Structural Equation Modelling for Causal Analysis Applied to Transport Systems

Lazos Filippidis [1)], Holger Schlingloff [2)]

[1)2)] Fraunhofer Institut für Rechnerarchitektur und Softwaretechnik FIRST
Kekulèstr. 7, Berlin, Germany, D-12489
[1)] lazos.filippidis@siemens.com
[2)] hs@informatik.hu-berlin.de

Abstract. We present a new approach regarding system and safety analysis which integrates the methods of safety barrier (SBA), fault tree (FTA) and failure mode and effect analysis (FMEA) into one method. Our approach uses results from the philosophical theories of transference processes and structural equation modelling (SEM). Based on these theories, formal basic causal patterns are derived to compose complex system structures. Using the SEM intervention method, we deduce automatically the consequences of failures. Our approach has been applied to an example taken from a transport system application.

1 Introduction

In safety-relevant systems as e.g. public transportation systems, the loss of safety-relevant functions may lead to injury, even death of persons or to high monetary damages. Therefore, the necessity to control the potential risks emanating from safety-relevant applications, i.e. to avoid or at least to mitigate them, is obvious. Thus, system analysts are interested in answering the question '*What has to happen, so that …*'. The answer enables the reasoning about causes and consequences, furthermore to decide, if potential risks are tolerable or not. In doing so, a complete causal analysis and prediction of the system behaviour are required even in cases of internal system malfunctions or faulty external stimuli.

1.1 Causal Analysis and Failure Analysis

In the past decades, many safety analysis methods have been proposed, e.g. **F**ault **T**ree **A**nalysis (FTA), **F**ailure **M**ode and **E**ffect **A**nalysis (FMEA), **E**vent **T**ree **A**nalysis (ETA) or **S**afety **B**arrier **A**nalysis (SBA), just to mention the most important ones (for an overview of safety methods refer to [1]). The probably most familiar methods FTA and FMEA are widely used in industry due to their intuitive applicability. Starting from an undesired top event, the FTA aims to find top-down all basic events (single or multiple failure events) leading to the undesired top event. In contrast, the FMEA is a bottom-up method and determines all consequences of single mode failures.

However, most common safety methods do not account on causality and causation formally, i.e. they do not take cause-effect-relations formally into account. Instead, they assume an intuitive understanding of the causal structure of the system to be analysed. Furthermore due to the manual construction, the results of most failure analysis techniques may be failure-prone, time-consuming and subjective depending on the expertise of the analyst [2][3]. Although there exist rule-based or data-based methods for FTA or FMEA, it is not easy to recover common causes, barrier or supervision functions, context-sensitive failures or failure masking (refer to examples in [3][4][2]). But in order to derive the complete system failure behaviour based on system specification, or to give indications of system improvements, a deep understanding of the causal structures is necessary. In the past, some approaches have been provided which attempt to integrate formally causal semantics into system specifications and analyses.

Moffett et al. have presented a method for requirements engineering which models causality formally by means of a *leads-to*-operator [5]. That approach is not capable of performing failure analysis. Johnson has analyzed several types of logical connectors regarding causal reasoning mainly for incident and accident analysis. He has shown that the material and the modal strict implication are not suitable for formal causal reasoning [6]. He has identified Ladkin's **W**hy-**B**ecause-**A**nalysis (WBA), an approach based on D. Lewis' counterfactual semantics, as a promising candidate for causal safety analysis. Indeed, today Ladkin's method seems to be the most elaborated formal technique for causal safety analysis [7]. Although the method has been developed for incident and accident analysis, the WBA is also applicable to FTA construction. But because of the vagueness of Lewis' counterfactual semantics given by a possible world interpretation, the causal relations between events or states remain an intuitive and subjective judgement. Furthermore, Lewis' counterfactual approach fails in cases of pre-emption [8].

Schellhorn and Ortmeier have presented formal fault tree semantics, whereas formal causal relations between events have been proposed [9][10]. These causal relations are used after the manual construction of the fault tree in order to formally verify the fault tree with respect to correctness and completeness.

We have proposed an algorithm based on structural equation modelling for reasoning about the system behaviour and analysing the consequences of failures but without having given the complete semantics of causal relationships [11]. Kunz et al. use structural equations to derive the system failure behaviour by using a tool-based counterexample search but without explaining the causal semantics of the structural equations [12]. All the discussed methods have in common that the system failure behaviour based on a causal structure must be foreseen intuitively.

Therefore, we first derive basic causal relation patterns from the philosophical results, from which complex system structures can be composed formally. Based on a formal causal model, the SEM and intervention method (refer to [13]) is used to synthesise the system behaviour both for the intended and the failure cases. The outline of the paper is as follows: First, we start with an example, which shows the drawbacks of classical failure analysis in more detail. Then, we provide a novel approach for modelling causality and causation based on information transfer semantics. The mathematical framework is given by structural equations which enables reasoning about the system behaviour in the conditional/ counterfactual sense ('*what will/would happen, if…*'). Based on the intervention method, we provide a novel *conditional analysis* algorithm to generate automatically the failure behaviour of a system. The paper ends with a fictive example of a transport system application.

1.2 Example of classical failure analyses and their problems

We start with an example which demonstrates the difficulties of classical fault tree generation and use the immediate cause concept to show the difficulties of classical fault tree construction (refer to Figure 1) [14]. We consider a gas tank which can be filled with gas by a pump. If the pump does not work properly, which for example yield a too high tank pressure or a too fast increase of the tank pressure, an LED (light emitting diode) turns on because of measuring the tank pressure increase. The LED-on indicates an operator to intervene manually in the process. Obviously, in our example the hazardous event is given by the combination of the events pump defect and LED off, that is, the LED is off, although the pump is defect yielding a dangerous increase of the tank pressure. Using the immediate cause concept, one analyses the output of the component A (LED), which might be faulty due to a failure of the component A itself or due to a faulty input to component A from component B (tank). The faulty output of component B is further analysed: The output of component B becomes faulty, if B itself is defect (tank defect) or if the input from C is faulty (pump defect).

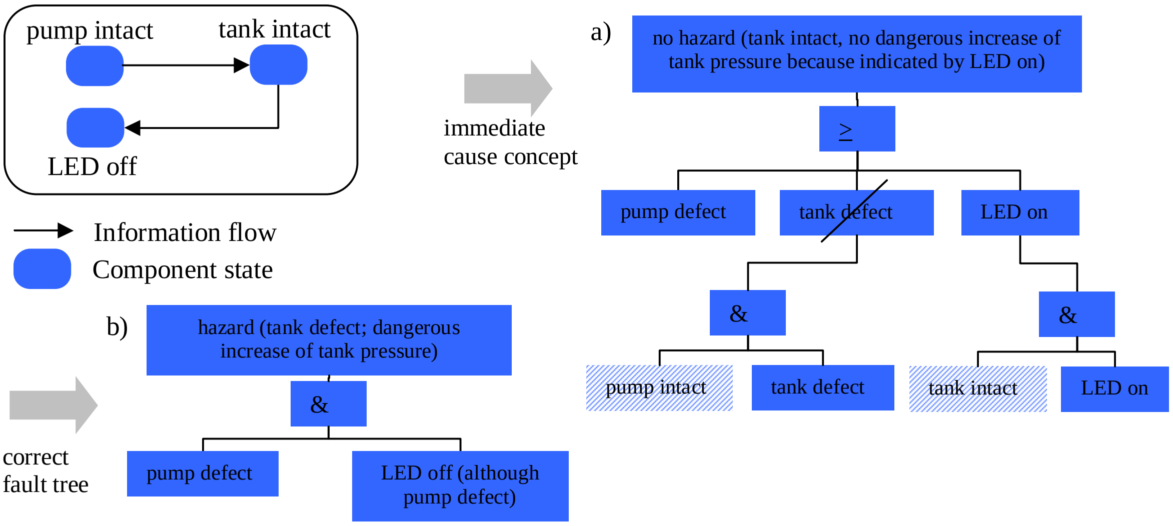


Figure 1. The principle of the immediate cause concept. a) The fault tree resulting from the immediate cause concept according to a serial system structure. The hatched events can be neglected in the AND-gates due to their occurrence probability of nearly one; the state 'tank defect although the pump is intact' is excluded for the hazard. b) The fault tree for the hazardous event.

In our example, the immediate cause concept yields the failures pump defect, LED on or tank defect, whereas the last event is excluded, because here we are interested in the external causes of the failure tank defect: The tank might be defect due to any other intrinsic reason, but not because the pump is defect.

Due to the fact that the probability of the intact states of the components is nearly one, the intact states (hatched in Fig. 1) of the AND-gates can be neglected. That leads to the well-known fault tree of a serial structure (pump defect OR LED on excluding the failure tank defect as mentioned above). But the construction does not result the hazardous failure combination of failure masking: LED off, although pump defect.

2 A novel structural equation approach for safety analysis based on formal causal modelling

The following sections present the results of our approach using formal causal semantics and the SEM method.

2.1 Preliminaries

A type E is a set of elements e with predication p(e), formally E(e)={e|p(e)}. The elements e are called instances of the type E; e=true means that the type E is instantiated, i.e. there exists an e with p(e)=true, e=false means that the type E is not instantiated, i.e. there exists no e with p(e)=true. Objects, events and states are elements of related types and are given intuitively. For example, an object type train with predication p(.)=is_train(.) is the set of all trains. According to [13], we define a causal model, interventions and structural equations.

Definition 2.1 (Causal model) *A causal model is a tuple* $M=<\boldsymbol{V},\boldsymbol{U},\boldsymbol{F}>$*, where* **U** *is a set of exogenous variables* $U_j \in \boldsymbol{U}$*,* $j=1\ldots m$*,* **V** *is a set of endogenous variables* $V_i \in \boldsymbol{V}$*,* $i=1\ldots n$*,* **F** *is a set of functions* $f_i \in \boldsymbol{F}$ *with* $\boldsymbol{F}: \boldsymbol{U} \cup \boldsymbol{V} \longrightarrow \boldsymbol{V}$*, where each function* $V_i=f_i(\boldsymbol{U},\boldsymbol{V})$ *is a mapping from* $\boldsymbol{U} \cup \{\boldsymbol{V} \setminus V_i\}$ *to* V_i*.* □

The exogenous variables are determined by factors outside M, the endogenous variables by factors in M. The set **F** of functions contains the structural equations of the causal model M. An intervention is the submodel $M_S=<\mathbf{V},\mathbf{U},\mathbf{F}_S>$, where $\mathbf{F}_S=\mathbf{F}\setminus\mathbf{S}\cup\{\mathbf{X}=\mathbf{x}\}$, $\mathbf{X}\subseteq\mathbf{U}\cup\mathbf{V}$, with **x** the possible values of **X** and $\mathbf{S}=\{f_j|X_j\notin\mathbf{X}\}\subseteq\mathbf{F}$ corresponding to the functions $X_i=f_i(\mathbf{U},\mathbf{V})$ [13]. In the next section, we define the causal relations by means of the changes of object properties. If an object type O(x)={x|p(x)=‘*x is an object of type O*’} is given, we define an object property of the object type O by means of its related attribute and value: ‘*The object x of type O has the property att with value val*’, formally [att(O(x))@val]=true with @={=,<,>,<>,=<,>=}, or ‘*The object x of type O does not have the property att with value val*’, formally ¬[att(O(x))@val]=true. We take the variables of a causal model M as the object type properties, the structural equations as the truth-value conditions, the truth-value assignments as the instantiations of objects with the corresponding properties.

In terms of safety analyses, objects are taken as system components, attributes and values with the corresponding truth-value assignments as states, truth-value assignment changes as events. Endogenous variables represent the properties of object types and exogenous variables represent all properties of external conditions, which result from objects not further specified within the causal model but influencing the properties of the object types in the causal model.

2.2 Philosophical background and causal semantics

Causal theories distinguish between type causation (*causality*) and token causation (*causation*). Whereas the first describes general causal relationships (‘*pushing a button causes turning on a lamp*’), the second describes singular causation (‘*the turning red of the signal P1 at 13.13pm causes the train DC1 to stop at station X1*’). The elements of the causal relations are either state or event types (type causation) or states or events (token causation) [8]. In the previous section, we have defined a causal model by means of variables and structural equations. Type causation is given by the truth-value conditions of the structural equations. Once, if a truth-value assignment is made (token causation) one can determine the truth values of the dependent variables. But so far, nothing has been said under which circumstances states or events are causally connected. For that, we use Dowe’s transference theory, which is strongly related to information transfer processes [15]: Dowe defines physical causation by means of an entity transfer between objects, which obeys a physical conservation law (e.g. a transfer of energy or momentum). He distinguishes between four causal relationships: Causation, prevention, omission and prevented omission. His approach of physical causation remains informal.

In order to reason formally about causes and their consequences, we extend Dowe’s informal approach to the formal structural equation modelling. The basic causal relations of Dowe’s approach have been adopted for technical system structures: If a causal relation between type C and type E is given, in technical applications further types B are taken as *barriers* corresponding to causal prevention and types S as *supervisions* corresponding to causal omission. The type C is taken as a *cause* and the type E as an *effect*. We define the transfer entity as an object type, which carries information content and might lead to an attribute value change.

2.3 Structural equation for basic causal patterns of technical applications

Let M=<**V**,**U**,**F**> be a causal model, whereas the endogenous variables $V_i \in \mathbf{V}$ with $V_i =_{def}$[att(O(x))@val] or $\neg V_i =_{def} \neg$[att(O(x))@val], respectively, define the properties of the object types O, which receive or send a transfer entity. To avoid eyestrain, we write only the variables V_i bearing in mind that the variables describe the attributes and values of the corresponding objects types. The exogenous variables represent the relevant starting conditions of the *causal story* to be analysed and are determined outside the model.

Truth-value assignments (causation) of the variables V_i or U_i, written v_i=true or u_j=true, mean that the corresponding object types with their properties are instantiated, v_i=false or u_j=false mean that the object types with their properties are not instantiated. **U**=**u** or **V**=**v** mean a fixed but arbitrary truth-value assignment. The general causal relations are given by the structural equations representing the *truth-value conditions* (causality). The truth-value assignments of the independent variables determine the truth value of the dependent variable V_i. Remind that omission is a causal relation, in which a non-occurrence of an event causes another event, prevention, in which an occurrence of an event causes the non-occurrence of another event, and prevented omission, in which a non-occurrence of an event causes the non-occurrence of another event [15].

Definition 2.2 (Structural equation of basic causal patterns) *Let C, E, S and B be variables of a causal model M. Then the basic causal patterns are given by the structural equations:*

- *Direct causation:* $E=C$;
- *Omission:* $E=\neg C$ *or* $E=C\lor S$;
- *Prevention:* $\neg E=C$ *or* $\neg E=\neg C\lor B$;
- *Prevented Omission:* $\neg E=\neg C$. □

The variables can be further decomposed, e.g. C might be a conjunction or disjunctions of other variables, formally $C=\lor_i \land_j C_{ij}$ with $C_{ij} \in \{C_1,\ldots,C_n\}$. Cases of over-determination (*parallel structures*), i.e. effects, which can be caused by more than one cause, or epiphenomena (*common causes*), i.e. effects, which are caused by only one cause, are modelled by means of standard logic disjunction or conjunction. The causal context is considered by means of a causal field C_F, which is conjunctively connected to the actual cause of a transfer [16].

Definition 2.3 (Serial structure, parallel structure, common cause, causal context) *Let C, C', E, E',* C_F *be variables of a causal model M. Then the structural equations of parallel, conjunctive, serial, common cause and context structures are:*

- *Parallel structure:* $E=C\lor C'$ *(over-determination);*
- *Conjunctive structure:* $E=C\land C'$*(conjunctive causes);*
- *Serial structure:* $E=C$; $E'=E$ *(causal chain);*
- *Common cause structure:* $E=C$; $E'=C$ *(epiphenomenon);*
- *Context structure:* $E=C\land C_F$ *(causal field).* □

Special types of over-determined causation are late or early pre-emption cases. For safety analysis, only early pre-emption has to be considered: Early pre-empted cases are types of singular causation, where an effect E might be caused by alternative causes C or C', but if one cause, e.g. C, is instantiated, the alternative causes are cut-off, i.e. cannot be instantiated, formally $E=C\lor\neg C'\oplus\neg C\lor C'$ ($\oplus$ exclusive-OR). Late pre-empted cases are types of singular causation, where an effect E might be caused by alternative causes, but as soon as the effect is instantiated alternative causes cannot further contribute to the instantiation of the effect E. In contrast to early pre-emption cases, the alternative causes are not cut-off. Because the scope of safety analysis is the derivation of causes contributing to undesired effects, it is sufficient to consider, if at least one cause of alternative causes can instantiate an effect and if one cause is instantiatable.

Beside the causal patterns given above, there are no more causal relation structures except causal interactions and causal cycles [17]. Causal interactions and cycles are not considered in our approach.

2.4 Reasoning about failures by means of interventions

After giving the basic structural equations of causal relations, it is possible to determine the failure behaviour of technical systems. For that, the intervention technique provided by the SEM method is used. Interventions are taken as an abnormal, i.e. failure behaviour of a technical application: In case of an intervention of a variable X of a causal model M, the variable X is set to a fixed truth value independently of the truth values of the other variables yielding a submodel of M. Then, the consequences of that intervention to a variable Y representing the undesired event are analysed.

The following algorithm evaluates systematically the effect of interventions to an endogenous variable Y. We summarize the algorithm for the *conditional analysis* briefly (in the following, all used indices are self-evident and are elements of the natural numbers).

Given a causal model M with the truth-value conditions, first the truth values of the exogenous variables **U** are assigned. The k^{th} truth-value assignment of **U** gives one possible *causal story* and corresponds to the relevant external conditions, which have to be fulfilled for a properly working technical application (e.g. the environmental temperature or the correct installation of the system). Because the variables $U_j \in \mathbf{U}$ can take values *true* or *false*, there exist 2^m truth-value assignments (*m* number of exogenous variables U_j). The system analyst chooses the k^{th} causal story $(\mathbf{U}=\mathbf{u})_k$ to be analysed, which represents the intact behaviour of the technical application. Derivations from the external conditions $(\mathbf{U}=\mathbf{u})_k$ result in other causal stories. Given the k^{th} causal story, the following algorithm of the *conditional analysis* starts by setting the endogenous variables successively to a fixed value [11]. The effect of these interventions with respect to the truth value of the endogenous variable Y (the undesired event) is determined by evaluating the truth values of all other variables of the model M. We write $[(\mathbf{W}=\mathbf{w})>(Y=y)|(\mathbf{U}=\mathbf{u})_k]$ for the conditional with $\mathbf{W} \subseteq \{\mathbf{V},\mathbf{U}\}$: On the condition $(\mathbf{U}=\mathbf{u})_k$, Y takes the truth value y (Y=y), if $\mathbf{W} \subseteq \{\mathbf{V},\mathbf{U}\}$ is set to $\mathbf{W}=\mathbf{w}$. The interventions of the endogenous variables are taken as *primary failures*. The effects of an intervention to other endogenous variables are taken as *command failures*. Interventions of the exogenous variables yielding other causal stories are taken as *secondary failures*. We abbreviate $V_{i1,i2,\ldots,ij}$ (indices $1 \leq i_1 < i_2 < \ldots < i_j \leq n$, $i_k \neq i_p$, *n* number of endogenous variables) for the ordered combination of variables $V_{i1}V_{i2}\ldots V_{ij}$, where $V_{i1},V_{i2},\ldots,V_{ij} \in \mathbf{V}$, and stipulate that there is no causal chain from Y to any of the variables $V_{i1},V_{i2},\ldots,V_{ij}$. That is, any intervention of $V_{i1},V_{i2},\ldots,V_{ij}$ might influence the truth value of Y but not vice versa.

```
PRECONDITIONS
        M=<U,V,F> a causal model; $Y \in \mathbf{V}$ investigated;
        p the maximum order of interventions; $FS=\emptyset$ a set (failure set);
INPUT
        $(\mathbf{U}=\mathbf{u})_k$ the $k^{th}$ truth-value assignment of
        the exogenous variables U;
PROCEDURE
        IF $[(\mathbf{U}=\mathbf{u})_k>(Y=y)]| (\mathbf{U}=\mathbf{u})_k]$ THEN STOP;
        $j=0$; $1 \leq i_1 < i_2 < ... < i_j \leq n$ ($i_k \in \{1,...,n\}$);
        WHILE $j<=p$ DO
          Set last intervention truth-value assignment
          $V_{i1,i2,\ldots,ij} = v_{i1,i2,\ldots,ij}$ and evaluate truth-value
          assignment $\mathbf{V}=\mathbf{v}$ in M=<U,V,F>;
          FOR EACH $V_{i1,i2,\ldots,ij} \notin FS$ DO
            FOR EACH $i_{j+1}>i_j$
            Intervention $V_{ij+1} = \neg v_{ij+1}$
              IF $[(V_{i1,i2,\ldots,ij+1} = v_{i1,i2,\ldots,ij+1})>(Y=y)]|(\mathbf{U}=\mathbf{u})_k]$
              THEN $V_{i1,i2,\ldots,ij+1} \in FS$ with failure state
              $V_{i1,i2,\ldots,ij+1} = v_{i1,i2,\ldots,ij+1}$
              ENDIF;
            $j=j+1$;
            ENDFOR;
          ENDFOR;
        ENDWHILE;
OUTPUT
        failure set FS of interventions of maximum order p
END.
```

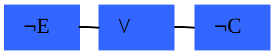
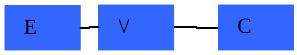
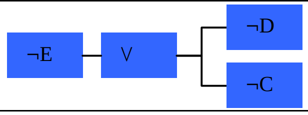
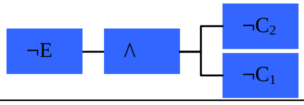
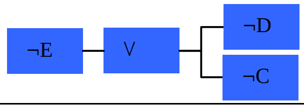
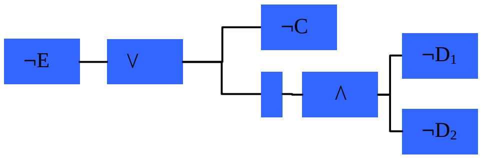
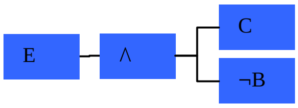
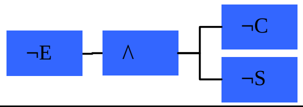
The intervention $V_{i1,i2,\ldots,ij}=v_{i1,i2,\ldots,ij}$ yielding Y=y (the undesired event) is stored to a failure set FS and is ruled out for further analysis. Analogously to the cut set order of FTA, the conditional analysis stops, if the maximum number *p* (normally $p<10$) of intervention combinations is achieved (therefore, the non-linear complexity of the algorithm does not concern). Systematically, all interventions up to the order *p* are analysed with respect to the effect Y=y. For example, the first order intervention $V_j=\neg v_j$ is taken to be an unexpected behaviour. If the intervention $V_j=\neg v_j$ does not lead to Y=y, the second order intervention V_jV_k ($j<k<n$) is investigated by negating the truth value $V_k=\neg v_k$ of the before analysed causal story with $V_j=\neg v_j$.

2.5 Fault Tree Construction

The conditional analysis yields the consequences of both single failures and multiple failures. Due to the fact that barriers are modelled by means of the corresponding causal pattern (see Definition 2.2), their failing can also be analysed by the intervention method. Thus, beside the FTA and FMEA the safety barrier analysis is integrated in our approach.

Table 1 shows the transformation of some basic causal relationships given by the structural equations into fault trees. The transformation is based on the intervention method and can be derived by the algorithm given above.

Table 1. Transformation of some basic causal patterns given by structural equations to fault trees. In favour of a condensed representation, the fault trees are horizontally represented with top-event on the left side (untitled events are intermediate events).

Basic causal pattern	Structural equation (right side of equations: desired event)	Transformation into Fault-Tree (top-event: undesired event)
serial structure (causal chain/ direct cause)	$E=C$	
serial structure (prevented omission)	$\neg E=\neg C$	
serial structure (causal chain/ indirect cause)	$E=D$; $D=C$	
parallel structure (over-determination)	$E=C_1 \vee C_2$	
conjunctive structure (necessary cause)	$E=C \wedge D$	
common cause (epiphenomenon)	$E=C \wedge (D_1 \vee D_2)$	
barrier (prevention)	$\neg E=\neg C \vee B$	
supervision (omission)	$E=C \vee S$	

3 Example and Application

We have applied our approach to a fictive technical application of a level crossing. The example is as follows: A train approaches the danger zone of a level crossing. Before its arrival at the danger zone, the train switches on a protection via two redundantly connected sensors in order to prevent a collision between the train and cars or pedestrians. The two sensors detect the train's approach. A car (exemplarily for the road traffic) stops due to the signal of the traffic lights and due to the closed barrier.

The physical transfer model is as follows. A train and a car are transferred to the danger zone of the level crossing. The information content of the train approach is transmitted to two sensors, e.g. by means of an electromagnetic field transmission. The two sensors (sensor#1 and sensor#2) send their information content of the train approach to the traffic lights and the level crossing barrier. The barrier and the traffic lights serve as a protection (*barrier*) with respect to the car transfer. The physical transfer of the car to the train represents the undesired event. A collision between the car and the train does not occur, that is, either the train or the car is not in the danger zone. The causal model M with the exogenous variables, the endogenous variables and the corresponding structural equations is given in Table 2.

The interventions of second order give three interventions resulting in the undesired event: Both sensors do not detect the train {v_3=false; v_4=false}, although the train is approaching, both the barrier and the traffic lights fail {v_5=false; v_6=false}, although the train is approaching, and although the train is not approaching, the train is in the danger zone {v_1=false; v_7=true}. The last intervention requires an explanation, because it seems contradictorily: A train, which does not approach, cannot occur in the danger zone. One would expect that

v_1=false results always in v_7=false. But if interventions are excluded, one has to be careful. In our example: If a train stops between the track position of the two sensors and the danger zone due to any reason, it might happen - depending on the system architecture - that after a while, e.g. after a timer is expired, the level crossing protection is released automatically. In that case, the train might not approach (v_1=false, approaching is in the past), but continues to moves into the danger zone (v_7=true). Thus, whether an intervention can occur or not, has to be assessed by the system analyst.

Table 2. Variables and truth-value assignments of the causal model of the level crossing example.

No.	Endogenous variables	Structural equation	Truth-value assignment	Causal pattern
1.	V_1=[train_location(train(x))=approach]	$V_1=U_1$	u_1=true v_1=true	Causation
2.	V_2=[car_location(car(x))=approach]	$V_2=U_2$	u_2=true v_2=true	Causation
3.	V_3=[train_detection(sensor#1(x))=detect]	$V_3=V_1$	v_3=true	Causation
4.	V_4=[train_detection(sensor#2(x))=detect]	$V_4=V_1$	v_4=true	Causation
5.	V_5=[traffic_guard(barrier(x))=closed]	$V_5=V_3 \lor V_4$	v_5=true	Over-determination
6.	V_6=[traffic_guard(traffic_lights(x))=red]	$V_6=V_3 \lor V_4$	v_6=true	Over-determination
7.	V_7=[train_location(train(x))=danger_zone]	$V_7=V_1$	v_7=true	Causation
8.	V_8=[traffic_rules(car_driver(x))=attended]	$V_8=U_3$	u_3=true v_8=true	Causation
9.	V_9=[car_location(car(x))=danger_zone]	$\neg V_9=\neg V_2 \lor ((V_5 \lor V_6) \land V_8)$	v_9=false	Barrier and causal field
10.	V_{10}=[train_collision(train(x))=collided]	$\neg V_{10}=\neg V_7 \lor (\neg V_9)$	v_{10}=false	Barrier

In Table 3, the FMEA (single mode failures) of the level crossing example and possible countermeasures are given. Every first order intervention yield v_{10}=false except the interventions v_8=false and v_9=true. These interventions lead to $\neg V_{10}(\neg v_{10}=\text{false})=\neg V_7(\neg v_7=\text{false}) \lor (\neg V_9(\neg v_9=\text{false}))$. First, although the barrier is closed (v_5=true) and the traffic lights are switched red (v_6=true), the car is in the danger zone (for example, because the car engine stops unexpectedly while the car in the danger zone). Second, the barrier is closed and the traffic lights are switched red, but cannot fulfil properly their intended functions, because the car driver does not attend to the traffic rules. This might happen, because the car driver ignores both the barrier and the traffic lights, and drives round the barrier. The structural equation approach aims at reasoning about the conditional '*what happens, if…*' and gives indications of technical countermeasures in order to mitigate or even avoid the consequences of failures. For instance, the possibility of driving round the barriers might be avoided by an on-board system, which stops a car automatically. Figure 2 shows the part of the fault tree revealed by our algorithm up to the second order of interventions.

Table 3. FMEA for the causal model of the level crossing.

No.	Failure mode	Failure consequence	Reason	Intervention	Countermeasures
1.	Car unexpected in the danger zone	Car collides with the train	Car engine fails	v_8=false	Automatic on-board car control (automatic stop, if level crossing is closed)
2.	No attendance to traffic rules	Car collides with the train	Car driver is inattentive	v_9=true	Automatic on-board car control (automatic stop, if level crossing is closed)

The reasons for the interventions might be further broken down by means of more endogenous variables. The scalability and granularity of the causal model depend on the information the analyst has and wants to integrate into the causal model. For example, one might model that the car engine works correctly. The car therefore does not stop in the danger zone unexpectedly as long as the car engine is intact.

If interventions of variables are excepted because of their non-occurrence or due to the inconsistency of their occurrence, one can exclude such interventions. For instance, if the barrier functions of the level crossing cannot be bypassed, the corresponding interventions of the barrier variables are not allowed. But in order to have a complete coverage of the intervention analysis, it is recommended to exclude such interventions *after* performing a complete intervention analysis.

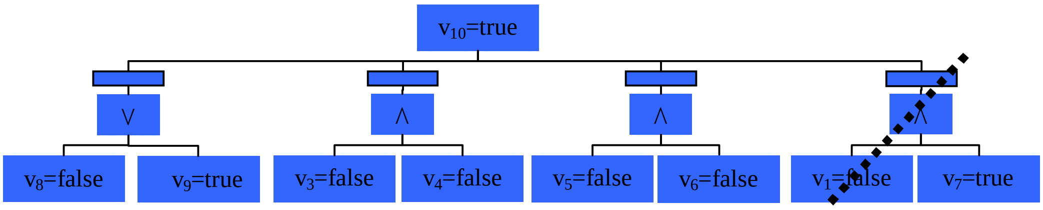


Figure 2. Cut-off of the fault tree (second order intervention) derived from the causal model of a level crossing. The crossed-out part might be contradictory and has to be ruled out by the system analyst (untitled events are intermediate events).

4 Conclusions

We have presented a new conditional analysis method for system and safety analysis, which integrates the methods of safety barrier (SBA), fault tree (FTA) and failure mode and effect analysis (FMEA) into one method. Our approach uses results from the philosophical theories concerning causality and causation. We have adopted the philosophical results to a formal framework of structural equation modelling (SEM): Basic causal patterns can be used to compose complex system structures. Using the intervention method provided by the SEM method, we have developed an algorithm to generate automatically the consequences of failures (primary, secondary and command failures). Beside the classical failure analysis, our approach might serve as a method to give countermeasures and prove their suitability for mitigation or avoidance of undesired events. In the next step, a tool support and the integration of the time parameter are planned (currently, our method is proprietarily implemented using standard mathematical tools).

References

1. Goldberg, B.E., Everhart, K., Stevens, R., Babbitt III, N., Clemens, P., Stout, L.: System Engineering “Toolbox” for Design-Oriented Engineers. Alabama, USA: NASA Reference Publication 1358 (1994)
2. Xiang, J., Ogata, K.: Formal Fault Tree Analysis of State Transition Systems. Fifth International Conference on Quality Software (QSIC'05). Melbourne (2005) 124-134
3. Szabó, G., Tarnai, G.: Automatic Fault-Tree Generation as a Support for Safety Studies of Railway Interlocking Systems. In: Proceedings of the IFAC Symposium on Control in Transportation Systems, Braunschweig (2000) 453-458
4. Papadopoulos, Y., Parker, D., Grante, Ch.: A Method and Tool Support for Model-based Semi-automated Failure Modes and Effects Analysis of Engineering Designs. In: Conferences in Research and Practice in Information Technology 38, Australian Computer Society (2004)
5. Moffett, J.D., Vickers, A.J.: Behavioural Conflicts in Causal Specification. Automated Software Engineering 7(3) (2000) 215-238
6. Johnson, C.W., Holloway, C.M.: A Survey of Causation in Mishap Logics. Reliability Engineering and Systems Safety 80(3) (2003) 271-291
7. Ladkin, P.: Causal System Analysis. Berlin: Springer (2006)
8. Collins, J.D., Hall, N., Paul, L.A. (eds.): Causation and Counterfactuals. Cambridge, USA: MIT Press (2004)
9. Schellhorn, G., Thums, A., Reif, W.: Formal Fault Tree Semantics. In Proceedings of The Sixth World Conference on Integrated Design & Process Technology. Pasadena, Canada (2002)
10. Ortmeier, F., Schellhorn, G.: Formal Fault Tree Analysis - Practical Experiences. Electr. Notes Theor. Comput. Sci. 185 (2007) 139-151
11. Filippidis, L.: Failure Effect Analysis Based on Causal Analysis. Prior Art Database. Intelectual Property at SIEMENS AG, IPCOM Disclosure Number IPCOM000175241D (2008)
12. Kuntz, M., Leitner-Fischer, F., Leue, L.: From Probabilistic Counterexamples via Causality to Fault Trees. In Proceedings of the Computer Safety, Reliability, and Security - SAFECOMP 2011. Naples (2011) 19-22
13. Pearl, J.: Causality (2^{nd} edition). New York, USA: Cambridge University Press (2009)
14. Stamatelatos, M., Vesley, W.: Fault Tree Handbook with Aerospace Application (Version 1.1). Washington, USA: NASA (2002)
15. Dowe, P.: Physical Causation. Cambridge: Cambridge University Press (2000)
16. Mackie, J.L.: Cement of the Universe. Oxford: Oxford University Press (1980)
17. Baumgartner, M., Graßhoff, G.: Causality and causal Reasoning (german). Bern: Bern Studies in the History and Philosophy of Science (2004)