Formalized Risk Assessment for Safety and Security

Joachim Draeger

Abstract

The manifold interactions between safety and security aspects in embedded systems makes it plausible to handle safety and security risks in a unified way. The paper develops a corresponding risk measure in the context of discrete event systems (DEVS). The chosen approach is based on a simulation of system dynamics, which allows risk assessments even in cases with stepwise system degradation, cascading failures, or cognitive attackers. The plausibility of the proposed risk measure is shown by its consistency with ‘classical’ notions of risk. Its non-computability, on the other hand, indicates a realistic behavior in the presence of complex dynamics. Power grids are discussed as an application example and indicate some of the advantages of the proposed method.

1 Introduction

1.1 Safety Risks and Security Risks

The notion of risk recaps the expected amount of losses related with the usage of a specific system $M$. This makes risk an important system property. The notion of risk is not uniquely defined, however. It can be characterized from at least two different perspectives, safety [67] and cyber security [10]. They are distinguished by who is typically acting on whom as given by Axelrod [6], whereby both safety and security usually make individual assumptions about $M$ [5, 25, 29]: Safety requires that the system must not harm the world; all deviations from the intended behavior are caused accidentally. In the contrary, security demands that the world must not harm the system, though intelligent adversaries belonging to the world are acting in an intentionally malicious way.

Due to these differences, safety and security risk assessments are typically executed independent from each other. This may be justified in some cases, but may be inappropriate in many others. Let us consider some examples, in which safety and security risks are intertwined.

- Let us assume that a decision has to be made whether free resources of system performance should be invested in system monitoring or system defense. Risk assessments from the safety resp. security perspective carried out independently may not help in finding an answer.

- In a cyber attack on a German steel mill in 2014, hackers used social engineering techniques for getting access to the control systems of the production plant. They modified the control systems in a way, that the safety of the plant was compromised. It was not possible anymore to shut down a blast furnace. The resulting damage of the plant was significant [47].

- The Stuxnet worm [40, 53] is an example of a self-propagating malware compromising specific industrial control systems. As a result, uranium enrichment facilities in Iran seem to suffer substantial damage.
Without a combined view at safety and security, the situations described above can not be appropriately modeled. Instead, trade-offs and overlaps between safety and security suggest the development of a unified approach to safety and security risk assessments as recommended in e.g. [48]. Knowledge about upcoming events, system characteristics, and system behaviour will contribute significantly to the quality of the intended assessments. The availability of such knowledge can not be taken as granted, however. According to the theorem of Rice [32], it will not be possible to decide about nontrivial properties of a general computable system. Only their enumeration can be realized e.g. by experimenting with simulations [28, 46], which explore the effects of faults and intrusions on the system. Consequently, in this paper a simulation-based risk notion is developed and analyzed. Up to now, the potential of such a risk concept does not seem to be discussed in necessary depth [44]. The basic idea of such an approach was already presented in [20], which can be considered as predecessor of the actual paper.

1.2 Related Work

Though the differences between safety and security poses a challenge for a common handling, an unified risk assessment is discussed and judged as possible e.g. in [12, 38]. Concepts of risk, which are applicable to both safety- and security-related situations, can be found in [6, 57]. Corresponding approaches for a common risk assessment process are developed in [51, 52]. Neither the cited notions of risk nor the risk assessment processes are simulation-based. An approach integrating safety and security risks based on fault trees and thus using a much stronger abstraction is given in in [27].

The paper [37] discusses a simulation-based approach to risk assessment for the special case of stochastically varying demands on a production facility. Similar considerations from the security risk point of view were made in [11, 19, 53, 69]. Another special case is considered in [8], wherein the authors are focusing on the Monte-Carlo simulation of air traffic control operations.

An application of discrete event simulation as specific simulation paradigm to cyber security problems is discussed in [22], though these considerations are not risk-related. A similar statement can be made about the paper [17], which models cyber attacks based on the DEVS formalism.

1.3 Structure of the Paper

Section 2 describes, how the systems under consideration can be formalized using the DEVS formalism. The system extensions, which are necessary for representing faults and threats and thus a off-nominal system behaviour, lead to a so-called risk system, which reproduces the nominal system behavior as a special case. In section 3, a simulation-based risk measure is defined on these risk systems enabling a unified risk assessment. The consistency of the proposed risk measure with classical notions of safety- and security-related risks is shown in section 4, which supports the view that it can be considered as well-defined. This section touches also the (non-)computability of the simulation-based risk measure. The final section 5 demonstrates the advantages of the new simulation-based risk measure using power grids as an example. The paper closes with an outlook.

2 Formalization of Systems

For executing the intended risk assessment for the system $S$, at first a suitable model of $S$ has to be constructed. This is done by representing $S$ using the DEVS
formalism \cite{70,71}. The DEVS formalism developed by Zeigler in 1984 is proposed due to its generality and flexibility. It has the capability to represent all kinds of systems, which have an input/output behavior describable by sequences of events. Despite of the capability to handle many types of discrete systems \cite{73}, the DEVS formalism in its original formulation is not able to handle stochastic aspects as they occur in the domain of safety and security quite regularly. This gap was closed by the introduction of the STDEVS formalism, which is an extension of the DEVS formalism. In \cite{43} it is shown that a DEVS model is a special case of a STDEVS model.

2.1 DEVS Models of Systems

In the following, the definition of a DEVS model is recapitulated for a better understanding. Doing so, we are following \cite{65,68}. Being precisely, we are talking about atomic DEVS models in the following. Though coupled DEVS models have been defined as well, which are more general from the structural point of view, it can be shown that coupled and atomic DEVS models have the same expressive power \cite{70,71}. For reasons of simplicity, we are thus restricting ourselves to atomic models.

\textbf{Definition 1 (DEVS Model).} An (atomic) DEVS model is an 8-tupel $M = (X, Y, Q, q_{\text{start}}, \delta_{\text{int}}, \sigma, \delta_{\text{ext}}, \lambda)$ with

- $X$ as set of input events
- $Y$ as set of output events
- $Q$ as set of states
- $q_{\text{start}} \in Q$ as initial state
- $\delta_{\text{int}}: Q \rightarrow Q$ as the internal transition function
- $\sigma: Q \rightarrow \mathbb{R}_0^+ \cup \{\infty\}$ as the time advance function
- $\delta_{\text{ext}}: \bar{Q} \times 2^X \rightarrow Q$ as the external transition function defined on $\bar{Q} = \{(q, t) | q \in Q, 0 \leq t \leq \sigma(q)\}$ as the total set of states
- $\lambda: Q \rightarrow Y \cup \{\phi\}$ as the output function

\textbf{Remark 1 (DEVS Model).} 

- The time advance function $\sigma$ gives the lifetime of an internal state $q \in Q$. The internal state $q' \in Q$ entered after reaching the end of the lifetime $\sigma(q)$ of $q$ is determined by the internal transition function $\delta_{\text{int}}$ via $q' = \delta_{\text{int}}(q)$. As time in the real world always advances, $\sigma(q)$ must be non-negative. The value $\sigma(q) = 0$ indicates an instantaneous transition. If the system is to stay in an internal state $q$ forever, this is modelled by means of $\sigma(q) = \infty$.
- The definition of the set $\bar{Q}$ of total states is based on the idea to supplement the internal state $q \in Q$ by the elapsed time $e \in [0, \sigma(q)]$ since the system has entered the state $q \in Q$.
- External events influence the system as described by the external transition function $\delta_{\text{ext}}: \bar{Q} \times 2^X \rightarrow Q$. This function can handle sets of events representing simultaneously occurring events. Such a capability is necessary, because different events coming from different sources may arrive at the same time.
The output event $\lambda(q)$ is generated when the time $\epsilon$ elapsed after entering the state $q \in Q$ reaches the lifetime $\sigma(q)$ of the state $q$, i.e. $\epsilon = \sigma(q)$. At all other times, the output is equal to the non-event $\phi$.

Incoming events can trigger transitions between states. Thus, the dynamics of DEVS models is based on the so-called time-advance function $\sigma$ and the state transition functions $\delta_{\text{int}}$ and $\delta_{\text{ext}}$. This leads to the following description of the dynamics of a DEVS model $M = (X, Y, Q, q_{\text{start}}, \delta_{\text{int}}, \sigma, \delta_{\text{ext}}, \lambda)$ [12]. Let $q \in Q$ be the actual state of $M$. We have to distinguish two cases. The first case is that no external event occurs, the second case handles the arrival of events $x \in 2^X$.

In the first case, the system dynamics is determined by the lifetime $\sigma(q)$ of $q$ and the internal transition function $\delta_{\text{int}}$, in the second case by the external transition function $\delta_{\text{ext}}$.

In the first case — i.e. without the occurrence of external events $x \in 2^X$ — the system remains in the state $q$ for time $\sigma(q) \in \mathbb{R}_0^+ \cup \{x\}$. This means:

- For $\sigma(q) = 0$, the state $q$ is immediately changed to the state $q' \in Q$ given by $q' = \delta_{\text{int}}(q)$. This state transition can not be influenced by external events.
- For $\sigma(q) = \infty$, the system stays in state $q$ as long as no external events $x$ occur.
- For $\sigma(q) \in \mathbb{R}^+$, the system outputs the value $\lambda(q)$ after expiration of the lifetime $\sigma(q)$ of the state $q$. Afterwards, the system state changes to $q' \in Q$ given by $q' = \delta_{\text{int}}(q)$.

In the second case — i.e. with occurrence of external events $x \in 2^X$ — the system changes to a new state $q' = \delta_{\text{ext}}(q, t, x)$, whereby $(q, t) \in Q$ is the actual total state of $M$ when the set $x$ of events occurs.

Summing up, events may trigger state transitions in a DEVS-model $M$. A state transition may also occur automatically after a certain time. When entering a new state, the model $M$ may generate an output event again. In [31] it is shown that an (atomic) DEVS has the computational power of a Turing machine. This means that everything representable on a common computer will also be representable in the DEVS paradigm. These are good news, since we are aiming at a general method. It is especially helpful for representing cognitive aspects, which may be important for the IT security perspective.

### 2.2 STDEVS Models of Systems

Stochastics is required for representing probabilistically occurring safety faults and security incidents. This is done by replacing the deterministic DEVS formalism by the corresponding probabilistic STDEVS formalism. In effect, an (atomic) STDEVS-model is an (atomic) DEVS model supplemented by mappings $P_{\text{int}}, P_{\text{ext}}$ providing transition probability informations for the internal and external transition functions $\delta_{\text{int}}, \delta_{\text{ext}}$. Thus, an (atomic) STDEVS model has the structure [15] [16]

$M = (X, Y, Q, q_{\text{start}}, \delta_{\text{int}}, P_{\text{int}}, \sigma, \delta_{\text{ext}}, P_{\text{ext}}, \lambda)$. In this definition, $\delta_{\text{int}} : Q \to 2^Q$ is the internal transition function, which describes the set of possible successor states $\delta_{\text{int}}(q) \subseteq 2^Q$ to the actual state $q$ for situations without occurrence of an external event. Thus, $\delta_{\text{int}}(q)$ contains all the subsets of $Q$ that the next state can belong to. The partial function $P_{\text{int}} : Q \times 2^Q \to [0, 1]$ gives the probability $P_{\text{int}}(q, Q')$ that the system model $M$ being in state $q$ makes a transition to a state $q' \in Q' \in \delta_{\text{int}}(q)$.

Concerning the requirements for the well-definedness of the probability spaces, see [15] [16].

Corresponding to $\delta_{\text{int}}$, $\delta_{\text{ext}} : Q \times \mathbb{R}_0^+ \times 2^X \to 2^Q$ is the external transition function. It describes the set of possible successor states $q' \in \delta_{\text{ext}}(q, t, x) \subseteq 2^Q$ for a situation
with occurrence of external events \( x \in 2^X \), when the system model \( M \) is in a total state \( (q, t) \in Q \). Analogously to \( P_{\text{int}} \), the partial function \( P_{\text{ext}} : Q \times X^+ \times 2^X \times \mathbb{Q}^\times \rightarrow [0, 1] \) gives the probability \( P_{\text{ext}}(q, t, x, Q') \) that the system model \( M \) being in the total state \( (q, t) \) makes a transition to a state \( q' \in Q' \in \delta_{\text{ext}}(q) \) at occurrence of \( x \).

For a STDEVS, the lifetime of a state \( q \in Q \) is defined in the same way as in the case of a DEVS, though concerning e.g. safety problems, a stochastic lifetime function \( \sigma \) would allow a much more canonical representation of stochastically occurring faults. Being more precise, the lifetime of a state \( q \in Q \) would then become a mapping \( \sigma \) from a state to a random variable with given stochastics. Such an approach is not realized here, however. A straightforward generalization to a stochastic version allowing any time span between two consecutive faults would lead to a tree of simulation traces containing branching points with uncountably many options for a continuation.

**Definition 2** (Language of a STDEVS system). Let \( M \) be a STDEVS model and \( h \in \mathbb{R}^+ \) be a nonnegative real number. The set of possible simulation traces of \( M \) limited to the time interval \([0, h]\) is called the language \( L(M, h) \) of \( M \) for the (time) horizon \( h \). Formally, a simulation trace is a sequence \((\rho_1, \ldots, \rho_k)\) representing the history of the corresponding simulation run consisting of elements \( \rho_j = (q_j, t_j, X_j) \in Q \times X^+ \times 2^X \). These elements \( \rho_j \) document the start resp. end states of all state transitions \( q_{j-1} \rightarrow q_j \) during the simulation run, eventually triggered by the set \( X_j \) of incoming events. In this definition, the start state \( q_0 \) of the first state transition (i.e. \( j = 1 \)) is equal to the initial state \( q_0 := q_{\text{start}} \) of \( M \). The case \( X_j = \emptyset \) indicates an internal state transition \( q_{j-1} \rightarrow q_j \), otherwise an external state transition is represented. The times \( t_j \) indicate, how long \( M \) was in the state \( q_{j-1} \) for \( j < k \). For \( j = k \), the time \( t_k \) is limited by the horizon \( h \). In this way, \( t_1 + \cdots + t_k = h \) is assured.

The language \( L(M, h) \) represents the possible behaviors of the system, which can be produced by different event sequences as input. The informations contained in the elements \( \rho_j \) of a simulation trace \( \tau = (\rho_1, \ldots, \rho_k) \in L(M, h) \) are rich enough for allowing a reconstruction of the probabilities for the occurrence of state transitions \( q_{j-1} \rightarrow q_j \) and of other properties.

For a DEVS resp. STDEVS model, an event may arrive anytime and may lead to various state transitions. Though the number of internal states in a DEVS resp. STDEVS model is finite and thus countable, of course, the set of total states described as a combination of internal states and timing informations is not. It can be shown, however, that in a DEVS model these principally uncountable many cases of model behavior will only lead to countably many different state transition sequences \([35, 39]\). Since a STDEVS model is in essence a DEVS model extended by probabilities of state transitions, the representing state-transition graph remains finite (in an appropriate representation) for a STDEVS as well. As a consequence, the tree of possible state sequences of \( M \) has a countable size and each node in the tree has only a finite number of branching options. For a given finite time horizon, the tree of simulation traces is thus finite, too, as long as the state-transition graph does not contain cycles with transition time equal to 0.

Since STDEVS models are a generalization of DEVS models and since the expressive power of the DEVS formalism corresponds to that of a Turing machine, the class of systems representable by a STDEVS model includes all Turing computable situations. Additionally, many stochastic discrete systems belong to this class as well. Again, remember that the extension of the modeling paradigm by stochastic aspects results from the requirement to represent faults and security-related incidences.
2.3 Inclusion of Safety and Security Risk Cases

The proposed approach of risk assessment is based on a STDEVS model $M$ of the system $S$ under consideration. It can not be expected, however, that an ordinary model $M$ of the system $S$ is suitable from the perspective of the intended risk assessment task. This is due to the fact that an ordinary model usually represents only the nominal behavior of $S$. A risk assessment will consider off-nominal modes of the system as well, which thus have to be represented in the model. As a consequence, we need an extension of $M$ covering safety- and security-related problems like error-modes and vulnerabilities w.r.t. specific threats. This can be realized in a three-step process.

In the first step, $M$ is supplemented by components of the system environment $U$, which are either affecting the system $S$ or affected by $S$ in a safety or security relevant way. Dependent on the situations considered as relevant, this may include components, which are related to safety and security only in an indirect way. Concerning security risk assessments, for example, the criticality of a violation of the system security will sometimes depend on the exploitation of this violation. If sensitive data have been exposed, the attacker may choose the option just to indicate that he has seen these data; but he may also use the option to publish these data. The criticality of the two choices may be very different.

In the second step, the safety and security problems themselves are represented in the model as well as components related to problem management. Especially the adversarial scenario given by cyber security can only be handled adequately if both sides — the attacked system $S$ and the attacker — are modeled at a similar level of detail. For example, a cognitive attacker requires a cognitive systems control as counterpart for assuring an appropriate defense. Such a counterpart keeps track on the attack to avoid unnecessary threats, and to organize the defense in an adequate manner. These actions of the defender are contributing to the controllability of a specific risk leading to a mitigation of its criticality.

In the third step, finally descriptions of the interactions between the system $S$ and its environment $U$ are added using the new components, which are introduced in the first and second step. These interactions are essential for safety and security considerations as discussed in the introduction.

After these extensions, the model $M$ describes both the nominal and off-nominal behavior of the system $S$. Moreover, $M$ is now necessarily a stochastic model, since e.g. a fault typically occurs with a certain probability. This makes $M$ suitable for the intended risk assessment. The STDEVS formalism seems to be a suitable modeling paradigm for the extended model $M$.

3 Principles of a Simulation-Based Risk Measure

3.1 Advantages of a Simulation-based Approach

The model $M$ modified by the extensions made in the last section provides a description of the nominal and off-nominal system behavior. In the following, a risk measure $R$ is defined for an unified assessment of safety and security risks and a simulation-based procedure for calculating $R$ based on $M$ is given. This includes, how specific faults, threats/vulnerabilities, and other off-nominal modes are contributing to the risk $R$. At first, though, some general remarks are made for safety and security.

In 'conventional' functional safety, a risk assessment is typically restricted to more or less instantaneous effects of a fault or a concurrent combination of faults. Correspondingly, conventional risk measures are usually following a static concept. The main reason for the preference of static methods is their simplicity. Static
methods provide results quite fast, they are well applicable to systems of significant size, and in many cases the results are a sufficiently good approximation to the real situation. In other cases, however, neglecting system dynamics will be an oversimplification [13]. Sometimes only the explicit inclusion of system dynamics allows the exploration of the propagation of effects across the system structure over time. This holds especially for the phenomenon of emergence in dynamic systems, i.e. the phenomenon of unexpected global behavior due to the behavior at the microscopic scale. Emergence can of course apply to the effects of faults etc. as well and may thus influence the results of an risk assessment. Indeed, [41] states that static risk measures suffer severe limitations as soon as process safety is considered.

For security, the inclusion of dynamics is even more important. Cyber security often assumes the existence of a cognitive attacker. This means that the attacker may follow a long-term strategy, which may correlate the probabilities of problem causes. Concerning risk, specifically the common assumption of statistical independence between consecutive events does no longer hold.

These arguments make the inclusion of dynamics in the risk assessment process advisable. Such an inclusion is possible by simulating system dynamics. Though this will make the risk assessment task more complicated, the higher quality — i.e. precision — of the risk assessment and the additional insight seems worth the effort. Taking dynamics into account means keeping track about changes in the system, which may be of importance for the risk assessment task due to modified transition probabilities, system parameters affected by the system evolution, or the occurrence of additional risk cases [42]. Thus, a simulation provides a forecast capability of potential future risks in some way.

For providing a notion of risk, which includes the dynamics of the system, we will take a closer look at the course of action after the occurrence of a fault or a realized threat. We start our considerations with a nominally behaving system. If a component of the system starts to behave off-nominal, then the system will usually alter the path of dynamics. In a STDEVS model $M = (X, Y, Q, q_{\text{start}}, \delta_{\text{int}}, P_{\text{int}}, \sigma, \delta_{\text{ext}}, P_{\text{ext}}, \lambda)$, this is represented as a state transition $q_1 \rightarrow q_1'$. $q_1, q_1' \in Q$. The new state $q_1' \in Q$ may be the first element of a state transition sequence, which transmits the information about the occurrence of the problem cause — in the following called cause for short — to other parts of the system (or its environment). There, the consequences of the cause may become effective by executing another change in the system state, i.e. a state transition $q_2 \rightarrow q_2'$. $q_2, q_2' \in Q_2$. Then the new state $q_2'$ is the (potentially disadvantageous) effect of the cause $q_1 \rightarrow q_1'$. Interpreting a cause as start point of a certain behavior the effect can be considered as a (disadvantageous) consequence of the behavior resulting from the cause.

Such a cause-and-effect resp. causality related perspective of risk is discussed in [23] [21], whereby effects are also called consequences. This kind of perspective is supported in [24] for safety and in [59] for security. Additionally, one has to note that in the description of the general cause-effect relationship given above, the state transitions $q_1 \rightarrow q_1'$ and $q_2 \rightarrow q_2'$ need not necessarily be different.

### 3.2 Criticality of a Simulation Trace

Main topic of the last section is the structural representation of system faults and threats/vulnerabilities, which may contribute to the risk $R$, in the model $M$. This is an important step towards calculating $R$, because we are now able to derive the existence of potential problems from the model $M$. For actually evaluating the contribution of this specific problem to the overall risk quantitatively, attributes have to be added for describing the properties of the problem under consideration. As typical for quantifying a risk, one has to know how frequent and how severe a specific system problem is. The severity is given as criticality $c: Q \rightarrow \mathbb{R}_0^+$ defined on the
total states $\bar{Q}$ of the STDEVS model $M$. It measures the amount of disadvantages resulting from the occurrence of a specific state $q \in Q$ for a certain duration $t \in \mathbb{R}_0^+$. According to this purpose, $c(q,t) \in \mathbb{R}_0^+$ will be a nonnegative real number. States with criticality larger than zero are representing modes of the system, which may contribute to the overall risk.

**Definition 3** (Criticality of an Effect). Let $M = (X,Y,Q,q_{\text{start}},\delta_{\text{int}},P_{\text{int}},\sigma,\delta_{\text{ext}},P_{\text{ext}},\lambda)$ be a STDEVS model. Let $\tau \in L(M,h)$ be an element of the language of $M$, i.e., a simulation trace of $M$, for the (time) horizon $h$. The trace $\tau = (p_1,\ldots,p_k)$, $k \geq 1$, with $p_j = (q_j,t_j,X_j) \in Q \times \mathbb{R}_0^+ \times 2^X$ gives the states $q_j$ together with their lifetimes $t_j$ and thus the total states $\bar{q}_j = (q_j,t_j)$. Then the criticality of a total state $\bar{q}_j = (q_j,t_j)$ is given by $c(q_j,t_j)$. Formally, $c$ is a mapping $c: \bar{Q} \rightarrow \mathbb{R}_0^+$. In the realm of criticality, both $q_j$ and $\bar{q}_j = (q_j,t_j)$ are called an effect.

A simulation trace $\tau$ may contain many effects $\bar{q}_1,\ldots,\bar{q}_k$. Since these effects $\bar{q}_j$ can at least potentially interact with each other, the overall criticality $c(\tau)$ of the simulation trace $\tau$ is usually calculated in a more complex way than simple summation of the single criticalities $c(\bar{q}_j)$. Sometimes, an additional problem can be neglected, because it does not influence the overall outcome. It is unimportant, for example, that a leaking fluid creates a hazard to slip, if the area of leakage is located in the center of a large explosion. On the other hand, some combinations of hazards may produce dangers disproportionally high. An example would be the disposal of two irritant chemicals, producing a deadly poison in combination [20]. Hazards and threats can also be uncorrelated with each other. As a conclusion, the criticality measure $c$ for simulation traces has to take the variety of relationships between hazard and threat effects into account. The precise shape of $c$ will depend on the specific application.

**Definition 4** (Criticality of Effects). Let $M = (X,Y,Q,q_{\text{start}},\delta_{\text{int}},P_{\text{int}},\sigma,\delta_{\text{ext}},P_{\text{ext}},\lambda)$ be a STDEVS model. Let $\tau \in L(M,h)$ be an element of the language of $M$, i.e., a simulation trace of $M$, for the (time) horizon $h$. The trace $\tau = (p_1,\ldots,p_k)$, $k \geq 1$, with $p_j = (q_j,t_j,X_j) \in Q \times \mathbb{R}_0^+ \times 2^X$ gives the states $q_j$ together with their lifetimes $t_j$ and thus the total states $\bar{q}_j = (q_j,t_j) \in \bar{Q}$. For handling stepwise system degradations and multiple failures, the domain of $c$ has to be extended from a single total state to a (temporally ordered) sequence $\bar{q} = (\bar{q}_1,\ldots,\bar{q}_k)$. Then, the extended criticality assignment function $c$ has the signature $c: \bar{Q} \times \cdots \times \bar{Q} \rightarrow \mathbb{R}_0^+$.

The definition above extends the criticality assignment function $c$ in such a way, that criticality correlations can be taken into account (see figure 2). The lifetimes $t_j$ of the total states $\bar{q}_j$ provide informations about time differences between the effects, which may influence $c$ as well. If the criticality correlation depends on additional parameters, the values of these parameters can typically be coded in the states $Q$ of a STDEVS model.

### 3.3 Probability of a Simulation Trace

The safety and security aspects lead to a probabilistic system $S$. Accordingly, its overall dynamical behavior displays a tree instead of a single path. The probability of taking a specific branching option in the tree is given at the elementary level by the probability $p(\gamma)$ of the corresponding transition $\gamma$ in the STDEVS model $M$ of $S$. For calculating the probability $p(\tau)$ of a whole simulation trace $\tau$, which may results from several such branching choices $\gamma_i$, we have to compose the probabilities $p(\gamma_i)$ assigned to these choices $\gamma_i$ with each other. This can be done in the usual way with help of the Bayes rule (see figure 3). Using Bayes rule has many advantages. Being based on conditional probabilities, it may support the inclusion of uncertainties and soft informations like the subjectivity of risk [9, 41] in the formalism.
Figure 1: The simulation of a deterministic model gives a unique sequence $\tau$ of system states. For stochastic models, the state sequence diversifies to a tree of possible simulation traces. The probability of transiting to a specific successor state at a branching point in the tree is determined by the probability $P_{\text{int}}(q', \{q''\})$ assigned to the corresponding state transition $q' \rightarrow q''$. Let us take a closer look at the simulation trace $\tau_{11}$ representing the state sequence $q_{\text{start}} \rightarrow q_1 \rightarrow q_{11}$. Using the abbreviations $T := q_{\text{start}} \rightarrow q_1$ and $T' := q_1 \rightarrow q_{11}$, the probability $p(\tau_{11})$ of the occurrence of trace $\tau_{11}$ is equal to the probability $p(T \land T') = p(T) \cdot p(T' | T)$ that both state transitions $T, T'$ occur. Applying Bayes rule, it holds $p(T \land T') = p(T) \cdot p(T' | T')$. In the example, $p(T) = p(q_{\text{start}} \rightarrow q_1)$ is the probability that the state $q_1$ is reached from the start state $q_{\text{start}}$. The probability $p(T | T')$ on the other hand is the probability that from the state $q_1$, which have been reached after execution of $T$, a transition to the state $q_{11}$ takes place. This means $p(T | T') = p(T') = p(q_1 \rightarrow q_{11})$.

**Definition 5** (Probability of Cause). Let $M = (X, Y, Q, q_{\text{start}}, \delta_{\text{int}}, P_{\text{int}}, \sigma, \delta_{\text{ext}}, P_{\text{ext}}, \lambda)$ be a STDEVS model. Let $\gamma = (q, t, X', q')$ be a state transition $q \rightarrow q'$ between states $q, q' \in Q$ eventually triggered by a set $X'$ of external events ($X' = \emptyset$ is a valid choice) at lifetime $t$ of state $q$. Then the probability of executing $\gamma$ is designated as $p(\gamma)$. The value of $p(\gamma)$ is given by the internal transition probability $P_{\text{int}}(q, \{q'\})$ for $X' = \emptyset$ and by the external transition probability $\gamma_{\text{ext}}(q, t, X', \{q'\})$ for $X' \neq \emptyset$ with the system being in the total state $(q, t)$. The 4-tupel $\gamma$ represents a so-called cause.

**Definition 6** (Probability of a Sequence of Causes). Let $M = (X, Y, Q, q_{\text{start}}, \delta_{\text{int}}, P_{\text{int}}, \sigma, \delta_{\text{ext}}, P_{\text{ext}}, \lambda)$ be a STDEVS model. Let $\tau \in L(M, h)$ be an element of the language of $M$, i.e., a simulation trace of $M$, with (time) horizon $h$. Assigned to $\tau = (\rho_1, \ldots, \rho_k)$ with $\rho_j = (q_j, t_j, X_j) \in Q \times R_+^+ \times 2^X$ is the (temporally ordered) sequence $\gamma = (\gamma_1, \ldots, \gamma_k)$ of state transitions. Formally, $\gamma_j$ is defined as $\gamma_j := (q_{j-1}, t_j, X_j, q_j)$. Remember, that it holds $q_0 := q_{\text{start}}$. Then the probability of the occurrence of the sequence $\gamma$ is designated as $p(\gamma)$ and given by

$$p(\gamma) = p(\gamma_1) \cdot p(\gamma_1 | \gamma_2) \cdot \ldots \cdot p(\gamma_1, \ldots, \gamma_{k-1} | \gamma_k)$$
according to Bayes rule. The expression \( p(\gamma_1, \ldots, \gamma_{j-1} | \gamma_j) \) results from the fact that when the state transition \( \gamma_j \) is triggered, the state transitions \( \gamma_1, \ldots, \gamma_{j-1} \) were already executed and have set the preconditions for \( \gamma_j \).

### 3.4 A Simulation-Based Risk Measure

A specific behavior of the model \( M \) corresponds to a specific simulation trace \( \tau = (p_1, \ldots, p_k) \in L(M, h) \). Using the causes \( \gamma = (\gamma_1, \ldots, \gamma_k) \) and the effects \( q = (q_1, \ldots, q_k) \) belonging to the trace \( \tau \), we are now able to assign both a probability and a criticality to \( \tau \) via the measures \( p(\gamma) \) and \( c(q) \) defined in the last section.

**Definition 7** (Probability and Criticality of Simulation Traces). Let \( M \) be a STDEV model and \( h \in \mathbb{R}_0^+ \) be a nonnegative real number being the horizon of the simulation. Let \( \tau \in L(M, h) \) be an element of the language of \( M \), i.e., a possible simulation trace of \( M \), for the (time) horizon \( h \). The trace \( \tau = (p_1, \ldots, p_k) \) is associated with a sequence \( \gamma = (\gamma_1, \ldots, \gamma_k) \) of causes and a sequence \( q = (q_1, \ldots, q_k) \) of effects. Then the probability \( p(\tau) \) and the criticality \( c(\tau) \) of the trace \( \tau \) are defined as \( p(\tau) := p(\gamma) \) and \( c(\tau) := c(q) \).

The probability \( p(\tau) \) and criticality \( c(\tau) \) assigned to a simulation trace \( \tau \) will depend on the length of \( \tau \), i.e., on the given horizon \( h \). If the horizon of the simulation is increased, the extended trace may contain additional causes and may thus have a modified probability \( p(\tau) \); similarly, the occurrence of additional effects on the extended trace may change its criticality \( c(\tau) \). Using the probability \( p(\tau) \) and criticality \( c(\tau) \) of the trace \( \tau \) we will now define a risk measure \( R \) for a trace \( \tau \).

**Definition 8** (Risk Measure for Simulation Traces). Let \( M \) be a STDEV model and \( h \in \mathbb{R}_0^+ \) be a horizon. Then a risk measure \( R: L(M, h) \rightarrow \mathbb{R}_0^+ \) can be defined for the simulation traces \( \tau \in L(M, h) \) of \( M \) by assigning a nonnegative real value to \( \tau \) defined by \( R(\tau) = p(\tau) \cdot c(\tau) \).

The overall behavior of a model \( M \) is represented by the set of all possible simulation traces. It is thus plausible to define a risk measure for \( M \) as sum over the risk values \( R(\tau) \) assigned to the different simulation traces \( \tau \in L(M, h) \) of \( M \). In this way, the risk \( R \) assigned to the system model \( M \) is the sum of the criticalities \( c(\tau) \) of the traces \( \tau \in L(M, h) \) weighted by their probabilities \( p(\tau) \). This corresponds to the classical form of a risk measure as expectation value of the criticality over all possible cases.

**Definition 9** (Risk Measure for DEVs Systems). Let us designate the class of all STDEV models by \( \mathcal{M} \). Let \( M \in \mathcal{M} \) be a STDEV model and \( h \in \mathbb{R}_0^+ \) be a horizon. Then a risk measure \( R: \mathcal{M} \times \mathbb{R}_0^+ \rightarrow \mathbb{R}_0^+ \) parameterized by the horizon \( h \) is defined on \( \mathcal{M} \) by

\[
R(M, h) := \sum_{\tau \in L(M, h)} R(\tau) = \sum_{\tau \in L(M, h)} p(\tau) \cdot c(\tau)
\]

### 4 Properties of the Simulation-Based Risk Measure

#### 4.1 Simulation-Based vs. Traditional Approaches

The capability of the risk measure \( R \) to reproduce classical risk measures of safety and security at least approximatively, provides a good argument for the plausibility of \( R \). Indeed, a very small time horizon \( h \) restricts the system dynamics in such a way that \( L(M, h) \) is limited to almost trivial sequences consisting typically of just one cause and one effect. Under these conditions, \( R(M, h) \) reproduces more
or less the classical safety risk measure $R'$ applied e.g. by the FMEA method. In the case of comparatively 'simple' systems, the errors induced by the simplifying assumption will usually remain small. Then, $R'$ may be an acceptable replacement for the risk measure $R(M, h)$. For 'complex' systems, the simplifications become either unrealistic (e.g. cascading failures in power grids), or insufficient (e.g. nuclear power plants), or will lead to results containing significant errors.

Structurally, the risk measure $R(M, h)$ of definition 9 and the classical safety risk measure $R_1$ are similar. According to [39], $R'$ is the sum of all losses over all potential problems weighted by their likelihoods. Main difference besides of the restriction $h \geq 0$ for $R'$ is that [39] speaks about likelihood and definition 9 about probability. This is caused by different perspectives. Whereas [39] uses an analytic perspective based on observations identifying equivalent problems in different contexts, the model-based approach proposed here generates all possible evolution paths in an individual way. Though technically, likelihoods and probabilities maybe different, but coincide with respect to their meaning. Summing up, we can state that the classical notion of risk is approximately reproduced by the simulation-based risk measure under the restriction $h \geq 0$ given above. Thus, our risk measure definition seems to be fine for safety risks.

Let us now consider the situation from the security risk point of view. The classical risk measure $R''$ used for security applications depends on another set of parameters than the classical safety risk measure $R'$. Whereas safety defines risk as a product of the probability, that a hazard is realized, and its criticality, security takes vulnerability as explicit factor into account [26, 60] according to

$$\text{risk} = \text{threat} \times \text{vulnerability} \times \text{criticality}$$

Since we already demonstrated the approximate correspondence between the proposed simulation-based risk measure $R$ and the classical safety risk measure $R'$ under the simplifying assumption $h \geq 0$, it suffices to show the embeddability of the security risk definition $R''$ in the safety risk definition $R'$ for indicating an
association between $R$ and $R''$. Such an embedding can be constructed in the following way. Since both definitions have criticality in common, the attributes of threat and vulnerability have to be put into relation to the probability of safety risks. More precisely, probabilities for the occurrence of specific threat/vulnerability combinations have to be given. Though quantitative risk-based considerations are not very common in IT security, they have been successfully elaborated anyway e.g. in [1, 4, 49, 50, 59, 63]. Indeed, attack methods like social engineering can be described very well by means of success probabilities [56]. As another example, effort measures typically used e.g. for cryptanalysis can be interpreted as probabilities by considering the ratio between successful attacks and overall attack trials [2]. Though this does not show the desired embeddability rigorously, it makes it at least plausible. The paper [64] supports this view by giving an explicit embedding. Additional support for the possibility to assign probabilities to threat-vulnerability pairs is provided by attack trees defining probabilities for the realization of a specific attack [3, 58].

Besides of the construction of the embedding given above, it exists another argument for a close relationship between safety and security risks. The notion of risk used in environmental safety domains like toxicology and ecology is bridging safety and security as well. It is based on the terms of exposure and impact [30, 45], which have a close correspondence to the terms of threats and vulnerabilities used in cyber security. The exposure-impact concept of environmental risk takes external reasons of risks into consideration similar to security and contrary to technical safety. Thus, safety-related impacts correspond to vulnerabilities and safety-related exposures to security threats. In effect, the overall probability of an actually occurring risk may be thought of as a product of the probability, that a specific problem raises and the probability that the problem is indeed able to affect the system. The topic is discussed further e.g. in [56, 59, 61, 66].

4.2 (Non)Computability of the Simulation-Based Risk Measure

We have already mentioned the large computational effort required for calculating $R(M, h)$. However, there are more fundamental questions to be discussed in this context. For example, it is natural to ask for the computability of $R(M, h)$ for $h \rightarrow \infty$. As it turns out, the risk measure $R(M, \infty)$ is usually enumerable but not decidable due to the infinite size of the language $L(M, h)$. This is an analogon to the undecidability results of many other questions like the issue whether a piece of code is a self-replicating malware or whether a control process will still terminate after the infection with a specific malware.

Since the extrapolation of the system dynamics can lead to evolution paths of infinite length, a criterion has to be given when the 'simulation' has to stop for assuring decidability. This is done here by using the time horizon $h$. Its influence on the risk assessment is decisive. If a small $h$ triggers a stop too early, devastating hazards may be missed; if the assessment process stops too late, the determination of the risk may be compromised because too much effort is wasted on unimportant aspects. This reminds at the quiescence search of algorithmic game theory [62]. In effect, no reliable stopping criterion can be formulated in an absolute sense.
5 Example Power Grids

5.1 Power Grid Systems and their Faults and Threats

The approach for a unified assessment of safety and security risks proposed here has many advantages from the theoretical point of view. At the downside, a systematic processing of all possible evolution paths based on simulation runs requires a significant computational effort. Though this makes an application in practice difficult, some properties of the corresponding system may indicate candidates of suitable application domains.

- For providing additional insight compared to classical risk assessment methods, the system should be prone to both safety and security risks. Furthermore, the system dynamics should enable fault and threat propagation.
- For assuring a simple systems model, the system should be as homogenous as possible. Furthermore, the risks associated with the system should be easily representable (e.g. by a flag indicating whether a component is working or not).

Distribution networks like power grids [55] have the desired properties. At the moment, power grids are intensively studied in Germany due to the intended exit from nuclear and fossil energy sources [13], which is accompanied by a transition from a centralized continuous to a decentralized, more or less fluctuating power supply. This requires corresponding modifications of the power grid itself, which have to be assessed w.r.t. potential safety and security risks.

5.2 Model Structure

Using a model of power grids, we demonstrate the principles of a combined simulation-based safety and security risk-assessment. We will not develop the corresponding DEVS model in detail but restrict ourselves to the concept level.

The power grid is represented as network \((V, E)\) with nodes \(V\) and edges \(E\) between the nodes. Each edge \(e \in E\) has two attributes, its flow capacity \(a_e\) and its actual load \(l_a\). The actual load \(l_a\) is determined by the flow across the network resulting from the supplies and demands \(C_v \in \mathbb{R}\) at the network nodes \(v \in V\). The attribute \(C_v\) of the nodes \(v \in V\) indicates a power consumption of an amount \(|C_v|\) in the case of \(C_v < 0\). For \(C_v > 0\), the node \(v\) is producing power with an amount of \(C_v\). The ratio between flow capacity \(a_e\) and actual load \(l_a\) determines the probability \(p_e\) that the link \(e \in E\) will fail in the next time cycle. As far as possible, the node \(v\) will try to avoid loads \(l_a\) exceeding the flow capacity \(a_e\) significantly for keeping the failure probability \(p_e\) low. The possible failures of the edges \(e \in E\) represent the safety aspects of the network \((V, E)\).

Criticalities \(c_v\) assigned to the nodes \(v \in V\) quantify the disadvantageous effects of a power loss for the consumers supplied by \(v\). The necessity to consider multiple concurrent failures requires a refined assessment taking correlations between node failures (and thus the corresponding criticalities) into account. Imagine a situation in which a hospital does not accept new patients due to power loss. Then new patients have to be transported to other hospitals located nearby, which may be usually acceptable. If the power loss does not affect a single hospital but all hospitals of a whole region, the situation is much more severe due to the long distances for transports to a region with intact power supply, say, 200 km away. Hence, the criticality \(c\) assigned to such a situation may be considerably larger than the sum of the criticalities \(c_j\) assigned to power-loss situations for single hospitals.

As described above, the nodes \(v \in V\) control the power flow across the network \((V, E)\) in such a way that the actual loads \(l_a\) on the edges \(e \in E\) are kept into the
limits given by the edge capacities \( a_e \) in the best possible way. For this purpose, the nodes \( v \in V \) use informations provided locally by other nodes \( v' \in V \) and are distributed via an information network \((V,F)\). These informations consist of the states of the edges \( e \in E \) incident to \( v' \) (working resp. not working) and of the power consumption or production at \( v' \) given by \( C_{v'} \). They provide (subjective) knowledge about the power grid \((V,E)\), which enables \( v \) to schedule the power flow incoming at \( v \) across the edges carrying the power outflow. As a consequence, every edge \( f \in F \) of the information network \((V,F)\) is a vulnerability, because a potential attacker may influence the power grid functionality by modifying the transmitted informations. Such a modification may happen intentionally with a certain probability \( p_f \), which represents the security part of the model.

5.3 Model Dynamics

For assessing the risk of network failure, safety and security aspects have to be taken into account simultaneously. Let us take a look at the risks associated with the simple power grid depicted in figure 3. The components of the given network consist of a single power producing node \( N_P \) and several nodes consuming power. The nodes are connected with each other by power transmission lines. Let us assume that the control component of the node \( N_C \) becomes a victim of a cyber attack. The attacker switches off a power transmission line, say the connection \( e_4 \) between the nodes \( N_C \) and \( N_D \). Now these nodes are not directly connected anymore. The breakdown of this transmission line changes the probabilities of many other potential faults due to the feedback mechanisms contained in the given example. The power supply of the four nodes \( N_D, N_E, N_F, N_G \) is not provided by the two lines \( e_4 \) between \( N_C \) and \( N_D \) and \( e_5 \) between \( N_C \) and \( N_E \) anymore. Only one of these connecting lines is left. The system tries to preserve the availability of the grid by rescheduling the power flow interrupted by the failure of \( e_4 \). The rescheduling leads typically to a higher load for the remaining operational network elements, which in turn leads to an increased probability of failure for them. This may lead to the failure of the next component of the network within short notice. When taking the rescheduling functionality of the network into consideration, an risk resp. reliability assessment considering only the instantaneous situation at the beginning is not valid anymore.

In effect, the rescheduling of the power flow may lead to a so-called cascading failure switching off large parts of the network. For the handling of such a cascading failure, the conventional methods of safety risk assessments are inappropriate [14], because this requires the inclusion of fault propagation mechanisms and thus an explicit modeling of system dynamics. The simulation-based risk measure presented here has such a capability and can thus handle a stepwise degradation of system capabilities and functionalities. Simulating system dynamics allows to check whether the effects of a fault or a fault sequence may act as causes of new faults due to overloads of remaining components. Describing the dynamics of such a cascade failure, and even more, predicting it trustworthy, is still a challenge for the reliability theory of networks [7]. The capability of such assessments would be of high interest, however, because the breakdown of the complete power grid (or at least essential parts of it) is a critical risk. Human lifes may depend on a working power supply (hospitals, infrastructure, military defence, etc.).

If the initial failure of the connection line of the power grid is caused by a self-replicating malware propagating across the information network \((V,F)\), the resulting situation is more complicated. Two kinds of dynamics are interacting with each other. First, malware is propagating along control nodes of the power grid. Second, if a power line fault happens, a fault sequence may be the consequence. These two kinds of dynamics are interacting because malware-infected control-nodes
may not react in the intended fault-mitigating way and instead worsen the problem. Another potential complication concerning the control mechanism would be the arousal of a new fault during the management of the actual fault leading to interferences between the fault propagation mechanism and the problem solution task of the control process. Furthermore, the individual control tasks for managing faults raised concurrently may interfere, too.

6 Outlook

The rapid spread of embedded systems lead to the statement that there is no safety without security and no security without safety. Accordingly, the paper develops a unified notion of risk applicable to both safety and security problems. This notion uses a simulation based approach in the context of STDEVS models. Its application to power grids shows that the proposed approach can handle situations, which are not appropriately dealt with conventional risk assessment methods. These advantages result from the inclusion of dynamics, which takes into account that individual risk cases may occur concurrently and consecutively and that errors and other off-nominal behaviors may propagate across the system. The simulation-based approach considers all these effects implicitly; eventually emerging interactions between propagating effects are included as well. Questions of controllability are calculated objectively instead of being estimated based on intuitive guesses.

Relying on a simulation model $M$ offers another advantage. Risk cases can be generated and assessed automatically based on $M$ with its probability and criticality attributes. Due to the large number of risk cases — remember that both safety and security risk cases are considered here — the large number of items to be processed makes the classical way of generating and assessing a list of risk cases manually hardly feasible. Thus, an automated model-based risk assessment turns out to be quite useful. The exploration of ways to refine the approach with respect to computational tractability may be the topic of forthcoming research, however.
Acknowledgements

I would like to offer my special thanks to M. Grössler for many valuable remarks.

References

[1] Abrahamson, D., A. Sepeda, Expanding Known Process Safety and Risk Analysis Concepts to Manage Security Concerns, in Proceedings of the 40th Loss prevention Symposium, 2006

[2] Alaboodi, Saad Saleh, Model-based Evaluation: from Dependability Theory to Security, Doctoral Thesis, University of Waterloo, 2013

[3] Arnold, Florian, et al., Time-dependent analysis of attacks, International Conference on Principles of Security and Trust, Springer 2014

[4] Aven, Terje, A unified framework for risk and vulnerability analysis covering both safety and security, Reliability Engineering & System Safety 92(6)(2007) 745-754

[5] Avizienis, A., J-C. Laprie et al., Basic concepts and taxonomy of dependable and secure computing, IEEE Trans Depend Secur Comput, 1(2004) 11-33

[6] Axelrod, Warren, Engineering Safe and Secure Software Systems, Artech House 2012

[7] Balduck, R. et al., Vulnerability assessment for cascading failures in electric power systems in Proceedings of Power Systems Conference and Exposition, IEEE 2009

[8] Blom, Henk, et al., Safety risk assessment by Monte Carlo simulation of complex safety critical operations, Developments in Risk-based Approaches to Safety. Springer 2006, pp. 47-67.

[9] Bobbio A., et al., Improving the analysis of dependable systems by mapping FTs into Bayesian networks, Journal of Reliability Engineering and System Safety 71(2001) 249-60

[10] Bosworth, Seymour, M. E. Kabay, Computer Security Handbook, Wiley 2002

[11] Branagan, Mark, A risk simulation framework for information infrastructure protection. Dissertation, Queensland University of Technology, 2012.

[12] Brewer, DFC, Applying security techniques to achieve safety, in Proceedings of the 3rd safety-critical systems symposium, Bristol, UK, 1993, pp. 246-56.

[13] Buchan, David, The Energiewende - Germany’s gamble, The Oxford Institute for Energy Studies, SP 26(2012), online http://www.oxfordenergy.org/wpcms/wp-content/uploads/2012/07/SP-26.pdf

[14] Cadini, Francesco, et al., Using Centrality Measures to Rank the Importance of the Components of a Complex Network Infrastructure, in Roberto Setola & Stefan Geretshuber (Eds.), Critical Information Infrastructures Security, Third International Workshop, Springer 2008

[15] Castro, R., E. Kofman, G. Wainer, A formal framework for stochastic DEVS modeling and simulation, in Hassan Rajaei et al., Proceedings of the 2008 Spring Simulation Multiconference, Ottawa, Canada 2008, pp. 421-428
[16] Castro, R., E. Kofman, G. Wainer, A Formal Framework for Stochastic DEVS Modeling and Simulation, in Transactions of the Society for Modeling and Simulation International, 86(2010) 587-611

[17] Chi, S.-D., et al., Network Security Modeling and Cyber Attack Simulation Methodology, in Vijay Varadharajan & Yi Mu, Information Security and Privacy, Proceedings of the 6th Australasian Conference, Sydney, Australia, Lecture Notes in Computer Science 2119(2001) 320-333

[18] Devooght, J., Dynamic Reliability: The Challenges Ahead, Fifth International Workshop on Dynamic Reliability: Future Directions, Greenbelt, Maryland 1998.

[19] Dissanayaka, Anuradha, et al., Risk-based dynamic security assessment, IEEE Transactions on Power Systems 26(3)(2011) 1302-1308.

[20] Draeger, J., Roadmap to a Unified Treatment of Safety and Security, in Proceedings of System Safety and Cyber Security, Bristol, UK, 2015

[21] Faber, M.H., et al., Principles of risk assessment of engineered systems, in Proceedings of the 10th International Conference on Applications of Statistics and Probability in Civil Engineering, Tokyo, Japan, 2007

[22] Felde, Magnus, Analyzing Security Decisions with Discrete Event Simulation. Master Thesis, Gjøvik University College 2010

[23] Fenton, Norman, and Martin Neil, Measuring your Risks: Numbers that would make sense to Bruce Willis and his crew, available online at http://www.agena.co.uk/resources/white_papers/Measuring_Risks.pdf

[24] Fenton, Norman, and Martin Neil, Risk Assessment and Decision Analysis with Bayesian Networks, CRC Press 2012

[25] Firesmith, D.G., Common Concepts Underlying Safety, Security, and Survivability Engineering, Technical Note CMU/SEI-2003-TN-033, Software Engineering Institute 2003

[26] Flammini, Francesco, et al., Optimisation of security system design by quantitative risk assessment and genetic algorithms, Int. J. of Risk Assessment and Management 15(2/3)(2011) 205-221

[27] Fovino, Nai, M. Masera, Integrating Cyber Attacks within Fault Trees, In Reliab. Eng. Syst. Saf. 94(2009) 1394-1402

[28] Gutierrez, Tomas Navarrete, Laurent Ciarletta, Vincent Chevrier, Multi-agent simulation based control of complex systems, in Proceedings of the 2014 international conference on Autonomous agents and multi-agent systems, ACM 2014, pp. 1517-1518

[29] StJohn-Green, M., et al., Combined security and safety risk assessment - what needs to be done for ICS and the IOTQ, in Proceedings of the 10th IET System Safety and Cyber Security Conference 2015

[30] Hakkert, A.S., L. Braimaister, The uses of exposure and risk in road safety studies, Report R-2002-12 SWOV Institute for Road Safety Research, Leidschendam 2002

[31] Hernandez, Alejandro, Norbert Giambiasi, State Reachability for DEVS Models, in A. Hernández, N. Giambiasi, Proc. of Argentine Symposium on Software Engineering 2005, pp. 267-277
[32] Hopcroft, John E., Rajeev Motwani, Jeffrey D. Ullman, Introduction to Automata Theory, Languages, and Computation, Pearson 2013

[33] Hwang, Moon H., Qualitative Verification of Finite and Real-Time DEVS Networks, in Proceedings of 2012 TMS/DEVS, Orlando, FL, USA

[34] Hwang, M.H., Revisit of system variable trajectories, in Proceedings of the Symposium on Theory of Modeling & Simulation - DEVS Integrative M&S Symposium, San Diego, CA, USA 2013

[35] Hwang, M.H., & Bernard Zeigler, A Reachable Graph of Finite and Deterministic DEVS Networks, in Proceedings of 2006 DEVS Symposium, Huntsville, Alabama, USA, pp. 48-56

[36] Hwang, M.H., & Bernard Zeigler, Reachability Graph of Finite & Deterministic DEVS, IEEE Transactions on Automation Science and Engineering 6(3)(2009) 454-467

[37] Jithavech, Id, & Krishna Kumar Krishnan, A simulation-based approach for risk assessment of facility layout designs under stochastic product demands, The International Journal of Advanced Manufacturing Technology 49(1-4)(2010) 27-40

[38] Jonsson, E., & T. Olovsson, On the integration of security and dependability in computer systems, in Proceedings of the IASTED international conference on reliability, quality control and risk assessment, Washington, DC, USA 1992, pp. 93-7

[39] Kaplan, S., & B. J. Garrick, On the Quantitative Definition of Risk, Risk Analysis Journal 1(1)(1981) 11-27

[40] Karnouskos, Stamatis, Stuxnet worm impact on industrial cyber-physical system security, in Proceedings of the 37th Annual Conference on IEEE Industrial Electronics Society, IEEE 2011.

[41] Khakzad, Nima, Faisal Khan, Paul Amyotte, Safety analysis in process facilities: Comparison of fault tree and Bayesian network approaches, Reliability Engineering & System Safety 96(8)(2011) 925-932

[42] Khakzad, Nima, Faisal Khan, Paul Amyotte, Dynamic risk analysis using bow-tie approach, Reliability Engineering & System Safety 104(2012) 36-44

[43] Kofman, E., & R.D. Castro, STDEVS, A Novel Formalism for Modeling and Simulation of Stochastic Discrete Event Systems, in Proceedings of AADECA, Buenos Aires, Argentina, 2006

[44] Kriaa, S., et al., A Survey of Approaches Combining Safety and Security for Industrial Control Systems, Reliab. Eng. Syst. Safe. 139(2015) 156-178

[45] Kron, W., Keynote lecture: Flood risk = hazard × exposure × vulnerability, in Flood defence, Science Press 2002, pp. 82-97.

[46] Law, Averill M., Simulation Modeling and Analysis, Mc Graw Hill 2006

[47] Lee, R., M. Assante, T. Connway, ICS CP/PE (Cyber-to-Physical or Process Effects) case study paper — German Steel Mill Cyber Attack. Technical report, SANS ICS 2014

[48] Leveson, N., Engineering a Safer World, MIT Press 2012

18
[49] Littlewood, B., Dependability assessment of software-based systems: State of the art, in Proceedings of the 27th international conference on software engineering, St. Louis, MO, USA 2005, pp. 6-7

[50] Littlewood, B, et al., Towards operational measures of computer security, Journal of Computer Security 2(1993) 211-29

[51] Mader, R., et al., A framework for model-based safety requirements roundtrip engineering

[52] Mohaghegh, Zahra, Reza Kazemi, Ali Mosleh, Incorporating organizational factors into Probabilistic Risk Assessment (PRA) of complex socio-technical systems: A hybrid technique formalization, Reliability Engineering and System Safety 94(2009) 1000-1018

[53] Mueller, Paul, & Babak Yadegari, The Stuxnet Worm, Departement des sciences de l'informatique, Université de l'Arizona 2012, online available at http://www.cs.arizona.edu/~collberg/Teaching/466-566/2012/Resources/presentations/2012/topic9-final/report.pdf

[54] Nejad-Hosseinian, Seyed Hamed, Automatic generation of generalized event sequence diagrams for guiding simulation based dynamic probabilistic risk assessment of complex systems, ProQuest 2007

[55] Pappu, Vijay, Marco Carvalho, Panos Pardalos, Optimization and Security Challenges in Smart Power Grids, Springer 2013

[56] Pieters, Wolter, et al., Reconciling Malicious and Accidental Risk in Cyber Security, Journal of Internet Services and Information Security 4(2)(2014) 4-26

[57] Pietre-Cambacedes, L., & M. Bouissou, Cross-fertilization between safety and security engineering, Reliability Engineering and System Safety 110(2013) 110-126

[58] Wang, Ping, et al., Threat Risk Analysis for Cloud Security based on Attack-Defense Trees, in Proceedings of the 8th International Conference on Computing Technology and Information Management, Seoul, Korea, IEEE 2012, pp. 106-111

[59] Pirzadeh, Jonsson, E., A Cause and Effect Approach Towards Risk Analysis, in James Walden, Laurie Williams, Proceedings of the Third International Workshop on Security Measurements and Metrics 2011, pp. 80-83

[60] Robbins, Philip, Security Risk Analysis and Critical Information Systems, Master Thesis, Hawaii Pacific University 2011

[61] Rot, Artur, IT Risk Assessment: Quantitative and Qualitative Approach, in Proceedings of the World Congress on Engineering and Computer Science, San Francisco, USA 2008

[62] Russell, Stuart, & Peter Norvig, Artificial Intelligence: A Modern Approach, Prentice Hall 2013

[63] Said, Fadi Haj, Security-based risk assessment for software architecture, Doctoral Dissertation, West Virginia University 2011

[64] Salvati, Domenico, Management of information system risks, Doctoral Thesis, ETH Zürich 2008
[65] Solcány, Viliam, Simulation Algorithms for DEVS Models, 2008, available online at [http://www2.fiit.stuba.sk/~solcany/files/devs_article.pdf]

[66] Sørby, Karine, Relationship between safety and security in a safety-security critical system: Safety consequences of security threats, 2003

[67] Spellman, F., & N. Whiting, The Handbook of Safety Engineering: Principles and Applications, Government Institutes 2009

[68] Vangheluwe, H.L.M., DEVS as a common denominator for multi-formalism hybrid systems modelling, in A. Varga, Proceedings of the IEEE International Symposium on Computer-Aided Control System Design 2000, pp. 129-134

[69] Winkelvos, Timo, Carsten Rudolph, Jurgen Repp, A property based security risk analysis through weighted simulation, in Proceedings of Information Security South Africa, IEEE 2011

[70] Zeigler, Bernard, Multifacettted Modeling and Discrete Event Simulation, Academic Press 1984

[71] Zeigler, Bernard, Tag Gon Kim, Herbert Prahofer, Theory of Modeling and Simulation, Academic Press 2000

[72] Zeigler, Bernard, DEVS today: Recent advances in discrete event-based information technology, in Proceedings of the 11th IEEE/ACM International Symposium on Modeling, Analysis and Simulation of Computer Telecommunications Systems, IEEE 2003

[73] Zeigler, B., & S. Valhe, Devs formalism and methodology: unity of conception/diversity of application, in Proceedings of the 25th Winter Simulation Conference, Los Angeles, CA 1993, pp. 573-579