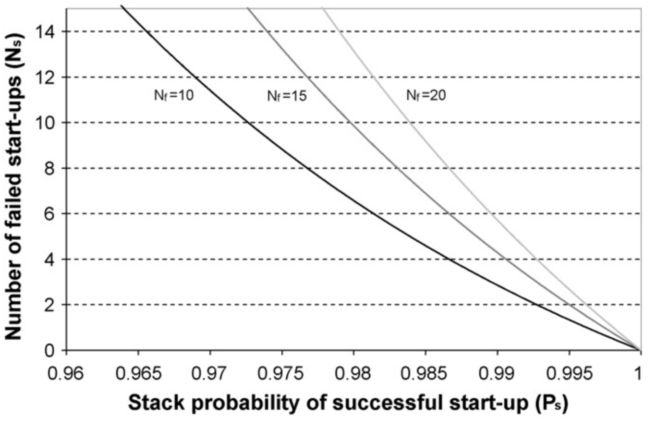

Fig. 10. Number of stack-induced failed start-ups as given by Eq. (14).

Despite the high level of inherent uncertainty, the results for the BoP section of the system indicate that SOFC systems show a potential for reasonably high reliability provided that the fuel cell stacks become sufficiently reliable. For the BoP section of the WFC20 α-prototype, the reliability prediction analysis yields an MTBF of 4400 h for 40,000 h of operation. It must be emphasized that these figures are based on the general system layout and do not account for design flaws such as faulty dimensioning or control errors. Rather the results reflect the achievable level of reliability once initial design flaws have been removed and the components within the system achieve their stated reliability requirements. Future reductions of the complexity of control together with component redundancy allow for improving the reliability further.

For SOFC stacks a qualitative model for assessing basic reliability requirements in terms of critical failure rates versus their predictability was developed. The results obtained for a 25 stack system demonstrate the importance of accounting for stack reliability issues in systems comprising multiple stacks. The model further highlights the essentiality of being able to predict critical failures when operating a configuration of multiple stacks having limited lifetime and reliability. With best case predictability, the average number of stack critical failures could be kept below 0.5 failures 40,000 h^{-1} of operating with a stack MTTF of only 20,000–30,000 h whereas for the worst-case scenario, over 5 failures occurred even with a stack MTBF of as high as 150,000 h. The requirements for stack robustness against stresses induced by thermal cycling rise along with increasing number of stacks and thermal cycles in a system. For a system comprising 25 stacks the probability of a stack to start up successfully needs to be in excess of 99.5% to allow for keeping the fraction of failed system start-ups below 10%.

The developed reliability simulation methodology proved to be well-applicable for both the BoP analysis and for analysing the qualitative stack model. The fault tree representation was found to be a convenient way of expressing system dependabilities whereas the dynamic simulation technique provided means for overcoming the most significant constraints of traditional static fault tree analysis. The methodology is as such suitable for an increased complexity and level of detail in the models and can easily be further improved to allow for a wide range of failure rate distributions. Currently, the accurateness of the modelling is constrained by the very limited availability of relevant reliability data. This constraint can, however, be expected to be constantly lifted as experiences from operating the first units are gained. 3000 h of operation data is currently available for the 5 kW prototype, and the 20 kW prototype is to be started up during fall 2006. Having implemented methodologies for active accounting for reliability at an early stage facilitates efficient collection of relevant data for future analyses as an essential part of the design towards reliable, maintainable and cost-efficient SOFC units.

Acknowledgments

The authors would like to express their gratitude to Wärtsilä Corporation and TEKES for the financial support and facilitation of the research.

References

[1] S. Virtanen, RAMS 98, International Symposium on Product Quality and Integrity—The Reliability and Maintainability Symposium, Anaheim, USA, 19–22 January, 1998, pp. 82–88.
[2] E. Fontell, T. Kivisaari, N. Christiansen, J.B. Hansen, J. Pålsson, J. Power Sources 131 (2004) 49–56.
[3] J.B. Hansen, J. Pålsson, J.U. Nielsen, E. Fontell, T. Kivisaari, et al., Extended Abstract Presented in 2003 Fuel Cell Seminar, Florida, November 2003.
[4] E. Fontell, J.B. Hansen, T. Kivisaari, J. Pålsson, M. Jussila, J.U. Nielsen, Fuel Cell Seminar—Abstracts CD, November 2004.
[5] E. Fontell, M. Jussila, J.B. Hansen, J. Pålsson, T. Kivisaari, J.U. Nielsen, Wärtsilä–Haldor Topsøe SOFC Test System: Extended Abstract Presented in 2005 International Symposium on Solid Oxide Fuel Cells, Quebec, Canada, May, 2005.
[6] E. Fontell, T. Phan, T. Kivisaari, K. Keränen, Trans. ASME 3 (2006) 242–253.
[7] P. O'Connor, Practical Reliability Engineering, fourth ed., John Wiley and Sons Ltd., Chichester, England, 2002.
[8] S. Virtanen, P. Hagmark, Reliability in Product Design—Seeking Out and Selecting Solution, Publication No. B22, Helsinki University of Technology, Laboratory of Machine Design, Otaniemi, Finland, 1997.
[9] J. Penttinen, Master's Thesis, Tampere University of Technology, Department of Information Technology, 2004 (in Finnish).
[10] D. Kececiougly, Reliability Engineering Handbook, Prentice Hall, New Jersey, 1991.
[11] R.Y. Rubinstein, Simulation and the Monte Carlo Method, John Wiley & Sons Inc., New York, 1981.
[12] Reliability Data for Safety Instrumented Systems, PDS Data Handbook, 2003 ed., SINTEF, March 2003.
[13] OREDA: Offshore Reliability Data, third ed., SINTEF Industrial Management, 1997.
[14] Safety Equipment Reliability Handbook, exida.com L.L.C., Sedersville, USA, 2003.
[15] T-Book Reliability Data of Components in Nordic Nuclear Power Plants, third ed., Vattenfall AB, Vällingby, Sweden, 1992.