Modelling and Analysis of Fire Sprinklers by Verifying Dynamic Fault Trees

Shahid Khan, Joost-Pieter Katoen
Software Modeling and Verification
RWTH Aachen University, Germany
{shahid.khan, katoen}@cs.rwth-aachen.de

Matthias Volk*
Formal Methods and Tools
University of Twente, The Netherlands
m.volk@utwente.nl

Ahmad Zafar, Falak Sher
DGB Technologies Pvt.
Lahore, Pakistan
{ahmad.zafar,chfalak}@dgbtek.com

***Abstract*—We study the reliability analysis of fire sprinkler systems. We show that the characteristic features of Dugan's dynamic fault trees (DFTs) such as spare management, temporal ordering of failures and functional dependencies, are natural and adequate mechanisms to model various relevant phenomena in realistic fire sprinklers. For DFT analysis, we employ probabilistic model checking, an automated technique to assess reliability along with correctness. This is to date the most scalable, numerical DFT analysis technique. We show how standard reliability measures of fire sprinkler systems can be efficiently computed using the STORM model checker. In addition, we consider metrics beyond standard reliability, e.g., the probability to fail without going through a degradation phase and the worst-case reliability achieved after degradation. We illustrate our approach by fire sprinkler systems in shopping centers.**

***Keywords*—Reliability; dependability; formal methods; probabilistic model checking; fault trees; fire safety analysis**

I. INTRODUCTION

Fire protection systems [1] are used to implement safety functions. They 1) detect, 2) localise, 3) report and 4) extinguish fire outbreaks. They consist of two subsystems: *fire detection*, and *fire suppression*. The former uses sensors and feedback loops to identify the presence of fire. A detected fire is reported to the fire brigade and personnel to initiate fire hazard procedures. Fire *suppression* systems aim to extinguish the fire to diminish the hazardous consequences of an outbreak. A fire protection system's effectiveness depends on its *efficacy* and *reliability*. The *efficacy* quantifies the success of the protection system on a fire outbreak – what is the probability that the fire is extinguished? The *reliability* is the probability that the protection system reacts to a fire outbreak by sending emergency signals and starting the extinguishing process. This paper focuses on the *reliability* aspects.

In this paper we develop a systematic approach for 1) *modelling* fire suppression systems by taking into account their most common elements and mechanisms, and 2) *analysing* the reliability of such models in a fully automated manner. Our approach combines dynamic fault trees (DFTs) [2] and probabilistic model checking (PMC) [3]. Our goals are 1) to demonstrate how the ingredients of DFTs are a natural fit to adequately model various system phenomena in fire sprinkler systems, and 2) to show how PMC techniques can numerically calculate standard reliability metrics and beyond of such systems. We consider the fire sprinkler systems of [4].

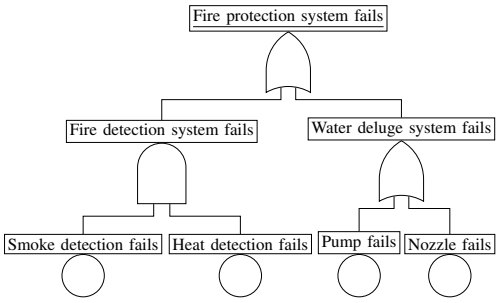

Fig. 1: SFT example of a fire protection system.

Static fault trees (SFT) [5] provide a top-down modelling approach widely used in reliability and safety engineering. SFTs are rooted directed acyclic graphs consisting of basic events and gates. Basic events represent the failure modes, whereas gates are logical connectives (AND, OR and their generalisation VOT) describing how these failure modes lead to the occurrence of an undesired event, i.e., top event. The top event (root) represents a system's failure. Fig. 1 shows a small sample SFT from [1] modelling a fire protection system consisting of a fire detection and a water deluge system. The failure of any of these subsystems leads to system failure. SFTs can be efficiently analysed using binary decision diagrams [5]. SFTs are popular in the industry but are incapable to model complex interdependencies of component failure modes such as temporal ordering and spare management. This has led to various dynamic extensions of SFTs [5].

Dynamic fault trees (DFTs) [2] are a prominent dynamic extension with PAND, SEQ, FDEP and SPARE as dynamic gates. These dynamic gates model temporal failure interdependencies. For instance, a PAND fails if its inputs fail in left-to-right order; if an input fails out-of-order, the PAND becomes fail-safe, i.e., it cannot fail anymore. An SEQ gate forces the failure order of its inputs. In contrast to a PAND, the failure of SEQ inputs cannot violate the imposed order. An FDEP gate models the direct dependence of one component failure on another. The SPARE manages a pool of spare subsystems and enables replacing of a failed component by a spare one. The enhanced expressive power of DFTs comes at the price of an involved interpretation [6] and an expensive analysis. Possible interpretations of DFTs, including the one used in this paper, are presented in [7]. Both qualitative and quantitative analyses of DFTs are considered in the literature.

*The work was done while M. Volk was at RWTH Aachen University.

| //$31.00 ©10.1109/LADC53747.2021.9672579

978-1-6654-7831-1/21/$31.00 ©2021 IEEE

The qualitative analysis is performed using cut sequences [8], the analogue of cut sets in SFTs. The quantitative analysis amounts to computing metrics such as the unreliability and the mean time to failure and cannot be accurately performed using cut sequences [6]. We consider quantitative analysis.

The quantitative analysis of a DFT is performed on its underlying continuous-time Markov chain (CTMC) [9]. Existing approaches either directly translate a DFT into a CTMC in a monolithic or compositional way, or via an intermediate model such as a Bayesian network or a generalised stochastic Petri net, see [5] for a detailed survey. Existing CTMC analysis techniques such as numerically computing transient and stationary distributions or discrete-event simulation can then be employed. Instead, we use probabilistic model checking [9], a fully automated technique which checks metrics – described in temporal logic – on probabilistic models. The flexibility of using logic enables determining a plethora of existing reliability measures and beyond. The main bottleneck is not the numerical analysis of the CTMC, but the efficient generation of such CTMCs from DFTs. Recent improvements in the CTMC-from-DFT generation [10] have led to a significant boost in scalability. Key techniques are symmetry detection (detecting similar substructures in a DFT), partial-order reduction (avoiding to consider state sequences that are permutations of equivalent ones), and modularisation (a known concept in DFT analysis) [11]. This is supported by STORM [12] which is a competitive probabilistic model checker (see qcomp.org).

This paper 1) illustrates that various reliability phenomena in fire sprinkler systems can be adequately modelled with DFTs (but not with SFTs), 2) exploits these observations to obtain a refined and more accurate fault tree model for the fire sprinkler system modelled as SFT in [4], and 3) uses probabilistic model checking to obtain probability per demand and hour, standard reliability metrics, as well as metrics that go beyond typical ones in a computation time of few seconds.

The paper is organised as follows. Sect. II presents preliminaries. Sect. III discusses various scenarios that require dynamic gates. Sect. IV introduces PMC and the considered reliability metrics. Sect. V presents the analysis results. Finally, Sec. VI concludes and presents future work.

II. PRELIMINARIES

A. Dynamic Fault Trees

DFTs were introduced by Dugan *et al.* [2] to mitigate the lack of expressiveness of SFTs. DFTs have four new gates: SPARE, PAND, FDEP and SEQ. DFTs were originally conceived to model non-repairable systems. (Its extensions towards repairs is a topic of current research.) We show the DFT gates and basic events in Fig. 2 and discuss here:

a) VOT: This gate, also called *KofN* gate, has two integer parameters, i.e., k and n with $1 \leq k \leq n$. Its output becomes true upon the failure of at least k inputs. AND and OR are special cases of VOT with $k{=}n$ and $k{=}1$, respectively.

b) PAND: This gate is similar to AND, i.e., the output of this gate becomes true once all inputs have failed. An additional constraint is that inputs must fail in a strict left-to-right order. Any out-of-order failure brings the PAND gate into a *fail-safe* state. Two variants of PAND exist: 1) inclusive PAND ($\text{PAND}_{\leq}$) where the simultaneous failure of inputs causes the output to fail and 2) exclusive PAND ($\text{PAND}_{<}$) where such simultaneous failure does not lead to a gate failure.

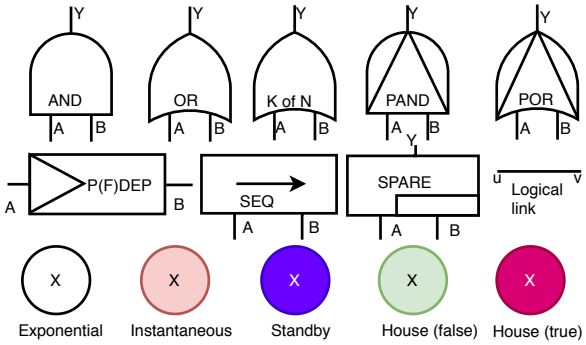

Fig. 2: DFT elements

c) POR: This gate is similar to OR, but it imposes an ordering constraint on the input failures: its output becomes true when the left-most input fails before the other inputs. The gate has inclusive ($\text{POR}_{\leq}$) and exclusive ($\text{POR}_{<}$) variants.

d) SPARE: This gate models spare management. It has one primary and at least one spare input. The children of SPARE have two operating modes: *active* and *standby*. The failure rate of a SPARE child in *standby* mode is modelled using a dormancy factor δ: $\delta{=}0$ ($\delta{=}1$) models a cold (hot) spare and $0 < \delta < 1$ a warm spare. Initially, SPARE activates its primary input and upon failure of the primary input, the gate claims and activates the spare input. The output of SPARE becomes true when all its claimed children failed and there is no child left to claim. As spare inputs can be shared among several SPARE gates—like a pool of spares shared by several subsystems—*spare races* can occur. A spare race is a scenario where at least two SPARE gates attempt to claim a shared spare child simultaneously. As a child can be claimed by at most one SPARE, a conflict occurs [13]. Such races are resolved using priorities, probabilities or non-deterministically.

e) PDEP: This gate is used to model common cause failures and imperfect coverage. It has a parameter $p \in [0, 1]$, a *trigger* and at least one dependent input. Upon failure of the trigger input, PDEP forces all dependent inputs to fail with a probability p. FDEP is a special case of this gate with $p{=}1$.

f) SEQ: This gate imposes an order on the failure of its inputs, i.e., the inputs must fail in left-to-right order. This gate has a dummy output (not connected anywhere in the DFT).

g) Basic events: These DFT elements are used to model the failure behaviours of elementary system components, see the last row of Fig. 2. The exponential basic event (EXP) models failures that occur according to a negative exponential distribution. The instantaneous type basic event (INST) models Bernoulli trials, i.e., on-demand failures. The standby type basic event (STDBY) models components having both standby and active behaviour. It has two associated failure rates: 1) active λ_a and 2) passive $\lambda_p = \delta \cdot \lambda_a$. STDBY is used

in conjunction with SPARE as there is no other activation controlling mechanism in DFTs. Two types of house events, i.e., false and true, are used to model given-fail and fail-safe behaviour, respectively. A house-true type basic event fails at the beginning of DFT analysis and remains failed thereafter. The complementary behaviour is achieved through house-false type basic event. It never fails throughout the DFT analysis.

DFTs are more expressive than SFTs. In our view, they are better suited to model fire suppression systems. We motivate their usage by modelling a monitored switch. It transfers the load from street power to a diesel generator which is in cold standby and is activated once the street power fails. This is naturally modelled by the SPARE gate (both sources fail) in Fig. 3. The switch should be operational before the street power fails as otherwise the system cannot perform the switching. If the transfer switch fails prior to a street power failure, the system immediately fails. Once the system has successfully switched to the diesel generator source, a failure of the switch does no longer contributes to a system failure. This is all modelled by the PAND gate (switching fails). The diesel generator is initially standby, i.e., it cannot fail unless switched to active mode. With a certain probability it fails to switch to active mode—this is also called failure on-demand. Such on-demand failures of backup sources and reconfiguration mechanisms are modelled by a PDEP gate. It models the scenario that upon failure of the street power, the diesel generator also fails with probability p which is the parameter of the PDEP gate.

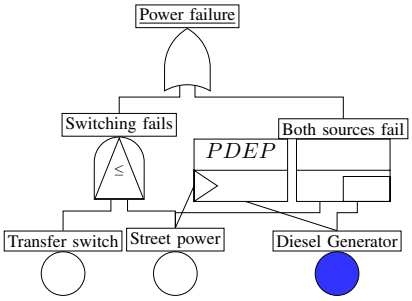

Fig. 3: DFT example

B. Case Study: Fire Suppression in Shopping Centers

We demonstrate our approach for sprinkler systems. They are pervasively used as fire suppression systems – about 40 million sprinkler heads are fitted per year. Buildings such as shopping centers, office centers, skyscrapers, data centers are equipped with sprinkler systems. Their effectiveness has been extensively studied [14]. Sprinkler systems exist in many design variants, e.g., wet pipe, dry pipe, foam-based, deluge type, etc. In wet-pipe sprinkler systems, pressurized water is available behind the sprinkler head. An increase in ambient temperature causes the breakage of the temperature-sensitive glass tube in the sprinkler head which in turn removes its seal and showers water through the head. In contrast, dry-pipe systems have air pressure in their pipes and water flows through pipes in case of a significant pressure drop in the pipes of the sprinkler system. Dry-pipe systems are often used at places with freezing temperatures. This paper focuses on the wet-pipe fire sprinkler systems of Australian shopping centers as reported by Moinuddin *et al.* [4]. They modelled the sprinkler systems as SFTs for the reliability analysis. Data was

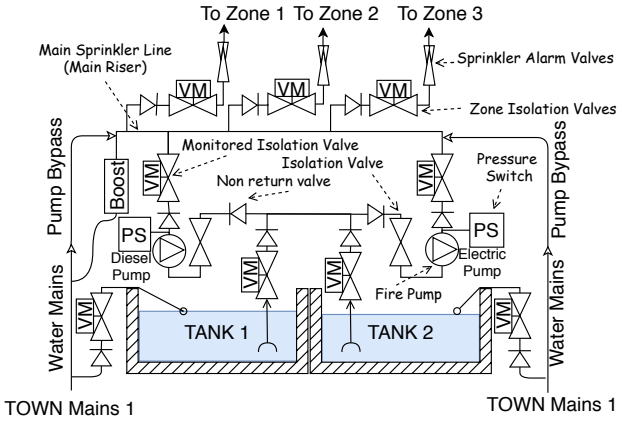

Fig. 4: Schematic of sprinkler system adopted from [4]

collected by a physical survey of eighteen shopping centers and combined with failure rates from the literature. Here, we discuss the details necessary to understand our work and the work of [4] on fire protection systems. We start with the hydraulic and electrical systems of the case study and then discuss the failure rates of basic events.

a) Hydraulic schematic: Fig. 4 depicts an abridged version of our case study (adopted Fig. 1 of [4]). The sprinkler system consists of two basement water tanks. Each tank is supplied by water mains through a non-return valve and a monitored isolation valve. The non-return valves are used to prevent backward water flow so that the water mains are not contaminated. The outlet of the water tanks is mutually connected through a monitored isolation valve and non-return valves. This mutually connected output is then fed to the diesel/electric fire pump sets which are actuated through a pressure switch whenever the pressure in the sprinkler system critically drops. In case of leaks or temperature-related pressure changes in the pipes of the sprinkler system, a jacking pump (not shown in Fig. 4) is used to maintain the pressure. The booster shown top-left in the schematic is primarily related to the fire brigade and is not part of our fault tree analysis. The generators and booster assemblies maintain pressure in the sprinkler lines. If the mains water pressure is significantly high, the pump assemblies are bypassed to directly feed the sprinkler system lines. Once we have significant pressure in the main sprinkler line (a.k.a.: riser), the water is distributed to different zones. Each distribution line has non-return valves, zone isolation valves and sprinkler alarm valves. Zone isolation valves are operated during maintenance-related activities. Each sprinkler zone consists of risers, range pipes (and possibly arm pipes), pipe support, and sprinkler heads.

b) Electric schematic: Although the detailed electric system is neither the focus of this paper nor provided in [4], we provide an abstract diagram in Fig. 5 of electrical connections to put our subsequent discussion into context. Several feedback and alarm signals are generated by the valves of the sprinkler system. These signals are wired to a *fire indication panel* (FIP) that indicates the status of various parts of the sprinkler system. The FIP is usually monitored by personnel. The signals are

also sent to the fire brigade for advice in case of a fire outbreak or other emergencies, e.g., no water is coming from the mains water source or water is tampered with. The FIP is powered by main power and has a standby energy source, i.e., UPS or backup batteries. The sprinkler system is powered by AC mains and a backup diesel generator. Switching between the AC mains and the diesel generator is achieved through an automatic transfer switch. The diesel fire pump also requires the power for initial drive (like a starter motor). Valves also require power to function but this is ignored here.

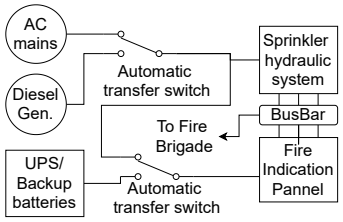

Fig. 5: Electrical diagram

Failure rates. Quantifying failure rates is a key step in reliability analysis. We discuss some relevant concepts. Failure rates define the frequency of failures. We let failure rates be governed by negative exponential distributions. The failure rate λ is defined per unit of time or demand. The routine maintenance (*proof test*) event is considered a *demand*. (This distinction of per time unit or demand is drawn in safety standards like ISO-26262 and IEC-61508 for high- and low-demand modes of operation.) Failure modes of safety functions are categorized as safe and dangerous. The former does (the latter does not) lead to the shut down of the system. Dangerous failure modes are divided into *dangerous detected* (they occur with rate λ_{DD} and are detected in self-diagnostic tests.) and *dangerous undetected* failure modes (they occur with rate λ_{DU} and are detected in proof tests.) Thus, the dangerous failure rate (λ_D) is $\lambda_D = \lambda_{DD} + \lambda_{DU}$. The dangerous detected failures are immediately repaired (or replaced), and the assumption of "as good as new" is applied. In this work, let

- *PFD(t)* be the probability of being in a failed state at time t due to a dangerous failure, i.e., $PFD(t) = 1 - e^{-\lambda_D \cdot t}$,
- *PFH* be the probability of dangerous failure per hour also called failure rate or failure frequency, and
- PFD_{avg} be the average probability of dangerous failure per demand, $PFD_{avg} = \frac{1}{T_p} \cdot \int_0^{T_p} PFD(t)\, dt$ where T_p is the proof test period.

IEC-61508 recommends *PFH* (PFD_{avg}) computation for high- (low-) demand modes of operation. As discussed by [15], $PFD_{avg} \approx PFH \cdot \frac{T_p}{2}$. Let $\lambda_D \cdot T_p << 1$, then $PFD_{avg} = \frac{1}{T_p} \int_0^{T_p} 1 - e^{-\lambda_D \cdot t}\, dt \approx \lambda_D \frac{T_P}{2}$. Thus, $PFH \approx \lambda_D$.

Now, we discuss the survey-based approach of [16] to compute the failure rate per demand from inventory data. [16] counted the total number of components and the number of failed component and calculated the *failure rate per year* as:

$$\frac{\text{total failures}}{\text{total number of components} \times \text{total number of years data available}}$$

This holds due to the memoryless property of the exponential distribution. As a next step, [16] obtained the proof test period T_p (in years) from the standard AS $1851-2005$ (superseded by AS $1851-2012$) and computed *failure rate per demand* as:

$$\textit{failure rate per year} \times T_p$$

The failure rates are assumed to be normally distributed.

TABLE I: Failure rates of fire sprinkler components

Component	Failure rate per demand	Maint. interval years	Failure rate per hour
Alarm check valve	6.67E-04	0.0833	9.14E-07
Main storm valve	8.14E-03	0.0833	1.12E-05
Zone Isolation valve	7.87E-03	0.0833	1.08E-05
Isolation valve	7.05E-04	0.0833	9.66E-07
Non-return valve	1.09E-03	0.0833	1.49E-06
Alarm motor	4.98E-03	0.0833	6.82E-06
Town main connection	1.06E-03	0.0833	1.45E-06
Water supply line	4.34E-06	0.0833	5.95E-09
Mains power	1.11E-03	0.0833	1.52E-06
Pressure switch	1.71E-03	0.0833	2.34E-06
Operator failure	3.00E-02	0.0833	4.11E-05
Sprinkler head	7.90E-02	0.0833	1.08E-04
FIP fire alarm panel	4.32E-02	0.0833	5.92E-05
FIP UPS/batteries	3.19E-02	0.0833	4.37E-05
Monitor alarm sensor	4.40E-03	0.0833	6.03E-06
Jacking pump	3.04E-04	0.0833	4.16E-07
Diesel pump	3.57E-04	0.0833	4.89E-07
Electric pump	7.44E-04	0.0833	1.02E-06
Diesel pump batteries	1.39E-02	0.0833	1.90E-05
Storage tank	2.09E-04	12	1.99E-09
Power generator	2.35E-03	0.0833	3.22E-06
UG pipe corroded	3.24E-05	1	3.70E-09
Wiring burnout	2.19E-04	0.0833	3.00E-07
Aut. transfer switch	1.71E-03	0.0833	2.34E-06
HW transient uncovered	1.00E-07	0.0833	1.37E-10
HW transient safety	1.00E-06	0.0833	1.37E-09
HW transient covered	9.90E-06	0.0833	1.36E-08
HW permanent covered	1.00E-08	0.0833	1.37E-11
HW permanent safety	1.00E-06	0.0833	1.37E-09
HW permanent covered	9.90E-07	0.0833	1.36E-09

For our case study, we had only *failure rates per demand* provided by [4]. We computed *failure rates per hour* using the approach of [16] in reverse. That is, we obtained failure rates per demand from [4], the maintenance interval from AS $1851-2012$ and computed the *failure rate per hour* as:

$$\frac{\textit{failure rate per demand}}{T_p} \times \frac{1}{8760}$$

The computed failure rates are provided in Table I. We could not find T_p for some components in the standard, for example, there is no direct entry for underground pipe corrosion checks in AS $1851-2012$; we assumed one year because this is the maintenance plan for corrosion checks of pipes and hangers in the standard. Similarly, AS $1851-2012$ recommends running the fire pumps on alternative power supplies for three minutes every six months. This six-month maintenance test should not undermine the monthly maintenance of diesel generator. Therefore, we choose one month T_p for diesel generator.

We conclude by discussing the sprinkler head. The maintenance standard recommends checking sprinkler inventory and sprinkler spanners every month. The installed sprinkler is inspected every six months for impairing conditions like physical damage, contamination, and paint on the heat response element of the sprinkler head. The detailed tests, including functional tests, leak resistance, and release temperature tests are recommended in 10, 25, and 30 yearly plan of AS1815-2012. The failure rates for sprinkler heads as used by [17] are

adopted from [18] who reported on 500 failures out of total 6350 heads yielding a failure rate per demand of $\frac{500}{6350} = 0.079$. Several failure modes causing the failure of sprinkler heads are discussed by [18]. They benchmarked the AS 1851.3 recommendation, i.e., a sprinkler head should be tested after 24 years of use and every six years thereafter. We assume one month T_p for the sprinkler head. The sprinkler head failure per hour is $\frac{500}{6350 \times 0.0833 \times 8760} = 1.08E{-}04$.

III. DFT Modelling

In this section, we discuss several aspects of sprinkler systems and illustrate how they can be naturally modelled using the dynamic features of DFTs. A general overview is given in Table II. We contrast the dynamic models to the SFT models of fire sprinkler systems given in [4]. We provide four (A to D) categories along with various examples.

A: Standby behaviours. System components can exhibit different failure behaviours in active and standby mode. We give some examples for the sprinkler system: **A.1: Diesel fire pump.** The *diesel fire pumps* are used along with electric fire pumps to maintain dropping water pressure in the main riser. Upon detecting a drop in the water pressure, electric pumps are started. If the water pressure drops further, diesel pumps are put in operation. The starting of the diesel fire pumps require an initial driving force, also called the cranking cycle/process. This driving force is provided by an electric motor that is part of the generator assembly. The electric power for this motor consists of a power supply and backup batteries ($12\ V$ or $24\ V$) depending on the size of the machine. (A similar mechanism is captured by the models in [4].) The batteries are initially in standby, and they only start depleting upon usage after the power supply fails. This is an example of standby behaviour.

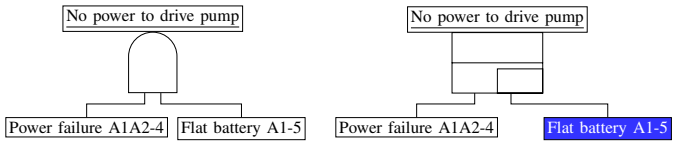

Fig. 6: Diesel pump drive: SFT from [4] (left) and DFT (right)

Fig. 6 (left) shows the SFT fragment from [4], whereas Fig. 6 (right) depicts a DFT model. We use boxes to represent gate inputs that represent subtrees. We use a SPARE gate rather than an AND gate and thus make battery depletion standby. The dormancy factor is set to zero, i.e., cold SPARE behaviour. We name SFT elements and the corresponding DFT elements identical to [4] to maintain the traceability. Blue boxes indicate the replacement of a relevant basic event in the subtree with standby events. The subtree *Flat battery A1-5* is discussed in Sect. C.2. Informally speaking, *Flat battery A1-5* is initially in cold standby mode, i.e., it cannot fail. Once *Power failure A1A2-4* fails, the SPARE gate activates its spare input, i.e., *Flat battery A1-5*. Such dynamic behaviour cannot be modelled in SFTs, see Fig. 6 (left), where the battery is always in an active mode and it can fail before the failure of power. Batteries can also fail due to other failure modes, e.g., exposure to high temperatures and the formation of gasses within battery cells but this is not considered here.

TABLE II: DFT modelling for common behaviours

Behaviour	DFT modelling
Standby behaviour	model with SPARE-gate
Common cause failures	model with FDEPs
Monitoring mechanism failures	model with PAND-gate
Complex BEs	create dedicated DFT sub-tree

A.2: Fire indication panel supply. Another example of standby behaviour are the *FIP backup power supplies*. Initially, it is powered by the main supply and it resorts to backup UPS and battery upon failure of the mains supply. The UPS and backup battery failure rates are merged into a single basic event. Without providing a further breakdown of UPS and batteries, we model this standby behaviour by a SPARE gate.
A.3: Mains power. Another standby behaviour is the *mains power* mechanism. The mains supply is taken from the street power and a generator is available as a backup source. As seen before, such behaviour is faithfully modelled by a SPARE.

B: Common cause failures. The causes that lead to the failure of more than one component/subsystem are called common causes. We provide some examples of common cause failures and argue that they are adequately modelled by FDEP gates.

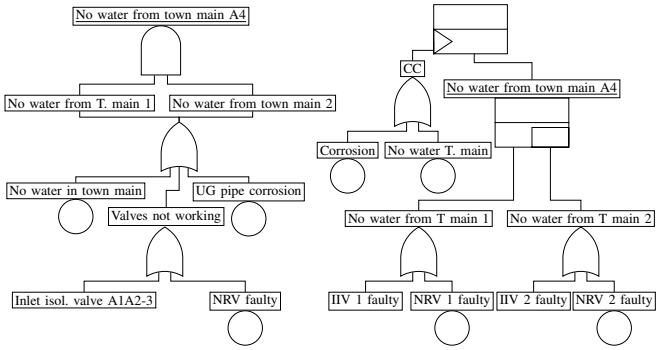

Fig. 7: Corrosion CC: SFT from [4] (left) and DFT (right)

B.1: Corrosion. In smaller buildings, town mains can directly supply water to the riser and standby storage tanks are also used, see also [4]. *Corrosion* is a possible cause of underground supply pipes failure. Halting the supply of the mains pipe causes a failure of the storage tanks: as there is no supply of water to the storage tank, the storage tanks cannot perform their function anymore. DFTs can model common causes by the corrosion effect through FDEPs, see Fig. 7 (right). In [4], the valve behaviour is merged into one basic event, in fact, each tank has a separate inlet as shown in Fig. 4. We propose to split this DFT as there is a separate set of valves for each storage tank, and we consider their failures separately. The DFT should be contrasted to the SFT of Fig. 7 (left).
B.2: Riser failure. Another common cause failure is the *water supply pipe (a.k.a.: main riser) damage*. A failure of the water supply pipe causes the failure of both pumps. This might seem surprising at first glance, but the water pipe is an interface failure. In this view, if the interface is unavailable it does not make sense to consider the pumps to be functioning. The

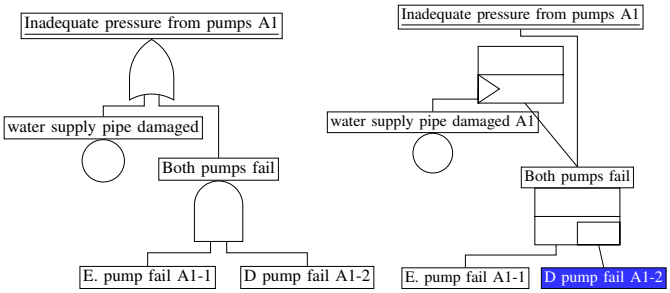

Fig. 8: Main riser CC: SFT from [4] (left) and DFT (right)

pumps do not fail according to their own failure rate, but with the failure rate of the water supply pipe. This common cause failure of the pumps is naturally modelled using an FDEP gate. The FDEP gates in a DFT increase its comprehensibility and help to easily identify common cause failures. The replacement of *Both pumps fail* with a SPARE gate is superfluous here, as—by assumption in [4]—a reduction in pressure switch results in starting the pump. Thus, once the pressure drops, both the electric and diesel pumps are started. A more natural reconfiguration strategy is to first try the electric pump, and, if it fails to maintain the pressure, then start the diesel fire pump. There is also a jacking pump attempting to respond to mild pressure losses due to temperature changes and leakages. The sprinkler system analysed by [19] starts the electric pump at 0.78 MP and the diesel pump at 0.73 MP. To model such strategies, a SPARE gate is adequate and indispensable.

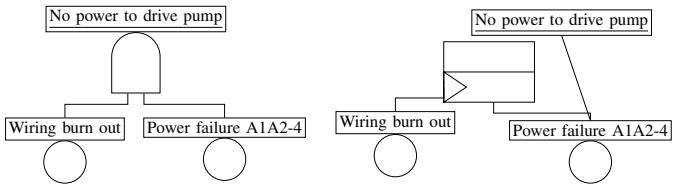

Fig. 9: Wiring CC: SFT form [4] (left) and DFT (right)

B.3: Wiring burnout. The last common cause failure we consider is *wiring burnout*. We consider the power failure of the drive pump. We propose to use an FDEP with trigger *Wiring burn out* and dependent input *Power failure*. Our motivation is twofold: (1) power is not delivered in the presence of wiring burnout, and (2) a wiring burnout is believed to have a severe effect on power delivery to other parts of the sprinkler system. This is reflected by our DFT in Fig. 9 (right). As depicted in Fig. 9 (left), the SFT of [4] models power failure of the drive pump by an AND gate which does not reflect the above issues.

C: Monitoring mechanism failures. Monitoring mechanisms perform an action upon the failure of a subsystem and are typical examples that can adequately be modelled by PAND gates as they require an ordering of their inputs.

C.1: Mains to backup switching. A diesel generator is used in sprinkler systems as a *backup power source*. The typical arrangement of such power management systems [20] uses transfer switches to switch from primary to secondary sources. These arrangements are examples of monitor-based switching and can be naturally modelled by PAND gates. We treated an example in Fig. 3 on page 3.

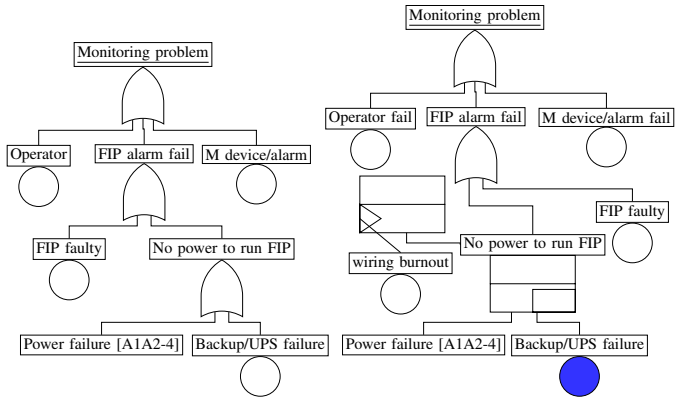

Fig. 10: Monitoring problem: SFT (left) and DFT (right)

C.2: Monitoring problem. The sprinkler system's *monitoring mechanism* consists of sensing devices such as feedback loops of various valve positions, temperature sensors, etc., an FIP to indicate the status of various devices, and an (typically human) operator for timely reacting to non-compliant situations. As timely reaction of the monitoring mechanism inhibits component failures from causing system-level failures, this is a classical application of PAND. Before looking into using these PAND constructs, we discuss the DFT of the monitoring mechanism itself, see Fig. 10 (right). The FIP has the standby power source *UPS*. As explained before, we model standby power sources using a SPARE gate. Moreover, we consider *Wiring burnout* as a common cause for an FIP power source failure. Both these facets are not captured by the SFT of Fig. 10 (left). We now consider the use of a PAND gate for monitor-based switching by some concrete examples.

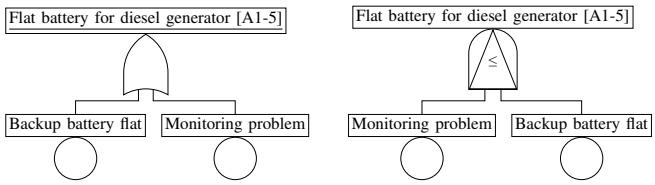

Fig. 11: Battery monitoring: SFT (left) and DFT (right)

C.2.1: Flat battery. In the *Flat battery for diesel generator A1-5* DFT—this replaces the box in Fig. 6 (right))—of Fig. 11 (right), the fault of a battery is PANDed with the monitoring problem. This means if the flat battery is corrected by monitoring, subsequent failures in monitoring will not cause failures due to a flat battery. This should be contrasted to the SFT of Fig. 11 (left). We believe that the OR gate in Fig. 11 (left) is a modelling flaw, as an AND gate is intended. Secondly, we consider a $\mathsf{PAND}_{\leq}$ gate to be more appropriate.

C.2.2: Multiple monitoring mechanism examples. Many instances in the sprinkler system of [4] use monitoring mechanism to monitor other alarm-initiating events. We propose to model each of these situations using a $\mathsf{PAND}_{\leq}$ with the monitoring problem as the first input. We justify this by considering DFT fragments for three cases. Consider Fig. 12 and suppose the main valve turns off before the monitoring problem occurs. The operator will take action and this failure will not propagate. A later monitoring problem will not cause

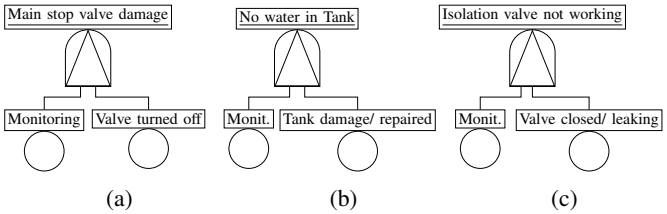

Fig. 12: (a-c) Modelling monitoring problem using PAND

the propagation of the previous valve failure as the operator has already handled it. Now, consider that the monitoring mechanism fails and one of the other valves closes/leaks.

As the monitoring failure has already occurred, this valve failure will not be addressed and may cause the failure of the output. The SFTs of [4] use an AND gate in such scenarios, which does not faithfully capture the situation.

D: Fire indication panel. As the FIP is an intricate component, we propose to model it as a separate DFT, see Fig. 13. This modelling is inspired by [21] and is explained as follows. An FIP failure can be caused by either hardware or test-independent failures, i.e., the failures that are not detectable by functional testing. Hardware failures are either transient or permanent. A transient failure could be due to a transient error that is either not covered by the safety mechanism or that was covered by a mechanism that already failed. The latter is adequately modelled by a SEQ gate which model that the BE *covered* can only fail once the safety mechanism has failed. We adopt the hardware failure rates from [21] and include Fig. 13 in the DFT of the sprinkler system. We believe that modelling FIP as a single BE (like in the SFT of Fig. 10) is an oversimplification. The key point we raise here is that the FIP DFT, as well as DFTs of other fault-tolerant subsystems (e.g., the fire detection system), have dynamic features that should be taken into account.

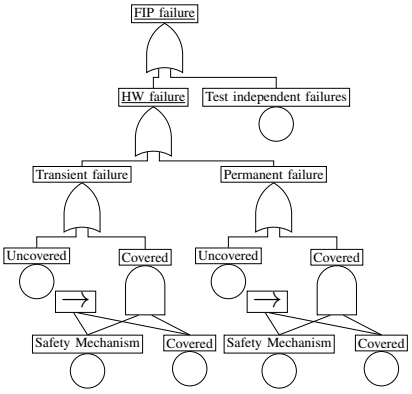

Fig. 13: A DFT for the FIP

IV. Probabilistic Model Checking

Model checking [3] is an automated verification technique to check whether a state-space-based model $\mathcal{M}$ satisfies a logical property ϕ, i.e., whether $\mathcal{M} \models \phi$ holds. In our setting, we use continuous-time Markov chains (CTMCs) as the underlying model $\mathcal{M}$ because the behaviour of DFTs can be captured by CTMCs in a natural way, see the small example below. We refrain from providing the details of how to obtain CTMCs from DFTs in an efficient manner; see also [10].

Example: We provide a simple example of a CTMC for a binary $\mathsf{PAND}_<$ gate with inputs A and B having failure rates λ_A and λ_B, respectively. The CTMC has initial state s_0.

Initially, either the first input (A) or the second input (B) can fail. The failure of input B before A leads to a fail-safe state. This is indicated by the label *fail-safe* of state s_2. The failure of A followed by B leads to a gate failure represented by label *failed* of state s_3.

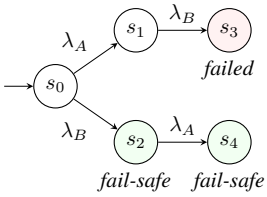

Fig. 14: CTMC example

A. Model-Checking Properties

All properties of fire sprinkler system that we consider are instantiations of the following types of properties.

a) Reach-avoid: This property quantifies the probability (starting in some state s) to eventually reach a set $T \subseteq S$ of target states while avoiding any bad state in $B \subseteq S$ in-between, logically $\mathsf{P}^s(S \backslash B \,\mathsf{U}\, T)$ where $S \backslash B$ is the complement of B. We often omit the superscript s if s is the initial state. A *reachability* property $\mathsf{P}^s(\Diamond\, T)$ is a special case of reach-avoid probability with $B = \emptyset$.

b) Time-bounded reach-avoid: This property is similar to the previous property, but an upper bound on the time t to reach T is imposed, i.e., $\mathsf{P}(S \backslash B \,\mathsf{U}^{\leq t}\, T)$. A *time-bounded reachability* $\mathsf{P}^s(\Diamond^{\leq t}\, T)$ is a special instance with $B = \emptyset$.

c) Expected time: The expected amount of time needed to reach a state in $T \subset S$ from state $s \in S$. It is logically defined as $\mathsf{ET}^s(\Diamond\, T)$. The expected time is only defined if T is reached from s with probability one.

B. Reliability Metrics

We consider the following reliability metrics phrased as model-checking queries. The formal definitions are listed in the last column of Table III. Let the label *sys_fail* (*degraded*) indicate the failure (degradation) of the system.

a) Unreliability: It is the probability of a system failure within time t. Reliability $R(t)$ is its complement.

b) Conditional reliability: It is the probability that a system will stay operational for t time units given that it has not failed within time $t' < t$. It is defined as:

$$\mathsf{R}(t \mid t') = \frac{\mathsf{R}(t+t')}{\mathsf{R}(t')} = \frac{1 - \sum_{s \in I} \mathsf{P}^s(\Diamond^{\leq t+t'}\, \mathit{sys\_fail})}{1 - \sum_{s \in I} \mathsf{P}^s(\Diamond^{\leq t'}\, \mathit{sys\_fail})}.$$

c) Average failures per hour: (AFPH). The system's failure rate equals the number of system failures per time unit. Average failure rates per hour are obtained by the system unreliability within its lifetime normalised by the lifetime. The *lifetime* is obtained from requirement specification documents.

d) Mean time to failure: MTTF is the expected time until a system failure, i.e., $\mathit{MTTF} = \mathsf{ET}^s(\Diamond\, \mathit{sys\_fail})$.

e) BX % life: It is used to assess product warranty times, e.g., $B(5)$ is the time when 5% of products have failed. Such *quantiles* are first considered in model checking by [22]. Given an unreliability threshold q, the aim is to compute t s.t.

$$q - \epsilon \leq \mathsf{P}^s(\Diamond^{\leq t}\, \mathit{sys\_fail}) \leq q + \epsilon \qquad (1)$$

where ϵ is the permissible tolerance. Quantiles can be approximated using binary search [22]. It starts with an initial guess

TABLE III: Summary of reliability metrics

	Measure	Model checking query
System	Reliability	$1 - \mathsf{P}^s(\lozenge^{\leq t}\ sys\_fail)$
	Cond. rel.	$\frac{\mathsf{R}(t+t')}{\mathsf{R}(t')}$
	AFPH	$\frac{1}{lifetime} \cdot \mathsf{P}^s(\lozenge^{\leq lifetime}\ sys\_fail)$
	MTTF	$\mathsf{ET}^s(\lozenge\ sys\_fail)$
	BX %	t s.t. $\mathsf{P}^s(\lozenge^{\leq t}\ sys\_fail) \leq q$
Degradation	FFA	$1 - \mathsf{P}\left(\lozenge^{\leq t}\ (sys\_fail \vee degraded)\right)$
	FWD	$\mathsf{P}\left(\neg degraded\ \mathsf{U}^{\leq t}\ (\neg degraded \wedge sys\_fail)\right)$
	MTDF	$\sum_{s \in degraded} \left(\mathsf{P}\neg degraded\ \mathsf{U}\ s\right) \cdot \mathsf{ET}^s(\lozenge\ sys\_fail))$
	MDR	$\arg\min_{s \in degraded} \left(1 - \mathsf{P}^s(\lozenge^{\leq t}\ sys\_fail)\right)$
	FLOD	$\sum_{s \in degraded} \left(\mathsf{P}(\neg degraded\ \mathsf{U}^{\leq t}\ s) \cdot \mathsf{P}^s(\lozenge^{\leq \text{operation\_time}}\ sys\_fail)\right)$
	SILFO	$1 - (FWD + FLOD)$

t_0 s.t. $\mathsf{P}(\lozenge^{\leq t_0}\ sys\_fail) > q$. We split the interval $[0, t_0]$ in half and compute the unreliability for $t_1 = \frac{t_0+0}{2}$. If this value exceeds q, then the new search interval is $[0, t_1]$, otherwise we use $[t_1, t_0]$ and continue. The iteration stops when the time estimate t' satisfies (1). The binary search approach only works for coherent DFTs. The presence of PAND gate may make a DFT non-coherent. The remaining reliability metrics are related to the system being in a degraded mode and are adopted from a recent model-checking study on autonomous driving using DFTs [21]. These metrics are defined in the lower part of Table III.

f) Full function availability: FFA denotes the probability of the system being fully available, i.e., neither in a failed nor degraded state. It is the complement of the time-bounded reachability for failed or degraded states.

g) Failure without degradation: FWD denotes the probability of system failure without being first degraded. It is a timed-bounded reach-avoid probability.

h) Mean time from degradation to failure: MTDF is the expected time between the system entering a degraded state until a complete failure. It is obtained by scaling the expected time of failure starting from each degraded state with the probability of reaching such state without being degraded first.

i) Minimal degraded reliability: MDR is the worst-case reliability from a degraded state. It is obtained as minimum over the unreliability for each degraded state.

j) System integrity under limited fail operation: SILFO has two parts: FWD and *failures under limited operation in degradation* (FLOD). The latter represents the unreliability while imposing a time limit on running a degraded system.

V. Experimental results and discussion

This section reports on our experiments using the DFT-to-CTMC conversion in the model checker Storm [12]. Storm also supports the computation of all reliability measures in Table III. The experiments were run on a machine having: Dual-Core Intel® Core $i7$, 3 GHz, 8 GB RAM. The source code and results are available for review [1].

A. Fire Sprinkler System Configurations

Various system configurations, summarised in Table IV, are based on the in-depth study reported in [4]. Shopping centers have a varying number of components, e.g., some of them do not have basement tanks and associated pumps. Others have pumps to directly draw water from town mains but no basement tanks, whereas some variants do have basement tanks. The fire pump sets used to supply water from the town mains and/or basement tanks can be electric/diesel, electric/electric, or diesel/diesel. If an electric fire pump is used, a backup diesel power generator is assumed to be present. Shopping centers have one or two connections from the town water main. Moreover, the pump bypassing mechanism is optional depending upon the town water mainline pressure. The sprinkler head failure consideration leads to three cases for each configuration: 1) two sprinkler head failures represent the combined failure of the sprinkler heads. The failure rate per demand for case-1 is $0.079^2 = 0.0062$; 2) only one sprinkler head failure suffices. The failure rate per demand for case-2 is 0.079; 3) the sprinkler system fails if one head fails or its eight surrounding heads all fail. The failure rate per demand for case-3 is $\left(\left(1-(1-0.079)^8\right) \cdot 0.079\right) = 0.038$. Likewise, the failure rate per hour for 1) case-1 is $\frac{0.0062}{0.0833 \times 8760} = 8.55E{-}06$, 2) case-2 is $1.08E{-}04$ and 3) case-3 is $5.22E{-}05$. The dormancy factor of all standby basic events is 0.1.

TABLE IV: Various configurations of fire sprinkler system

Type of system		Sprinkler head case-1	case-2	case-3
Basement tank with pump and pump bypass	Electric/diesel	I	II	III
	Electric/electric	IV	V	VI
	Diesel/diesel	VII	VIII	IX
Basement tank with pump but no pump bypass	Electric/diesel	X	XI	XII
	Electric/electric	XIV	XV	XVI
	Diesel/diesel	XVII	XVIII	IXX
Without basement tank and pump	2x town mains	XX	XXI	XXII
	1x town mains	XXIII	XXIV	XXV

The hydraulic schematic of our case study provided in Fig. 4 on page 3 depicts a sprinkler system supplied by two town mains; it has an electric/diesel pump set assembly, two water tanks, and a pump bypass arrangement. This system corresponds to the configurations I, II, and III of Table IV.

B. Degradation

The system is considered in a *degraded mode* when at least one component from a set of redundant components failed. The redundant components are: the backup diesel generator, one pump of diesel/electric fire pump set, water mains, pressure switch, power supplies of FIP, and diesel fire pump drive.

C. Results

Let us first provide some statistics about the DFTs and their underlying CTMCs, see Table V. We list the number of basic events, the number of dynamic gates (such as PAND, FDEP and SPARE gates), and the total number of DFT elements including basic events and static/dynamic gates. Then the state-space size for each CTMC is provided. We identify degradation states in the last row which considers the DFT used for failure probability per hour (PFH) analysis. The degraded states make up 6% of the total state space.

We discuss the results for PFD_{avg} and *PFH* analysis, see Sec. II for their definition. To compare with the SFT analysis results of [4], we perform the SFT analysis using Storm.

[1] https://github.com/moves-rwth/dft-bdmp/tree/master/2021-LADC

TABLE V: DFT and state space size statistics

Configuration	Dynamic fault tree			Continuous time Markov chain		
	# BE	# dyn.	# elem.	# states	# transitions	# deg. states
SFT-all cases*	32	0	65	2718	21305	–
DFT-all cases *(PFD)*	58	22	117	6884039	23275459	–
DFT-all cases *(PFH)*	53	21	109	1036790	12114151	62208
diesel/electric	34	15	69	6313	17037	–
electric/electric	33	13	67	2929	6889	–
diesel/diesel	36	17	72	23185	63225	–

* All three cases, i.e., case-1, case-2 and case-3, see Table IV

TABLE VI: Failure probability on demand

Config. #	PFD_{avg} [4]	PFD_{avg} SFT	PFD_{avg} DFT	PFD(t)-SFT @730 hours	PFH-SFT
I	0.0174	0.016378	0.016012	0.016378	$2.243561E{-}05$
II	0.0894	0.085404	0.085101	0.085404	$11.69917E{-}05$
III	0.0488	0.047224	0.046811	0.047223	$6.46890E{-}05$

(SFTs can be efficiently analysed using binary decision diagrams and a Markovian analysis for SFTs is an overkill but provides us with a comparison basis.) The re-construction of the SFT of [4] was complicated because a few basic event failure rates were missing in the available documentation. In such cases, we used failure rates for matching names, e.g., the failure rate of *main riser* was missing and we used the *water supply line* failure rate. The DFTs for various system configurations were built using the principles discussed in Sec. III and were analysed using STORM.

1) PFD_{avg}: We assign failure rates per demand to the basic events and compute PFD_{avg} as the time-bounded reachability probability to reach a *sys_fail* state within one time unit (a.k.a: one demand). Table VI lists the values reported in [4] (second column) and the calculated PFD_{avg} values for the SFT using STORM (third column). The difference between these values is most likely due to different failure rates for the components for which exact values in [4] are absent. The difference between the PFD_{avg} values of SFT (third column) and DFT (fourth column) can be attributed to the introduction of standby and fail-safe behaviour which results in lower failure probabilities for the DFT than for the SFT.

2) PFH: For the *PFH* analysis, we change the failure rates of basic events from per demand to per hour. (These failure rates are listed in the fourth column of Table I.) Computing the time bounded reachability probability for 1 time unit yields *PFH* values which are reported in the last column of Table VI. Attempting to correlate PFD_{avg} to *PFH* values, we get $2.24356E{-}05 \times \frac{730}{2} = 0.0081884$ which is exactly half of the PFD_{avg} value of SFT (third column). This is because we followed the approach of [4] for component level failure rate calculation and ignored the multiplication of component-level per demand failure rates by two while calculating failure rates per hour. We also compute $PFD(t)$ for t=730 hours reported in the fifth column. It matches the values of PFD_{avg} of SFT (third column). This hints that the PFD_{avg} values in [4] correspond to $PFD(T_p)$. These discrepancies are neither a limitation nor the main message of the presented approach but arise due to different computation variants for PFD_{avg} and *PFH*.

3) Fire pumps reliability: The analysis of [4] indicates that the system reliability is insensitive to the fire pump set configurations. To quantify the effect of the fire pump configuration in isolation, we create and analyse DFTs for the different fire pump sets. We obtain for electric/electric, electric/diesel, and diesel/diesel the failure probabilities on demand: $32.46E{-}5$, $10.05E{-}5$, and $9.15E{-}5$, respectively. The PFD_{avg} for the electric/electric configuration is about three times higher than for the electric/diesel setting. The electric/diesel and the diesel/diesel setting have comparable PFD_{avg} values. The electric/diesel variant has the advantage of using different types of redundancy (electric and diesel). This is less vulnerable to common cause failures such as the shortage of diesel supplies. Nevertheless, the difference in the unreliability values is insignificant.

4) Beyond standard measures: We now provide the results for the reliability measures in Sec. IV-A for the mission time of 730 hours (one month). For conditional reliability and SILFO, we consider one additional week, i.e., 180 hours. The detailed results for each case are provided in Table VII. There is a slight variation in the results for each case. These variations suggest that the first configuration is slightly better. This is expected as this configuration considers a system failure if two sprinkler heads fail; effectively it considers a redundancy of heads. The third column, i.e., unreliability is equivalent to $PFD(t)$ where t=730 hours. The fourth column lists the failure probability per hour. The next measure (column 5) reveals that the probability of the system being fully functional at 730 hours is only 2.4%. There is thus a high chance that the system will be degraded at a proof test. Note that the failure without degradation (column 6) probability resembles unreliability. A close inspection of the DFT structure reveals that none of the more important components causes a system degradation; rather, the system directly fails. Ideally, the FWD measure should be as low as possible. On the other hand, FFA should have a high value. This suggests that *the unreliability of critical components, e.g., zone isolation valve and sprinkler heads should be reduced by adding more redundancy*. The conditional reliability measure (column 8) yields a 99% probability of the system remaining functional after a successful operation of one month. The B(5) (column 9) measure asserts that 5% population of this particular type of sprinkler system will fail approximately in five months. *This suggests periodic inspection intervals must not exceed 3–5 months*. Our results are thus consistent with monthly inspection schedules as recommended in fire maintenance standards. Finally, we consider failures under limited operation in degradation (FLOD) (column 10). In our experiment setting, we consider a system demand (i.e, a fire breakout) that occurred after 730 hours and we are interested in a system failure within 180 hours. The probability of this event is $3.5E{-}5$. This property can be used to analyse, e.g., minimum evacuation times of the buildings under different fire occurrence scenarios. We assume minimum evacuation time of 6 hours and run another experiment for configuration I. STORM returns a value of $1.574E{-}6$.

Table VII also provides the computation times of STORM. (The CTMC state-space sizes are listed in Table V). We observe that computing quantiles $B(X)$ is most time consuming. This is due to the repeated computation of time-bounded reachability until the binary search-based algorithm converges

TABLE VII: Reliability measures

	Config. #	unreliability	PFH	FFA	FWD	MDR	R(180|730)	B(5)	FLOD	SILFO
Reliability measures	I	$9.8792E{-}03$	$1.3533E{-}05$	$2.3874E{-}02$	$9.8085E{-}03$	$1.9362E{-}02$	$9.9393E{-}01$	3484	$3.4914E{-}05$	$9.8434E{-}03$
	II	$1.0129E{-}02$	$1.3876E{-}05$	$2.4121E{-}02$	$1.0057E{-}02$	$1.9610E{-}02$	$9.9387E{-}01$	3430	$3.5783E{-}05$	$1.0093E{-}02$
	III	$9.9887E{-}03$	$1.3683E{-}05$	$2.3982E{-}02$	$9.9173E{-}03$	$1.9471E{-}02$	$9.9390E{-}01$	3460	$3.5294E{-}05$	$9.9526E{-}03$
Computation time (in s)	I	9.54	9.44	0.23	0.43	12.53	0.95	174.22	53.27	65.80
	II	12.41	11.00	0.53	0.46	13.32	1.19	168.00	56.93	70.25
	III	13.69	11.05	0.47	0.40	13.63	0.97	174.84	61.30	74.93

to acceptable bounds. We set the stopping threshold to 0.001, i.e., our implementation stops as soon as it reaches a time point where the number of failed components is between 4.9% and 5.1%. A higher precision will require more computation time.

D. Discussion of the Approach

Compared to [4], our approach was able to compute results beyond standard dependability measures which are not supported on the static model. We compare our results for PFD_{avg} to [4] in Table VI. For all other results, no previous results exist.

We see two main benefits of the presented approach. First, this paper underscores the need for faithful modelling of a given system. We presented several scenarios which are more realistically modelled using the dynamic constructs of DFTs compared to SFTs. Note, that this observation is not specific to sprinkler systems and any system previously modelled by SFTs can be translated to DFTs. Second, our approach demonstrates the use of probabilistic model checking for system dependability analysis. In particular, analysing the various properties – that go beyond standard dependability measures – can be instrumental in a detailed dependability analysis of the prevailing industrial systems. We believe that faithful modelling and insightful analysis using formal approaches can complement traditional industrial practices that are based on SFT analysis. Finally, we remark that the approach presented here is a generic framework and the interpretation of results heavily depends on the reliability parameters and models used as input. That is, if the input model does not faithfully reflect the system under consideration and reliability parameters do not reflect physical components, then the detailed analysis will bring no value to the system dependability.

VI. CONCLUSION

This paper discussed the modeling of various reliability aspects of fire sprinkler systems using DFTs. We focused on the adequacy of dynamic elements to model different facets. Probabilistic model-checking techniques have been employed to analyse standard reliability measures and metrics that go beyond. This is illustrated by analysing different configurations of fire sprinkler systems in shopping centers. Our DFT models and analysis results were compared to existing results for static fault tree models. Future work consists of validating the models against real-life fire sprinkler systems and to synthesise optimal system configurations for given reliability metrics.

REFERENCES

[1] J. Andrews, "Tutorial Fault Tree Analysis," in *Proc. of the 16th Int. System Safety Conference*, 1998.

[2] J. B. Dugan, S. J. Bavuso, and M. A. Boyd, "Dynamic fault-tree models for fault-tolerant computer systems," *IEEE Trans. on Reliability*, vol. 41, no. 3, pp. 363–377, 1992.

[3] C. Baier and J.-P. Katoen, *Principles of Model Checking*. MIT Press, 2008.

[4] K. Moinuddin, J. Innocent, and K. Keshavarz, "Reliability of sprinkler system in Australian shopping centres–a fault tree analysis," *Fire Safety J.*, vol. 105, pp. 204–215, 2019.

[5] E. Ruijters and M. Stoelinga, "Fault tree analysis: A survey of the state-of-the-art in modeling, analysis and tools," *Comput. Sci. Rev.*, vol. 15, pp. 29–62, 2015.

[6] S. Junges, D. Guck, J.-P. Katoen, and M. Stoelinga, "Uncovering dynamic fault trees," in *DSN*. IEEE Comp. Soc., 2016, pp. 299–310.

[7] S. Junges, J.-P. Katoen, M. Stoelinga, and M. Volk, "One Net Fits All - A Unifying Semantics of Dynamic Fault Trees Using GSPNs," in *Petri Nets*, ser. LNCS, vol. 10877. Springer, 2018, pp. 272–293.

[8] Z. Tang and J. B. Dugan, "Minimal cut set/sequence generation for dynamic fault trees," in *RAMS*, 2004, pp. 207–213.

[9] C. Baier, E. M. Hahn, B. R. Haverkort, H. Hermanns, and J.-P. Katoen, "Model checking for performability," *Math. Struct. Comput. Sci.*, vol. 23, no. 4, pp. 751–795, 2013.

[10] M. Volk, S. Junges, and J.-P. Katoen, "Fast dynamic fault tree analysis by model checking techniques," *IEEE Trans. Ind. Informatics*, vol. 14, no. 1, pp. 370–379, 2018.

[11] R. Gulati and J. B. Dugan, "A modular approach for analyzing static and dynamic fault trees," in *RAMS*. IEEE, 1997, pp. 57–63.

[12] C. Dehnert, S. Junges, J.-P. Katoen, and M. Volk, "A storm is coming: A modern probabilistic model checker," in *CAV (2)*, ser. LNCS, vol. 10427. Springer, 2017, pp. 592–600.

[13] H. Boudali, P. Crouzen, and M. Stoelinga, "A rigorous, compositional, and extensible framework for dynamic fault tree analysis," *IEEE Trans. Dependable Secur. Comput.*, vol. 7, no. 2, pp. 128–143, 2010.

[14] K. Frank, N. Gravestock, M. Spearpoint, and C. Fleischmann, "A review of sprinkler system effectiveness studies," *Fire Sci. Rev.*, vol. 2, 2013.

[15] J. Braband, R. vom Hövel, and H. Schäbe, "Probability of failure on demand – the why and the how," in *SAFECOMP*, ser. LNCS, vol. 5775. Springer, 2009, pp. 46–54.

[16] K. Moinuddin, I. Thomas, S. Chea, and I. Bennetts, "Factors affecting the reliability of sprinkler system in australian high rise office buildings," *Fire Safety Science*, vol. 7, pp. 80–80, 2007.

[17] K. Moinuddin and I. Thomas, "Reliability of sprinkler system in Australian high-rise office buildings," *Fire Safety J.*, vol. 63, pp. 52–68, 2014.

[18] S. Zhuiykov and V. Dowling, "Maintenance testing of sprinkler heads: Qualitative analysis causes of failures," *Fire Safety Science*, vol. 8, pp. 811–822, 2005.

[19] U. Hauptmanns, M. Marx, and S. Grünbeck, "Availability analysis for a fixed wet sprinkler system," *Fire Safety J.*, vol. 43, no. 7, pp. 468 – 476, 2008.

[20] P. Gull and W. C. Sodemann, "Backup power management system and method of operating the same," 2006, US Patent 7,015,599.

[21] M. Ghadhab, S. Junges, J.-P. Katoen, M. Kuntz, and M. Volk, "Safety analysis for vehicle guidance systems with dynamic fault trees," *Reliab. Eng. Syst. Saf.*, vol. 186, pp. 37–50, 2019.

[22] C. Baier, C. Dubslaff, J. Klein, S. Klüppelholz, and S. Wunderlich, "Probabilistic model checking for energy-utility analysis," in *Horizons of the Mind. A Tribute to P. Panangaden*. Springer, 2014, pp. 96–123.