Proceedings of the 33rd European Safety and Reliability Conference (ESREL 2023)
Edited by Mário P. Brito, Terje Aven, Piero Baraldi, Marko Čepin and Enrico Zio

doi: 10.3850/978-981-18-8071-1_P344-cd

Dynamically resolving and abstracting Markov models for system resilience analysis

Ivo Häring[1], Nikhilesh Sandela[2], Teo Puig Walz[1], Georg Vogelbacher[1], Alexander Richter[1], Aishvarya Kumar Jain[1], Mayur Dhanani[3], Sunil Mopuru[4], Konstantin Kirchheim[5], Fabian Höflinger[1], Jörg Finger[1]

[1]*Fraunhofer EMI, Germany.* [1]*E-mails: {ivo.haering; teo.puig.walz; georg.vogelbacher; alexander.richter; aishvarya.kumar.jain; mayur.dhanani; sunil.kumar.reddy.mopuru; fabian.hoeflinger; joerg.finger}@emi.fraunhofer.de*
[2]*Digital Engineering, University Magdeburg, Germany. Email: nikhilesh.sandela@st.ovgu.de;*
[3]*Renewable Energy Systems, Hochschule Nordhausen, Germany, Email: mayur.dhanani@hs-nordhausen.de*
[4]*Hochschule Bremerhaven, Germany. Email: smopuru@studenten.hs-bremerhaven.de*
[5]*Otto-von-Guericke Universität Magdeburg, Germany. Email: konstantin.kirchheim@ovgu.de*

Regarding the modeling of quasi-static systems with minor failures for failure prediction and maintenance, Markov models have shown to be very successful. Finite discrete state models can be considered as best practice in this domain, often even assumed to be homogeneous. The question arises if Markov models are also capable to model resilience of systems including major disruptions, where great fractions of the system and its functionality fail. To this end, analytical propositions are made that define model extensions. An initial scalable system is defined, including expected refinements and abstractions. In further phases, major disruptions occur. The disruptions can cause branching points opening routes to model extensions or abstractions. Also independent of disruptions, new states and transitions are introduced or merged for model granularity adoption. Overall system behavior can be interpreted in terms of system improvement with or without new system states or functionalities and corresponding transitions, reaching the ex-ante system state as before the disruption, reaching a deteriorated system state, or finally various degraded and failed overall system states. Definitions such as states, absorbing states and critical transitions are reinterpreted or extended to allow for dynamically resolving or abstracting the Markov model. The main results are extended definitions and derivations when compared to traditional Markov models. Based on the analytical expressions, an example is provided where the formalism could be applied with advantage for autonomous driving safety assessment by considering increasing or decreasing levels of resolution of subsystems or subfunctions.

Keywords: Resilience quantification, dynamic Markov model extension, analytical system assessment, branching point, hierarchical Markov model, abstraction and refinement.

1. Introduction

Markov models are used in a wide range of domains including medicine success prediction (Sonnenberg and Beck 1993), predictive reliability assessment (Yosri et al. 2021), and autonomous driving (AD) safety assessment (Nyberg 2018) (Bonderson 2018) (Heinrich, Plinke, and Hausschild 2017) (Häring et al. 2022).

However, limitations of classical Markov models are well known, in particular regarding state explosion, time-independence of transitions if used in their simplest form and last but not least the assumption of memoryless transitions(Horeis et al. 2020).

Expandable Markov approaches that allow for modification of the overall state space have already been used for the realization of AD functions (Pouya and Madni 2021). Markov subsystem decomposition for a nucelar system is described in (Liang et al. 2022). Also the use of subsystem models in Petri nets are defined scaling approaches (Naybour, Andrews, and Chiachio-Ruan 2019).

In the following it is proposed to connect Markov models by allowing overall state space refinements and abstractions in a controlled way, depending on the emerging time history.

Section 2 gives an overview of the proposed approach providing a modelling flow and its visualization. In section 3 the modelling approach is formalized based on a structural-functional system model. Section 4 illustrates for a sample AD system the effect of a dominating state transition for illustration of the need for the proposed approach. Section 5 concludes by summarizing the findings of the formal exercise.

2. Methodology

The scaling Markov approach can be divided in a sequence of iteratively conducted steps, see Fig. 1. Fig. 1 shows that after initial conditions the probability distribution time history of the discrete system states is propagated till a refinement or abstraction criterion is met to trigger state modification.

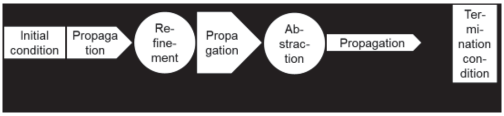

Fig. 1. Hierarchically scaling overall Markov system model propagation.

The steps can be summarized as follows:

1. System definition in terms of hierarchical subsystems and/or system function definitions. Thus, each overall system state can be described by using up to several resolution levels (hierarchical system and state structure)
2. System state transitions on system level are allowed between subsystems of same resolution level.
3. In addition, system can extend or absorb subsystems: system structural transitions, system state space extensions, and reductions, e.g. based on similar share of probability for each state, minimum and/or maximum resolution.
4. Quantification of transitions on system level, e.g., using discrete time-independent or time depenent transition probability matrix ($\mathbb{P}$) or continuous transition rate matrix ($\mathbb{Q}$), respectively (discrete and continuous time Markov chains)
5. Overall system states can be characterized at each point in time as initial (only one), transient and absorbing (up to several final states).
6. Overall system states can be interpreted in addition terms of overall system health, e.g. overall system reliably or safety.
7. Conduct steps 1 to 7 till overall system state space is explored, i.e., e.g., sufficient equally distributed resolution at all times.

3. Method details and formalization

3.1 *Scaling Markov state space*

First the scaling state space is presented including the cardinality of the subsystems or subfunctions, i.e. the number of their possible finite states. To this end a hierarchical and scaling structure is introduced in Fig. 2. Fig. 2 represents a possible system structure.

In Fig. 2, each column corresponds to a feasible system resolution. The light green marked subsystems and the dark green marked subsystems represent possible combinations of system resolutions given the knowledge of the system structure of Fig. 2. In a modelling process, some higher resolved areas could not yet be realized in terms of, e.g., requiring model parameter determination on demand.

<table>
<tr><th colspan="6">Resolution level</th></tr>
<tr><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>...</td></tr>
<tr><th colspan="6">Sample number of subsystems and/or subfunctions</th></tr>
<tr><td>1</td><td>3</td><td>6</td><td>12</td><td>14</td><td>...</td></tr>
<tr><td rowspan="14">S_0</td><td rowspan="6">S_1</td><td rowspan="2">S_11</td><td>S_111</td><td>S_1111</td><td rowspan="14">...</td></tr>
<tr><td>S_112</td><td>S_1121</td></tr>
<tr><td rowspan="2">S_12</td><td>S_121</td><td>S_1211</td></tr>
<tr><td>S_122</td><td>S_1221</td></tr>
<tr><td rowspan="2">S_13</td><td>S_131</td><td>S_1311</td></tr>
<tr><td>S_132</td><td>S_1321</td></tr>
<tr><td rowspan="4">S_2</td><td rowspan="2">S_21</td><td>S_211</td><td>S_2111</td></tr>
<tr><td>S_212</td><td>S_2121</td></tr>
<tr><td rowspan="2">S_22</td><td>S_221</td><td>S_2211</td></tr>
<tr><td>S_222</td><td>S_2221</td></tr>
<tr><td rowspan="4">S_3</td><td rowspan="4">S_31</td><td rowspan="2">S_311</td><td>S_3111</td></tr>
<tr><td>S_3112</td></tr>
<tr><td rowspan="2">S_312</td><td>S_3121</td></tr>
<tr><td>S_3122</td></tr>
<tr><th colspan="6">Sample numbers of sates of subsystems and/or subfunctions</th></tr>
<tr><td rowspan="14">4</td><td rowspan="6">4</td><td rowspan="2">4</td><td>4</td><td>4</td><td rowspan="14">...</td></tr>
<tr><td>3</td><td>4</td></tr>
<tr><td rowspan="2">3</td><td>4</td><td>4</td></tr>
<tr><td>3</td><td>3</td></tr>
<tr><td rowspan="2">2</td><td>2</td><td>2</td></tr>
<tr><td>2</td><td>2</td></tr>
<tr><td rowspan="4">3</td><td rowspan="2">2</td><td>2</td><td>3</td></tr>
<tr><td>3</td><td>3</td></tr>
<tr><td rowspan="2">2</td><td>4</td><td>4</td></tr>
<tr><td>4</td><td>4</td></tr>
<tr><td rowspan="4">2</td><td rowspan="4">2</td><td rowspan="2">2</td><td>2</td></tr>
<tr><td>2</td></tr>
<tr><td rowspan="2">2</td><td>2</td></tr>
<tr><td>4</td></tr>
<tr><th colspan="6">Sample total numbers of sates</th></tr>
<tr><td>4</td><td>24</td><td>192</td><td>221184</td><td>3538944</td><td>...</td></tr>
</table>

Fig. 2. Hierarchical and scaling overall system models.

The light green overall system is obtained from the second column system by higher resolving subsystem S_2. For the dark green overal system, S_1 is further resolved into S_{12} and S_{13}, while S_3 is resolved into S_{311} and S_{312}. In this way, only one-step resolution increases in terms of division of subsystems or subfunctions can be used to refine system models.

In a similar way abstractions of system models can be constructed, e.g., the second column is abstracted from the light green model by summarizing S_{21} and S_{22} in S_2. The dark green model is an abstraction of the second right column requiring 6 single combination steps.

The assumption is that at each point in time, it is known in which state-space time propagation takes place. Within one state space, propagation obeys the total law of probability. Also, when switching between state spaces probability is conserved, as shown in the following.

3.2. *Sequence of overall state spaces and allowed transitions*

Next, we consider a sequence of state spaces and propagations therein. State-space abstractions and refinements are introduced. The modeling can use state space topology information or probability distribution information, e.g. in terms of minimum or maximum probability thresholds or by requiring comparable resolution.

We define a sequence of allowed product state spaces based on Fig. 2

$$S^j = \prod_{i=1}^{N_j^S} S_i^j = S_1^j \times S_2^j \times \ldots \times S_{N_j^S}^j, \qquad (1)$$

where $j = 0, 1, 2, \ldots$ labels an allowed sequence of state spaces that increase or decrease resolution. The cardinalities of the respective state and subsystem state spaces are

$$N^{S,j} = |S^j| = \prod_{i=1}^{N_j^S} |S_i^j| = \prod_{i=1}^{N_j^S} N_i^{S,j}. \qquad (2)$$

Examples of cardinality numbers from subsystem state spaces are given in Fig. 2 showing the rapid state explosion, see last line in Fig. 2 according to (2). Hence it is desirable that we can extend and reduce the Markov state space.

To define an allowed state space extension based on a given subsystem or subfunction structure as exemplified in Fig. 2, we require that per extension only one subsystem or subfunction is further resolved. For instance, in Fig. 2 the resolution from the first column state space S_0 to the second column $S_1 \times S_2 \times S_3$ is allowed but from S_0 to the light green shaded state space $S_1 \times S_{21} \times S_{22} \times S_3$ is not. In the latter case we have to reach the light green state in two steps.

Allowed extensions can be characterized as replacing one state space of a subsystem or subfunction with a product state space of at least 2 other subsystems or subfunctions,

$$S_1^j \times S_2^j \times \ldots \times S_k^j \times \ldots \times S_{N_j^S}^j \leftrightarrow S_1^{j+1} \times \ldots \times S_{k,1}^{j+1} \times S_{k,2}^{j+1} \times \ldots \times S_{k,N_k^{j+1}}^{j+1} \times \ldots \times S_{N_j^S}^{j+1}, \qquad (3)$$

where $j = 0, 1, \ldots$ and $N_k^{j+1} \geq 2$. Allowed refinements and abstractions are determined by the system structural functional model as given in Fig. 2. For instance, when resolving $S_1 \times S_2 \times S_3$ to $S_{11} \times S_{12} \times S_{13} \times S_2 \times S_3$ then $N_k^j = N_1^1 = 3$. Note that the sequence of allowed state spaces given in (1) is not unique according to the transition requirement (3). This can be inferred from the different options to reach the dark green state of Fig. 2.

The abstraction or coarsening of the state space is achieved by a mapping from right to left as described in (3).

How to distribute probabilities on new states when the state space is refined? We observe what a suitable labeling of state probabilities reveals, see Fig. 3. By construction of the labeling of system states the number of subsystems or functions considered (Fig. 2) determines the number of labels used in Fig. 3.

Overall state propabilities labeling for column state spaces					
P_1 P_2 P_3 P_4	P_111 P_112 P_113 P_114 P_121 P_122 P_123 P_124 P_131 P_132 P_133 P_134 P_211 P_212 P_213 P_214 P_221 P_222 P_223 P_224 P_231 P_232 P_233 P_234	P_111111 P_111112 P_111113 P_111114 P_111121 P_111122 P_111123 P_111124 P_111131 P_111132 P_111133 P_111134 P_111211 …	P_111111111111 P_111111111112 …	P_11111111111111 P_11111111111112 …	…
Number of labels used					
1	3	6	12	14	…
Number of refinements that need to be prarametrized					
1	2	5	2	…	…
Number of abstractions that need to be given					
0	1	2	5	2	…

Fig. 3: State labeling for column states of Fig. 2.

Fig. 3 shows that if we replace a single system or function with 4 states with 3 subsystems or subfunctions with 4, 3, and 2 states, respectively, a single label has to be replaced by three labels, see the first and second column of Fig. 3. This also happens if the second state space (sample label marked blue in Fig. 3) is extended in two state spaces (see the third column of Fig. 3). Similarly, the last state space of second column (sample label marked bold black in Fig. 3) is expanded in three states.

3.3. *Redistribution of state probabilities for state space refinement and abstraction*

More specifically we have for instance to decide how to distribute the probability of $P_1(t)$ at the moment of transition to an extended model on the state space probabilities $P_{111}(t), P_{112}(t), P_{113}(t), P_{114}(t), P_{121}(t), P_{123}(t), P_{124}(t), \ldots, P_{134}(t)$, see Fig. 2. And in the same way for $P_2(t)$, $P_3(t)$, and $P_4(t)$. When interpreting for instance $P_1(t)$ as the probability of fully operational on system level with no degradation and the column 2 system of Fig. 2 as a 1 out of 3 system, 2oo3 or 3oo3 system, then it becomes obvious what possible choices can be made. Only $P_{111}(t)$ would fit if one interprets the subsystem label as all 3 subsystems or subfunctions are fully operational. Similarly, degraded operational $P_2(t)$ could be interpreted, e.g. as a combination of $P_{112}(t)$, $P_{113}(t)$, $P_{121}(t)$, and $P_{211}(t)$. The higher resolved subsystem states and functions depend on the system structural-functional model, as given exemplary in Fig. 3.

Also, the quantitative distribution depends on the system considered. For example, first the transition from S^0 to S^1 is quantified. For each overall system state probability $P_i(t)$, $i = 1, 2, \ldots, N_1^{\mathrm{S},0} = 4$ we set, using the notation of (2),

$$P_i^0(t) = \sum_{i_1=1}^{N_1^{\mathrm{S},1}=4} \sum_{i_2=1}^{N_2^{\mathrm{S},1}=3} \sum_{i_3=1}^{N_3^{\mathrm{S},1}=2} P_i^0(t)\, w_{i_1 i_2 i_3}^{0\to 1,i} = \sum_{i_1=1}^{N_1^{\mathrm{S},1}=4} \sum_{i_2=1}^{N_2^{\mathrm{S},1}=3} \sum_{i_3=1}^{N_3^{\mathrm{S},1}=2} P_{i_1 i_2 i_3}^1(t)\ . \quad (4)$$

The distribution weights are chosen constant over time with $0 \le w_{i_1 i_2 i_3}^{0\to 1,i} \le 1$. To preserve total probability, we require that at the point in time where the higher resolution is conducted the following normalization conditions hold

$$\sum_{i_1=1}^{N_1^{\mathrm{S},1}=4} \sum_{i_2=1}^{N_2^{\mathrm{S},1}=3} \sum_{i_3=1}^{N_3^{\mathrm{S},1}=2} w_{i_1 i_2 i_3}^{0\to 1,i}(t) = 1. \quad (5)$$

For defining the reverse mapping from S^1 to S^0 according to (1) and (3), we assume a well-defined mapping of each discrete finite product state with high resolution to a product state of lower resolution

$$\{P_{i_1 i_2 i_3}^1(t)\} \to \{P_i^0(t)\}, \quad (6)$$

where indices are as in (4). For instance, $P_{111}^1(t)$, e.g. all subsystems or functions fully operational, contributes to the full operational overall state $P_1^0(t)$ only. These transition modls can be seen as an additional requirement contributing to the functional-structural model of Fig. 2.

The generalization of (4) and (6) reads

$$P^j_{i_1,i_2,\ldots,i_k,\ldots,i_{\mathrm{N}_\mathrm{j}^\mathrm{S}}}(t) = \sum_{i_1=1}^{N_{\mathrm{k}_1=k}^{\mathrm{S,j+1}}} \sum_{i_2=1}^{N_{\mathrm{k}_2}^{\mathrm{S,j+1}}} \cdots \sum_{i_3=1}^{N_{\mathrm{k}_1+\mathrm{N}^{\mathrm{S,j+1}}-\mathrm{N}^{\mathrm{S,j}}}^{\mathrm{S,j+1}}} P^j_{i_1,i_2,\ldots,i_k,\ldots,i_{\mathrm{N}_\mathrm{j}^\mathrm{S}}}(t) \cdot w^{j\to j+1,\, i_k}_{i_1,i_2,\ldots,i_{k-1},i_{k_1=k},i_{k_2},\ldots,i_{\mathrm{k}_1+\mathrm{N}^{\mathrm{S,j+1}}-\mathrm{N}^{\mathrm{S,j}}},\ldots,i_{\mathrm{N}^{\mathrm{S,j+1}}}} = \sum_{i_1=1}^{N_{\mathrm{k}_1=k}^{\mathrm{S,j+1}}} \sum_{i_2=1}^{N_{\mathrm{k}_2}^{\mathrm{S,j+1}}} \cdots \sum_{i_3=1}^{N_{\mathrm{k}_1+\mathrm{N}^{\mathrm{S,j+1}}-\mathrm{N}^{\mathrm{S,j}}}^{\mathrm{S,j+1}}} P^{j+1,\, i_k}_{i_1,i_2,\ldots,i_{k-1},i_{k_1},i_{k_2},\ldots,i_{\mathrm{k}_1+\mathrm{N}^{\mathrm{S,j+1}}-\mathrm{N}^{\mathrm{S,j}}},\ldots,i_{\mathrm{N}^{\mathrm{S,j+1}}}}(t). \quad (7)$$

In this case subsystem or subfunction $\mathrm{S}_\mathrm{k}^\mathrm{j}$ and its states labeled with index i_k is refined by using the subsystems or subfunctions $\mathrm{S}^{\mathrm{j+1}}_{\mathrm{k}_1=k}$, $\mathrm{S}^{\mathrm{j+1}}_{\mathrm{k}_1=k+1}$, …, $S^{j+1}_{\mathrm{k}_1+\mathrm{N}^{\mathrm{S,j+1}}-\mathrm{N}^{\mathrm{S,j}}}$ and their indices $i_{k_1}, i_{k_2}, \ldots, i_{\mathrm{k}_1+\mathrm{N}^{\mathrm{S,j+1}}-\mathrm{N}^{\mathrm{S,j}}}$ labelling their states.

General normalization condition reads in this case for all structural-functional allowed subsystem or subfunction states that are resolved $j \to j+1$ and $1 \le k \le \mathrm{N}_\mathrm{j}^\mathrm{S}$

$$\sum_{i_1=1}^{N_{\mathrm{k}_1=k}^{\mathrm{S,j+1}}} \sum_{i_2=1}^{N_{\mathrm{k}_2}^{\mathrm{S,j+1}}} \cdots \sum_{i_3=1}^{N_{\mathrm{k}_1+\mathrm{N}^{\mathrm{S,j+1}}-\mathrm{N}^{\mathrm{S,j}}}^{\mathrm{S,j+1}}} w^{j\to j+1,\, i_k}_{i_1,i_2,\ldots,i_{k-1},i_{k_1=k},i_{k_2},\ldots,i_{\mathrm{k}_1+\mathrm{N}^{\mathrm{S,j+1}}-\mathrm{N}^{\mathrm{S,j}}},\ldots,i_{\mathrm{N}^{\mathrm{S,j+1}}}} = 1 \quad (8)$$

Note that in (7) and (8) the labeling of the constant weights could be simplified as for each allowed transition in a given sequence according to (1) only one state is further resolved or a well-defined set of states is abstracted. However, the transition weights should be provided along with the structural-functional model of the scalable Markov model. The proposed labeling allows to parametrize all allowed transitions in a well-defined way that is independent of the sequence that is applied in an allowed scaling model sequence according to Fig. 1. Fig. 3 lists the number of refinements that need to be parametrized for the sample structural model, which proves to be rather limited.

The general abstraction can be defined by using that each higher resolved discrete finite

Markov state can be mapped to a single less resolved state

$$\{P^{j+1,\,i_k}_{i_1,i_2,\dots,i_{k-1},i_{k_1}=k,i_{k_2},\dots,i_{k_1+N^{S,j+1}-N^{S,j}},\dots,i_{N^{S,j+1}}}(t)\} \rightarrow \{P^{j}_{i_1,i_2,\dots,i_k,\dots,i_{N^S_j}}(t)\}. \quad (9)$$

In summary, for state space refinement existing state probabilities for each state are distributed on higher resolved state space using (7). Abstraction or combination of states to a less dimensional state space is conducted using (9). In both cases, only one component of the product state space (1) is resolved or a set of product spaces is removed per resolution step. Note that transitions in the sense of (8) and (9) can also be used in both directions, respectively.

3.4. *Propagation of time-dependent state probabilities within state space*

Now we are in the standard situation within one state space S^j according to (1). In this case, we have the overall time-dependent state space probabilities labeled as $P^j_{i_1,i_2,\dots,i_{N^{S,j}}}(t)$. With (2) we can define the single index m such that it labels the product states from 1 to $N^{S,j}$ using

$$m_{old} = 0,$$
$$\sum_{i_1=1}^{N_1^{j,S}}\sum_{i_2=1}^{N_2^{j,S}}\cdots\sum_{i_{N^S_j}=1}^{N^{j,S}_{N^S_j}}\{m_{new} = m_{old} + 1,$$
$$m_{new} \text{ label for } \left(i_1, i_2, \dots, i_{N^S_j}\right), m_{old} = m_{new}\}. \quad (10)$$

Based on the state space labeling (10) we define an overall system state vector for S^j as $\vec{P}^j(t) = (P^j_1(t), P^j_2(t), \dots, P^j_{N^{S,j}}(t))^T$. Assuming that the transition rates are independent of time and assume in addition equidistant small time-steps $\Delta t > 0$, the following scaling discrete time Markov model (SDTMM) can be derived, as a generalization of DTMM.

SDTMM consists of initial conditions to start propagation within S^j, in particular also S^0,

$$\vec{P}^0\left(t_0^{P,j} = t_j\right) = (P^j_1(t_0^{P,j}), P^j_2(t_0^{P,j}), \dots, P^j_{N^{S,j}}(t_0^{P,j}))^T. \quad (11)$$

Conditions for refining subsystem state spaces can be defined as, e.g.,
if $P^j_m\left(t_n^{P,j}\right) \geq P_{crit\ max}$ for any m at earliest n≥1 find refinement that reduces

$$\max_m P^j_m(t_n) \text{ most.} \quad (12)$$

And for coarsening state space, e.g.,
if $P^j_m\left(t_n^{P,j}\right) \leq P_{crit\ min}$ for any m at earliest n≥1 find abstraction that increases

$$\min_m P^j_m(t_n^{P,j}) \text{ most.} \quad (13)$$

We assume that the propagation is conducted until, e.g., (12) or (13) holds. In this case, we set $t_{j+1} = t^{P,j}_{N^{P,j}} = t_j + N^{P,j}\,\Delta t, N^{P,j} \geq 1$.

For the propagation times $t_n^{P,j} = t_j + n\,\Delta t, n = 0,1,\dots,N^{P,j}$ used in (12) and (13) we obtain the state vectors using the transition probability matrix multiplied n-times by itself

$$\vec{P}^j\left(t_n^{P,j}\right) = \mathbb{P}^n_{j,\Delta t}\,\vec{P}^j\left(t_0^{P,j}\right), \quad (14)$$

where the transition probability matrix elements for overall state space S^j are given by

$$\mathbb{P}^n_{j,\Delta t} = \begin{bmatrix} p^{j,\Delta t}_{1\to 1} & p^{j,\Delta t}_{2\to 1} & \cdots & p^{j,\Delta t}_{N^{S,j}\to 1} \\ p^{j,\Delta t}_{1\to 2} & p^{j,\Delta t}_{2\to 2} & \cdots & p^{j,\Delta t}_{N^{S,j}\to 2} \\ \vdots & \vdots & \ddots & \vdots \\ p^{j,\Delta t}_{1\to N^{S,j}} & p^{j,\Delta t}_{2\to N^{S,j}} & \cdots & p^{j,\Delta t}_{N^{S,j}\to N^{S,j}} \end{bmatrix}^n \quad (15)$$

The matrix elements in (15) are given for $1 \leq \iota, \kappa \leq N^{S,j}$, $\iota \neq \kappa$, by

$$p^{j,\Delta t}_{\iota\to\kappa} = P\left(X\left(t_1^{P,j} = t_0^{P,j} + \Delta t\right) = \kappa \middle| X\left(t_0^{P,j}\right) = \iota\right)$$
$$= 1 - \exp\left(-\lambda^j_{\iota\to\kappa}\Delta t\right)$$
$$= \lambda^j_{\iota\to\kappa}\Delta t + o((\lambda^j_{\iota\to\kappa}\Delta t)^2), \text{ if there is just one } 1\leq\nu\leq N_j^S \text{ with } i_\nu(\iota) \neq i_\nu(\kappa)$$
$$\text{and 0 otherwise.} \quad (16)$$

The approximation in the last equality of (16) assumes that $\lambda^j_{\iota\to\kappa}\Delta t \ll 1$. The condition given in (16) ensures that only transitions are modeled for which one subsystem or subfunction changes its state. This means that it is sufficient to know all allowed state transitions on subsystems or subfunction level to build the overall transition probability matrix (15), e.g., within the subsystems of S^2 of Fig. 2.

The diagonal elements of (15) read

$$p^{j,\Delta t}_{\iota\to\kappa} = P\left(X\left(t_1^{P,j} = t_0^{P,j} + \Delta t\right) = \kappa \middle| X\left(t_0^{P,j}\right) = \iota\right)$$
$$= 1 - \sum_{\substack{\kappa=1 \\ \kappa\neq\iota}}^{N^{P,j}} p^{j,\Delta t}_{\iota\to\kappa}, \text{ if } \iota=\kappa, \quad (17)$$

where $\iota, \kappa = 1,2,\dots,N^{S,j}$. This condition ensures that the probability flow out of each state is balanced by the reduction of the probability of staying in the state. Thus, the sum over all column elements of (15) is unity.

The first element of the vector at the left-hand side of (14) is for $n = 1$ obtained by multiplying the first row of the matrix at the right-hand side with the column vector, etc. This shows that (14) can be derived using the total law of probability and assuming that the Markov states are independent of each other.

In a similar fashion, a scaling continuous time Markov model (SCTMM) can be derived. In this case we replace for instance (14) by

$$\frac{d}{dt}\vec{P}^j(t) = \mathbb{Q}_j\ (t)\ \vec{P}^j(t), \quad (18)$$

where the transition rate $\mathbb{Q}$-matrix (Meyna and Pauli 2010) is used. In this case, the transition points can be at arbitrary times, and transition rates can be time-dependent.

4. Sample system resolution and criticality analysis of dominating state

4.1. *Sample scaling system refinement and abstraction*

Table 1 shows a sample AD system functional structural architecture that follows the requirements introduced in Section 3.1 along with Fig. 2 and Fig. 3. It shows an increasing refinement of an autonomous vehicle (AV) using 1, 4, 10 and 24 subsystems with respectively 2 states or subfunctions that can be considered as an example of a sustainable system when compared to traditional vehicles, given its potential advantages as resource sharing, less carbon intensive driving patterns, and reduction of accidents. The functional-structural architecture used is based mainly on (Behere and Törngren 2015) (Novickis et al. 2020) (Behere and Törngren 2017) (Zhang et al. 2021).

4.2. *Dominating state without application of dynamic scaling Markov model*

Fig. 4 shows the effect of a single dominating AD state on the probability distribution of all other AD states. This is generated by a single constant failure rate according to (16) that is increased from a level similar as all failure rates in Fig. 4A by orders of magnitude till Fig. 4F.

To show the impact of the critical transition on the final probability distribution and reliability of the overall AD system, Fig. 4A and Fig 4.B illustrate the original distribution with non-critical transition rates between states $\lambda^{\mathrm{j}}_{\iota\to\kappa} = \lambda^{\mathrm{j}}_{371\to 567} = 2.5 \cdot 10^{-5}h^{-5}$ and $1.0 \cdot 10^{-5}h^{-5}$ according to equation (16). In total $\mathrm{N}^{\mathrm{S,j}} = 1024$ states were considered.

This is a resolution between level 2 and 3 of Fig. 2 and of level 2 of Table 1. Here achieved by resolving only 10 subsystems or subfunctions with 2 states respectively, i.e. $2^{10} = 1024$. These AD subsystems are used: sensor fusion, object detection, trajectory planning, motion control, ego driver, pedestrian, weather, lighting, traffic density, and street geometry. Similarly one might consider 5 subsystems or functions with 4 states, respectively. Note that the three first standard subsystems of level 1 resolution of Table 1 are extended with the environment subsystem.

All the allowed constant transition rates according to (16) between other states in plot Fig. 4A are of the same order ranging from $2.0 \cdot 10^{-5}h^{-1}$ to $2.5 \cdot 10^{-5}h^{-1}$. Plots Fig. 4B to Fig. 4F illustrate changes in the probabilities if a critical transition rate has the values $1.0 \cdot 10^{-5}h^{-1}$, $1.0 \cdot 10^{-3}h^{-1}$, $2.0 \cdot 10^{-3}h^{-1}$, $1.0 \cdot 10^{-2}h^{-1}$, and $1.0 \cdot 10^{-1}h^{-1}$.

Reliability is defined as AD system being in fully operational states (states with failure of none or one component) or fail-operational states (states with failure of any two technical components as well with failure of ego driver along and of one environmental component). In total there are 925 reachable states.

Fig. 4 was computed using the CTMM approach. The redistribution of state probabilities clearly shows the effect of the critical transition on the overall probability distributions. Whereas Fig. 4A and Fig. 4B still show that in the asymptotic realm, many states are of the same order of magnitude, state probabilities are more and more compressed starting with Fig. 4C till in Fig. 4F only one asymptotic state remains.

For practical applications, this implies that only little information would be available when sticking to the initial state space definition, since the AD dominating failure mode is not further resolved. This asks for SCTTM approach.

5. Conclusions

The formal presentation of even the simplest possible realization of the probability distribution time history flow for an up- and down-scaling Markov model with exponential transition modeling assuming equidistant time steps (SDMM) requires that, in addition to the structural-functional modelling of the system, the

Table 1: Scaling structural-functional state space of an autonomous vehicle including its environment.

Resolution level					
0	**1**	**2**	**3**	**4**	**…**
Sample number of subsystems, components, subcomponents, and functionalities					
System level model	**Subsystem level model**	**Component level model**	**Subcomponent level model**	**Functionality level model**	
1	**4**	**10**	**23**	**25**	
System	**Perception**	Sensing and sensor fusion	Camera, LiDAR, Radar	ADAS (Advanced Driver Assistance System)	
			GPS/GNSS, Ultrasonic	ACC (Adaptive Cruise Control)	
		Mapping, localization and navigation	Communication, WIFI	AEB (Autonomous Emergency Braking)	
			IMU (Inertial Measurement Unit)	F/R CW (Forward/Rear Collision Warning)	
		Semantic understanding	IoT (Internet of Things), V2X, HMI	LDWS (Lane Departure Warning System)	
			Object detection and tracking	Object detection	
	Decision and control	Planning	Path planning	Blind spot detection	
			Trajectory planning and generation	ESC (Electronic Stability Control)	
			Motion planning	LKA (Lane Keeping Assist)	…
			Motion control	Park assist (Valet parking)	
				Collision avoidance	
	Vehicle platform manipulation	Execution	Platform stabilization	Trajectory Tracking	
			Trajectory execution	Speed control	
				Driver Monitoring System	
		Actuation	Steering	EBS (Electronic Braking System)	
			Throttle	ABS (Anti-lock Braking System)	
			Brakes	Predictive braking	
	Environment	Traffic infrastructure	Surrounding objects: static and dynamic	Obstacle detection	
			Traffic signs	Traffic sign recognition	
			Road markings	Lane detection	
		Other road participants	Other vehicles	Vehicle detection	
			VRU (Vulnerable Road User): pedestrian, cyclist, etc.	Pedestrian detection	
		Weather and lighting	Rain, fog, snow, glare, darkness, etc.	Eco maneuvering, Night vision	
		Other characteristics	Street geometry (highway, urban, etc.)	IAS (Intersection Assistant System)	
			Traffic density (light, heavy, etc.)	TJC (Traffic Jam Chauffeur)	

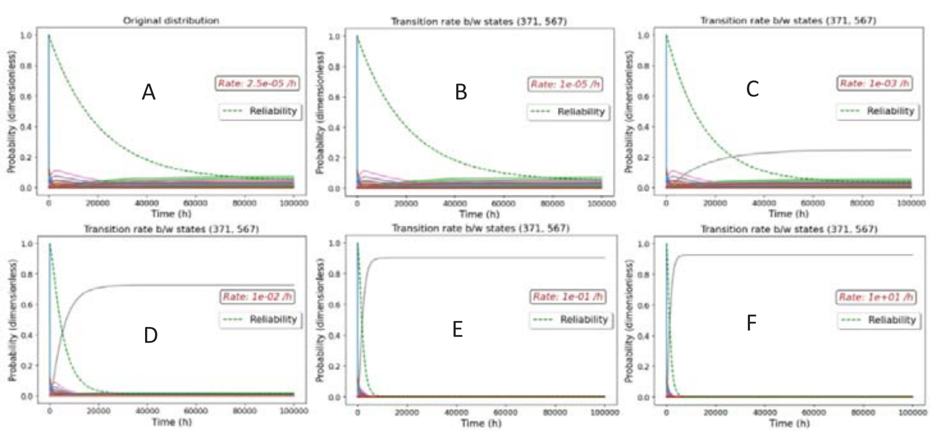

Fig. 4. Impact of single increasingly dominating transition on overall state space probability time histories.

dynamic refinements and extension need to be modelled, i.e. how the probabilities at transition points are distributed or summarized. Conditions and parametrization options for such scaling points have been provided.

It was observed that the number of needed scaling models scales surprisingly moderately when compared to state space explosion numbers when allowing only stepwise scaling and can be seen as refinement or formalization of the structural-functional modelling. Also, within propagation phases transient and absorbing states can be identified.

Further work could further extend the initial sample application of the approach to autonomous vehicles. It so far only shows how to identify single critical state transitions in rather moderately large state spaces. Besides full-scale implementation of the approach, also generalizations from the base-line formalism are a natural step ahead, in particular beyond time-dependent transitions only and going beyond the classical Markov assumption.

Acknowledgement

All authors acknowledge funding within the German BMWK project Real Driving Validation (RDV), Funding Number: 19A21051D.

References

Behere, Sagar, and Martin Törngren. 2015. "A Functional Architecture for Autonomous Driving." In *Proceedings of the First International Workshop on Automotive Software Architecture (WASA'15)*, edited by Philippe Kruchten, Yanja Dajsuren, Harald Altinger, and Miroslaw Staron, 3–10. New York, NY, USA: ACM.

Behere, Sagar, and Martin Törngren. 2017. "Systems Engineering and Architecting for Intelligent Autonomous Systems." In *Automated Driving*, edited by Daniel Watzenig and Martin Horn, 313–51. Cham: Springer International Publishing.

Bonderson, C. 2018. "Modelling of safety concepts for autonomous vehicles using semi-Markov models: Examensarbete." https://pdfs.semanticscholar.org/22fb/3be001a8539da6b9dea8963337eeef98eda2.pdf.

Häring, Ivo, Yupak Satsrisakul, Jörg Finger, Georg Vogelbacher, Corinna Köpke, and Fabian Höflinger. 2022. "Advanced Markov modeling and simulation for safety analysis of autonomous driving functions up to SAE 5 for development, approval and main inspection." In *Proceedings of 32nd European Safety and Reliability Conference*, edited by ESREL 2022, 104–11. Dublin, Ireland.

Heinrich, J, F Plinke, and J Hausschild. 2017. *State-based safety and availability analysis of automated driving functions using Monte Carlo simulation:* CRC Press: 1975–82.

Horeis, Timo F., Tobias Kain, Julian-Steffen Muller, Fabian Plinke, Johannes Heinrich, Maximilian Wesche, and Hendrik Decke. 2020. "A Reliability Engineering Based Approach to Model Complex and Dynamic Autonomous Systems." In *2020 International Conference on Connected and Autonomous Driving (MetroCAD)*, edited by MetroCAD, 76–84.

Liang, Qingzhu, Yinghao Yang, Hang Zhang, Changhong Peng, and Jianchao Lu. 2022. "Analysis of simplification in Markov state-based models for reliability assessment of complex safety systems." *Reliability Engineering & System Safety* 221: 108373. doi:10.1016/j.ress.2022.108373.

Meyna, Arno, and Bernhard Pauli. 2010. *Taschenbuch der Zuverlässigkeitstechnik: Quantitative Bewertungsverfahren.* 2., überarb. und erw. Aufl. Praxisreihe Qualitätswissen. München: Hanser.

Naybour, S., J. Andrews, and M. Chiachio-Ruan. 2019. "Efficient Risk Based Optimization of Large System Models using a Reduced Petri Net Methodology." In *Proceedings of the 29th European Safety and Reliability Conference (ESREL 2019)*, edited by Michael Beer and Enrico Zio, 828–33. Singapore: Research Publishing Services.

Novickis, Rihards, Aleksandrs Levinskis, Roberts Kadikis, Vitalijs Fescenko, and Kaspars Ozols. 2020. "Functional Architecture for Autonomous Driving and its Implementation." In *2020 17th Biennial Baltic Electronics Conference (BEC)*: IEEE.

Nyberg, M. 2018. *Safety analysis of autonomous driving using semi-Markov processes:* Taylor and Francis Group. Accessed October 17, 2019. https://doi.org/10.1201/9781351174664, https://www.taylorfrancis.com/books/e/9781351174664: 781–88.

Pouya, Parisa, and Azad M. Madni. 2021. "Expandable-Partially Observable Markov Decision-Process Framework for Modeling and Analysis of Autonomous Vehicle Behavior." *IEEE Systems Journal* 15 (3): 3714–25. doi:10.1109/JSYST.2020.3010473.

Sonnenberg, F. A., and J. R. Beck. 1993. "Markov Models in Medical Decision Making: a Practical Guide." *Medical decision making : an international journal of the Society for Medical Decision Making* 13 (4): 322–38. doi:10.1177/0272989X9301300409.

Yosri, Ahmed, Yasser Elleathy, Sonia Hassini, and Wael El-Dakhakhni. 2021. "Genetic Algorithm-Markovian Model for Predictive Bridge Asset Management." *J. Bridge Eng.* 26 (8). doi:10.1061/(ASCE)BE.1943-5592.0001752.

Zhang, Shuai, Bin Lei, Shuai Chen, and Lei Sha. 2021. "Research on subjective evaluation method of automatic emergency braking (AEB) for passenger car." In *6th International Symposium on Vehicle Emission Supervision and Environment Protection (VESEP2020), E3S Web of Conferences*. Vol. 268, edited by Y. Yan, Li, M., L., X. Hou, and Y. Long, 1037 Volume 268.