Criticality Analysis of Process Systems

Thomas V. Thomaidis, Ph.D., FTS SA, Volos
Stratos Pistikopoulos, Professor, Centre for Process Systems Engineering, London

Key Words: Effective Risk Assessment / Analysis, Fault Trees, FMEA, DFLD, Flexibility, Reliability, Criticality, Preventive Maintenance, Process Systems

SUMMARY & CONCLUSIONS

This paper presents a systematic methodology for formal criticality analysis of process systems, which properly accounts for process interactions, equipment failure, stochastic process variations and events related to process safety. Important extensions are also presented for the use of such criticality analysis tools for safety and maintenance considerations. In the first part a quantitative measure for estimating the expected level for critical operations of process systems is introduced. Next a systematic algorithm of rating the equipment or events according to an associated criticality index is presented, coupled with a methodology for condition based maintenance for enhancing overall system efficiency and safety. The developed tools and the algorithms are demonstrated via a realistic case study of a compressor system, where (*FOR)* and (*COR*) are properly identified for the operable states. The proposed methodology is applied in order to rank the critical parts of the equipment or events, and then to result in the maintenance policy which fulfill certain efficiency and safety targets. While the criticality analysis methodology developed in this work predicts variable information regarding the overall system expected critical operations, the relative importance of the equipment to the process and identification of process and/or reliability bottlenecks, its link to the design optimization algorithm has not been formally established. However, as it is shown via the case study, the proposed methodology could be an efficient tool for the proper balance of preventive and condition based maintenance activities and the prediction of their impact to process operational decisions.

NOTATION LIST

R_{LB}, Lower bound of system reliability
$P_k(t)$, State probability as a function of time
MC, Set of minimal cut sets of the system
c, Minimal cut set $c,\ c \in MC$
$r_l(t)$, Probability of event l occurring from 0 to t for simplicity is used as r_l
$\rho_l(t)$, Probability of failure of part l occurring from 0 to t for simplicity is used as ρ_l
$J(\bar{J})$, Set of operable (failed) equipment
K, Set of system states
K_{OP}, Set of operable system states
T_S, Maintenance suspension period
t_C, Maintenance completion time
T_{pm}, Nominal operational period before the execution of a new maintenance task
T_{mop}, Minimum operational period
$FR(t)$, Combined Flexibility-Reliability for the system as a function of time
FR^T, Combined Flexibility-Reliability Target for the system over a time horizon
$CRI(t)$, Criticality Index of a system as a function of time
CRI^T, Criticality Index Target of a system over a time horizon
CR_k, Criticality index of a state $k,\ k \in K_{OP}$
SF_k, Stochastic flexibility index of state $k,\ k \in K_{OP}$
m, Subsystem or component / event in aggregated system
l, Basic event (e.g. failure of equipment)
k, System state
$*$, To which component / event criticality analysis is performed

NOMENCLATURE

AGAN, As Good As New
AGAO, As Good As Old
COR, Critical Operating Regions for the process model
DFLD, Directed Functional AND/OR Logic Digraphs
FOR, Feasible Operating Regions for the process model
MTTR, Mean Time To Repair

FMECA, Failure Mode Effect and Criticality Analysis

ASSUMPTIONS

1. Equipment is classified as maintainable and non-maintenanble; the latter include those components whose maintenance requires system shutdown.
2. Scheduling and ordering of maintenance tasks is based on the equipment / subsystems with the highest *criticality index* (at the time of execution), provided that enough maintenance resources are available.
3. None maintenance task can be interrupted for the execution of another maintenance task (unless maintenance resources for its completion are not available).
4. After maintenance, an equipment is considered As Good As New (AGAN)
5. Continuous plant operations are considered. Therefore, three shifts per day are employed for the maintenance crews.
6. Equipment failure rates are described by Weibull distribution functions, Table (2)
7. The occurrence of external events are defined by exponential distributions functions, Table (3)
8. Repair rates for the maintainable equipment considered as constants, so MTTR is also constant.

Assumption 1 is imposed to prevent unnecessary plant shutdowns due to maintenance activities. Assumption 2 allows for a relative rating of the significance of execution maintenance tasks. Assumption 3 prevents unnecessary swaps between maintenance tasks and potential suspension of maintenance jobs. Assumption 4 is used for convenience; a different model, the As Good As Old (AGAO) can also he used. Assumption 5 is only imposed for computational reasons; other operating patterns can also be incorporated. Assumption 6 is considered for flexibility. Assumption 8 is introduced for simplicity in the proposed maintenance algorithm.

1. *INTRODUCTION*

Traditional sensitivity analysis based on reliability models, such as logic-tree or fault-tree analysis, together with existing FMECA techniques, are powerful and well established methods for the identification of critical parts of equipment / events affecting the system functionality and safety. Such methods usually employ DFLD representation, which can be easily transformed to fault-trees. However, they share a common limitation since they do not explicitly take into account process models and process interactions; this can severely overestimate the real system efficiency and also provide misleading information regarding critical components. This work presents a methodology for criticality analysis of process systems which embodies: logic-tree, DFLD principles, explicit process and safety models, equipment reliability data and occurrence probabilities of external events, in a uniform way. The output of such a criticality analysis is used as a guide for improvements towards system design and condition-based maintenance activities.

2. *METHODOLOGY FOR CRITICALITY ANALYSIS OF PROCESS SYSTEMS*

The objective of the criticality analysis method is to identify the relative importance of equipment (un)availability (or other external events affecting the process operations) over a time horizon by taking into account process interactions, reliability models, parameter variations and operational characteristics of a process.

Criticality analysis comprises:

- ❑ Aggregation of parts of equipment into subsystems in order to reduce the size of the system state space
- ❑ Transformation of the aggregated process flow-sheet into directed logic functional digraphs (DFLD)
- ❑ Automatic translation of DFLDs into corresponding fault-trees; here, degraded operating modes for equipment are also taken into account
- ❑ Estimation of state probabilities as a function of time and system's efficiency (via a corresponding stochastic flexibility index and combined flexibility-reliability index) for all feasible states
- ❑ Estimation of a system criticality index as a function of time
- ❑ Estimation of a combined flexibility-reliability-criticality index for each part of equipment or event
- ❑ Criticality based maintenance

In the next section, we describe in detail these theoretical developments.

3. *SYSTEM AGGREGATION, DFLDs AND FAULT-TREE GENERATION*

The aggregation procedure is employed for complex large-scale systems in order to reduce the size of the corresponding state space. Its basic idea is to substitute sets of equipment whose individual availability does not explicitly affect process performance by a single component. Note that aggregation is valid for sets of equipment which have single (or multiple) input(s) and single output to the remaining system, and for certain types of multiple input output subsystems (Van Rossen, 1994); however, in general, caution and engineering judgment must be exercised in the use of aggregation techniques in the context of process / reliability analysis.

Having defined an equivalent aggregated system, the next step is to transform it to a representation, which can be easily analyzed in terms of reliability performance. Here, directed functional logic AND/OR digraph representations are employed (Lapp and Powers 1977, Andrews 1990; Ulerich and Powers1988; Chang and Hwang 1992; Garibba et al. 1977; Rasmuson and Marshall, 1978). Such a representation transparently accounts for all patterns of interconnections and functional relations between components of complete flow-sheet. A major advantage of using digraph representation is that it can automatically be transformed into fault-trees

(Iverson l992), which can subsequently be analyzed in a straightforward way. A particular useful feature of fault-trees analysis is that minimal cut sets are easily identified, based on which a lower bound on system reliability can be obtained (Jensen and Bellmore, 1969; Billinton and Allan1983; Hillier and Lieberman 1990),

$$R_{LB} = \prod_{c \in MC} \left[1 - \prod_{l \in c} r_l \right] \quad (1)$$

Note that for the cases when the reliability of individual components in a system is very high (close to unity), the approximation in eq (1) provides a very good estimation for the actual system reliability. If an exact evaluation of reliability is required, then the expression in eq (1) can be further extended to include extra terms (higher order cut sets). Note also that the degraded operating modes (i.e. when the assumption of one failure mode is not valid) can be captured in the above representation. This requires some extra mathematical manipulations, as discussed in (Thomaidis 1995).

4. *CRITICALITY RATING OF PROCESS SYSTEMS*

In this section a new quantitative metric will be introduced for measuring the expected level of critical operation of process systems taking into account interactions between process undesired critical operations (as a result of systems malfunctioning, equipment degradation or the occurrence of certain events). In the sequel a relative criticality index is defined for ranking all equipment or events according to their relative importance (sensitivity) for system operations.

4.1 *System Criticality index, CRI*

The metric of combined flexibility-reliability index (Thomaidis & Pistikopoulos, 1995) employed for measuring overall system efficiency by explicitly taking into account interactions between process models and availability of equipment over time.
The combined Flexibility Reliability index FR is given as a function of time as follows

$$FR(t) = \sum_{k \in K} SF_k P_k(t) \quad (2)$$

eq. (2) estimates the average system efficiency by summing the stochastic flexibility index, (Straub and Grosmann 1993), of all operable system states weighted by the associated state probability. At the limiting case where $SF_k = 1 : k \in K_{OP}$, the combined flexibility reliability index equals to system reliability. In other words the upper bound for the combined flexibility-reliability index is the system reliability.
Similarly a system criticality index *CRI(t)* can be computed based on the concept of the combined flexibility - reliability index, as follows.
The enforcement of safety constraints, such as temperature, pressure or concentration limits, which can lead to critical operating conditions of the process or even a system upset can be explicitly included in the process model (see also the case study in section 6). Then, the initial *FOR* is divided in two parts: the reduced *FOR* and the *COR*. The second can be depicted as a part of the initial feasible region (due to the enforcement of safety constraints). This concept is explicitly shown in figures (1.a, 1.b and 6).

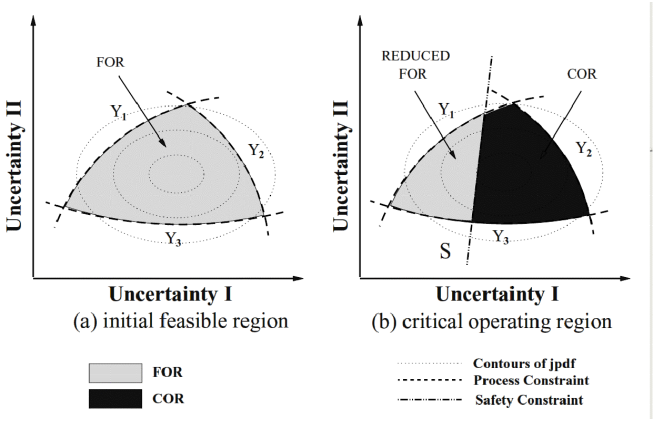

Figure 1: Feasible and Critical Regions vs. process and safety constraints

The criticality of each system state CR_k can be defined as the expected probability of the system in state *k* to operate in the *COR* associated with this state. Then CR_k can be computed by integrating the joint probability density function of the uncertain parameters within the *COR* area, similarly to the estimation of the stochastic flexibility index, (Straub and Grosmann 1993).
The system criticality Index CRI(t) then can be estimated as a function of time as follows

$$CRI(t) = \sum_{k \in K} CR_k P_k(t) \quad (3)$$

4.2 *Combined Flexibility-Reliability Criticality Index, Frc*

Based on the information provided by the analysis presented in the previous section, a ***combined flexibility-reliability criticality index*, *FRC***, is defined in this section, which provides a measure of the relative importance (sensitivity) of a system, subsystem, equipment or event from an overall operability perspective. The criticality index can be computed based on the *combined flexibility-reliability index FR(t)*, as follows.
We are interested in the sensitivity of $FR(t)$ to the probability of an event ρ_{l^*}. Then we define the combined flexibility-reliability-criticality index as follows

$$FRC_{l^*}(t) = \frac{\partial FR(t)}{\partial r_{l^*}} = \sum_{k \in K} \left\{ SF_k \frac{\partial P_k(t)}{\partial r_{l^*}} \right\} \quad (4)$$

since the estimation of SF_k is not influenced by ρ_{l^*}, since can also be part of a subsystem *m*, this implies

$$\frac{\partial P_k(t)}{\partial r_{l^*}} = \frac{\partial P_k(t)}{\partial \rho_m}\frac{\partial \rho_m}{\partial r_{l^*}} \tag{5}$$

In order to evaluate $FRC_{l^*}(t)$, we need to estimate the terms $\frac{\partial P_k(t)}{\partial \rho_m}$ and $\frac{\partial \rho_m}{\partial r_{l^*}}$. This will be based on the evaluation of system state probabilities (reliability) by using minimal cut sets as follows,

$$\frac{\partial P_k}{\partial \rho_m} = \begin{cases} \prod_{j\in \bar{J}_k \setminus m}\rho_j \prod_{j\in \bar{\bar{J}}_k}(1-\rho_j), \text{if } m \in \bar{J}_k, k \in K \\ \prod_{j\in \bar{\bar{J}}_k}\rho_j \prod_{j\in \bar{J}_k \setminus m_k}(1-\rho_j), \text{if } m \in J_k, k \in K \end{cases} \tag{6}$$

For the estimation of the term $\frac{\partial \rho_m}{\partial r_{l^*}}$ two cases exist. The first is when $l^* = m$, in which case

$$\frac{\partial \rho_m}{\partial r_{l^*}} = \frac{\partial \rho_m}{\partial \rho_m} = 1 \tag{7}$$

if $\rho^* \in m$ then $\frac{\partial \rho_m}{\partial \rho_{l^*}} = \partial \frac{\prod_{c\in MC}\left[1-\prod_{l\in c} r_l\right]}{\partial r_{l^*}}$ (8) where eq (1) was employed for the approximation of ρ_m. Eq (8) then can be simplified as follows:

$$\frac{\partial \rho_m}{\partial \rho_{l^*}} = -\prod_{c\in\{MC_m \setminus MC_m^*\}}\left[1-\prod_{l\in c} r_l\right]\frac{\partial \prod_{c\in MC_m^*}\left[1-\prod_{l\in c} r_l\right]}{\partial r_{l^*}} \tag{9}$$

where

$$\frac{\partial \prod_{c\in MC_m^*}\left[1-\prod_{l\in c} r_l\right]}{\partial r_{l^*}} = -\sum_{c^*\in MC_m^*}\left\{-\prod_{l\in(c^*\setminus l^*)} r_l \prod_{c\in\{MC_m^*\setminus c^*\}}\left[1-\prod_{l\in c} r_l\right]\right\}$$

where c^* is a minimal cut from MC_m^*. From the above and eq (9) follows that:

$$\frac{\partial \rho_m}{\partial \rho_{l^*}} = \prod_{c\in\{MC_m \setminus MC_m^*\}}\left[1-\prod_{l\in c} r_l\right]$$

$$\sum_{c\in MC_m^*}\left\{\prod_{l\in(c^*\setminus l^*)} r_l \prod_{c\in\{MC_m^*\setminus c^*\}}\left[1-\prod_{l\in c} r_l\right]\right\} \tag{10}$$

Based on the above analytical expressions the criticality index $FRC_{l^*}(t)$ can be estimated following the next steps:

STEP 1**:** At a given time t,

- Deduce minimal cut sets of aggregated system and associated subsystems
- Estimate SF_k for all operable states $k \in K_{OP}$
- Estimate reliability of equipment and the sets of operable / degraded / failed components for all states $k, k \in K$
- use eq (1) to estimate probabilities of all subsystems m

STEP 2:

For each event l^* and for all states $k \in K_{OP}$, use eq (6) and eq (10) to estimate $\frac{\partial P_k(t)}{\partial r_{l^*}}$

Calculate the combined flexibility-reliability-criticality index $FRC_{l^*}(t)$ using eq (4)

Note that based on the above algorithm, equipment / subsystems / events can be ranked according to their corresponding criticality index. For comparison purposes, a scaled $rFRC_{l^*}(t)$ can be defined,

$$rFRC_{l^*}(t) = \frac{FRC_{l^*}(t)}{\max_l\{FRC_{l^*}(t)\}} : \quad 0 \le rFRC_{l^*}(t) \le 1 \tag{11}$$

by scaling all indices with the determined higher critical value. The results from such a relative ranking can be used as guidelines for preventive maintenance planning as discussed in the next section.

5. *IMPLICATIONS FOR CONDITION-BASED AND PREVENTIVE MAINTENANCE*

In this section, we present an algorithm for the planning and execution of preventive and condition-based maintenance. The algorithm relies on the criticality analysis step of section 4; additionally, it requires quantitative information regarding

maintenance resources (number of service crews, man hours, personnel, job durations) and maintenance tasks (equipment maintenance specifications, list of scheduled preventive maintenance activities).

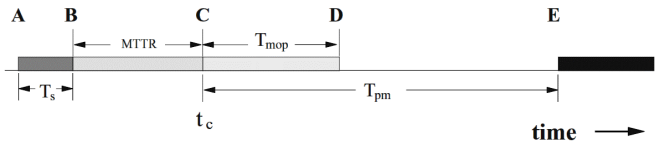

Figure 2: Equipment time ages

The operating cycle of each equipment is modeled using the representation depicted in figure (2). Note that the operating window reserved for maintenance activities and a normal operational stage (A-E). The first time-stage is further divided into two periods, period A-B during which a maintenance task may be suspended (for example due to unavailability of a qualified service crew), and period B-C with a corresponding duration equal to MTTR. Normal operation is also divided into two periods, period C-D a minimum operational time during which no preventive maintenance activities are allowed, and period D-E, during which no preventive maintenance activities are scheduled but condition-based maintenance may be performed (if required). The representation also allows for extra operational time (E+), if the operation of the equipment is pushed beyond the nominal operational window.

The basic steps of the proposed algorithm have as follows:

STEP 1 - Set operational targets for system performance, FR^T combined flexibility-reliability target, CRI^T target for maximum acceptable level for critical operation (optional)

STEP 2

i - Set t = 0; the operation of the process begins

ii- Calculate FR(t) (or primal CRI(t)) as a function of time

iii- If $FR(t) < FR^T$ or $t > T_{pm}$ go to maintenance block, STEP 3

iv- If $FR(t) < FR^T$ and all repairable equipment have been maintained, STOP; the plant requires shut-down and maintenance of equipment.

STEP 3 - Maintenance block

i- Use criticality analysis algorithm (section 4) to obtain criticality indices of equipment $FRC_l(t)$; rank equipment according to their criticality index values, rFRC; set t = t*, where t* represents the time when maintenance task performed.

ii- If $T_{mop} < t^* < T_{pm}$, execute maintenance tasks associated with the most critical piece of equipment as follows:

iii- If maintenance resources are available proceed with the list of critical pieces of equipment in the order of ranking; if not, proceed with the next most critical component in the list; push the unaccomplished maintenance task further in the time schedule.

iv- During the execution of maintenance task, if maintenance resources are not available (for example the personnel of a service crew in the next shift is not qualified to perform this maintenance task) then mark the current job as "*suspended*" and push it further in time – note that "*suspended*" jobs have priorities according to their criticality index values.

v- After the completion of a maintenance task, check for 'suspended' maintenance tasks and complete them depending on resources availability.

vi- GO back to STEP 2 (ii)

The proposed algorithm systematically identifies opportunities for maintenance execution based on a formal assessment of the deterioration of the system's performance over time and the relative effect of restoring the performance of critical equipment to process efficiency. Although cost considerations have not yet been taken into account, one can easily envisage the extension of the algorithm to include cost by employing expected profit criteria rather than an operability measure. Section 6 further discusses applications of the proposed algorithm.

6. *CASE STUDY: COMPRESSOR SYSTEM*

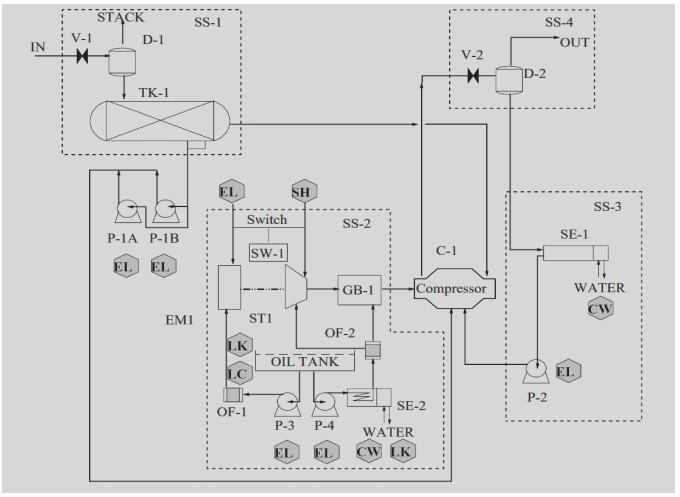

Figure 3: Process Configuration

Consider the compressor system as a part of a complex process configuration, shown in figure (3). It comprises a tank (TK-1) for storage of a liquid solution, which feeds a flash gas polytropic compressor (C-1); the compressor is powered by a steam turbine (ST-1) backed up by an electric motor (EM-1) which takes over automatically when the steam is low (SH) or the turbine fails. A number of secondary equipment for controlling the process are also shown in figure (3): heat exchanger (SE-1) to keep the outlet temperature of the compressor below a specified safety level, heat exchanger (SE-2) for controlling the lubricant oil temperature in the turbine and the gear box, oil filters (OF-1) and (OF-2) and control valves (V-1) and (V-2) associated with a knock out drums (D-1) and (D-2), respectively. The process model describing the operation of the flash gas polytropic compressor is shown in table (1) along with process and safety constraints, process data and data describing stochastic

variations in the model. A number of external events affecting the operability of the system are also considered.

Reliability data for the equipment are given in table (2), where a time horizon of 1000 hrs is considered for setting the operational targets. For proceeding further with any operability study, the creation of the directed functional logic diagrams (DFLD) and the state space representation are required. Note that the original process configuration involves 16 parts of equipment and 12 external events. Therefore, its corresponding state space for operability analysis would involve approximately 256 x $l0^6$ discrete operating states (considering only one failure mode for the equipment)! However, the state space can be drastically reduced applying the aggregation techniques described by (Thomaidis 1995).

Process model for adiabatic compressor					
$W_s^c = \frac{k \cdot R \cdot T_{in}}{(k-1) \cdot 3600} F_{in} \left[\left(\frac{P_{out}}{P_{in}} \right)^{\frac{n-1}{n}} - 1 \right]$			$T_{out} \le T_{in} \left(\frac{P_{out}}{P_{in}} \right)^{\frac{n-1}{n}}$		
$W_s^c \le W_{st} \cdot n_m, \quad W_s^c \le W_{el} \cdot n_m$			$T_{\min} \le T_{out} \le T_{\max}$		
Parameter	Value	Description	Parameter	Value	Description
T_{in}	300 K	Inlet compressor temperature	κ	1.29 (constant)	Cp / Cv
n	1.398	Pressure Ratio (constant)	n_m	0.85 (constant)	Mechanical Efficiency
Process constraints					
Maximum available horsepower			Allowed outlet temperatures		
Steam turbine 60 Kwatt			SS-3 $T_{\max} = 440$ K		
Electric Motor 36 Kwatt			SS-3 $T_{\min} = 410$ K		
Uncertain parameters			M	σ	range (μ +/- 4σ)
Compression ratio $\left(\frac{P_{out}}{P_{in}} \right)$			3	0.25	1 to 5
Flow-in rate F_{in}			30	2.50	25 to 35

Table 1: Process model and data for the compressor

Flexibility analysis is performed then on the structurally feasible operating states, whereas, critical regions of operation and critical for the process safety state should be identified.

Name	Type	MTTR (hr)	Weibull parameters	
			a (h^{-1})	b
Compr. C-1	Compressor	72.0	1000000	1.0
SS-4 V-2	Valve	16.0	1250000	1.0
SS-1 V-1	Valve	16.0	1250000	1.0
Pump P-IA	Centrifugal Pump	32.0	100000	1.0
Pump P-IB	Centrifugal Pump	32.0	100000	1.0
Gearbox	Gear Assembly	24.0	333333	1.0
EISwitch	Electric Switch	16.0	1428571	1.0
EM-1	AC-Motor	16.0	200000	1.0
OilPump3	Oil Lub Pump	30.0	166667	1.0
OilPump4	Oil Lub Pump	30.0	166667	1.0
Level Ctr.	Level Controller	24.0	2000000	1.0
Oil Heat Ex.	Heat Exchanger	72.0	66667	1.0
ST-1	Steam Turbine	48.0	500000	1.0
Oil Filter1A	Oil Filter	4.0	1000000	1.0
Oil Filter1B	Oil Filter	4.0	1000000	1.0
Oil Filter2A	Oil Filter	4.0	1000000	1.0
Oil Filter2B	Oil Filter	4.0	1000000	1.0
CooIHeatEx	Heat Exchanger	72.0	66667	1.0
Pump P-2	Centrifugal Pump	32.0	100000	1.0

Table 2: Reliability and maintenance data for the equipment

In order to cope with a large state space required for the representation of the problem the system is aggregated into smaller subsystems as follows (see figures (3)): equipment and upstream events associated with the gear box (GB-1) can be represented by subsystem (SS-2), because the occurrence of any of those events affects the (un)availability and the operational behavior of the power system.

Type of event	Exponential Distribution: λ(10^{-6} h^{-1})
Electrical Supply	1
Leakage	1
Steam Supply	3
Cooling water supply	5

Table 3: Probability functions of external events

The heat exchanger (SE-1) with its corresponding pump (P-2) and external electrical event (EL) can be embedded in subsystem (SS-3). Subsystems (SS-1 and SS-4) have been simplified, for demonstration purposes. So the availability of those subsystems is actually described by the availability of a single component valve (V-1) and (V-2) respectively. The resulting aggregated system consists of four subsystems (SS-1, SS-2, SS-3, SS-4), two pumps (P1-A, P1-B) and the associated electrical events, the compressor (C-1), the logical AND gates and the utility (dummy) node (LU-1). The aggregated system and the embedded subsystems are then transformed into logic functional diagrams, as shown in figures (4), and (5).

State No	Stochastic Flexibility Index %	Critical Operation %	Subsystem – Equipment No 123456789111 012	State No	Stochastic Flexibility Index %	Critical Operation %	Subsystem – Equipment No 123456789111 012
1	100	-	111111111111	34	50	45	101111111011
2	70	-	D11111111111	40	70	-	D11111111101
3	50	45	101111111111	41	50	48	101111111101
7	100	-	111111101111	47	100	24	111111111001
5	100	-	111111110111	74	45	24	D01111110111
9	100	-	111111111011	54	70	-	D11111100111
10	100	-	111111111101	55	50	45	101111100111
12	45	24	D01111111111	90	45	24	D01111111011
22	70	-	D11111101111	112	45	24	D01111111101
23	50	24	101111101111	133	70	-	D11111111001
27	70	-	D11111110111	134	50	48	101111111001
28	50	48	101111110111	180	45	24	D01111100111
32	100	-	111111100111	273	45	24	D01111111001
33	70	-	D11111111011	Total No of Aggregated System States 768			
Description		Equipment No		Operating Modes			
Subsystem-1,3,4		7,2,6		1: Fully operable, 0: Failed			
Subsystem-2		1		1: Fully operable, D: Degraded, 0: Failed			
Single Equipment		5, 8, 10		1: Fully operable, 0: Failed			
Events		9, 11		1:Yes, 0: No			
AND - gates		4, 12		Nodes of the DFLD			
Utility node		3		Utility node of the DFLD			

Table 4: Operating states and the corresponding flexibility indices – and critical operation for the aggregated system

Note that DFLD diagraphs account for the degraded operating modes of a system (due to partial equipment availability) as well.

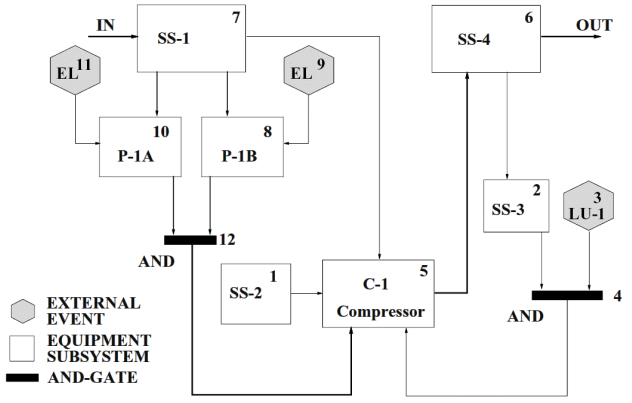

Figure 4: Functional Logic AND/OR digraphs for the aggregated system

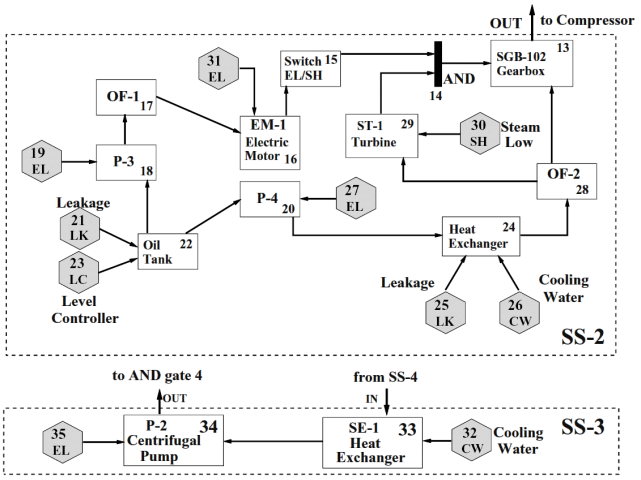

Figure 5: Functional Logic AND/OR digraphs for subsystems SS2 & SS-3

For example, the power supply system is operable when either the steam turbine is available (fully powered) or the electric motor takes over (partially powered) see figure (6) and table (4). Analysis from hereafter proceeds at both, the aggregated and the basic subsystems level - this decoupling allows approximations for the consideration of a very large number of equipment, events and subsystems.

6.1 *Flexibility-Reliability-Criticality Analysis*

The aggregated system results in a state space involving 768 discrete operating states out of which only 27 are operable, as determined by a DFLD structure and the flexibility analysis step, see table (4). Flexibility analysis results are shown in table (4) and figure (6), which depicts the corresponding

regions of feasible operation in the state space of the two uncertain parameters (pressure ratio and flowrate). One of the process constraints, i.e. the minimum outlet temperature of the compressor, is enforced due to safety considerations.
Operating states resulting in critical operation (from safety point of view) can be identified as part of the methodology described in section 4 and are depicted in figure (6), cases (c) and (d) (see also table (4)).

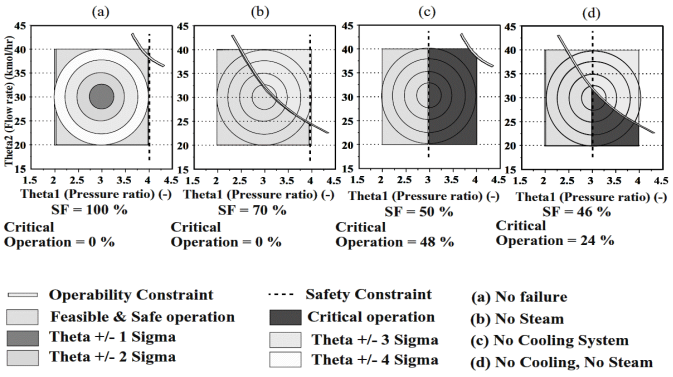

Figure 6: Feasible Region of operation and Regions of Critical Operation

Figure (6.a) describes the fully operable state (1) (all equipment up, no external event); figure (6.b) corresponds to states (2, 22, 27, 33, 40, 84, 133) in which the compressor is not available as a result of equipment failure (i.e. failure of steam turbine which forces electric motor to backup the steam turbine, degraded operation D) or occurrence of an external event (i.e. low pressure on the high pressure steam line, event (SH)); figure (6.c) shows the feasible region of operation when the system operates in a degraded operating state in which the cooling system (SS-2) is not available. Note here, that although the system is capable of operating within the entire feasible region the unavailability of the cooling system imposed an extra safety constraint (dashed line) forces the system to operate within the dashed reduced feasible area. However, if failure of the cooling system occurs (and no control action is taken) while the compressor is operating in the dark (critical) area then the process operation becomes critical (outlet temperature greater than 410 K, see table (1). In this case the probability for critical operation is evaluated within the dark area. Note that operation in these states is undesired and should be avoided. Similarly, figure (6.d) describes the situation when both steam turbine and cooling system are unavailable, states (12, 23, 47, 74,90,112, 180, 273). One can observe here that despite the higher degree of system degradation the probability for critical operation is reduced, reflecting the reduction of the feasible region of operation.
The fault-tree of the aggregated system and the corresponding subsystems are shown in figures (7-10). The minimal cut sets of the Aggregated system and the subsystems are shown in table (5).

	1st Order cut sets	2nd Order cut sets
Aggregated System	{6} {7} {1} {5}	
Subsystem SS-2	{13} {24} {27} {21} {23} {20} {25} {26} {28}	{29,31} {29,17} {29,19} {29,18} {29,16} {29,15} {30,15} {30,31} {30,17} {30,19} {30,18} {30,16}
SS-3	{32} {33} {34} {35}	

Table 5: Minimal Cut Sets of the aggregated system and the subsystems.

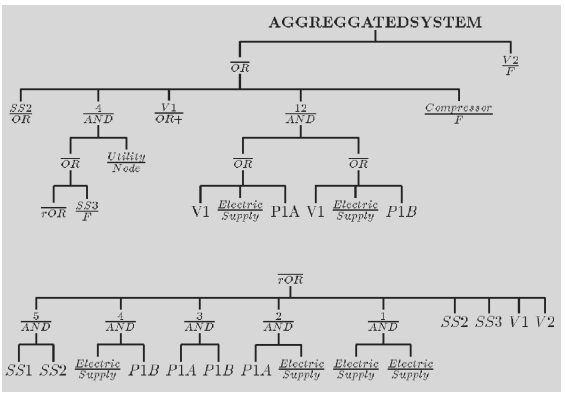

Figure 7: Fault-Tree for the aggregated system

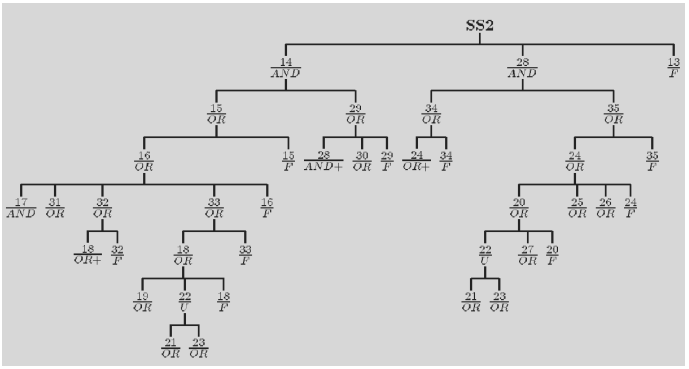

Figure 8: Fault-Tree of Subsytem 2 (1st part)

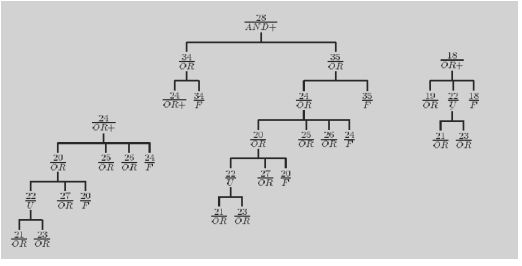

Figure 9: Fault-Tree of Subsytem 2 (2nd part)

Aggregated System Node No	Node ID	Type of node {Operating modes}			
Subsystems					
1	SS-2 PwrGn	Sub System {2}	Power Generation subsystem		
2	SS-3 CIUnt	Sub System {1}			
Single Equipment					
			Maintenance Scheduling		
			n_p	T_{pm} hrs	T_{mop} hrs
5	StmCmpress	Steam Compressor {1}	5	8064	8063
6	SS-4 / V-2	Throttle Valve {1}	1	8064	8063
7	SS-l / V-l	Throttle Valve {1}	1	8064	8063
8	Pump P-IA	Centrifugal Pump {1}	3	2000	672
10	Pump P-IB	Centrifugal Pump {1}	3	2050	722
External Events					
9	ElctrcEvnt	Electrical Supply {1}			
11	ElctrcEvnt	Electrical Supply {1}			
Logic gates : 3 - Utility node, 4 & 12 – AND gates					

Table 6: Maintenance data of equipment, description of events (Aggregated system)

Node No	Node ID	Type of node / {Operating modes}	Maintenance Scheduling		
			n_p	T_{pm} hrs	T_{mop} hrs
Power generation system – Equipment					
13	Gearbox	Gear Assembly {1}	3	8064	8063
15	EI Switch	Electric Switch {1}	1	2688	1344
16	EM-1	AC-Motor {1}	2	8064	6720
18	Oil Pump3	Oil Lubricating Pump {1}	2	4032	3360
20	Oil Pump4	Oil Lubricating Pump {1}	1	8064	8063
23	Level CTR	Level Controller {1}	2	8064	8063
24	Oil HEX	Oil Heat Exchanger {1}	2	8064	8063
29	ST-1	Steam Turbine {1}	3	4032	1344
17 28	Oil Filter1 Oil Filter2	Oil Filters {1}	1	2100	1000
Power generation system - External events					
21	OilTankLeak	Leakage			
22	OilTank	Fully reliable part			
25	OilHExLeak	Leakage			
26	CwaterHex	Cooling water supply			
27	EIForEIMot	Electrical supply			
30	StmForTurb	Steam supply			
31	EIEvt EM-l	Electrical supply			
19	EIEvtPump3	Electrical supply			
AND gates : 14, 17, 28					
Cooling system – Equipment					
33	CooI HEX	Heat Exchanger	5	4032	2688
34	Pump P-2	Centrifugal Pump	3	4032	3360
Cooling system - External Events					
32	CWaterHEX	Cooling water supply			
35	EIEvt P-2	Electrical supply			

Table 7: Maintenance data of equipment, description of events

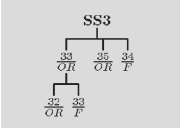

Figure 10: Fault-Tree of Subsytem 3

Note that a scaled rFRC index can be defined ($0 < rFRC < 1$) by criticality analysis. The results of the criticality analysis are summarized as follows.

From the estimated criticality indices, FRC and rFRC, it is identified that subsystem 2 (SS-2, node 1) is the most critical component at the aggregated level with the oil heat exchanger (SE-2, node 24) as the part of equipment that affects most the overall process system's performance. If a preventive maintenance planning is forced to improve the availability of the oil heat exchanger (SE-2) (the most critical part of the equipment) to a value of 0.9851, or if a more reliable equipment was used, the results of this case study indicate the incremental benefits that the process achieves (i.e. its operability is improved from FR(H) = 0.7480 to FR(H) = 0.855 over the specified time horizon) whereas the new ranking order of critical parts, note that in this case the compressor becomes the most critical equipment. Note also that the criticality of external events can also be assessed within this framework; process interactions, equipment availability and probability of events are all taken into account.

6.2 *MAINTENANCE PLANNING*

The proposed methodology, as discussed in detail in section 5, for the identification of critical parts of equipment, critical events and *COR*, can be further utilized to reveal the most important maintenance tasks (from operability and a safety point of view). In this section three different maintenance policies have been examined. The first policy is the most relaxed, since very low operability bounds have been chosen, whereas the bound for critical operation is relatively high (CRI^T=0.05). Operability targets for the second (B) and third (C) policy have been set as follows: (FR^T_B= 0.90, FR^T_C= 0.99) and maximum allowed probability for critical operation (CRI^T=0.05) for both. The assumption of three service crews (performing up to 5 maintenance task each) operating over three shifts (8 hrs per shift) has been made. Reliability and maintenance data for the equipment and the parameters for the probability functions of the external events are shown in tables (2-3) and (6).

The results obtained from the application of the proposed algorithm in section 5, are pictorially shown for the maintenance policy (C) in figures (11), (12), for which the following remarks can be made:

The system forces to its operability limits. Since the operability level in general is lower than the target throughout the time horizon; therefore maintenance tasks are executed whenever it is possible, figure (11). As a result of this policy is the most dense maintenance planning with (124) maintenance tasks over the time horizon see figure (12) and table (7).

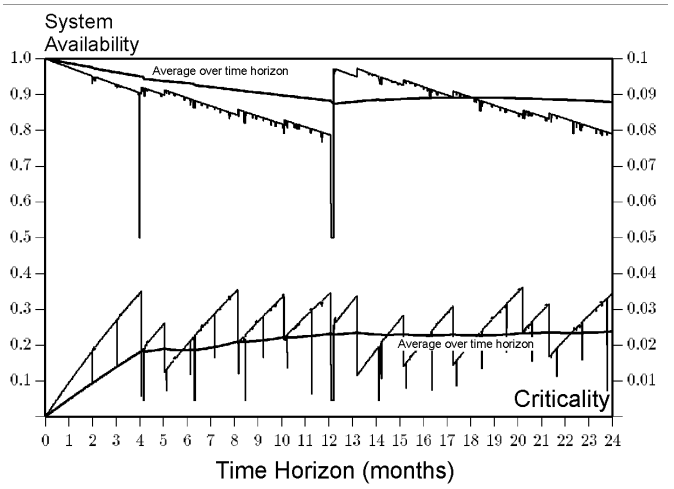

Figure 11: System Flexibility-Availability & Criticality responses over a 24 months time horizon

Details about the exact planning (selectively for months: 3, 13, 15, 24) of maintenance tasks are shown in figure (12), the system's combined Flexibility-Reliability FR(t) and the combined Reliability-Criticality index FRC(t) as a function of time are shown in figure (11).

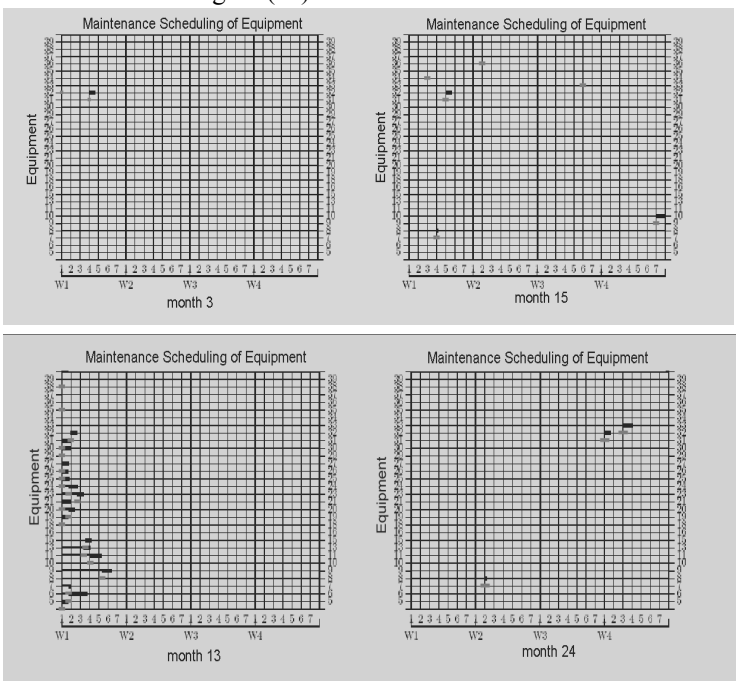

Figure 11: Maintenance scheduling of equipment for months (3, 13, 15, 24)

The above case study highlights the interactions between process model, equipment reliability and execution of condition-based maintenance, as well as the effects of external events on overall system performance.

REFERENCES

1. J. Andrews, ‘Applications on the digraph method of fault tree construction to a complex control configuration’, Reliability Eng. And Systems Safety, vol. 28, 1990, pp. 357-384.

2. R. Billinton and R.N. Allan, ‘Reliability Evaluation of Engineering Systems; Concept and Techniques’ Prenum Press, New York and London, 1983.

3. C. Chang and H. Hwang, ‘New Development of the Digraph-Based Techniques for Fault-Tree Synthesis’, Ind. Eng. Chem. Res. 31(6), 1992, pp. 1490-1502.

4. Garriba et.al., ‘Efficient construction of minimal cut sets from Fault-Trees’, IEEE Trans on Reliability R-26(2), 1977, pp.88-93.

5. F. S., Hillier and G.J. Lieberman, ‘Introduction to Operations Research’, Mc-Graw Hill, Ind. Engng. Sers., 1990.

6. D. L. Iverson, ‘Automatic Translation of Digraph to Fault-Tree Models’, Proceeding Annual Reliability and Maintainability Symposium, 1992, pp.354-362.

7. P. A. Jensen and M. Bellmore, ‘An Algorithm to determine the reliability of a complex system’, IEEE Trans. on Reliability R- 18(4), 1969, pp.169-174.

8. S. A. Lapps and G.J. Powers, ‘Computer-aided Synthesis of Fault-trees’, IEEE Trans. on Reliability, vol. 26, 1977, pp.2-13.

9. D. M. Rasmuson and N. H. Marshal ‘FATRAM - A core efficient cut-set algorithm’, IEEE Trans on Reliability R-27(4), 1978, pp.250-253.

10. T. V. Thomaidis and E. N. Pistikopoulos, ‘Integration of Flexibility, Reliability and Maintenance in Process Synthesis and Design’, Comp. Chem. Engng., vol. 18, 1994a , S259-263.

11. T. V. Thomaidis and E.N. Pistikopoulos, ’Flexibility, Reliability and Maintenance in Process Design’, Foundation of Computer Aided Process Design, FOCAPD ’94, 1994 b, Snowmass Colorado.

12. T. V. Thomaidis and E.N. Pistikopoulos, ‘Optimal Design of Flexible and Reliable Process Systems’, IEEE Trans. on Reliability, 44(2), 1995, pp. 243-250.

13. T. V. Thomaidis, ‘Incorporation of Flexibility, Reliability, Availability, Maintenance & Safety in Process Operations and Design’, Ph.D. Thesis, the University of London, 1995.

14. N. H. Ulerich and G. J. Powers, ‘On-Line Hazard Aversion and Fault-Tree Diagnosis in Chemical Process: The Digraph + Fault-Tree Method’, IEEE Trans. on Reliability 37(2), 1988, pp. 171-177.

15. J. C. P. Van Rossen, ‘Criticality Rating and Safety Analysis in F.R.A.M.S.’, Technical Report. Imperial College of science, Technology and Medicine, Centre for Process Systems Engineering, London, 1994.

16. D. A. Straub and I. E. Grossmann, ‘Design optimization of stochastic flexibility’, Comp. Chem. Engng. 17(4), 1993, pp. 339-354.

BIOGRAPHIES

Thomas V. Thomaidis, Ph.D.
Future Technology Systems - FTS SA
Technology Park of Thessaly,
A’ Industrial Area, 38500 Volos, Greece

email: thomastv@fts.gr

1996 -	Consultant Engineer and Researcher in Future Technology Systems sa
1991-1995	Doctoral Degree (Ph.D.) in Process Systems Engineering, IC London
1993	KSLA/Shell Research B.V. Amsterdam, NL
1991-1992	MSc Degree & Diploma of Imperial College (DIC) in Chemical Engineering, IC London
1990-1991	Researcher in Chemical Process Engineering Research Institute CPERI Thessaloniki, GR. Researcher
1986-1990	Diploma in Chemical Engineering Aristotle University of Thessaloniki, GR
1986, 1989	KSLA/Shell Research B.V. Amsterdam, NL
1986, 1989	North Aegean Petroleum Company, Kavala, GR - Offshore Eng.
1982-1986	BSc. in Petroleum Engineering Polytechnic School of Kavala, GR

Professor Stratos Pistikopoulos, Director
Centre for Process Systems Engineering, Imperial College London
Roderic Hill Building, South Kensington campus,
London SW7 2AZ, UK

email: e.pistikopoulos@imperial.ac.uk,

1999-	Professor of Chemical Engineering, Imperial College London
1996 – 1999	Reader in Process Systems Engineering, Department of Chemical Engineering, Imperial College London
1991 – 1996	Lecturer, Department of Chemical Engineering, Imperial College London
1990 – 1991	Research Associate, Chemical Process Engineering Research Institute, Thessaloniki, Greece
1988 – 1990	Research Chemical Engineer, Koninklijke Shell Laboratorium, Amsterdam
1984 – 1988	PhD in Chemical Engineering, Carnegie Mellon University, USA.
1979 – 1984	Diploma in Chemical Engineering, Aristotle University of Thessaloniki, Greece.