This document is downloaded from the
Digital Open Access Repository of VTT

Title	Risk importance measures in the dynamic flowgraph methodology
Author(s)	Tyrväinen, Tero
Citation	Reliability Engineering and System Safety. Elsevier . Vol. 118 (2013), pages 35 - 50
Date	2013
URL	http://dx.doi.org/10.1016/j.ress.2013.04.013
Rights	Post-print version of the article. This article may be downloaded for personal use only.

VTT
http://www.vtt.fi
P.O. box 1000
FI-02044 VTT
Finland

By using VTT Digital Open Access Repository you are bound by the following Terms & Conditions.

I have read and I understand the following statement:

This document is protected by copyright and other intellectual property rights, and duplication or sale of all or part of any of this document is not permitted, except duplication for research use or educational purposes in electronic or print form. You must obtain permission for any other use. Electronic or print copies may not be offered for sale.

Risk importance measures in the dynamic flowgraph methodology

T. Tyrväinen

VTT Technical Research Centre of Finland, Systems Research, P.O. Box 1000, FI-02044 Espoo, Finland

Abstract

This paper presents new risk importance measures applicable to a dynamic reliability analysis approach with multi-state components. Dynamic reliability analysis methods are needed because traditional methods, such as fault tree analysis, can describe system's dynamical behaviour only in limited manner. Dynamic flowgraph methodology (DFM) is an approach used for analysing systems with time dependencies and feedback loops. The aim of DFM is to identify root causes of a top event, usually representing the system's failure. Components of DFM models are analysed at discrete time points and they can have multiple states. Traditional risk importance measures developed for static and binary logic are not applicable to DFM as such. Some importance measures have previously been developed for DFM but their ability to describe how components contribute to the top event is fairly limited. The paper formulates dynamic risk importance measures that measure importances of states of components and take the time-aspect of DFM into account in a logical way that supports the interpretation of results. Dynamic risk importance measures are developed as generalisations of the Fussell-Vesely importance and the risk increase factor.

Keywords:
Dynamic flowgraph methodology, risk importance measure, multi-state

1. Introduction

Risk importance measures [1, 2, 3, 4] are important in the reliability analysis of complex systems, such as safety systems in nuclear power plants. They can be used to analyse which components or basic events are most important with regard to the system's reliability, the probability that the system does not fail. The importance of a component depends not only on the reliability of the component but also on the impact of its behaviour on the consequences of interest. Risk importance measures reveal which are the beneficial ways to improve the system's reliability.

Dynamic reliability analysis methods [5] have been studied extensively since 90's because traditional methods, such as fault tree analysis, can describe system's dynamical behaviour only in limited manner. Dynamic methods can represent system's evolution in time more accurately than traditional methods and they can be used to identify time-dependent failure condition combinations that cause the system's failure. There are well-established techniques for the computation of risk importance measures in fault tree and event tree analyses [6, 7]. However, in dynamic reliability analysis, fewer importance measures have been developed [8]. The limitations are even more evident with regard to dynamic reliability analysis approaches that include components with more than two states.

This paper presents two new risk importance measures for a dynamic reliability analysis approach called dynamic flowgraph methodology (DFM)

[9, 10, 11, 12]. A brief conference paper on these importance measures was already published in 2012 [13] but this paper presents the work in a comprehensive and more general form.

Risk importance measures are typically calculated from minimal cut sets which are usually the most essential result of reliability analysis. A minimal cut set is a minimal combination of basic events that is sufficient to cause the top event. If one of the basic events is taken away from a minimal cut set, the remaining combination of basic events is not sufficient to cause the top event anymore.

Two risk importance measures are generalised into the dynamic and multi-state case of DFM: the Fussell-Vesely measure and the risk increase factor (also known as the risk achievement worth). They are the most often used risk importance measures in the reliability analysis of nuclear power plants [1]. These two measures form a combination that can describe fully the influence of the component's unavailability. Fussell-Vesely measures how large portion of the top event probability is caused by the minimal cut sets that contain a given basic event and the risk increase factor measures how much the probability of the top event increases if a given basic event occurs. Hence, Fussell-Vesely measures the direct effect of the component's unavailability, whereas the risk increase factor depends more on the component's position in the system's structure and the reliability of other components.

If P, V, L and M are basic events and PL, VL, PM and VM are minimal cut sets, Fussell-Vesely of basic event V can be calculated (using so-called "MCS upper bound" to calculate the top event probability) as presented in (1) and the risk increase factor as presented in (2).

$$I^{FV}(V) = \frac{Q^V_{TOP}}{Q_{TOP}} \tag{1}$$
$$= \frac{1-(1-Q(VL))\cdot(1-Q(VM))}{1-(1-Q(PL))\cdot(1-Q(VL))\cdot(1-Q(PM))\cdot(1-Q(VM))},$$

where the notation $Q(CS)$ means the probability of minimal cut set CS and Q_{TOP} is the top event probability.

$$I^{I}(V) = \frac{Q_{TOP}(V=1)}{Q_{TOP}} \tag{2}$$
$$= \frac{1-(1-Q(L))\cdot(1-Q(M))}{1-(1-Q(PL))\cdot(1-Q(VL))\cdot(1-Q(PM))\cdot(1-Q(VM))}.$$

Components can usually fail in more than one way. For example, a valve could be failed open or close. The state in which a component is failed is called a failure state in this paper. The paper concentrates on calculating the new risk importance measures for failure states of components in DFM.

The paper is structured as follows. Section 2 briefly presents dynamic flowgraph methodology. Section 3 reviews previous research and specifies the objectives of the paper. New dynamic risk importance measures are formulated in sections 4 and 5 and a case study is presented in Section 6. The significance of the dynamic risk importance measures and possibilities for further research are discussed in Section 7, and Section 8 concludes the study.

2. Dynamic flowgraph methodology

Dynamic flowgraph methodology [9, 10, 11, 12] is an approach for analysing systems with time dependencies and feedback loops. It is typically used to model and analyse digitally controlled systems which include both hardware and software components. For example, modern nuclear power plants include digitally controlled safety systems. The multi-state logic of DFM is an advantage in modelling of that kind of systems because their components do generally not behave in binary manners. Another advantage of DFM is that only one model is needed to represent the complete behaviour of a system and different states of the system can be analysed using the same model [10].

A DFM model is a directed graph which consists of nodes that represent the system's components and variables and edges that represent the dependencies between nodes. A node can have a finite number of states and the state of a node is determined either by a probability model or by states of its input nodes at specified time steps. Input dependencies of a node are represented in a decision table which is an extension of a truth table.

The aim of DFM is to identify root causes for a top event, which is defined as a condition that particular nodes are in particular states at particular time steps. The result is a set of prime implicants which are generalisations of minimal cut sets. A prime implicant is a minimal combination of basic events and other conditions that is sufficient to cause the top event. In DFM analysis, a basic event or a condition is represented as a literal which is a node in a state at a time step and a prime implicant is a set literals. Hence, prime implicants of DFM can be understood as timed minimal cut sets.

An example on DFM analysis results is provided next. To keep the focus on concepts that are most relevant with regard to this paper, the actual DFM model is not presented at this point. Expression $F(-2) = 0$ is a literal representing node F in state 0 at time step -2, and $\{N(-3) = -1, T(-3) = 1, R(-3) = 1, F(-2) = 0, F(-1) = 1\}$ and $\{C(-3) = 0, T(-3) = -1, R(-3) = 0, R(-2) = 1\}$ are prime implicants of top event $\{T(-1) = 1, T(0) = 1\}$ of an example system that is presented later in Section 4.5 if the initial time is -3. If the state of a node is determined by its input nodes, the node can appear in prime implicants only at the initial time, such as N, T, and C in this example. Negative time steps are used in this paper, because the same notation has been used in previous DFM papers [9, 10, 11, 12] because DFM models are mostly analysed deductively from effects to causes.

3. Towards dynamic risk importance measures

3.1. Previous research

In DFM modelling, risk importance measures need to be constructed so that they map information from prime implicants to values that represent the significances of different components. Thus, the time aspect of DFM should be taken into account in dynamic risk importance measures as well as the multi-state logic.

In the context of DFM, not much research has been conducted on risk importance measures. References [14] and [15] present some DFM importance measures as generalisations of fault tree analysis importance measures. The importance measures presented in [14] measure importances of different nodes in DFM models. They do not consider which state or states of a node appear in prime implicants even though the state information can play an important role in the interpretation of DFM results. Significances of nodes they provide can be useful but their ability to describe how components contribute to the top event is fairly restricted in many cases.

In [15], importance measures are formulated for literals of DFM models. They consider each time point separately while analysts are mainly interested in the overall importances of nodes and states of nodes. For example, if literals $V(-t_1) = s$ and $V(-t_2) = s$ represent node V in state s at time steps $-t_1$ and $-t_2$, importance measures are only calculated for these literals separately even though they represent the same condition. The importance of node V or state s is not directly provided. This paper aims to develop risk importance measures that measure importances of states of nodes and still maintain the information about time steps of literals in the results.

3.2. Other methodologies

Markov models constitute a dynamic reliability analysis approach that is comparable to DFM [16]. Markov models can be used to analyse dynamic multi-state systems as DFM models. Some studies have been carried out on risk importance measures for Markov models [8, 17, 18]. However, it would not be practical to use similar importance measures in DFM because they rely on the perturbation of transition rate matrices of Markov models and DFM models are not based on transition rates.

There are two types of importance measures for multi-state systems [19]. Measures of type 1 are formulated for components and they measure the significance that a component has to the system's reliability as a whole.

Type 1 measures are useful when analysing whether the number of redundant components needs to be increased. Measures of type 2 are formulated for states of components and they measure how a certain state or states of a component affect the system's reliability. Different states of a component can assume quite different values of a type 2 measure. For example, the top event probability might increase if a valve is in state 'failed-close' but the same analysis might show that the top event probability decreases if the valve is in state 'failed-open'. Type 2 measures provide guidance on how a component should be changed so that the system's reliability improves. Many risk importance measures of traditional fault tree analysis can be generalised for multi-state systems.

An approach of type 2 is to transform a multi-state component into a binary component by dividing the states into two sets with regard to a specified performance level [20]. For example, if a pump can function in 'low', 'medium', 'high' or 'very high' power, states 'low' and 'medium' could form one group and states 'high' and 'very high' one group. When a multi-state component is treated as a binary component, traditional risk importance measures can be applied to it. Another approach to measure the importance of a multi-state component is composite importance measures [21], which are weighted averages of type 2 state importances and represent type 1 measures. For example, an average of the risk increase factors of valve's 'failed-close', 'failed-open' and possible other states weighted with state probabilities could be calculated to get a value that measures the significance of the valve as a whole. Both approaches could be applied in DFM.

The modelling of the time-dependent failure behaviour of a component can be performed similarly in the reliability analyses of multi-phase missions [22] and in DFM, even though only a single mission is considered in DFM. In multi-phase missions, basic events can occur during different phases similarly to time steps in DFM. In [23], importance measures are formulated for phase specific events. Correspondingly, in DFM, importance measures can be formulated for time step specific events.

3.3. Conclusion on objectives

The dynamic risk importance measures, the dynamic Fussell-Vesely and the dynamic risk increase factor, are formulated for the different states of nodes. The dynamic Fussell-Vesely is formulated also for different time steps and the dynamic risk increase factor takes the time aspect into account in its own way.

The paper especially focuses on computing dynamic risk importance measures for failure states of components. It is presented how the information about failure states in prime implicants can be tracked by tracing the graph model backwards and utilised to calculate risk importance measures to provide more specific information on how components contribute to the top event probability.

4. The dynamic Fussell-Vesely

4.1. The basic form

Dynamic risk importance measures need to take the multi-state logic and time aspect of DFM into account in a logical way that supports the interpretation of results. For coherent systems, Fussell-Vesely can be interpreted as how much the top event probability would relatively decrease if a component was perfect. In coherent systems, only component failures can cause the top event but in incoherent systems, a failure of a component may actually prevent the top event from occurring and the act of repairing might cause the top event [24]. In multi-state reliability analysis, a system can be defined as coherent if only one state per node appears in prime implicants. Even though DFM models are usually incoherent, they can be coherent with regard to some nodes.

The dynamic Fussell-Vesely (DFV) should be constructed in such a way that the idea about the decrease of the top event probability is maintained. For systems that are coherent with regard to the considered state of the node, the DFV should be possible to interpret so that it indicates how much the top event probability would decrease if the node could be made not to be in the considered state at least until a particular time step. Thus, as the definition of Fussell-Vesely deals with minimal cut sets that include a particular component failure, the definition of the DFV should consider prime implicants that include a particular node in a particular state before or at a particular time step.

Let us assume that the time step of the latest literal in the top event is 0 meaning that it is the last time step of the analysis and the initial time is $-n$ ($n \in \mathbb{N}$). These notations are valid for the rest of the paper. The dynamic Fussell-Vesely is defined in its basic form in Definition 1.

Definition 1. *The dynamic Fussell-Vesely measure of state s of node i at time step $-t$ is*

$$I^{DFV}(i(-t)=s) := \frac{Q_{TOP}^{i(-t)=s}}{Q_{TOP}}, \tag{3}$$

where Q_{TOP} is the top event probability and $Q_{TOP}^{i(-t)=s}$ is the probability that a prime implicant, including node i in state s before or at time step $-t$ $(0 \leq t \leq n)$, causes the top event.

When time steps of literals are not considered interesting, all the attention can be paid to $I^{DFV}(i(0)=s)$ because it takes all time steps into account.

4.2. Importances of failure states

In DFM, components are often modelled with two nodes: one that represents the functional state of a component and one that determines if the component is failed or not. Let the following definitions apply for the rest of the paper:

1. The node whose state determines if the component is failed or not is called a ‘failure node’.

2. A component is failed when the failure node is in state 1 and it functions normally when the failure node is in state 0.

3. The initial state of a failure node is 0.

4. The time lag of a failure node is 0.

5. The node that defines the functional state of a component is called a ‘component node’.

These definitions are used in the DFM tool YADRAT [12]. With these definitions, a failure event can be interpreted as a change of failure node’s state from 0 to 1. When a failure node is in state 0, the component is in one of its normal states determined by the component node. The failure state is defined by the combination of a failure node being in state 1 and the state of the component node. For example, if a component node of a water level measurement sensor has states ‘low’, ‘medium’ and ‘high’, the water level measurement sensor component has normal states ‘low’, ‘medium’ and ‘high’ and failure states ‘failed-low’, ‘failed-medium’ and ‘failed-high’.

If a component is modelled using two nodes, the failure state of a component cannot directly be read from a prime implicant. A prime implicant only shows that the failure node is in state 1. The failure state can depend on the initial states of nodes and other literals that appear in the prime implicant. The dynamic Fussell-Vesely cannot therefore directly be calculated for failure states according to Definition 1. Equation (4) presents the specific definitions of the dynamic Fussell-Vesely for a failure state of a component.

$$I_{fs}^{DFV}(i(-t) = s) := \frac{Q_{TOP}^{f(-t)=1,\, i(-t)=s}}{Q_{TOP}}, \tag{4}$$

where f is a failure node connected to component node i and $Q_{TOP}^{f(-t)=1,\, i(-t)=s}$ is the probability that a prime implicant, including a failure in state s of component node i before or at time step $-t$ $(0 \leq t < n)$, causes the top event.

4.3. Measuring incoherency of a component

When a failure node is in state 0, the corresponding component is functioning as it is meant to. It might be interesting to know if a system is incoherent with regard to a failure of a given component. It could therefore be useful to measure how much state 0 of a failure node contributes to the top event. However, if the dynamic Fussell-Vesely of state 0 of a failure node was calculated according to Definition 1, the interpretation of the result would not come naturally because a failure node is defined to be initially in state 0. But, let the time aspect be inverted so that the definition considers prime implicants that contain a failure node in state 0 at time step $-t$ or later instead of at time step $-t$ or before. In this case, the measure can be interpreted as how much the top event probability relatively decreases if the component fails at a given time step at the latest, if the system is coherent with regard to state 0 of the failure node. The DFV measure is formulated for state 0 of a failure node in (5).

$$I_0^{DFV}(f(-t)=0) := \frac{Q_{TOP}^{f(-t)=0}}{Q_{TOP}}, \tag{5}$$

where $Q_{TOP}^{f(-t)=0}$ is the probability that a prime implicant, including a literal representing failure node f in state 0 at time step $-t$ or later, causes the top event.

4.4. Computation

In the calculation of the dynamic Fussell-Vesely, each prime implicant is examined. If a prime implicant contains the considered node in the considered state (or the considered component in the considered failure state) in the considered time frame, its contribution is added to the DFV.

It is possible that the failure state of the considered component is not unambiguous in a prime implicant. A failure can lead to different states of the component node in separate scenarios. Probabilities for different failure states are therefore solved and a prime implicant's contribution to a failure state DFV presented in (4) is the probability of the prime implicant multiplied by the probability that the component fails to the considered failure state.

The failure state probabilities can be solved deductively by backtracking the model or inductively by simulating different scenarios. The deductive approach is chosen here for the same reason why DFM models are most often analysed deductively: the number of scenarios to be simulated grows easily large with complex models. The backtracking process to solve failure state probabilities starts from the component node at the failure time step. The state probabilities of the component node can be calculated when the state probabilities of its input nodes are known. Hence, the state probabilities of the input nodes are needed and they can be calculated from the state probabilities of the input nodes of the input nodes of the component node. Because of this, the backtracking algorithm is based on the recursive calling of a function that calculates the state probabilities of an output node from the state probabilities of the input nodes. When the state probabilities of input nodes are known, the state combination probabilities of input nodes can be calculated and the probability of an output state is the sum of probabilities of those input state combinations that lead to the considered output state.

The recursive calling of the function continues till the initial time is reached or the considered node is a stochastic node. In these cases, the state probabilities are obtained from the probability model of the node. In the calculation of the DFV, the backtracking is performed under the conditions set by a prime implicant. This means that the states of some nodes are known and the state probabilities are obtained from this information, not from the probability model or calculated as conditional probabilities if the prime implicant information does not imply a certain state but affects the probability model.

The backtracking algorithm implemented in the YADRAT tool is illustrated using flow charts in Figures 1 and 2. YADRAT contains three types of nodes: deterministic nodes, failure nodes and random nodes. The state of a deterministic node is determined by its input nodes through a decision table, except at the initial time step at which the state is determined by a probability model. A failure node is a non-decreasing binary node that is initially in state 0 and whose state is determined by a probability model. A random node is a multi-state stochastic node whose state is determined by a probability model. Each node type is treated differently in the backtracking.

4.5. Backtracking example

Figure 3 shows an example of a DFM model based on a tank system with a digitally controlled valve and Table 1 gives an example of a decision table. In the model, node C represents the functional state of a valve, N represents water level measurement value and T represents water level. Nodes F and R determine if the valve and the water level measurement are failed and they

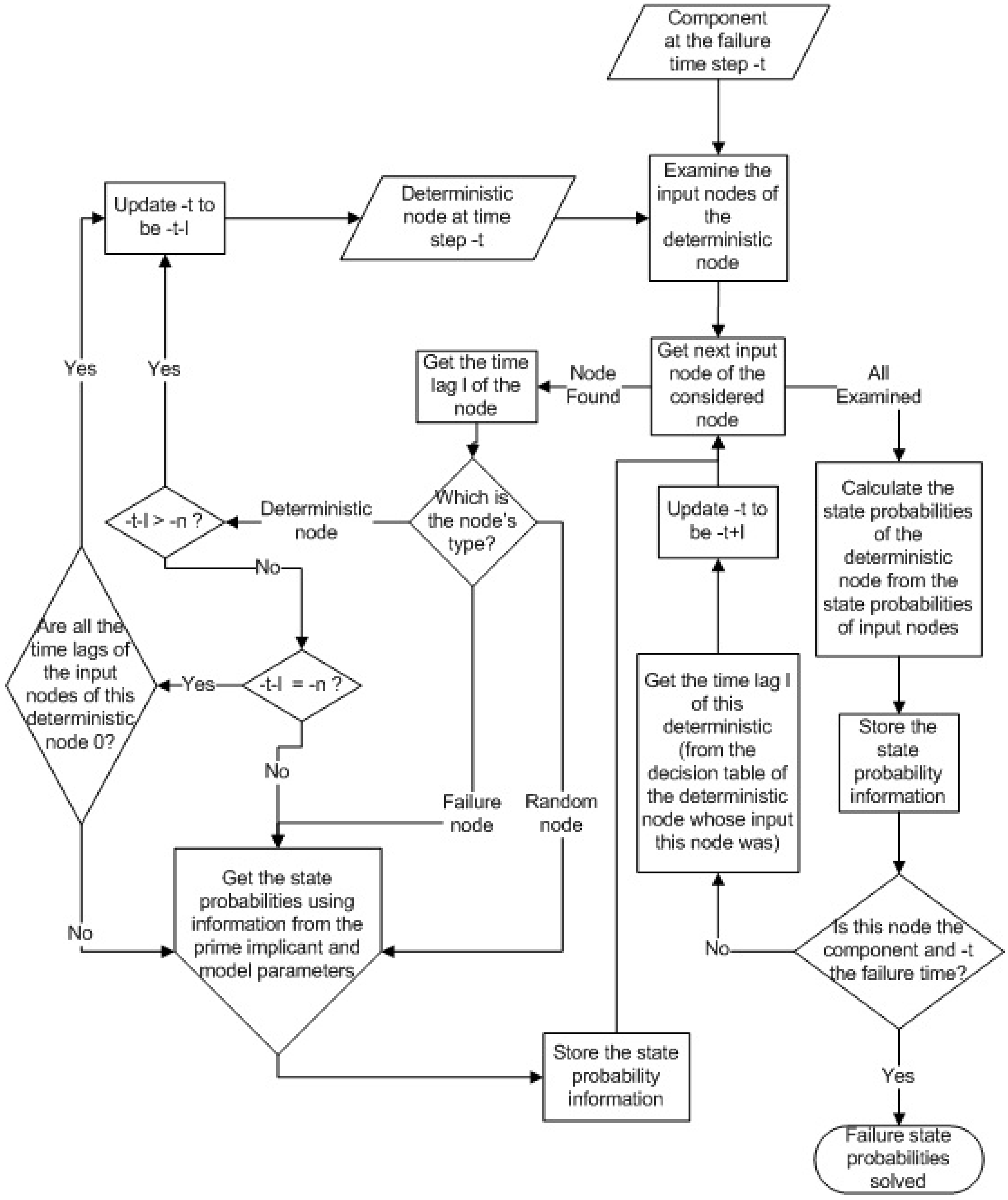
Component at the failure time step -t
Examine the input nodes of the deterministic node
Update -t to be -t-l
Deterministic node at time step -t
Get next input node of the considered node
Node Found
All Examined
Get the time lag l of the node
Yes
Yes
Which is the node's type?
Deterministic node
-t-l > -n ?
No
Are all the time lags of the input nodes of this deterministic node 0?
Yes
-t-l = -n ?
No
Failure node
Random node
Update -t to be -t+l
Get the time lag l of this deterministic (from the decision table of the deterministic node whose input this node was)
Calculate the state probabilities of the deterministic node from the state probabilities of input nodes
Store the state probability information
Get the state probabilities using information from the prime implicant and model parameters
No
No
Is this node the component and -t the failure time?
Store the state probability information
Yes
Failure state probabilities solved

Figure 1: A flow chart of the backtracking process to solve failure state probabilities. The calculation of the state probabilities of failure nodes, random nodes and deterministic nodes at the initial time is illustrated in its own flow chart in Figure 2.

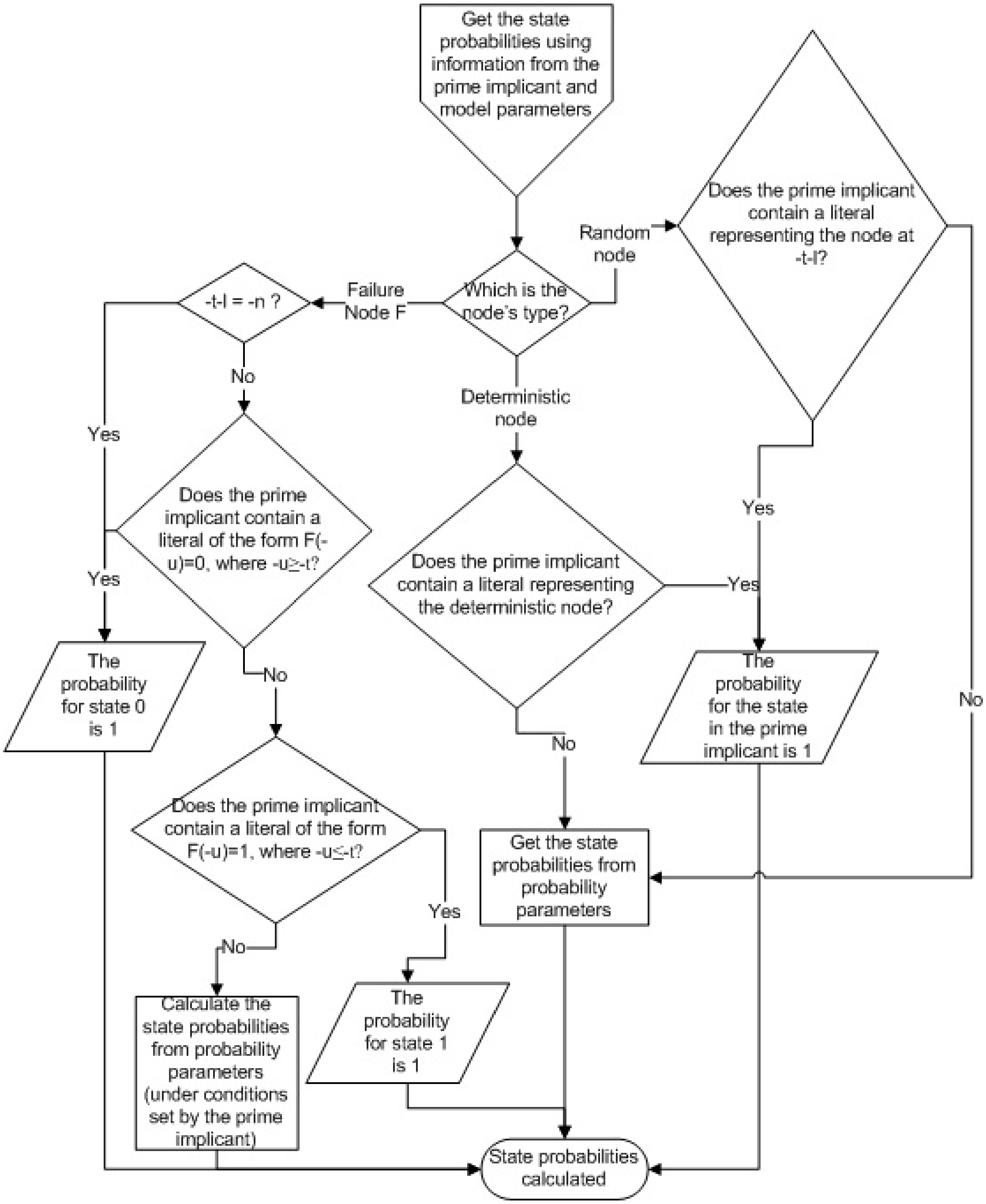
Get the state probabilities using information from the prime implicant and model parameters
Which is the node's type?
Random node
Failure Node F
Deterministic node
Does the prime implicant contain a literal representing the node at -t-l?
-t-l = -n ?
No
Yes
Does the prime implicant contain a literal of the form F(-u)=0, where -u≥-t?
Yes
No
Does the prime implicant contain a literal representing the deterministic node?
Yes
Yes
No
No
The probability for state 0 is 1
The probability for the state in the prime implicant is 1
Does the prime implicant contain a literal of the form F(-u)=1, where -u≤-t?
Get the state probabilities from probability parameters
Yes
No
Calculate the state probabilities from probability parameters (under conditions set by the prime implicant)
The probability for state 1 is 1
State probabilities calculated

Figure 2: A flow chart of the calculation of the state probabilities of failure nodes, random nodes and deterministic nodes at the initial time. This flow chart is a subpart of the flow chart presented in Figure 1 and it takes the node, time step -t and time lag l as inputs from Figure 1.

change states stochastically. Each row of the decision table represents a state combination of input nodes (F, N and C) and the output column determines to which state of the output node C each state combination of input nodes leads to. The time lag row determines the delays in the dependencies between the input nodes and the output node. In Table 1, node C depends on its own state at the previous time step because the time lag is 1. From Table 1, it can be seen that the valve remains in failure state 'failed-0' or 'failed-1' after the failure, because node C stays in the same state it was at the previous time step when F is in state 1.

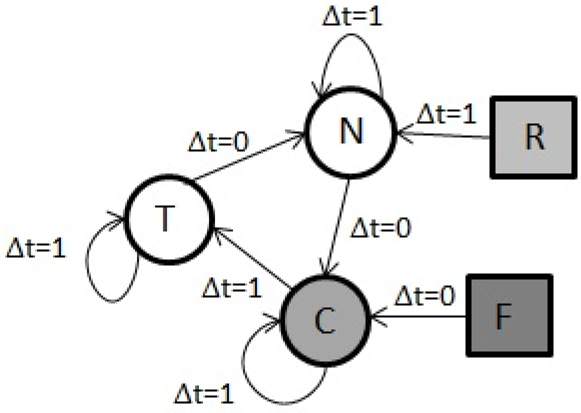

Figure 3: A DFM model from the DFM tool YADRAT

A set of literals $\pi = \{N(-3) = -1, T(-3) = 1, R(-3) = 1, F(-2) = 0, F(-1) = 1\}$ is a prime implicant of top event $\{T(-1) = 1, T(0) = 1\}$ of the system presented in Figure 3 when the initial time is -3. Node F is the failure node of the valve. The failure time is therefore -1. Hence, the failure state probabilities are the state probabilities of $C(-1)$. Under the failure condition, component node C is remains in the same state it was

Table 1: The decision table of component node C

	Output	**Inputs**		
Node	C	F	N	C
Time lag		0	0	1
	0	0	-1	0
	0	0	-1	1
	0	0	0	0
	1	0	0	1
	1	0	1	0
	1	0	1	1
	0	1	-1	0
	1	1	-1	1
	0	1	0	0
	1	1	0	1
	0	1	1	0
	1	1	1	1

in at the previous time step. Thus, the failure state probabilities are the state probabilities of $C(-2)$. As node C is a deterministic node, its state probabilities are defined by the state probabilities of its input nodes. The state probabilities of $F(-2)$, $N(-2)$ and $C(-3)$ therefore have to be solved. Probability $Q(F(-2) = 0 \mid \pi) = 1$ because prime implicant π contains a literal $F(-2) = 0$. Node N is a deterministic node. Hence, the state probabilities of its input nodes should be examined to determine its state probabilities at time step -2. The initial state of component node C does not appear in prime implicant π. The state probabilities of $C(-3)$ are therefore obtained from the probability parameters. If $Q(N(-2) = s \mid \pi) = n_{2,s}$ for all $s \in \{-1, 0, 1\}$, $Q(C(-3) = r) = c_{3,r}$ for all $r \in \{0, 1\}$, $n_{2,-1} + n_{2,0} + n_{2,1} = 1$ and $c_{3,0} + c_{3,1} = 1$, Table 1 indicates that $Q(C(-2) = 0 \mid \pi) = n_{2,-1} + n_{2,0}c_{3,0}$ and $Q(C(-2) = 1 \mid \pi) = n_{2,1} + n_{2,0}c_{3,1}$. The backtracking structure of

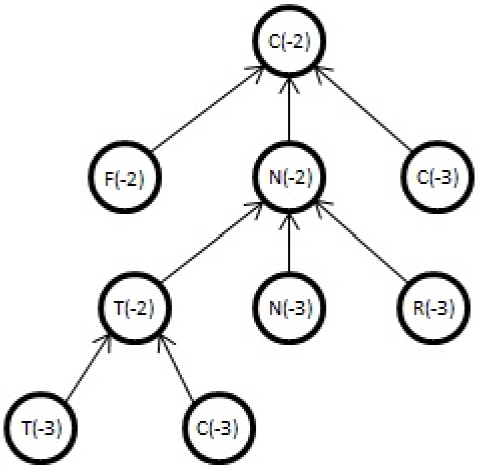

Figure 4: The backtracking tree starting from the node C at time step -2.

this example is illustrated in Figure 4. The progression of the backtracking algorithm is illustrated more closely in Appendix A.

4.6. Solving accurate failure state probabilities

Sometimes the solving of failure state probabilities has to be divided into different scenarios to obtain correct results. When the backtracking process diverges, different branches are examined independently even though they can contain the same nodes. This type of dependencies are taken into account by backtracking the model to identify those nodes that appear in multiple branches and solving failure state probabilities separately in different scenarios related to them. Here, a scenario means that the nodes are set to particular states at particular time steps and the backtracking is performed under that state combination assumption. The probabilities of the state combinations are calculated and accurate failure state probabilities are computed as weighted sums of failure state probabilities related to different scenarios.

There are cases in which the accurate failure state probabilities can be solved by a single backtracking without dividing the solving process into different scenarios and only applying the algorithm presented in Figures 1 and 2. If a single backtracking gives an unambiguous failure state, the result is always accurate because the backtracking covers all the possible scenarios. However, in some cases, the backtracking can imply a possibility of a failure state that is not really possible. Hence, it is computationally most efficient to calculate the failure state probabilities first with a single backtracking and if the failure state is not unambiguous, calculate accurate probabilities by examining different scenarios separately.

4.7. The non-decreasing property of failure nodes

The non-decreasing property of a failure node has to be taken into account in the DFV calculation. Let F be a failure node and $-t$ a time step. Literal $F(-t) = 1$ represents a condition that the corresponding component is failed at time step $-t$. Due to the non-decreasing property of failure nodes, this condition can be satisfied by a failure that occurs at time step $-t$ or earlier. Hence, when DFV values are calculated for the state 1 of F, it must be taken into account that condition $F(-t) = 1$ can be caused by a failure at an earlier time step. For this reason, a prime implicant that includes condition $F(-t) = 1$ also contributes to the DFV values of earlier time steps than $-t$. If prime implicant π includes literal $F(-t) = 1$ and $-u < -t$, the contribution of π to $I^{DFV}(F(-u) = 1)$ is $Q(F(-u) = 1 \mid \pi) \cdot Q(\pi)$.

Conditional probability $Q(F(-u) = 1 \mid \pi)$ is usually

$$\frac{Q(F(-u) = 1)}{Q(F(-t) = 1)} \tag{6}$$

but if prime implicant π includes, for example, literal $F(-u) = 0$, $Q(F(-u) = 1 \mid \pi) = 0$ as condition $F(-u) = 0$ implies that the component must be functioning at time step $-u$.

Let s be a state of component node C. The contribution of prime implicant π to $I_{fs}^{DFV}(C(-u) = s)$ is

$$Q(F(-u) = 1 \mid \pi) \cdot Q(\pi) \cdot Q(C(-u) = s \mid \pi_{F(-u)=1}), \tag{7}$$

where $\pi_{F(-u)=1}$ is a modified version of prime implicant π that includes literal $F(-u) = 1$ instead of $F(-t) = 1$.

5. The dynamic risk increase factor

5.1. Definition

The risk increase factor measures how much the unavailability of a system increases if a component fails. Thus, in the calculation of the risk increase factor it must be assumed that a component is failed. In DFM, a component can fail at different time steps. The failure of a component does not usually cause system's failure immediately. To provide all the available time for the failure to affect the system, let the dynamic risk increase factor (DRIF) be defined so that the component fails at the earliest possible time step. When a component is failed, it remains failed for the rest of the scenario.

To formulate a more general version of DRIF, let the idea that the condition lasts the whole scenario be applied to a state of a node and the dynamic risk increase factor be formulated so that it measures how much the top event probability increases if the considered node is in the considered state at all time steps. The definition is presented in Definition 2.

Definition 2. *The dynamic risk increase factor for a state of a node is*

$$I^{DI}(i = s) := \frac{Q_{TOP}(i(-t) = s,\ \forall\, t \in \{0, 1, ..., m-1, m\})}{Q_{TOP}}, \tag{8}$$

where $Q_{TOP}(i(-t) = s,\ \forall\ t \in \{0, 1, ..., m-1, m\})$ *is the probability that the top event occurs assuming that a node* i *is in state* s *at every time step starting from* $-m$ $(0 \leq m \leq n)$ *which is the earliest possible time step for the node* i *to be in state* s *considering the initial conditions.*

The earliest possible time step for a node to be in a state can vary. For example, a failure node is defined to be initially in state 0. Hence, it can be in state 1 only starting from time step $-n+1$. Similarly, for random nodes and component nodes, all states might not be initially possible.

5.2. Computation

In the calculation of the DRIF, a conditional top event probability is needed. Possibilities are to identify new prime implicants of the conditional top event either by deriving them from originally identified prime implicants or performing a completely new DFM analysis with a modified top event or develop an algorithm to calculate the conditional top event probability “directly” from the model without identifying prime implicants first. A completely new DFM analysis for each DRIF value would be too time-consuming. The computation of the top event probability without identifying prime implicants is an interesting problem that could be examined in the future but in this paper, prime implicants of the conditional top event are derived from the original prime implicants which is more straightforward.

Prime implicants of the conditional top event can be derived from the original prime implicants in the following way. The prime implicants are examined one by one. Those prime implicants that contradict with the condition (contain a node at a specific time step in a wrong state) are removed and the literals that appear in the condition are removed from the prime implicants because their conditional probability is 1. After this, if accurate results are wanted, all duplicate prime implicants and implicants that are not prime implicants anymore have to be removed from the set. This can be done by comparing changed prime implicants with each other and comparing the untouched prime implicants with the remaining changed prime implicants. Figure 5 presents a flow chart to illustrate the identification of new prime implicants.

Table 2 presents the prime implicants of the top event $\{T(-1) = 1, T(0) = 1\}$ of the system presented in Figure 3. When the DRIF is calculated for the failure of the valve, the condition is $\{F(-2) = 1, F(-1) = 1, F(0) = 1\}$. When the new prime implicants are derived, prime implicants 10 and 13 from Table 2 are removed because they contain literal $F(-2) = 0$. Literals $F(-2) = 1$ and $F(-1) = 1$ are removed from other prime implicants. 11 non-minimized implicants are left (Table 3). When these implicants are compared

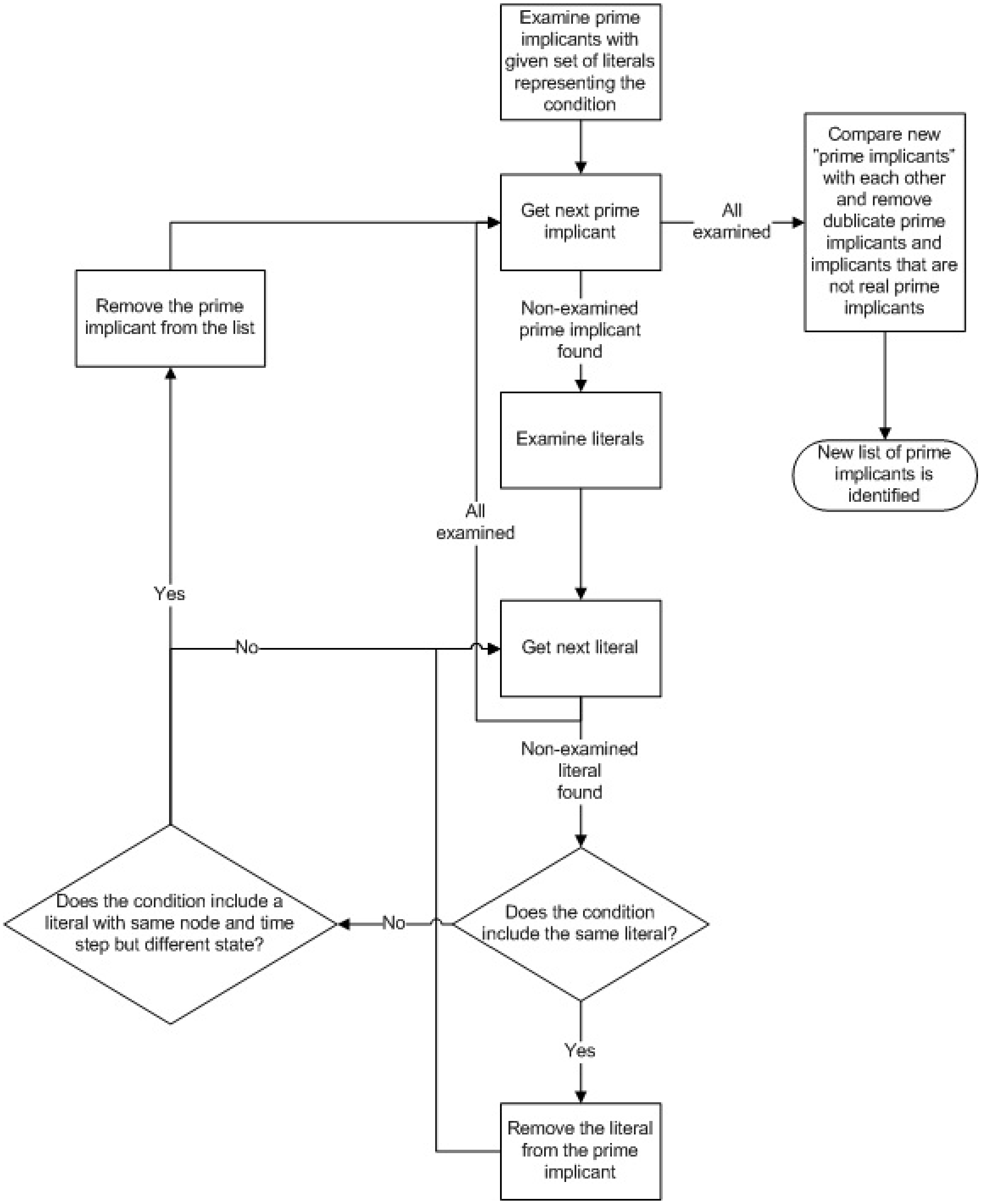
Examine prime implicants with given set of literals representing the condition
Get next prime implicant
All examined
Compare new "prime implicants" with each other and remove dublicate prime implicants and implicants that are not real prime implicants
New list of prime implicants is identified
Remove the prime implicant from the list
Non-examined prime implicant found
Examine literals
All examined
Yes
No
Get next literal
Non-examined literal found
Does the condition include a literal with same node and time step but different state?
No
Does the condition include the same literal?
Yes
Remove the literal from the prime implicant

Figure 5: A flow chart representing the identification process of prime implicants of the conditional top event

Table 2: The prime implicants of the top event $\{T(-1) = 1, T(0) = 1\}$ of the system presented in Figure 3

No.	**Prime implicant**
1	$\{C(-3) = 0, F(-2) = 1\}$
2	$\{C(-3) = 0, F(-1) = 1, T(-3) = -1, R(-3) = 0\}$
3	$\{C(-3) = 0, F(-1) = 1, T(-3) = -1, N(-3) = 0\}$
4	$\{C(-3) = 0, F(-1) = 1, T(-3) = -1, N(-3) = -1\}$
5	$\{C(-3) = 0, T(-3) = -1, R(-3) = 0, R(-2) = 1\}$
6	$\{C(-3) = 0, T(-3) = -1, N(-3) = 0, R(-2) = 1\}$
7	$\{C(-3) = 0, T(-3) = -1, N(-3) = -1, R(-2) = 1\}$
8	$\{C(-3) = 0, F(-1) = 1, N(-3) = 0, R(-3) = 1\}$
9	$\{C(-3) = 0, F(-1) = 1, N(-3) = -1, R(-3) = 1\}$
10	$\{N(-3) = -1, R(-3) = 1, F(-2) = 0, T(-3) = 1, F(-1) = 1\}$
11	$\{C(-3) = 0, N(-3) = 0, R(-3) = 1, R(-2) = 1\}$
12	$\{C(-3) = 0, N(-3) = -1, R(-3) = 1, R(-2) = 1\}$
13	$\{N(-3) = -1, R(-3) = 1, F(-2) = 0, T(-3) = 1, R(-2) = 1\}$

to each other, it is noticed that only $\{C(-3) = 0\}$ is a prime implicant and others are non-minimal implicants.

The dynamic risk increase factor can be calculated for a failure state of a component assuming that the failure node is in state 1 starting from the first time step after the initial time and that the component node remains in the corresponding state after the failure. The failure node in state 1 does not always guarantee a particular failure state. It must therefore be assumed that the initial conditions are such that the component fails to the considered failure state. If the failure causes the component node to remain in its previous state, it is assumed that the initial state of the component node is the state that corresponds to the considered failure state. If the component always fails to the same failure state, no initial condition assumption is needed. If the component node can change state after the failure, the DRIF should only

Table 3: The non-minimized implicants of the conditional top event

No.	Prime implicant
1	$\{C(-3)=0\}$
2	$\{C(-3)=0, T(-3)=-1, R(-3)=0\}$
3	$\{C(-3)=0, T(-3)=-1, N(-3)=0\}$
4	$\{C(-3)=0, T(-3)=-1, N(-3)=-1\}$
5	$\{C(-3)=0, T(-3)=-1, R(-3)=0, R(-2)=1\}$
6	$\{C(-3)=0, T(-3)=-1, N(-3)=0, R(-2)=1\}$
7	$\{C(-3)=0, T(-3)=-1, N(-3)=-1, R(-2)=1\}$
8	$\{C(-3)=0, N(-3)=0, R(-3)=1\}$
9	$\{C(-3)=0, N(-3)=-1, R(-3)=1\}$
10	$\{C(-3)=0, N(-3)=0, R(-3)=1, R(-2)=1\}$
11	$\{C(-3)=0, N(-3)=-1, R(-3)=1, R(-2)=1\}$

be calculated for state 1 of the failure node because the component does not necessarily remain in the same failure state for the whole scenario.

Component node C in Table 1 is stuck in its previous state when failure node F turns to state 1. Hence, in the calculation of $I^{DI}(C=0)$ with the initial time -3, the condition is that $F(-t)=1$ for all $-t \in \{0,-1,-2\}$ and $C(-3)=0$ and similarly, in the calculation of $I^{DI}(C=1)$, the condition is that $F(-t)=1$ for all $-t \in \{0,-1,-2\}$ and $C(-3)=1$.

There are also cases in which the failure state at time step $-n+1$ is determined in a more complicated way and more complex initial state assumptions are needed. Generally, the initial conditions that are needed to produce the failure state need to be identified. The result is a set of initial state combinations. The DRIF is calculated separately with each initial state combination assumption and the final DRIF for the failure state is calculated as a weighted average of the DRIFs of the initial state combinations that lead to the failure state. These cases are not considered further in this paper because more simple cases are more common.

Other than for failure states of components, there is no easy and efficient way to calculate the DRIF for states of deterministic nodes because only initial states of deterministic nodes appear in prime implicants and there is therefore no easy way to derive the prime implicants for the conditional top event from the original prime implicants. The conditions that would be needed to produce the condition that the considered deterministic node would be in same state at all time steps should be solved. After that, the DRIF should be calculated assuming each of those conditions separately, and finally, a weighted average should be calculated. This could not be efficiently done with complex models because the number of different conditions would be large in many cases. However, a risk increase factor can be calculated for initial states of deterministic nodes by only assuming that a node is in a particular state at the initial time.

6. Importance analysis of an emergency core cooling system

6.1. Emergency core cooling system

In this section, an emergency core cooling system of a boiling water reactor [12] is analysed with the DFM tool YADRAT. The system is shown in Figure 6. The purpose of this system is to provide adequate water cooling of a reactor core if the ordinary cooling system is not functioning. An on-off control system regulates the water level in the pressure vessel by controlling

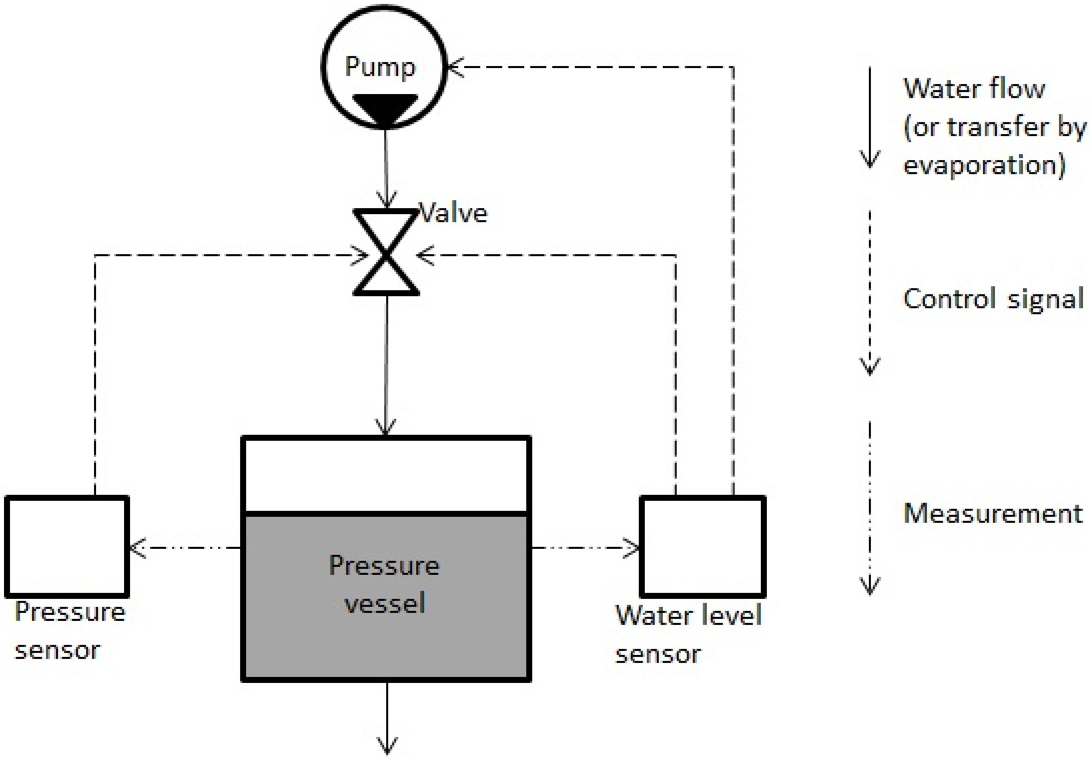

Figure 6: An emergency core cooling system of a boiling water reactor

a pump and a regulation valve. Sensors measure the water level and the pressure which are utilised in controlling of the valve, while only the water level measurement affects controlling of the pump. The water level can decrease due to evaporation. If the water level is low, more water is pumped into the pressure vessel until an upper limit is reached. The regulation valve is opened if both water level and pressure are measured to be under lower limit.

6.2. System reliability model

Figure 7 presents the node structure of a DFM model from the YADRAT tool based on the emergency core cooling system [12]. This model contains one pump line that includes four components: a water level sensor modelled with component node WLM and failure node WLM-fail, a pressure sensor modelled with component node PM and failure node PM-fail, a regulation valve modelled with component node V and failure node V-fail and a pump modelled with component node P and failure node P-fail. Component node P has two states: ‘on’ and off’ but the pump can only fail to failure state ‘failed-off’, which means that it does not pump any water. The valve can be failed in state ‘failed-close’ or ‘failed-open’. The water level measurement can be frozen in state ‘failed-low’, ‘failed-medium’ or ‘failed-high’, while the pressure measurement can be frozen in state ‘failed-low’ or ‘failed-high’.

An exponential model is used for failure probabilities. The failure rates are presented in Table 4. A failure rate is here the probability that the component fails during one time step.

Table 4: The failure rates of the components

Failure node	**Failure rate** $[1/\Delta t]$
P-fail	0.01
V-fail	0.02
WLM-fail	0.03
PM-fail	0.04

The pump line also contains a random node PL that represents a pump leakage signal and several deterministic nodes that represent the signals between the sensors, the control logic and the actuators. The model also in-

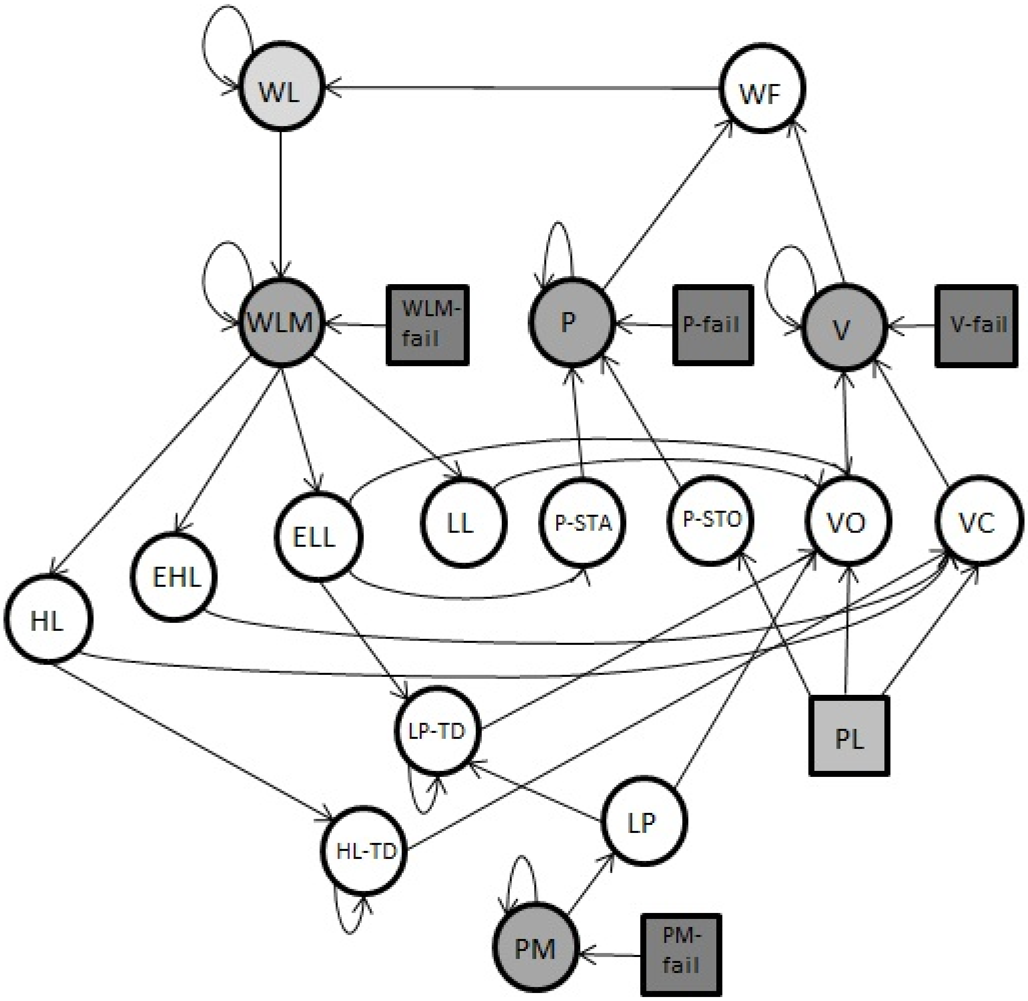

Figure 7: A DFM model based on the emergency core cooling system

cludes two deterministic nodes to represent the water inflow (WF) and the reactor water level (WL). The nodes of the model are described more in Appendix B.

6.3. Results

The analysed case was that the water level is low four time steps in a row (top event $\{WL(-3) = low, WL(-2) = low, WL(-1) = low, WL(0) = low\}$) which is a long enough time to be critical with regard to cooling of the core. The initial time was chosen to be -5 because earlier experiences had shown that all the relevant prime implicants can be identified using this time frame and same patterns are only repeated in prime implicants using a longer time frame.

The number of identified prime implicants was 338 and five of them are presented in Table 5. These five prime implicants were chosen because they represent different prime implicant types. They are not necessarily the most important prime implicants. In prime implicants 2 and 4, the regulation valve fails in state 'failed-close'. In prime implicant 3, the pressure measurement is frozen in state 'failed-high'. In prime implicant 5, the failure states of the water level measurement and valve are not unambiguous but can be different in different scenarios. The water level measurement is frozen in state 'failed-low' with a probability of 0.5 and in state 'failed-medium' with a probability of 0.5, and the valve is failed in state 'failed-open' with a probability of 0.17 and in state 'failed-close' with a probability of 0.83. Prime implicant 1 includes only an initial condition of the water level WL, initial conditions of components, a pump leakage signal at the initial time, a condition that the

Table 5: Examples of prime implicants

	tot-pr.	**pr.**	**Node**	t	**State**
1	3.5E-2	0.330	WL	-5	high
		0.500	V	-5	close
		0.500	PL	-5	true
		0.500	PM	-5	low
		0.885	PM-fail	-2	0
		0.970	WLM-fail	-4	0
2	1.0E-2	0.500	V	-5	close
		0.020	V-fail	-4	1
3	1.0E-2	0.500	V	-5	close
		0.500	PM	-5	high
		0.040	PM-fail	-4	1
4	9.9E-3	0.500	V	-5	close
		0.500	PL	-5	true
		0.040	V-fail	-3	1
5	1.4E-5	0.330	WL	-5	low
		0.500	P	-5	on
		0.500	PL	-5	true
		0.100	PL	-4	true
		0.059	V-fail	-2	1
		0.941	WLM-fail	-3	0
		0.030	WLM-fail	-2	1

pressure measurement is functioning at time step -2 and a condition that the water level measurement is functioning at time step -4.

Table 6 presents both accurate and approximated DFV values for failure states of components. Approximated results were calculated using a single backtracking for each failure in a prime implicant in the solving of failure state probabilities and accurate results were calculated by dividing the failure state probability solving process into different scenarios as described in Section 4.6.

Figure 8 presents the DFV values for component failures and pump leak-

Table 6: The dynamic Fussell-Vesely values for failure states. Those DFV values that are 0 are left out.

Component node	**failure state**	**Time**	**DFV accu.**	**DFV appr.**
P	failed-off	0	0.198	0.198
	failed-off	−1	0.198	0.198
	failed-off	−2	0.184	0.184
	failed-off	−3	0.151	0.151
	failed-off	−4	0.089	0.089
V	failed-open	0	0.00004	0.0003
	failed-open	−1	0.00004	0.0003
	failed-open	−2	0.00003	0.0001
	failed-open	−3	0.00003	0.00003
	failed-open	−4	0.00003	0.00003
	failed-close	0	0.289	0.289
	failed-close	−1	0.289	0.289
	failed-close	−2	0.262	0.262
	failed-close	−3	0.197	0.197
	failed-close	−4	0.087	0.087
WLM	failed-high	0	0.060	0.062
	failed-high	−1	0.060	0.062
	failed-high	−2	0.060	0.062
	failed-high	−3	0.060	0.060
	failed-high	−4	0.036	0.036
	failed-medium	0	0.083	0.081
	failed-medium	−1	0.083	0.081
	failed-medium	−2	0.083	0.081
	failed-medium	−3	0.059	0.059
	failed-medium	−4	0.034	0.034
	failed-low	0	0.00004	0.00004
	failed-low	−1	0.00004	0.00004
	failed-low	−2	0.00004	0.00004
PM	failed-high	0	0.119	0.119
	failed-high	−1	0.119	0.119
	failed-high	−2	0.119	0.119
	failed-high	−3	0.084	0.084
	failed-high	−4	0.042	0.042

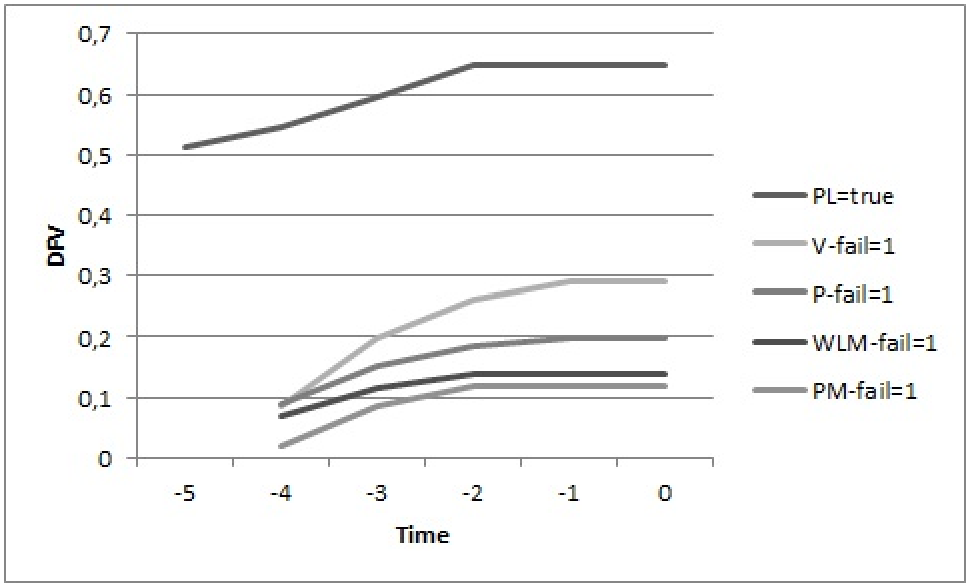

Figure 8: The dynamic Fussell-Vesely values for component failures and pump leakage signal. On the right side of the graph, curves are ordered according to their end points.

age signal and Figure 9 presents the DFV values for 0-states of failure nodes in the form of a graph. Table 7 presents the DRIF values for failure states of components, Table 8 for component failures and Table 9 for the states of the random node.

The valve clearly has more significant effects to the system's reliability than other components. It has the largest DFV values except for time step -4 (Figure 8) and also according to the dynamic risk increase factor, its failure in state 'failed-close' has the worst effect on the system (Table 7). However, the valve's failure in state 'failed-open' decreases the top event probability significantly and the failure of the valve therefore has the smallest DRIF value of the component failures (Table 8). According to both importance measures, the pump is more important than the sensors even though its failure rate is smaller. This is logical because the pump and the valve directly affect the

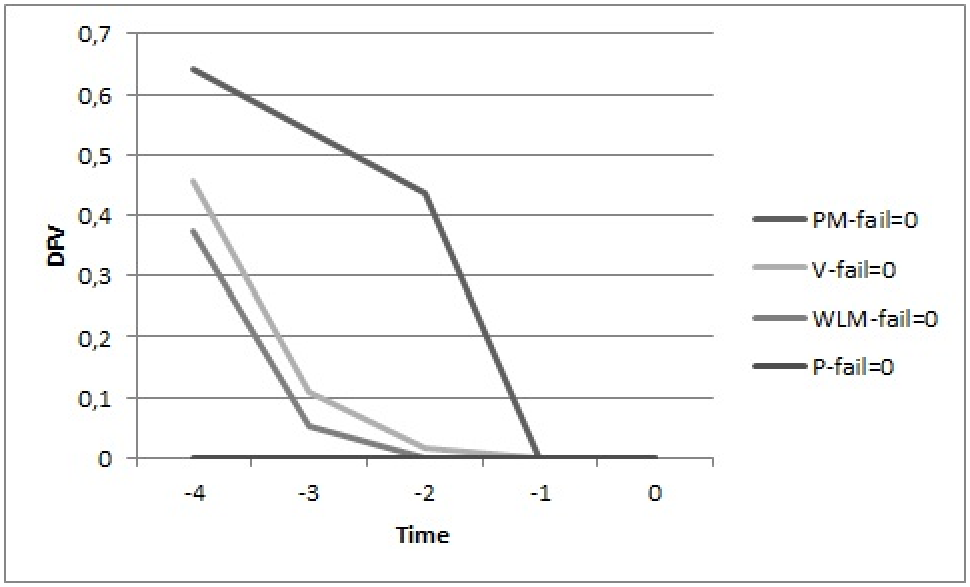

Figure 9: The dynamic Fussell-Vesely values for 0-states of failure nodes. On the right side of the graph, curves are ordered according to their starting points.

Table 7: The dynamic risk increase factor values for failure states

Component node	**Failure state**	**DRIF**
P	failed-off	1.51
V	failed-open	0.17
	failed-close	1.81
WLM	failed-high	1.50
	failed-medium	1.44
	failed-low	0.30
PM	failed-high	1.42
	failed-low	0.46

Table 8: The dynamic risk increase factor values for component failures (1-states of failure nodes)

Failure node	**DRIF**
P-fail	1.51
V-fail	0.99
WLM-fail	1.20
PM-fail	1.10

Table 9: The dynamic risk increase factor values for states of the random node

Random node	**State**	**DRIF**
PL	true	1.51
	false	0.55

water flow. However, the top event is most often caused by the pump leakage signal (PL in the 'true' state).

When analysing the time-dependent behaviour of DFV values in Table 6 and Figure 8, it has to be remembered that DFV values are calculated cumulatively. The DFV values indicate that early failures of time steps -4 and -3 contribute most to the top event in all cases. This is logical because they have a more long lasting effect on the water level than later failures. The pump is the easiest component to analyse here because it always fails in the same way and its failure always has the same impact. The earlier the pump fails the more likely it is causing the top event as can be seen from the DFV values in Table 6. The DFV values of PM and WLM are also consistent with the intuitive idea that the earlier failure is more likely to cause the top event than a later failure.

The valve however has the largest addition to the cumulative DFV at time step -3. The reason for this is that component node V is more likely to be in state ‘close’ at time step -4 than at the initial time -5, and hence, the valve is more likely to be stuck in the harmful failure state ‘failed-close’ at time step -3 than at time step -4. High pump leakage signal probability 0.5 at the initial time is the main reason why component node V is more likely to be in state ‘close’ at time step -4. If component node V is in state ‘open’, the valve is closed due to the pump leakage signal unless it is fails.

For the pump and valve, failures of time step -1 can still contribute to the top event but failures of time step 0 cannot. This is because failures of the valve and the pump affect the water level with a delay of one time step. Measurement failures have to occur at time step -2 at the latest to contribute to the top event because they affect the water level with a delay of two time steps.

All possible failure states except the ‘failed-low’ state of the pressure measurement appear in the prime implicants. State ‘low’ of WLM, together with state ‘low’ of PM, sends the valve a signal that it needs to open so that more water can be pumped into the pressure vessel. Hence, failure state ‘failed-low’ cannot contribute to decreasing the water level but only increasing it. Failure state ‘failed-low’ of the water level measurement had small dynamic Fussell-Vesely values even though it cannot really cause the water level to decrease. In some of those prime implicants that had the water level measurement failed, such as in prime implicant 5 in Table 5, the situation was that either the sensor failed in state ‘failed-medium’ and partly caused the top event, or the sensor failed in state ‘failed-low’ and some other conditions caused the top event. None of the prime implicants implied that the water level measurement was frozen in state ‘failed-low’ with certainty.

Hence, failure state ‘failed-low’ did appear in some prime implicants but did not really contribute to the top event. In those cases, the failure of the water level measurement appeared in the prime implicants because in some scenarios, the failure in the ‘failed-medium’ state was needed to cause the top event. Failure state ‘failed-open’ of the valve had small DFV values for the same reason.

It seems worth highlighting that failure state ‘failed-medium’ of the water level measurement had larger overall DFV value (DFV value of time step 0) than failure state ‘failed-high’. This was because the failure in state ‘failed-medium’ at time step -2 can contribute to the top event but the failure in state ‘failed-high’ at time step -2 cannot. If the water level measurement is frozen in state ‘failed-high’ at time step -2, it means that the water level must have been ‘high’ at time step -4 and thus, the water level could not have been ‘low’ at time step -3.

Some differences appeared between accurate and approximated failure state DFV values because failure states were not calculated correctly using a single backtracking in every case. For example, approximated results imply that the failure in state ‘failed-high’ of the water level measurement at time step -2 contributes a little to the top event even though it is impossible as explained in the previous paragraph. The reason for this was that node WLM-fail at time step -4 appeared in two different branches of backtracking. The positive probability for failure state ‘failed-high’ came from an impossible scenario in which WLM-fail was in state 1 in one branch and 0 in another. Wrong failure state probabilities are always a result of taking this kind of impossible scenarios into account. These impossible scenarios appear in the calculations more likely if there are more time steps to backtrack. In other words, wrong results are more likely with late failures than with earlier failures because the backtracking process is longer and nodes are analysed at more time steps. In this example, wrong failure state probabilities were calculated only for failure times -2 and -1 as can be seen from the DFV values in Table 6.

As the wrong failure state probabilities are more likely to appear with late failures, those prime implicants for which wrong failure state probabilities are calculated are likely to have small probabilities and small effect to DFV values. Because of this, approximated DFV values are most often very close to accurate values. Also, even if impossible scenarios appear in backtracking, they do not necessarily lead to wrong failure state probabilities. In this example, the most important prime implicant for which wrong probabilities were calculated formed the portion of 0.89% of the top event probability, and as total, such prime implicants formed the portion below 2.5% of the top event probability. The only real issue that wrong failure state probabilities caused to complicate the analysis of results was the implication that the failure in state 'failed-high' of the water level measurement at time step -2 could contribute to the top event and even that is not very significant with regard to final conclusions drawn about the system.

The system is not coherent with regard to failure events, except the failure of the pump. The results of Figure 9 indicate that some prime implicants include failure nodes in state 0. State 0 of PM-fail, in particular, contributes significantly to the top event. When this condition appears in prime implicants, it ensures that the pressure measurement cannot fail in state 'failed-low', which would prevent the top event from occurring. Hence, according to the DFV values, failure state 'failed-low' would prevent the top event from occurring in many cases.

From the dynamic risk increase factor values (Tables 7 and 8), it can be seen that some failure states increase the top event probability and some decrease it. Failure state 'failed-open' of the valve, failure state 'failed-low' of the water level measurement and failure state 'failed-low' of the pressure measurement decrease the top event probability because they can only cause the water level to increase not decrease. Those failure states that had significant DFV values in Table 6 can cause the water level to decrease and hence, they have DRIF values larger than 1. The failure of the regulation valve in state 'failed-close' at time step -4 causes the top event to occurs with certainty.

The pump leakage signal has the highest DFV values (0.648 when all time steps are taken into account) and same or higher DRIF value (1.51) than any of the component failures. The best way to improve the reliability of this system would therefore be to reduce the probability of the pump leakage signal which could be done by reducing the probability of the spurious signal and the probability of the pump leakage. It would also be beneficial to improve the reliability of the valve and the pump. Results also indicate that the top event probability would lower if the control system was changed so that the valve was more open and the measurement sensors displayed low values for the water level and the pressure all the time. However, this type of change is neither practically possible nor sensible and it might cause the water level to be high all the time which could be harmful too. Because of this, it would be worthwhile to analyse the system with the top event $\{WL(-3) = high, WL(-2) = high, WL(-1) = high, WL(0) = high\}$ as well. With this top event, the results would be quite different.

7. Discussion

7.1. Benefits

The dynamic risk importance measures are an important contribution to the dynamic flowgraph modelling because the previously developed importance measures [14, 15] were not designed to measure significances of node's states properly while the states of nodes often play an important role in the interpretation of DFM results. The dynamic risk importance measures take the time aspect of DFM into account in a logical way that supports the interpretation of results. In addition, they can provide detailed information on how components modelled with two nodes contribute to the top event. In principle, they could also be applied in all dynamic methods that rely on variables with a finite number of states. The time aspect of the dynamic risk importance measures could also be generalised to the case of continuous time.

7.2. The dynamic Fussell-Vesely

The Fussell-Vesely measure is the importance measure used most often because it is simple to compute and it encapsulates purely the information from minimal cut sets or prime implicants. The dynamic Fussell-Vesely has the same qualities. The dynamic Fussell-Vesely takes into account both the probability that the node is in the considered state and how the node and the state interconnect with other nodes. However, the DFV does not take the incoherency of a system into account because it does not consider that the prime implicants can include the node in different states. This limits the interpretation of the DFV values calculated for component failures. The incoherency can only be taken into account by calculating separate DFV values for the state 0 of a failure node. For example, the results of Figure 8 could not indicate that the system was incoherent with regard to some failure nodes and the incoherency only came evident when the results of Figure 9 were analysed.

If the system is coherent with regard to a failure, other risk importance measures that depend on the conditional top event probability with a condition that the considered component is functioning can also be derived from Fussell-Vesely. The same cannot be done in the incoherent case. The fractional contribution [25] gives same results as Fussell-Vesely in coherent case and takes the incoherency into account in incoherent case. But, the dynamic fractional contribution would be computationally more demanding as new prime implicants of the conditional top event should be identified.

7.3. The failure state approach

The failure state approach used in the calculation of the dynamic risk importance measures for components provides information about the state of a failed component as discussed in Section 4.2. This information cannot directly be read from prime implicants. The failure state approach is useful because a failure state (or failure mode) is really an important factor when analysing causes of a top event even if only the failure is the fundamental cause from the mathematical point of view. There are also other ways to model different failure modes in DFM. One way is to use a so-called "multi-state failure node" that contains separate states for different failure modes. If a "multi-state failure node" is used instead of modelling presented in this paper, there is no need to solve failure states. This requires own failure node state for each failure state, and hence, the decision table of the component grows large, which makes the DFM model computationally more demanding.

The solving of accurate failure state probabilities is based on an examination of different scenarios related to nodes that appear in different branches of backtracking as discussed in Section 4.6. This can be very demanding for components of complex systems because the number of different scenarios can be large. In some cases, it is better to compute approximations by a single backtracking than to examine all the different scenarios. In the example case presented in this paper, accurate failure state probabilities, which affected the DFV results in Table 6, were calculated in two seconds. The same model was also analysed with -6 as the initial time instead of -5 (results not presented here) and in that case, the computation lasted two minutes while approximated results were obtained in a second. Thus, one time step more to backtrack makes a significant addition to computation demands. But, the effect that inaccurate failure state probabilities have on DFV values was small in all the examined example cases such as in the results presented in Table 6. Hence, when only approximations of failure state DFV values are needed, the use of a single backtracking may be sufficient.

7.4. The dynamic risk increase factor and other importance measures

Like the traditional risk increase factor, the dynamic risk increase factor mainly depends on how other components can keep the system operating while the considered component is failed or node is in a given state. When used independently, the DRIF gives a fairly restricted view on how a state of a node contributes to the top event but it is a good complement to the DFV. The DRIF can be used to derive some other dynamic risk importance measures that rely on the conditional top event probability with an assumption that a node is in a given state at all time steps.

There are many other importance measures that could also be generalised in dynamic and multi-state cases. Other often-used importance measures include Birnbaum importance, the risk decrease factor (also known as the risk reduction worth), the criticality importance and the partial derivative [1]. For some risk importance measures, there is more than one way in which the generalisation to the dynamic case can be made. In the dynamic risk increase factor, it is assumed that the condition starts at the first possible time step. The DRIF could also be generalised for other time steps. A similar idea has been considered in relation to multi-phase missions [23]. This could bring worthwhile additional information in some cases when the system is incoherent with regard to the considered node but mostly not. The computation of the DRIF for a failure state with an assumption of a late failure would be significantly more demanding than the computation of the DRIF with the failure at the first possible time step, because not only initial conditions would affect the failure state but also the states of the random nodes and failure nodes at earlier time steps than the considered failure time. All the different state combinations of affecting nodes at relevant time steps should be considered when the assumption of a failure state is made. Computation demands would, of course, be much smaller if failure states were not considered.

Many risk importance measures rely on the calculation of a conditional top event probability. In those importance measures that include a failure assumption, the failure condition can be replaced with an assumption that a node is in a particular state at particular time steps. An assumption that a component is functioning can also be replaced with an assumption that a node is not in a particular state at particular time steps. In these cases, a new set of prime implicants is identified for the conditional top event. If accurate results are to be produced, the identification of new prime implicants is computationally demanding when the original set of prime implicants is large.

The computation of differential risk importance measures, such as the partial derivative and the differential importance measure [26], would be easier in DFM because prime implicants of the conditional top event would be the same as the original prime implicants. Only manipulation of probability parameters and recalculation of probabilities would be required in the calculation of the conditional top event probability. It would however be difficult to apply differential risk importance measures to failure states unless a separate probability is assigned to each failure state.

7.5. Measuring the importance of a node

This paper focused on importance measures that measure the importance of a state of a node. Sometimes, analysts are more interested in the overall importances of nodes so that the most critical components of a system can be identified. To measure the overall importances of nodes, the composite importance measure approach presented in [21] could be applied to the dynamic risk increase factor. The Fussell-Vesely presented in [21] differs significantly from the dynamic Fussell-Vesely as it relies on the computation of the top event probability with an assumption that the node is in a certain state. Instead, the Fussell-Vesely from [14] could be generalised to take the time aspect into account. In the risk increase factor presented in [14], it is assumed that the node is in its worst state at each time step. The worst state can be different at different time steps. In the dynamic risk increase factor, it is assumed that a node is in the same state at each time step, which makes these measures fundamentally different. However, the worst state approach could be applied to the dynamic risk increase factor to formulate an overall DRIF measure for a node. If the worst state was the same at every time step, these measures would give the same value, but if the worst state differed, the risk increase factor from [14] would give a larger value.

7.6. DFM tool development

Other YADRAT tool related research includes modelling of common cause failures and other dependencies between failures as well as a study of different component reliability models. Group importance measures are investigated in relation to dependent failures. Dynamic risk importance measures, for example, can be formulated separately for each failure state combination of a common cause failure group. An interesting question is how the time aspect of DFM is considered in group importance measures. In addition to failure nodes and random nodes, different stochastic node types will be developed when some component reliability models are implemented in YADRAT. The computation of dynamic risk importance measures has to be studied in relation to different dynamic constraints of stochastic nodes.

The main challenge in DFM tool development is to provide trustworthy results in a reasonable calculation time. In the dynamic risk importance measure calculation, this means that it is usually better to compute approximations rather than to try to aim for accurate values. It is also important in the development of dynamic risk importance measures in DFM to consider what information is actually useful, as the main objective of risk importance measures is to provide guidance for the system's design. The information given by importance measures needs to be kept simple enough so that the analysts can interpret it.

8. Conclusion

The dynamic risk importance measures use all the information that is available in prime implicants of DFM to measure significances of node's states unlike any other importance measure. With dynamic risk importance measures calculated for different failure states of components and states of failure nodes, the component's influence on the system's reliability can be analysed more comprehensively than with just risk importance measures calculated for failure events. As the dynamic Fussell-Vesely is calculated for time steps, it is also possible to judge at which points of the time line certain failures and conditions need to occur to contribute to the top event.

Acknowledgements

The author would like to thank Kim Björkman, Jan-Erik Holmberg, Ahti Salo, Antti Toppila and other participants of the seminar on scientific publishing for their help, not to forget Ilkka Männistö.

References

[1] Van Der Borst M, Schoonakker H. An overview of PSA importance measures. Reliability Engineering and System Safety. 2001; 72:241-5.

[2] Zio E. Risk importance measures. In: Pham H. Safety and risk modeling and its applications. London: Springer-Verlag; 2011. p. 151-95.

[3] Kuo W, Zhu X. Some recent advances on importance measures in reliability. IEEE transactions on Reliability. 2012; 61:344-60.

[4] Kuo W, Zhu X. Relations and generalizations of importance measures in reliability. IEEE transactions on Reliability. 2012; 61:659-74.

[5] Labeau PE, Smidts C, Swaminathan S. Dynamic reliability: Towards an integrated platform for probabilistic risk assessment. Reliability Engineering and System Safety. 2000; 68:219-54.

[6] Cepin M. Fault tree analysis. In: Cepin M. Assessment of Power System Reliability - Methods and Applications. London: Springer; 2011. p. 61-87.

[7] Rauzy A. Binary decision diagrams for reliability studies. In: Mistra KB. Handbook of performability engineering. London: Springer; 2008. p. 381-96.

[8] Do Van P, Barros A, Bérenguer C. Reliability importance analysis of Markovian systems at steady state using perturbation analysis. Reliability Engineering and System Safety. 2008; 93:1605-15.

[9] Garrett CJ, Guarro SB, Apostolakis GE. The dynamic flowgraph methodology for assessing the dependability of embedded software systems. IEEE transactions on Systems, Man and Cybernetics. 1995; 25:824-40.

[10] Al-Dabbagh AW, Lu L. Reliability modeling of networked control systems using dynamic flowgraph methodology. Reliability Engineering and System Safety. 2010; 95:1202-9.

[11] Al-Dabbagh AW, Lu L. Dynamic flowgraph modeling of process and control systems of a nuclear-based hydrogen production plant. International Journal of Hydrogen Energy. 2010; 35:9569-80.

[12] Björkman K. Solving dynamic flowgraph methodology models using binary decision diagrams. Reliability Engineering and System Safety. 2013; 111:206-16.

[13] Tyrväinen T, Björkman K. Modelling common cause failures and computing risk importance measures in the dynamic flowgraph methodology. Proceedings of the 11th International Probabilistic Safety Assessment and Management Conference & The Annual European Safety and Reliability Conference; 2012 Jun 25-29; Helsinki, Finland. Helsinki: The International Association for Probabilistic Safety Assessment and Management (IAPSAM); 2012. 30-Th4-1.

[14] Karanta I. Importance measures for the dynamic flowgraph methodology. Espoo (Finland): VTT Technical Research Centre of Finland, Systems Research; 2011 Dec. Report No. VTT-R-00525-11.

[15] Houtermans MJM. A method for dynamic process hazard analysis and integrated process safety management [doctoral thesis]. Eindhoven (Netherlands): Technische Universiteit Eindhoven; 2001 May. http://alexandria.tue.nl/extra2/200111699.pdf.

[16] Aldemir T, Guarro SB, Mandelli D, Kirschenbaum J, Mangan LA, Bucci P, et al. Probabilistic risk assessment modeling of digital instrumentation and control systems using two dynamic methodologies. Reliability Engineering and System Safety. 2010; 95:1011-39.

[17] Huang CY, Chang YR. An improved decomposition scheme for assessing the reliability of embedded systems by using dynamic fault trees. Reliability Engineering and System Safety. 2007; 92:1403-12.

[18] Do Van P, Barros A, Bérenguer C. From differential to difference im-

portance measures for Markov reliability models. European Journal of Operational Research. 2010; 204:513-21.

[19] Ramirez-Marquez JE, Rocco CM, Gebre BA, Coit DW, Tortorella M. New insights on multi-state component criticality and importance. Reliability Engineering and System Safety. 2006; 91:894-904.

[20] Levitin G, Podofillini L, Zio E. Generalised importance measures for multi-state elements based on performance level restrictions. Reliability Engineering and System Safety. 2003; 82:287-98.

[21] Ramirez-Marquez JE, Coit DW. Composite importance measures for multi-state systems with multi-state components. IEEE transactions on Reliability. 2005; 54:517-29.

[22] Burdick GR, Fussell JB, Rasmuson DM, Wilson JR. Phased mission analysis: A review of new developments and an application. IEEE transactions on Reliability. 1977; R-26:43-49.

[23] Vaurio JK. Importance measures for multi-phase missions. Reliability Engineering and System Safety. 2011; 96:230-235.

[24] Contini S, Cojazzi GGM, Renda G. On the use of non-coherent fault trees in safety and security studies. Reliability Engineering and System Safety. 2008; 93:1886-95.

[25] Mankamo T, Pörn K, Holmberg JE. Uses of risk importance measures. Technical report. Espoo (Finland): VTT Technical Research Centre of Finland; 1991. VTT Research notes 1245. ISBN 951-38-3877-3.

[26] Borgonovo E, Apostolakis GE. A new importance measure for risk-informed decision making. Reliability Engineering and System Safety. 2001; 72:193-212.

Appendix A. Backtracking algorithm example

This section presents how the backtracking algorithm presented in Figures 1 and 2 progresses step by step in the backtracking example of Section 4.5. Some parts of the process are cut out to keep the length of the example moderate. The state probabilities of node A at time step $-u$ are represented by a vector $SP(A(-u)) = (a_{u,0}, a_{u,1}, ..., a_{u,b})$, where b is the number of states of A and $a_{u,s}$ is the probability of state s. All calculated state probabilities are always stored. The backtracking process starts from the component node at the failure time:

1. Component node C at $-t = -1$.

2. The input nodes are F, N and C.

2.1. Examine F.

2.1.1. The time lag $l = 0$.

2.1.2. The node type is failure node.

2.1.3. $-t = -1 \neq -3$.

2.1.4. The prime implicant does not contain a literal of the form $F(-u) = 0, -u \geq -1$.

2.1.5. The prime implicant contains literal $F(-1) = 1$.

2.1.6. The probability for state 1 is 1.

2.1.7. $SP(F(-1)) = (0, 1)$.

2.2. Examine N.

2.2.1. The time lag $l = 0$.

2.2.2. The node type is deterministic node.

2.2.3. $-t - l = -1 > -3$.

2.2.4. $-t = -t - l = -1$.

2.2.5. Deterministic node N at $-t = -1$.

2.2.6. The input nodes are R, T and N

2.2.6.1. Examine R.

2.2.6.1.1. The time lag $l = 1$.

2.2.6.1.2. The node type is random node.

2.2.6.1.3. The prime implicant does not contain a literal representing R at $-t - l = -2$.

2.2.6.1.4. State probabilities $r_{2,0}$ and $r_{2,1}$ are obtained from the probability parameters.

2.2.6.1.5. $SP(R(-2)) = (r_{2,0}, r_{2,1})$.

2.2.6.2. Examine T.

2.2.6.2.1. The time lag $l = 0$.

⋮

2.2.6.2.x. $SP(T(-1)) = (t_{1,0}, t_{1,1}, t_{1,2})$.

⋮

2.2.6.3. Examine N.

2.2.6.3.1. The time lag $l = 1$.

⋮

2.2.6.3.x. $SP(N(-2)) = (n_{2,-1}, n_{2,0}, n_{2,1})$.

⋮

⋮

2.2.x. $SP(N(-1)) = (n_{1,-1}, n_{1,0}, n_{1,1})$.

⋮

2.3. Examine C.

2.3.1. The time lag $l = 1$.

2.3.2. The node type is deterministic node.

2.3.3. $-t - l = -2 \geq -3$.

2.3.4. $-t = -t - l = -2$.

2.3.5. Deterministic node N at $-t = -2$.

2.3.6. The input nodes are F, N and C.

⋮

2.3.8. $SP(C(-2)) = (c_{2,0}, c_{2,1}) = (n_{2,-1} + n_{2,0}c_{3,0}, n_{2,1} + n_{2,0}c_{3,1})$ (calculated in Section 4.5).

2.3.9. This node is component node C but $-t = -2$ is not the failure time -1.

2.3.10. The time lag $l = 1$.

2.3.11. $-t = -t + l = -1$.

3. State probabilities are calculated by summing the probabilities of the rows in Table A.10:

$$c_{1,0} = n_{1,-1}c_{2,0} + n_{1,0}c_{2,0} + n_{1,1}c_{2,0} = c_{2,0} = n_{2,-1} + n_{2,0}c_{3,0} \qquad \text{(A.1)}$$

and

$$c_{1,1} = n_{1,-1}c_{2,1} + n_{1,0}c_{2,1} + n_{1,1}c_{2,1} = c_{2,1} = n_{2,1} + n_{2,0}c_{3,1}. \qquad \text{(A.2)}$$

Table A.10: Probabilities of the rows in the decision table of C

	Output	**Inputs**			**Prob**
Node	C	F	N	C	
Time lag		0	0	1	
	0	0	-1	0	$0 \cdot n_{1,-1} \cdot c_{2,0} = 0$
	0	0	-1	1	$0 \cdot n_{1,-1} \cdot c_{2,1} = 0$
	0	0	0	0	$0 \cdot n_{1,0} \cdot c_{2,0} = 0$
	1	0	0	1	$0 \cdot n_{1,0} \cdot c_{2,1} = 0$
	1	0	1	0	$0 \cdot n_{1,1} \cdot c_{2,0} = 0$
	1	0	1	1	$0 \cdot n_{1,1} \cdot c_{2,1} = 0$
	0	1	-1	0	$1 \cdot n_{1,-1} \cdot c_{2,0} = n_{1,-1}c_{2,0}$
	1	1	-1	1	$1 \cdot n_{1,-1} \cdot c_{2,1} = n_{1,-1}c_{2,1}$
	0	1	0	0	$1 \cdot n_{1,0} \cdot c_{2,0} = n_{1,0}c_{2,0}$
	1	1	0	1	$1 \cdot n_{1,0} \cdot c_{2,1} = n_{1,0}c_{2,1}$
	0	1	1	0	$1 \cdot n_{1,1} \cdot c_{2,0} = n_{1,1}c_{2,0}$
	1	1	1	1	$1 \cdot n_{1,1} \cdot c_{2,1} = n_{1,1}c_{2,1}$

4. $SP(C(-1)) = (n_{2,-1} + n_{2,0}c_{3,0}, n_{2,1} + n_{2,0}c_{3,1})$.
5. This node is C and $-t = -1$.
6. Failure state probabilities are $n_{2,-1} + n_{2,0}c_{3,0}$ and $n_{2,1} + n_{2,0}c_{3,1}$.

Appendix B. Emergency core cooling system model

Each node of the emergency core cooling system model presented in Figure 8 is briefly described in Table B.1.

Table B.1: The nodes of the emergency core cooling system model (Figure 8).

Node	**Description**
EHL	Is true if the water level measurement is high. The node is used in controlling the valve.
ELL	Is true if the water level measurement is low. The node is needed for starting the pump and opening the valve.
HL	Is true if the water level measurement is high. The valve can open only if this node is true.
HL-TD	Time delay condition for the closing of the valve.
LL	Is true if the water level measurement is low. The node is used in controlling the valve.
LP	Is true if the pressure measurement is low. The node is needed for opening the valve.
LP-TD	Time delay condition for the first opening of the valve.
P	Represents pump which can be on or off. The pump is controlled by start and stop commands.
PL	Is true if pump leakage signal is sent. If the signal is sent, the pump is commanded to stop and the valve commanded to close.
PM	Represents pressure measurement which can be low or high. It is assumed that the pressure is high/low every other time step.
P-STA	Start command is sent to the pump when this node is true.
P-STO	Stop command is sent to the pump when this node is true.
V	Represents valve which can be open or closed. The valve is controlled by open and close commands.
VC	Close command is sent to the valve when this node is true.
VO	Open command is sent to the valve when this node is true.
WF	Water flow is high if the pump line pumps water into the pressure vessel.
WL	Represents water level which can be low, medium or high. Level rises if water flow is high and lowers if water flow is low.
WLM	Water level measurement measures the water level from previous time step.