
Simulation model for simple yet robust resilience assessment metrics for engineered systems

Patriarca, Riccardo*[1]

De Paolis, Alessandro[1]

Costantino, Francesco [1]

Di Gravio, Giulio[1]

[1] Sapienza, University of Rome, Department of Mechanical and Aerospace Engineering, Rome (ITALY)

** Corresponding author: Via Eudossiana, 18 – 00184 Rome (Italy). riccardo.patriarca@uniroma1.it*

Printed and proofed version available here:
http://www.sciencedirect.com/science/article/pii/S0951832021000351

Simulation model for simple yet robust resilience assessment metrics for engineered systems

Abstract

Modelling system properties is a central step to carry out time-dependent simulations of system' s operating conditions. In this paper, we present a simulation model combined with simple metrics that focus on system's resilience at a technical level, represented through absorption, adaptation and recovery. Following the techno-centric perspective of this research, the components' reliability is considered as the main performance of interest for the analysis. When a failure occurs, according to a certain probability, performance is restored after a certain recovery time. This latter is a stochastic variable that relies on recovery functions specific for every component. The model has been applied in a case study referred to a hot water generation plant for hospitals. The case study shows how the model allows depicting performance levels and its flexibility for multiple management strategies, supporting what-if scenarios analyses.

Keywords: Resilience; Resilience assessment; Resilience indexes; Reliability; Simulation model; Industrial plants.

1. Introduction

Resilience is considered a necessary property of modern industrial systems to ensure certain performance levels in response to internal or external disturbances [1], being capable of adapting existing resources and skills to new situations and operating conditions [2].
For the scope of this article, a system is considered more or less resilient depending on how it absorbs the downgrading effects of failures, adapts to reach a different equilibrium state, and recovers to certain performance levels.

The assessment of resilience performance is a largely debated topic in recent literature. Nevertheless, there is no unique consensus on what the most representative metrics are for such a purpose [3]. Starting from the seminal work by Holling for ecological systems [4], several authors have specialized resilience metrics (e.g.) stressing technical [5], socio-technical [6], or even societal aspects [7]. Regardless of the investigation focus, it is possible to distinguish between two main categories when referring to planning and modelling resilience: qualitative and quantitative [8]. The former category includes refers to assessment criteria without numerical descriptors, usually based on semi-quantitative judgements from experts, while the latter refers to either domain-agnostic set of measures or to domain-specific representations [8]. Considering the purpose of this paper, the domain-agnostic frameworks are the more relevant ones. One of the most common approaches in this area relates to the notion of *resilience triangle*, where robustness, rapidity, resourcefulness, and redundancy are used to compare actual and -planned performance levels [2]. Further elaborations of this idea have been proposed to trade-off lost functionality and recovery time [9], or to encompass partial recovery from multiple sequential events [10]. A similar concept has been used to visualize resilience comparing economic worst-case scenarios to experienced situations [11], even in terms of time-dependent analyses [12]. Such assessments can be performed in static or probabilistic terms. Probabilistic approaches have in general a higher potential to capture the uncertainty linked to a system behavior, usually ascribed to the loss of performance, the length of recovery, as well as the modality of restoration [13]. A probabilistic modelling also ensures the capacity to include stochastic disruptions [14], [15], which are more representative of real scenarios, as well as potential cascading effects. Other approaches rely on topological properties of the system, interpreted as a network [16]: in these works, resilience has been related to indexes based on network theory (e.g. closeness centrality [17], shortest distance [18]), as well as customized component importance measures [14].

Following recent literature related to the resilience engineering (i.e. the discipline focused on enhancing the ability of a system to adapt or absorb disturbances, disruption and change [19]), it is possible to draw a summary of resilience intended as an inherent a capacity of a system: resilience is something the system does, not something the system has [20]. On this context, the notion of being resilience can be ascribed to the capability of a system to tolerate disruptions and sustain its functioning [21], [22], as well as to mitigate loss through adaptive responses [23], and to recover against experienced critical effects [24].

Summarizing the concepts emerging from literature on resilience to define metrics domain-agnostic metrics usable at a system level, this paper models resilience as a combination of the ability to absorb disruptions, to continue operation in degraded states and to recovery to a certain performance level [25].

More specifically, the capacities considered in this study are interpreted as follows:

- *Absorption*: the ability which ensures a system can absorb the impacts of disturbances and minimize consequences with minimum effort [26]
- *Adaptation*: the ability of a system to adapt to unwanted situations by undergoing some modifications in order to better withstand current and future impacts [27]
- *Recovery*: the ability of a system to return to a desired service level, from a disrupted system state [28]. Such service level can be an improved state if compared to disrupted state, the original performance level, or a level beyond original ones.

On such premises, this paper relies on a recently published contribution about the definition of resilience metrics [25], which explicitly encompasses the above-mentioned dimensions of analysis. The aim of this work consists of supporting the generalizability of resilience assessment via absorption, adaptation, and recovery for techno-centric analyses, including a stochastic perspective. In pragmatical terms, this manuscript aims to propose a conceptual simulation model and the respective pseudo-code to be used for simulating the properties of engineered systems in light of a technical resilience research perspective [25].

The remainder of the paper is organized as follows: Section 2 presents the proposed methodology, Section 3 details the logic of the simulation model, Section 4 presents the case study, while Section 4 summarizes the outcome of the study, its strengths, weaknesses and the potential for future research.

2. **Methodology**

While the methodology may remain applicable for a wide range of systems, including socio-technical systems, once ensured the definition of specific functional mechanisms and performance metrics, this paper in-depth explores a techno-centric research dimension for engineered systems. Therefore, the developed simulation model is quantitative and it relies on reliability probabilistic assessments, as well as the analytical formulation proposed in [25].

Besides component-specific functions for reliability, a generic distribution for modelling components' repairability has been adopted for maintainability. These latter are intended to support the quantification of resilience through the definition of metrics aligned with the system capacities at the core of this article. The metric framework presented in [25] has been selected because of its userfriendly nature aligned with the decision-maker perspective, along with its customizability for different systems and scenarios.

*2.1 **Techno-centric metrics***

The techno-centric resilience metrics are defined in a case with no degradation due to aging: maximum level of performance is reached every time performance is restored to the original state. Figure 1 sketches the performance over time in case of component's failure and its effect on the system. F_0 and F_f are respectively the initial and the final performance levels at time T_0 and T_f. At T_0, a failure occurs, the performance decreases and a stable level is reached, keeping it from F'_{l1} (at time T_{l1}) to F'_{l2} (at time T_{l2}). From this point, the system starts restoring its lost performance up to the level F_f, where a new steady state is reached. F_{l1} and F_{l2} are the performance levels, respectively, at time T_{l1} and T_{l2}, in case the disruptive event would have not occurred [25].

Two important hypotheses have been considered in this work: (i) the linearity of performance, (ii) and the possibility to recover post-recovery performance after a certain transient period following a failure, as sketched in Figure 1.

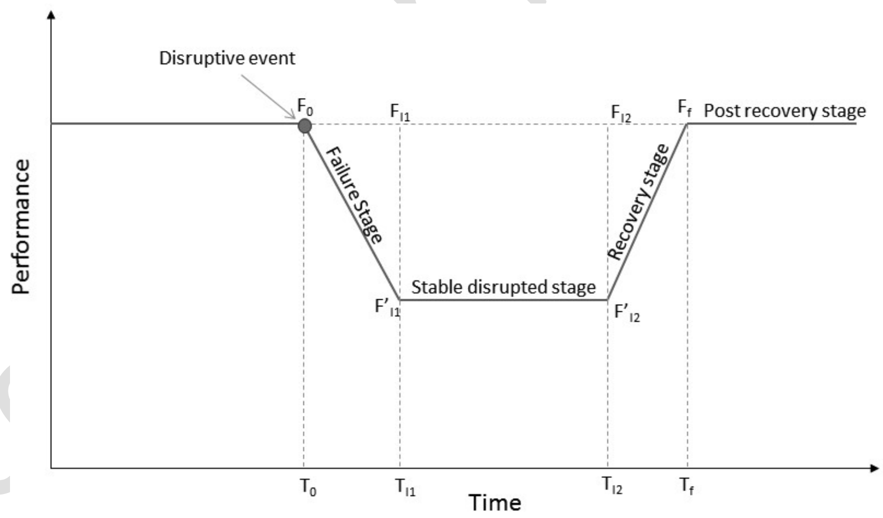


Figure 1. Performance over time and variable of interest (adapted from [25]).

Considering the description of resilience capacities previously, the absorption metric can be obtained as the ratio of the residual performance to the original performance at the time of the disruptive event occurs (1):

$$Ab = \left(\frac{F'_{l1}}{F_0}\right) * C_{Ab} \tag{1}$$

Where C_{Ab} is the ageing factor (2):

$$C_{Ab} = 1 + \left(\frac{F_0 - F_{l1}}{F_0}\right) \tag{2}$$

C_{Ab} is equal to 1 under the assumptions about no ageing effect $F_0 = F_{l1}$.

The adaptation metric is defined by the time interval in which the system achieves a new stable post-failure state and maintains it until the recovery actions take place (3):

$$Ad = 1 - \left(\frac{T_{l2} - T_{l1}}{T_f - T_0}\right) \tag{3}$$

The longer the time for recovery operations (i.e. the greater the difference $T_f - T_0$), the lower the adaptive capacity of the system.

The recovery capacity metric is defined as the slope of the recovery curve in comparison with the ideal linear recovery slope of 90 degrees (4):

$$Rec = \frac{Arctan\left[\dfrac{F_f - F'_{l2}}{\left(\dfrac{T_f - T_{l2}}{T_f - T_0}\right)}\right]}{90} * C_T \tag{4}$$

Where C_T is the recovery duration factor (5):

$$C_T = \frac{T_{l2} - T_0}{T_f - T_0} \tag{5}$$

The final resilience metric is then obtained by the following Boolean relation among absorptive, restorative, and adaptive capacities of the system (6):

$$Re = Ab \vee (Ad \wedge Rec) = Ab + Ad * Rec - Ab * Ad * Rec \tag{6}$$

The absorption capacity is assumed an independent attribute: unlike adaption and recovery, it is not reactive but it is rather an inherent systemic property of the system [25].

Greater absorption capacities translate into a less significant impact on other capacities and consequently minor requested efforts and resources following the disruption. Greater adaptive capabilities indicate higher performance levels for post-destructive event. The obtained score for Resilience (Re) is thus a metric ranging between 0 and 1, which remains significative especially for relative comparisons among different configurations.

*2.2 **Conceptual representation of the simulation model***

Figure 2 sketches the logic of the simulation model for the engineered systems being considered, which is hereafter described in conceptual terms. *R(t)* is the array of reliability functions of each component/subsystem. These functions allow defining the array of *States(t)*, i.e. the failure states that could occur in a specific time instant. Following a *Recovery time* (modelled as a stochastic variable), the system performance is restored at its original state, i.e. as it was before the degradation event occurs, depending on the respective *Recovery function(s)*. *Time* interval varies based on the observation period under examination. The core of the simulation model (described in detail in §2.3) offers the results of the simulation which allows to track for each time interval the performance of the system for each time instant.

As such, it remains possible to assess overall resilience levels and compare the response to specific events in terms of absorption, adaptation and recovery [25].

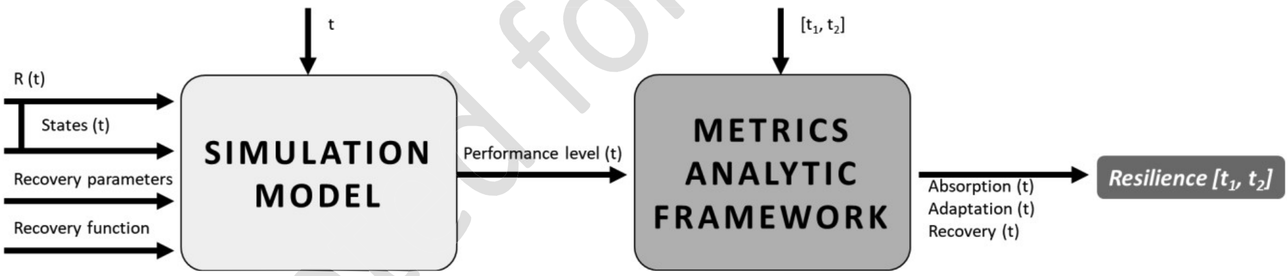


Figure 2. Model scheme of the proposed approach to facilitate the calculation of resilience metrics.

*2.3 **Detailed logic of the simulation approach***

The simulation model scheme depicted in Figure 2 represents the core of the approach. For every time instant, it starts from the reliability functions R(t) in order to define the failure probability of every component/subsystem and associate the occurred system state and system performance in a range 0-100%. For example, considering power grids' resilience at a regional level, this indicator could be the percentage of critical services still having power, or at a plant level, the power that the grid itself can provide. A different scale can be adopted in case other types of metrics should be considered (e.g. number of customers not experiencing an outage) without compromising the validity of the proposed approach [29].

A simplifying assumption considers every subsystem to be independent from the others: the failure of a single component does not influence the reliability of the remaining ones. A pseudo-code is reported to synthetize the logic of the simulation model, which is the basis to run the proposed analytic framework.

```
for t = 1 to K (K is the final instant of the observation period)

        for i = 1 to N (N is the number of system components)
                Probability_failure_Component_i (t) = 1 – Reliability_Function_Component_i(t)
        end i

                P_failure_Matrix (t) = [PfailureComponent_i, …, PfailureComponent_N]

        Safe_State(t) = 1 - product [P_failure_Matrix(t)] (for each t, it includes the "no failure" probability)

        P_state_Matrix (t) = [P_failure_Matrix(t,:), Safe_State(t)^T] (for each t, a probability matrix for all failure states and
        safe state)

        Active_state(t) developed as the most likely state in t: A Monte Carlo simulation is performed based on a discrete
        probability distribution function suggested in P_state_Matrix (t) for m iterations. The most probable state is
        selected.

        for i = 1 to N (N is the number of system components)
                Functionality_i (t) = Functionality_Component_i (t)
        end i

                Note that "Functionality_i (t)" is obtained as follows to combine failure probability, detectability, and maintainability:
                If t = time instant of fault of component_i
                        Functionality_i (t)= Percentage_Performance_i_loss (vulnerability activated)
                else if t = time_instant_fault_Component_i + Recovery_time_Component_i(t)
                        Functionality_i (t) goes back to the original state before the fault occurs (recovery completed)
                else
                        Functionality_i (t) = Functionality_i (t -1) (steady state)
                end if

        Functionality_Matrix (t) = [Functionality_i(t), …, Functionality_N (t)]

        System_Functionality (t) = product [Functionality_Matrix(t)]

end t
        Select a relevant time interval [t_1, t_2]

        Calculate Ab, Ad, Rec, and Re in [t_1, t_2] (through indexes described in §2.1).
```

This pseudo-code has been used as a basis for the development of scripts subsequently implemented in MATLAB.

3. **Case study**

The proposed simulation approach has been validated in an industrial service plant of hot water generation for hospitals. The plant presented in [30] served as a relevant use case for the analysis, considering its criticality in terms of number of served users, components reliability, and expected high service levels. As for traditional approaches rooted in industrial systems engineering [31], Figure 3 presents a reliability block diagram of the system: five principal subsystems can be identified, and where relevant, their sub-components (ratios represent the redundancy level, i.e. contemporarily required/total number of items).

At a functional level, the natural gas mains carry the gas inside two co-generators (set in parallel), in which the combustion takes place, enabling at the same time electric energy production and heat generation. The exhausted high temperature gases are directed towards a heat exchanger, where water in the pipes absorbs the heat. Successively five pumps placed in parallel active redundancy (four pumps have to work to guarantee the system's performance) carry the hot water towards three tanks (set in active redundancy parallel, i.e. two tanks have to work to avoid the service interruption). The tanks have the aim to provide the hot water to the users of the hospital.

Such sub-systems (i.e. Natural gas mains, Cogenerators, Heat Exchange, Pumps, Thermal Storages) are placed in series: it is thus important to guarantee the functioning of every element or subsystem otherwise in case of serious failures the whole system is forced to stop.

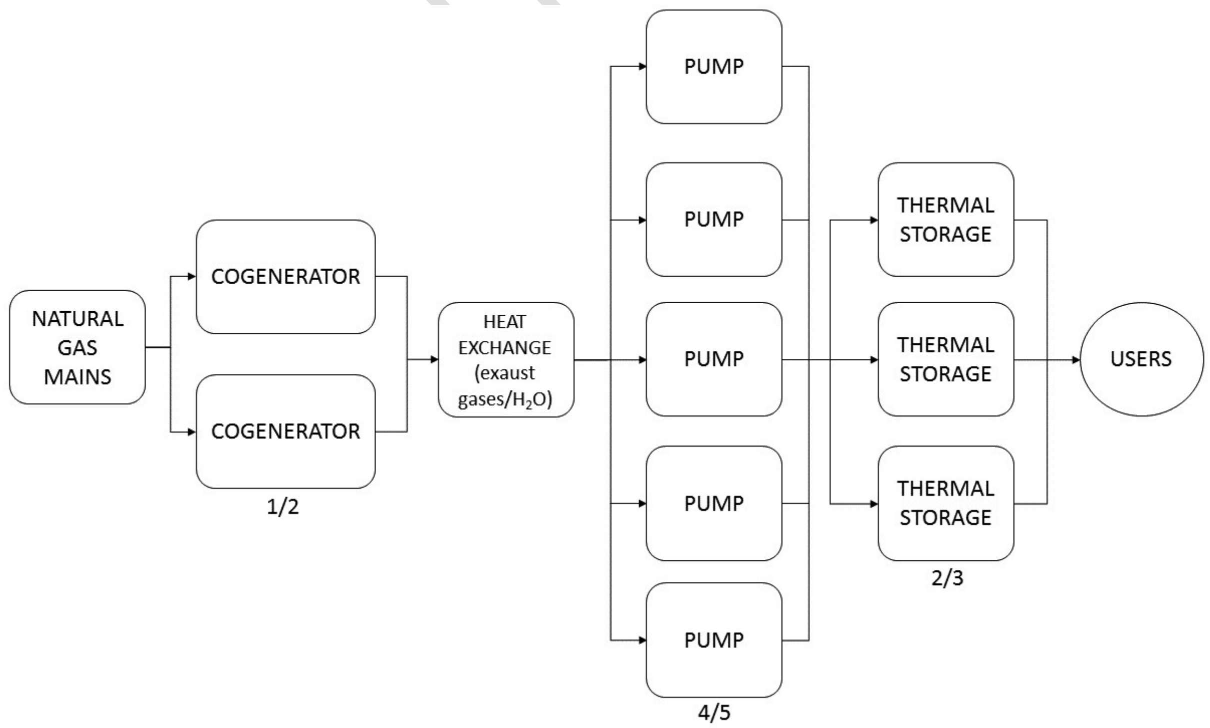


Figure 3. Reliability Block Diagram of the hot water generation system under examination.

Since the hospital structure has to be active constantly, a simulation time span of 365 days has been considered (K=365). The information on the plant have been complemented with data available in previous literature or similar plants to define the reliability function of each component, i.e. Reliability_Function_Component$_i$(t). In particular, the reliability function of natural gas mains is modelled as a function of a normal distribution (Φ) [32] (7):

$$R_1(t) = 1 - \Phi\left(\frac{t - \mu_1}{\sigma_1}\right) \tag{7}$$

where μ_1 is the distribution mean, σ_1 is the variance and *t* is simulation time.
The two co-generators' reliability function is individually modelled through an exponential distribution [33] (8):

$$R_{2'}(t) = e^{-\lambda_2 t} \tag{8}$$

where λ_2 is the scale parameter, assumed 1/MTBF (mean time between failure), t is the simulation time. Considering the co-generators layout (set in parallel, n_cog=2), the reliability function of the subsystem is (9):

$$R_2(t) = 1 - \prod_{i=1}^{n\_cog} \left(1 - R_i(t)\right) \tag{9}$$

The heat exchanger's reliability is modelled through a Weibull probability distribution (10):

$$R_3(t) = e^{-(\lambda_3 t)^{a_3}} \tag{10}$$

where λ_3 is the scale parameter, a_3 is the shape parameter.
The pumps' reliability is modelled as well through a Weibull distribution, and the corresponding sub-systems is represented through an active redundancy function [34] (11):

$$R_4(t) = \sum_{j=y}^{v} \left(\binom{v}{j} R_{4'}(t)^j \left(1 - R_{4'}(t)\right)^{v-j}\right) \tag{11}$$

where *v=5* is the number of pumps in the subsystem; *y=4* is the number of pumps which have to be contemporarily active to guarantee the performance of the whole system; $R_4,(t)$ is the reliability function of the single pump, obtained through (10).

The three tanks are set in parallel with partial active redundancy and their reliability function is given by an exponential distribution probability of failure [35]: $R_5,(t)$ individual reliability as for (*8*), $R_5(t)$ sub-system reliability as for (11) where v=3 and y=2).

The system reliability is the series of the sub-system's reliability (12):

$$R_{system}(t) = \prod_{i=1}^{N} R_i(t) \tag{12}$$

where R_i is the reliability of the single component/subsystem in a specific instant of time. Figure 4 sketches the values of reliability over time for exemplary components subsystem, and for the entire system.

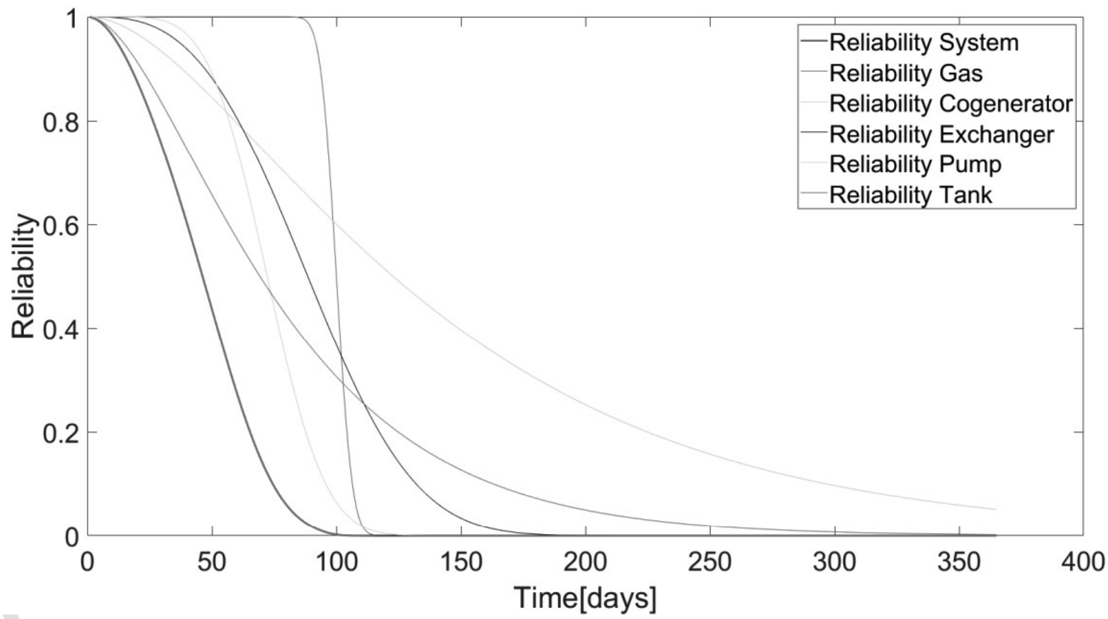


Figure 4. System' and sub-systems' reliability over simulation time (t=365 days; Gas = Natural Gas Mains, Co-generator = Co-generator sub-system, Exchanger = Exchanger sub-system, Pump = Pump sub-system, Tank = Tank sub-system).

4. **Results**

Starting from the analysis of the functional properties of the plant, it has been possible to identify 51 relevant states: 50 failure cases and a safe state (no failure). The gas mains and the heat exchanger are single elements that corresponds to minimal cut sets for the system: if one of them breaks, the system reaches zero performance. For co-generators, pumps and tanks, different performance losses can be defined, depending on the health state of the component, i.e. full functioning, degraded, not functioning. For structural reasons (as expressed earlier) redundancies for subsystems 2, 4, 5 allow maintaining system performance at 100%, if a single component breaks. Nevertheless, if a second component breaks before the conclusion of the maintenance intervention, the system performance downgrades to 0%. On the contrary, if one or more components of the subsystem are in a degraded state, different performance loss are assessed depending on the component type, following these functional rules: (i) 50% performance loss if a co-generator breaks, (ii) 20% performance loss if a pump breaks, (iii) 30% performance loss if a tank breaks. Combined system states have been identified as well, (e.g.) if two co-generators, two pumps or two tanks break at the same time, the system performance goes to 0% both in the degradation state and the efficient one.

Reconsidering the reliability block diagram of the system in light of these rules, a set of 50 system states has been considered to be representative of the most representative conditions in which the system may be when exposed to failures. The states have been obtained combining different types of failure and degradation states for each component. An additional state (state #51) has been added to consider the condition in which no failures occur. It is worthy noticing how the list of states could be expanded through the adoption of combinatorial modelling [36], beyond the scope of this article. The list of the 51 system states has been included in Appendix 1, while Figure 5 presents a summary of frequencies of states for the simulation interval (t=365).

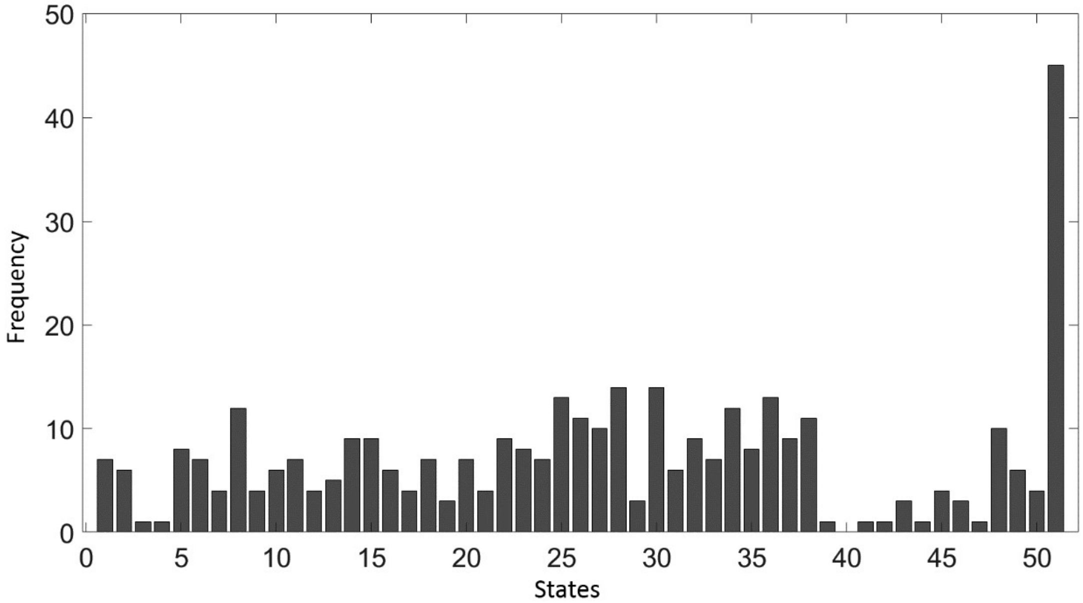


Figure 5. Frequency of the different 51 system states.

It appears clearly that state #51 (no failure occurs, fully functioning system) has the higher frequency: in the first days of observation (for approximately 45 days, cf. Figure 4) all components are considered as good as new, and then, progressively decrease their individual reliability implying a minor frequency of the no-failure state itself. Recovery_time_Component$_i$(t) has been modelled as an exponential distribution with different average values for each component (λ_rec_i).

For the calculation of the Active_state(t) to be selected among the 51 states, a Monte Carlo simulation is developed through m iterations for each state. The number m is calculated as (13):

$$m = \left[\frac{100\ S_x z_c}{E\bar{x}}\right]^2 \tag{13}$$

where (S_x) is the max variance value of states probabilities collected in the P_state_Matrix(t); $\bar{x}$ is its corresponding mean, E is the percentage error equal to 5% , which implies a confidence interval of $z_c = 2$. As such, m=600 iterations are run for every time instant t.

The described approach has been coded in MATLAB resulting in an efficient script list, i.e. the average running time of the simulation (600 iterations for each t, t=1,…,365 days) on an Intel Core 5 processor with 8 GB RAM is about 8 seconds.

Multiple settings can then be considered. For the analysis, it is imagined to be capable of acting only the repairing time through the parameter Recovery_time_Component$_i$(t). This is expected to understand the effects on system performance of different type of maintenance. This is for example the case where the decision maker may need to consider different performance-based contracts from one or more MRO (Maintenance, Repair Overhaul) companies. In this case, the MRO company takes in charge all the maintenance activities to restore system's functioning following a failure state.

We assume here some possible cases (e.g.) respectively λ_rec_i=1, 2, 3 for every i, and λ_rec_i specifically assigned to each component ($\lambda\_rec_1 = 2, \lambda\_rec_2 = 2, \lambda\_rec_3 = 2, \lambda\_rec_4 = 1, \lambda\_rec_5 = 3$), as respectively depicted in Figure 6 A, B, C, D. It is worth mentioning how the Figure represents system performance, which then allow calculating each metric *Ab, Ad, Rec,* and *Re*.

The green color defines the functioning zones: the greater their extension, the more resilient is the system, i.e. a larger functioning time is guaranteed even in case of failures. With reference to the fourth simulation which presents a more realistic case (Figure 6D), it is proposed the computation of the resilience metrics proposed in §2.1.

Besides the overall calculation of resilience performance which could be ascribed to the area under the performance curve as for resilience metrics [1], it is possible to decompose and specialize such distinction in terms of the three capabilities of the system. With respect to the values selected in the simulation presented for Figure 6D, Figure 7 details the proposed metrics for an exemplar time interval [t1, t2] with three potential system states activated (i.e. Scenario 1: failure of the Natural Gas Mains, performance level set to 0; Scenario 6: Co-generator-2 in degraded state, performance set to 0.5; Scenario 45: Thermal Storage-1 in degraded mode, performance set to 0.7; cf. Appendix).

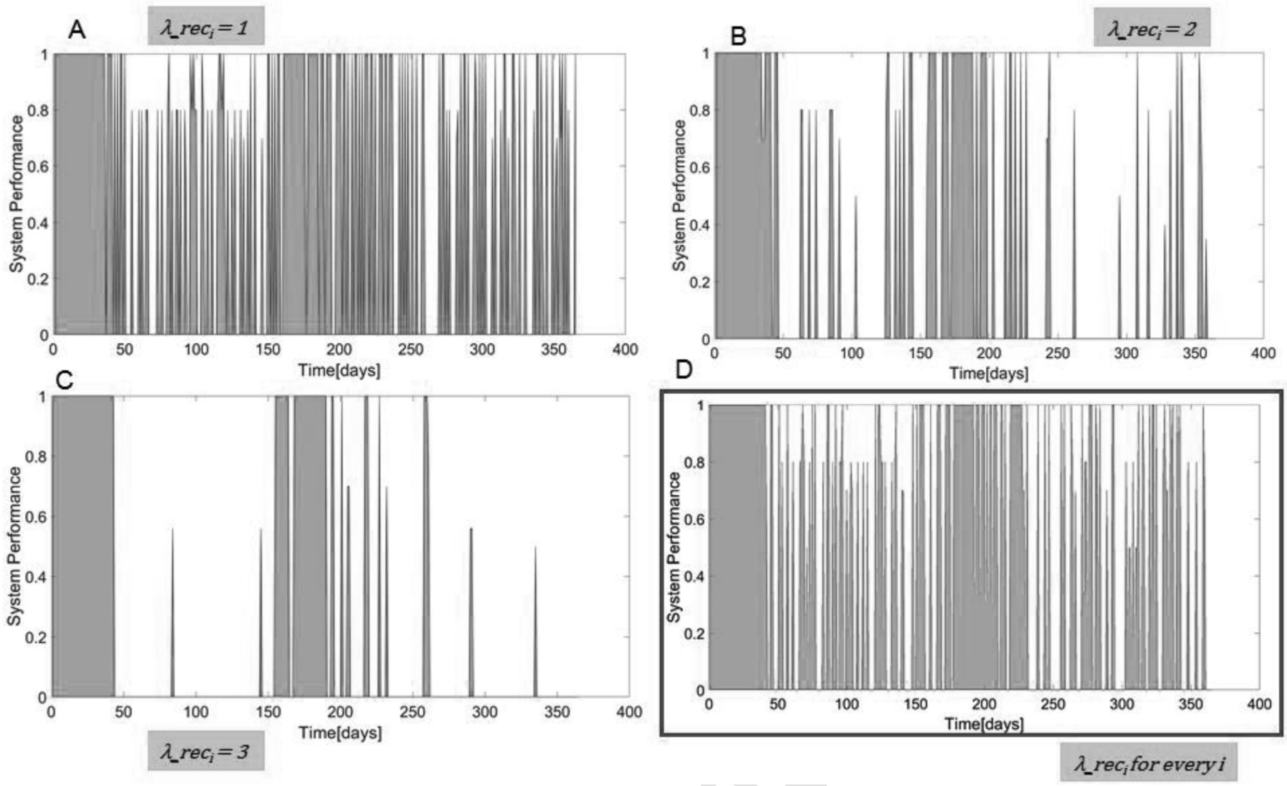
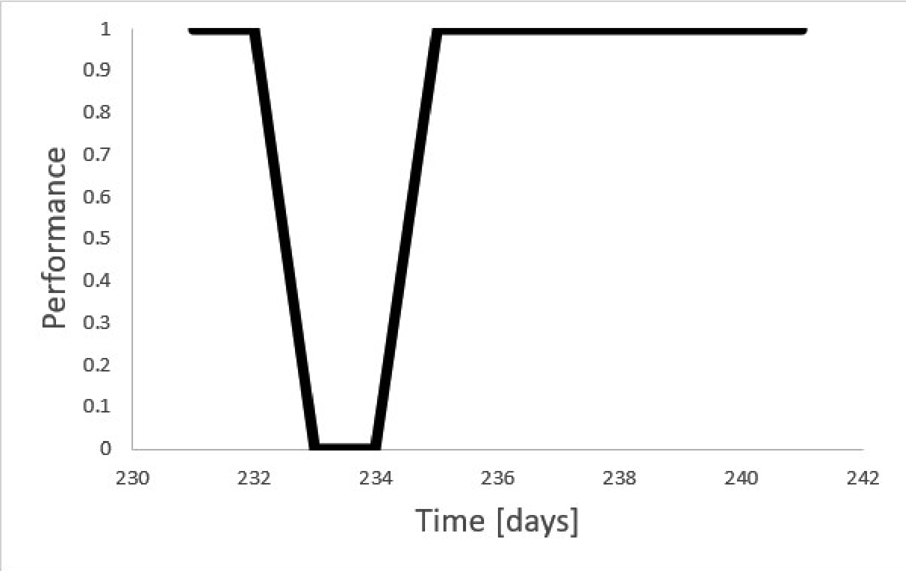


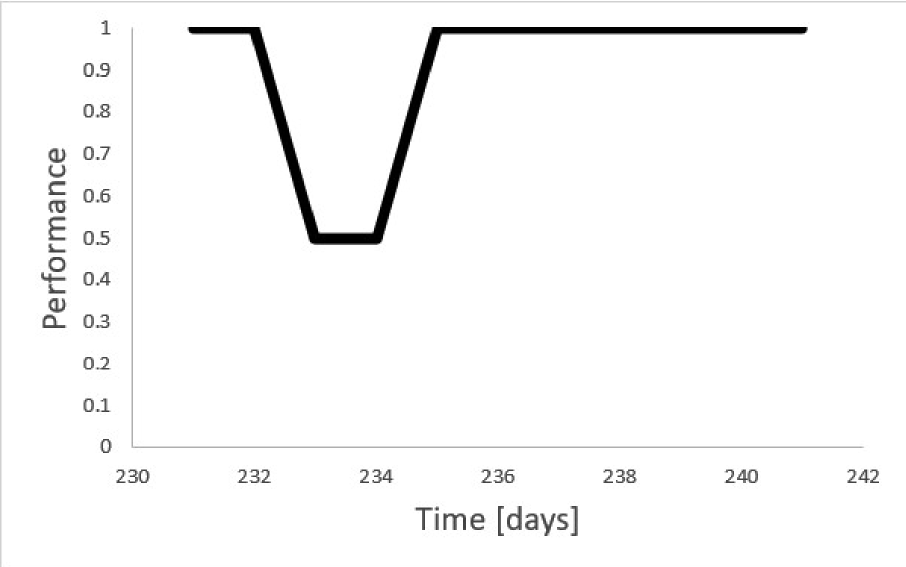
Figure 6. Simulation results for different recovery parameters. Green areas represent functioning intervals.

In addition to the baseline calculations, the simulation model can be set to define additional what-if scenarios. For example, it could be possible to use the presented simulation logic to calculate the proposed metrics for different - actual or potential - system's configurations. Figure 8 shows the performance obtained in Scenario 45 used as a baseline (degradation level = 0.7, $\lambda\_rec_5 = 0.7$) in comparison to two what-if scenarios related to alternative system architectures with different component's reliability and/or repairability.



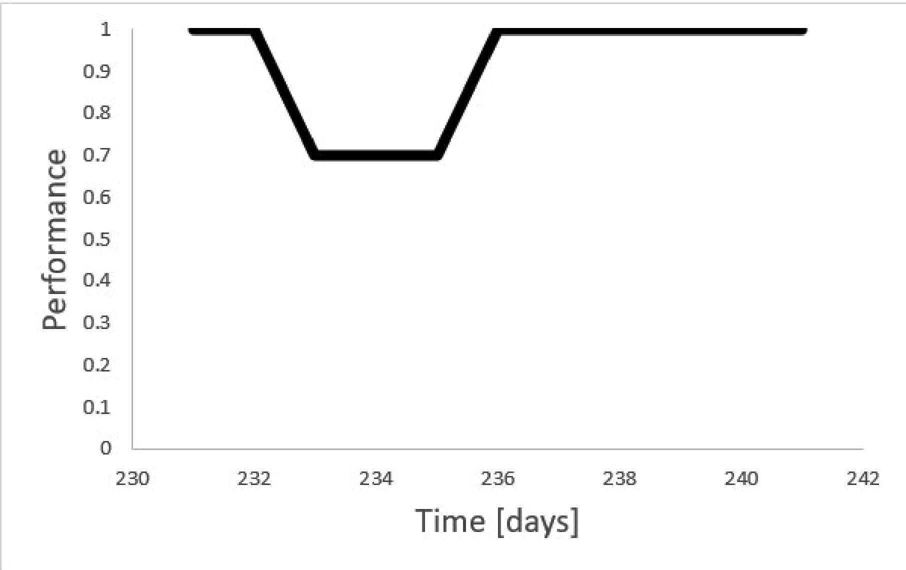
Scenario 1

A_b	0.0000
A_d	0.6667
Rec	0.0093
Res	0.0062



Scenario 6

A_b	0.5000
A_d	0.6667
Rec	0.0073
Res	0.5024



Scenario 45

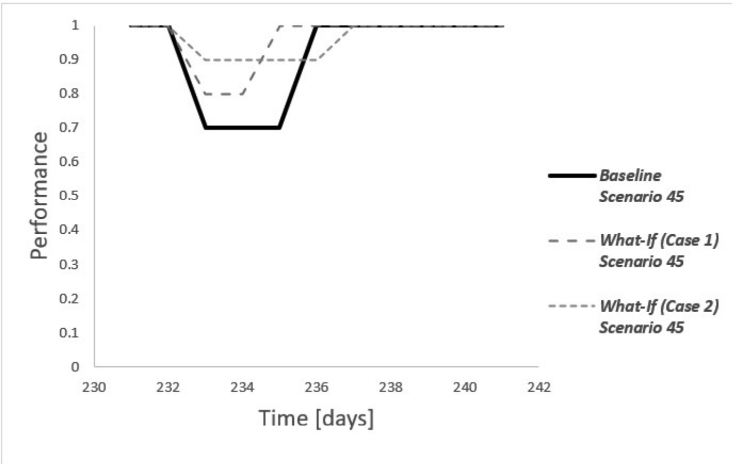
A_b	0.7000
A_d	0.5000
Rec	0.0073
Res	0.7011

Printed and proofed version available here:
http://www.sciencedirect.com/science/article/pii/S0951832021000351

Figure 7. Exemplar calculation of resilience abilities for different scenarios.

For the sake of simplicity, it has been considered just λ_rec and the degradation level and the corresponding metric values, i.e. Case 1, degradation level = 0.8, $\lambda\_rec_5 = 2$; Case 2, degradation level = 0.9, $\lambda\_rec_5 = 4$. Case 2 appears to be more advantageous, even if ascribed to a sensibly higher repairability time, if compared to Case 1.

Even though the values presented here are used just for demonstration purposes, they constitute an example of how - at decision-making level - it could be possible to assess different system configurations and choose the alternative that is more aligned to service level targets. Additional implications for management should be derived linking such techno-centric analyses to economic assessments for each setting being evaluated, running dedicated cost-benefit analyses.



Baseline Scenario 45

A_b	0.7000
A_d	0.5000
Rec	0.0073
Res	0.7011

What-If (Case 1) Scenario 45

A_b	0.8000
A_d	0.5000
Rec	0.0056
Res	0.8006

What-If (Case 2) Scenario 45

A_b	0.9000
A_d	0.6000
Rec	0.0016
Res	0.9001

Figure 8. Exemplar what-if analyses applied to a selected scenario.

5. **Conclusions**

The proposed model is able to reproduce the behavior of an engineered system through a time-dependent simulation. The case study refers to a simulation for resilience analysis of industrial plants, but it can be adapted to other types of systems. The pseudo-code proposal ensures some flexibility and reproducibility in other contexts, while the bond between reliability and performance is the fulcrum of the simulation. The robustness of the approach is intended to gather evidence suitable for other types of systems, extending the modelling towards dimensions referred to social aspects, as well as natural hazards, once the proper dimensions for performance investigations have been defined. For example, the probability of failure defining the techno-centric dimension of this research, should be substituted by the functional variability of performance, or the frequency linked to certain events (e.g. natural hazards), and the associated expected loss of performance.

Enlarging the scope in this direction, it would be possible to extend the study of plant resilience in a way that allows understanding where to invest corporate profits in order to continuously improve processes and avoid production stops. In particular, developing what-if scenarios, the simulation model allows to change any of the parameters and check the respective effects. Such actions are tightly linked with the decision-maker perspective, supporting systematic explorative analysis for return of investments. In practical terms, the simulation model might be updated, adding or removing system states, as well as modifying recovery options and parameters in order to deal with the needs of the system at hand.

Nevertheless, the proposed approach has some limitations. Firstly, the linearity of the proposed model is considered a viable solution to obtain simple yet credible descriptions of the system's properties. However, it might be not fully representative of a complex large-scale system's needs. In those cases, it could be assumed as a first approximation, referring to more detailed approach for non-linear behaviors. Furthermore, no degradation for ageing is considered, as well as component inter-dependence. The former limitation could be ascribed in future work making explicit usage of the coefficient C_{Ab}, while the latter requires more advanced system modelling. Again, it is worth mentioning that the techno-centric perspective adopted in this study does not necessarily require human and organizational aspects to be explicitly modelled. However, this could be a relevant added value when considering restorative capacities that require a human intervention (e.g. maintenance operations), or in general, socio-technical operations. On the other hand, when considering large-scale technical system, it could be of interest to include as well a societal dimension of analysis [37], to understand the criticality of some failures or external disruption, which could include both natural hazards [38], [39], as well as cyber threats [40]. This way the proposed approach could be used as a basis to ensure its applicability towards socio-technical systems, as prescribed by resilience engineering [41]. Emphasizing the benefits of simulated approaches for modern and future socio-technical systems, the implementation of such aspects is left to future research.

References

[1] B. M. Ayyub, “Systems resilience for multihazard environments: Definition, metrics, and valuation for decision making,” *Risk Anal.*, vol. 34, no. 2, pp. 340–355, 2014.

[2] M. Bruneau *et al.*, “A Framework to Quantitatively Assess and Enhance the Seismic Resilience of Communities,” *Earthq. Spectra*, vol. 19, no. 4, pp. 733–752, 2003.

[3] S. Dekker, “Resilience engineering: Chronicling the emergence of confused consensus,” in *Resilience Engineering: Concepts and Precepts*, E. Hollnagel, D. D. Woods, and N. Leveson, Eds. Ashgate Publishing, Ltd., 2006, pp. 77–94.

[4] C. S. Holling, “Resilience and Stability of Ecological Systems,” *Annual Review of Ecology and Systematics*, vol. 4, no. 1. pp. 1–23, 1973.

[5] B. M. Ayyub, “Practical Resilience Metrics for Planning, Design, and Decision Making,” *ASCE-ASME J. Risk Uncertain. Eng. Syst. Part A Civ. Eng.*, vol. 1, no. 3, p. 04015008, 2015.

[6] M. Ottens, M. Franssen, P. Kroes, and I. Van De Poel, “Modelling infrastructures as socio-technical systems,” *Int. J. Crit. Infrastructures*, vol. 2, no. 2–3, pp. 133–145, 2006.

[7] H. Cai, N. S. N. Lam, Y. Qiang, L. Zou, R. M. Correll, and V. Mihunov, “A synthesis of disaster resilience measurement methods and indices,” *Int. J. Disaster Risk Reduct.*, vol. 31, no. April, pp. 844–855, 2018.

[8] S. Hosseini, K. Barker, and J. E. Ramirez-Marquez, “A review of definitions and measures of system resilience,” *Reliab. Eng. Syst. Saf.*, vol. 145, pp. 47–61, 2016.

[9] C. W. Zobel, “Representing perceived tradeoffs in defining disaster resilience,” *Decis. Support Syst.*, vol. 50, no. 2, pp. 394–403, 2011.

[10] C. W. Zobel and L. Khansa, “Characterizing multi-event disaster resilience,” *Comput. Oper. Res.*, vol. 42, pp. 83–94, 2014.

[11] A. Rose, “Economic resilience to natural and man-made disasters: Multidisciplinary origins and contextual dimensions,” *Environ. Hazards*, vol. 7, no. 4, pp. 383–398, 2007.

[12] D. Henry and J. Emmanuel Ramirez-Marquez, “Generic metrics and quantitative approaches for system resilience as a function of time,” *Reliab. Eng. Syst. Saf.*, vol. 99, 2012.

[13] S. E. Chang and M. Shinozuka, “Measuring improvements in the disaster resilience of communities,” *Earthq. Spectra*, vol. 20, no. 3, pp. 739–755, 2004.

[14] K. Barker, J. E. Ramirez-Marquez, and C. M. Rocco, “Resilience-based network component importance measures,” *Reliab. Eng. Syst. Saf.*, vol. 117, 2013.

[15] S. A. Torabi, M. Baghersad, and S. A. Mansouri, “Resilient supplier selection and order allocation under operational and disruption risks,” *Transp. Res. Part E Logist. Transp. Rev.*, vol. 79, pp. 22–48, 2015.

[16] J. Gao, B. Barzel, and A.-L. Barabási, “Universal resilience patterns in complex networks,” *Nature*, vol. 530, no. 7590, pp. 307–312, 2016.

[17] M. Omer, A. Mostashari, and U. Lindemann, “Resilience Analysis of Soft Infrastructure Systems,” *Procedia Comput. Sci.*, vol. 28, pp. 565–574, 2014.

[18] P. Franchin and F. Cavalieri, “Probabilistic Assessment of Civil Infrastructure Resilience to Earthquakes,” *Comput. Civ. Infrastruct. Eng.*, vol. 30, no. 7, pp. 583–600, 2015.

[19] A. W. Righi, T. A. Saurin, and P. Wachs, “A systematic literature review of resilience engineering: Research areas and a research agenda proposal,” *Reliab. Eng. Syst. Saf.*, vol. 141, 2015.

[20] E. Hollnagel, *Safety-II in Practice*. Routledge, 2017.

[21] R. R. Tan, K. B. Aviso, M. A. B. Promentilla, F. D. B. Solis, K. D. S. Yu, and J. R. Santos, “A SHOCK ABSORPTION INDEX FOR INOPERABILITY INPUT–OUTPUT MODELS,” *Econ. Syst. Res.*, vol. 27, no. 1, pp. 43–59, 2015.

[22] B. Fahimnia and A. Jabbarzadeh, “Marrying supply chain sustainability and resilience: A match made in heaven,” *Transp. Res. Part E Logist. Transp. Rev.*, vol. 91, pp. 306–324, 2016.

[23] A. Rose and S.-Y. Liao, “Modeling regional economic resilience to disasters: A computable general equilibrium analysis of water service disruptions,” *J. Reg. Sci.*, vol. 45, no. 1, pp. 75–112, 2005.

[24] D. D. Woods, “Essential characteristics of resilience,” in *Resilience Engineering: Concepts and Precepts*, E. Hollnagel, D. D. Woods, and N. Leveson, Eds. Ashgate Publishing, Ltd., 2006, pp. 21–34.

[25] R. Yarveisy, C. Gao, and F. Khan, “A Simple yet Robust Resilience Assessment Metrics,” *Reliab. Eng. Syst. Saf.*, vol. 197, no. 106810, 2020.

[26] R. Francis and B. Bekera, “A metric and frameworks for resilience analysis of engineered and infrastructure systems,” *Reliab. Eng. Syst. Saf.*, vol. 121, pp. 90–103, 2014.

[27] O. Ladipo, G. Reichard, A. McCoy, A. Pearce, P. Knox, and M. Flint, “Attributes and metrics for comparative quantification of disaster resilience across diverse performance mandates and standards of building,” *J. Build. Eng.*, vol. 21, no. November 2018, pp. 446–454, 2019.

[28] S. Zhao, X. Liu, and Y. Zhuo, “Hybrid Hidden Markov Models for resilience metrics in a dynamic infrastructure system,” *Reliab. Eng. Syst. Saf.*, vol. 164, no. February, pp. 84–97, 2017.

[29] E. Vugrin, A. Castillo, and C. Silva-Monroy, “Resilience metrics for the electric power system: A performance-based approach,” Albuquerque, NM, United States, 2017.

[30] L. Peruzzi, F. Salata, A. De Lieto Vollaro, and R. De Lieto Vollaro, “The reliability of technological systems with high energy efficiency in residential buildings,” *Energy Build.*, vol. 68, no. PARTA, pp. 19–24, 2014.

[31] S. B. Gershwin, *Manufacturing Systems Engineering*. MIT Press, 2002.

[32] H. Su, J. Zhang, E. Zio, N. Yang, X. Li, and Z. Zhang, “An integrated systemic method for supply reliability assessment of natural gas pipeline networks,” *Appl. Energy*, vol. 209, no. May 2017, pp. 489–501, 2018.

[33] M. Nasir, W. M. W. Muhamad, and R. A. R. Maarof, “Reliability based redundancy assessment of a cogeneration plant,” *Pertanika J. Sci. Technol.*, vol. 27, no. 1, pp. 225–246,

2019.

[34] F. Mulubrhan, A. A. Mokhtar, and M. Muhammad, "Integrating reliability analysis in life cycle cost estimation of heat exchanger and pump," *Adv. Mater. Res.*, vol. 903, pp. 408–413, 2014.

[35] J. E. van Zyl, O. Piller, and Y. le Gat, "Sizing municipal storage tanks based on reliability criteria," *J. Water Resour. Plan. Manag.*, vol. 134, no. 6, pp. 548–555, 2008.

[36] C. Wang, L. Xing, and J. Weng, "A new combinatorial model for deterministic competing failure analysis," *Qual. Reliab. Eng. Int.*, vol. 36, no. 5, pp. 1475–1493, 2020.

[37] G. P. Cimellaro, C. Renschler, A. M. Reinhorn, and L. Arendt, "PEOPLES: A Framework for Evaluating Resilience," *J. Struct. Eng.*, vol. 142, no. 10, p. 04016063, 2016.

[38] A. Misuri, G. Landucci, and V. Cozzani, "Assessment of safety barrier performance in Natech scenarios," *Reliab. Eng. Syst. Saf.*, vol. 193, 2020.

[39] A. C. Caputo, B. Kalemi, F. Paolacci, and D. Corritore, "Computing resilience of process plants under Na-Tech events: Methodology and application to sesmic loading scenarios," *Reliab. Eng. Syst. Saf.*, vol. 195, 2020.

[40] C.-L. Zhang, G.-H. Yang, and A.-Y. Lu, "Resilient observer-based control for cyber-physical systems under denial-of-service attacks," *Inf. Sci. (Ny).*, vol. 545, pp. 102–117, 2021.

[41] R. Patriarca, J. Bergström, G. Di Gravio, and F. Costantino, "Resilience engineering: Current status of the research and future challenges," *Saf. Sci.*, vol. 102, pp. 79–100, 2018.

Printed and proofed version available here:
http://www.sciencedirect.com/science/article/pii/S0951832021000351

Appendix – List of system states

System States	Natural Gas Mains	Cogenerator 1	Cogenerator 2	Heat Exchange	Pump 1	Pump 2	Pump 3	Pump 4	Pump 5	Thermal Storage 1	Thermal Storage 2	Thermal Storage 3	SYSTEM PERFORMANCE
1	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	0.0
2	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	1.0
3	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	1.0
4	✓	✗	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	0.0
5	✓	!	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	0.5
6	✓	✓	!	✓	✓	✓	✓	✓	✓	✓	✓	✓	0.5
7	✓	!	!	✓	✓	✓	✓	✓	✓	✓	✓	✓	0.0
8	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓	0.0
9	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	1.0
10	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	1.0
11	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	1.0
12	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	1.0
13	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	1.0
14	✓	✓	✓	✓	✗	✗	✓	✓	✓	✓	✓	✓	0.0
15	✓	✓	✓	✓	✗	✓	✗	✓	✓	✓	✓	✓	0.0
16	✓	✓	✓	✓	✗	✓	✓	✗	✓	✓	✓	✓	0.0
17	✓	✓	✓	✓	✗	✓	✓	✓	✗	✓	✓	✓	0.0
18	✓	✓	✓	✓	✓	✗	✗	✓	✓	✓	✓	✓	0.0
19	✓	✓	✓	✓	✓	✗	✓	✗	✓	✓	✓	✓	0.0
20	✓	✓	✓	✓	✓	✗	✓	✓	✗	✓	✓	✓	0.0
21	✓	✓	✓	✓	✓	✓	✗	✗	✓	✓	✓	✓	0.0
22	✓	✓	✓	✓	✓	✓	✗	✓	✗	✓	✓	✓	0.0
23	✓	✓	✓	✓	✓	✓	✓	✗	✗	✓	✓	✓	0.0
24	✓	✓	✓	✓	!	✓	✓	✓	✓	✓	✓	✓	0.8
25	✓	✓	✓	✓	✓	!	✓	✓	✓	✓	✓	✓	0.8
26	✓	✓	✓	✓	✓	✓	!	✓	✓	✓	✓	✓	0.8
27	✓	✓	✓	✓	✓	✓	✓	!	✓	✓	✓	✓	0.8
28	✓	✓	✓	✓	✓	✓	✓	✓	!	✓	✓	✓	0.8
29	✓	✓	✓	✓	!	!	✓	✓	✓	✓	✓	✓	0.0
30	✓	✓	✓	✓	!	✓	!	✓	✓	✓	✓	✓	0.0
31	✓	✓	✓	✓	!	✓	✓	!	✓	✓	✓	✓	0.0
32	✓	✓	✓	✓	!	✓	✓	✓	!	✓	✓	✓	0.0
33	✓	✓	✓	✓	✓	!	!	✓	✓	✓	✓	✓	0.0
34	✓	✓	✓	✓	✓	!	✓	!	✓	✓	✓	✓	0.0
35	✓	✓	✓	✓	✓	!	✓	✓	!	✓	✓	✓	0.0
36	✓	✓	✓	✓	✓	✓	!	!	✓	✓	✓	✓	0.0
37	✓	✓	✓	✓	✓	✓	!	✓	!	✓	✓	✓	0.0
38	✓	✓	✓	✓	✓	✓	✓	!	!	✓	✓	✓	0.0
39	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	1.0
40	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	1.0
41	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	1.0
42	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✗	✓	0.0
43	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	✗	0.0
44	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✗	0.0
45	✓	✓	✓	✓	✓	✓	✓	✓	✓	!	✓	✓	0.7
46	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	!	✓	0.7
47	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	!	0.7
48	✓	✓	✓	✓	✓	✓	✓	✓	✓	!	!	✓	0.0
49	✓	✓	✓	✓	✓	✓	✓	✓	✓	!	✓	!	0.0
50	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	!	!	0.0
51	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	1.0

Figure 9. List of system states being considered in the analysis and respective system performance levels: each component may be in a functioning state (green icon), degraded state (yellow icon), or failed state (red icon).