A Framework for the Resilience Analysis of Electric Infrastructure Systems Including Temporary Generation Systems

Shahaboddin Sean H. Toroghi[1], Valerie M. Thomas[2]

1- School of Building Construction, and School of computer science, Georgia Institute of Technology, Toroghi@Gatech.edu

2- School of Industrial and Systems Engineering, and School of Public Policy, Georgia Institute of Technology

Abstract

A quantitative framework is developed to assess the resilience of an electric infrastructure system, including the contributions of temporary service systems. The framework incorporates five dimensions of resilience – robustness, resourcefulness, redundancy, rapidity, and readjust-ability – under various setups for supplementary generation. It differentiates and prioritizes affected end-users. Notional examples illustrate the framework. The formula-based framework demonstrates the resilience contribution of temporary distributed generation (DG) technologies, and shows how differentiating among affected end-users supports the assessment of system resilience.

Keywords – resilience system; end-user prioritization; decentralized electricity generator; distributed; back-up.

1. Introduction

Recent natural disasters have shown the need for stable energy service, particularly for modern economies such as the United States [1]. The U.S. electric infrastructure system contains more than 6,413 power plants providing service through approximately six million miles of high-voltage transmission lines extending across the United States and serving 300 million customers [2,3]. The energy infrastructure system supports the other critical infrastructures; if energy service is disrupted, other critical infrastructures, including transportation, food, and water, are affected [4]. Between 2003 and 2012, severe weather caused 679 power outages nationwide with annual costs between $18 billion and $33 billion [5]. Cyber attack is also a rising threat to the electric infrastructure system [6].

The concept of resilience addresses system failures with a focus on failure prevention and recovery efforts. Resilience engineering (RE) is a paradigm for system safety that focuses on providing the capacity to proactively manage an incident, while continuously monitoring system performance [7]. The degree of system safety can change continuously over time [8]. Furthermore, the RE views the safety of a system as a characteristic of how the system performs with a focus on the whole system, rather than its individual components [9]. As RE has developed over time, its focus is now on overall system performance, rather than on properties of system components [10,11]. The view of resilience in a system has shifted from maintaining or regaining a stable state to the ability of a system to sustain its required operation, with continuous adaptation and adjustment of its function prior, during, and following an incident [12]. To do so, a metric system is needed for the system manager to evaluate the resilience capacity of a system, and to compare among available options. From the perspective of a variety of disciplines, the aggregated properties of a resilient infrastructure design includes one or more of the following abilities: the ability to anticipate, to absorb changes, to resist, to adapt, to recover (quickly), to reduce the chance of failure, to provide minimum service while under stress, to provide minimum service during changes in the service level, and to sustain a shock [13–16]. Developing a resilient infrastructure system with a desirable level of preparedness requires a metric system that quantifies its ability to react to stresses that challenge its performance.

Resilience metrics enable system designers and strategy developers to evaluate and compare the resilience capability of a system through monitoring the performance level at different points in time, pre- and post-incident. Bruneau et al. offered a broad definition of resilience covering actions that reduce losses from an incident, including the effects of mitigation and recovery [17]. Then they proposed a deterministic static metric that measures the loss of service performance in the case of hazardous incidents (i.e., earthquake) [18]. Henry and Ramirez-Marquez present a time-dependent resilience metric that defines resilience as the ratio of the performance recovery over the total loss due to a disruptive incident [18]. Cimellaro et al. proposed a resilience metric based on quality of service with a weighting factor that represents the importance of pre- and post-incident service qualities and control time [19].

While proposed metrics focus on the primary system as the service provider, there are often ancillary systems that provide service after an incident and during the recovery process. Emergency electricity generators, which in this paper hereafter are called distributed generation (DG) systems, act as temporary energy-generation systems and substitute for grid electricity. Beyond conventional emergency diesel generators, the emergence of decentralized renewable electricity generating systems, such as rooftop photovoltaic systems, provide an alternative for grid electricity [20,21]. The recent diffusion of electric vehicles provides an additional option for emergency source of electricity to a building or grid s[22]. These temporary services have not been counted in previous resilience metric systems [23].

Previous resilience metrics focus on overall system performance ([17,18,24–26]). In practice, the electrical infrastructure system operator may recognize that critical end-users, such as hospitals, transportation fuel-distribution systems, or financial hub systems have needs and resilience requirements that differ from those of routine end-users, such as residential sectors. Generalizing affected end-users into a single category limits the evaluation of resilience to an overall average.

Here we develop a resilience assessment framework for electric infrastructure systems, capable of comparing different generation technology setups, and differentiating among users affected by an incident. Doing so enables us to include the resilience contribution of temporary electricity generators, and to evaluate the resilience of a system customized for its end-user categories. The framework separately evaluates five dimensions of resilience [13,17,27]: robustness, redundancy, resourcefulness, rapidity, and readjust-ability. The remainder of the paper is organized as follows: Section 2 explains the concept of resilience and the proposed formulations for a resilience assessment, which we use to define the framework in section 3. Section 4 illustrates the use of our framework via two notional examples. Section 5 compares the results of the framework with a previously proposed metric and discusses resilience assessment with regard to end-users.

2. Methodological Background: State of Knowledge Pertaining to Resilience Assessment Models and Measurements

The core resilience objective of systems is to withstand turbulence and rapidly return to a near pre-incident service level [13,14,26,28]. The term *resilience* was first proposed to describe the dynamic capability of an ecological system to remain in equilibrium under stress [29]. *Resilience* is defined as the ability of a system to resist, absorb, and adapt to disruptions and return to normal functionalities [13], and resilience of the electric infrastructure system is a part of the broader domain of engineered system resilience [30]. System resilience can be addressed from a range of perspectives, including socio-ecological resilience [31], organizational resilience) [32], and in the context of the broader psychological and management aspects of system resilience [33]. This article focuses on providing a quantitative framework for an infrastructure system. Youn et al. defined engineering resilience as the sum of reliability (i.e., the passive survival rate) and restoration (i.e., the proactive survival rate) capacity. Bruneau et al. expressed four dimensions of resilience for an infrastructure system [17]: 1- robustness (the ability of a system to prevent the dissemination of damage during a hazardous incident), 2- rapidity (the speed of a system to return to its original state), 3- resourcefulness (the capability of a system to respond to a hazardous incident and mobilize needed resources/services), and 4- redundancy (the ability of a system to provide service using other resources in case of an incident). Later, the authors proposed a deterministic static metric for the resilience that examines loss of the community service in the case of a hazardous incident (e.g., earthquake) [16].

Henry and Ramirez-Marquez developed a time dependent metric that quantifies resilience as the ratio of system performance to its performance loss [18]. They also proposed three main system states: 1-steady state (before an incident occurs), 2-disrupted state (after the disruptive incident occurs until the system reaches a new steady state), and 3-stable recovered state. Their proposed resilience metric does not differentiate the end-user and incident types. Cimellaro et al. proposed a resilience metric based on the quality of service with a weighting factor that represents the importance of pre- and post-incident service qualities and control time [34]. Francis and Bekera based their dynamic measurement metric on three resilience capacities: 1-capacity of a system to absorb the impact, 2-the ability of a system to adjust to an undesirable situation by adapting, and 3-the speed of recovery for [25].

While the above resilience assessment methods are useful, they fall short in some areas. One is the exclusion of emergency electricity generators capable of providing temporary service to end-users. Another is the limited evaluation of the capability of a system to adapt, which we name readjust-ability. Third is the limited categorization of end-users. To address these factors, we present a quantitative resilience framework tailored to an electric infrastructure system with temporary electricity generators and a range of end-user types.

3. Proposed Framework

Our framework starts with the resilience concepts and frameworks discussed earlier and extends them to address vulnerability differences across end-users and the impacts of incident types on system performance. The time dimension, emphasized in previous frameworks and the DHS protection plan, is an important factor in evaluating resilience in the proposed model [1,35].

We divide end-users into three categories (*priority, urgent, and routine*). In Figure 1, the three performance-time charts represent the performance levels for each end-user category. Performance level is defined as the percentage of end-users who have access to the service. The DG systems provide service during normal system operation or may provide service only after an incident and during the recovery process. We denote the electricity provided by DG systems as F_{DG} in Figure 1.

Performance-level, the y-axis in Figure 1, is defined as the fraction of electricity demand delivered to the customers. Henry and Ramirez-Marquez suggested dividing the performance-time chart into multiple time segments, to enhance the expression of the resilience and recovery process [18]. We divide the timeframe into two main phases: pre- and post-incident. An *incident* is an event that causes damage to a system and the service level drops from the pre-incident performance level (F_s) to a lower disrupted level (F_d). Unlike previous models, our model has an additional input value, representing the service provided by DG systems (F_{DG}) after the incident. Because the DG systems maintain a minimum post-incident service level (F_{DG}), the affected elements can still function to some level, even when the primary system is down. We express the post-incident recovery process with respect to each end-user group. In Figure 1, t_p, t_u, and t_r represent the incremental recovery durations for the *priority*, *urgent*, and *routine* demand groups, respectively.

3.1. Demand Types

We define *Routine* consumption as all electricity demand not recognized as critical infrastructure according to Presidential Policy Directive 21 [36]; this consists mainly of residential demand. Within critical infrastructures, as defined by the U.S. Department of Homeland and Security [37], we define *Priority* sectors as end-users that require continuous access to electricity to avoid a major loss of life or economic impacts, for instance to prevent a nuclear meltdown or to operate medical equipment (Table 1).

We define the *Urgent* sectors as those that require electric power to operate and avoid major loss of life or economic impact, but they can tolerate interruptions or intermittent power. For instance, water services may be delivered for only a portion of the day without a significant loss of life while electricity infrastructure is in a recovery mode. Depending on the specific infrastructure system of a given location, the categorization may vary. For instance, in a financial hub, the financial services infrastructure may have a higher priority than the defense industrial base.

Table 1 – Demand-type categorization.

	System component		
	Priority	Urgent	Routine
Electricity Demand Sectors	Nuclear Reactors, Materials, and Waste Emergency Services Healthcare and Public Health Energy Defence Industrial Base Communications	Water and Wastewater Systems Transportation Systems Food and Agriculture Chemical Information Technology Government Facilities Commercial Facilities Critical Manufacturing Financial Services Dams	Residential Other

To reflect the consequence of an incident on each demand type, we separate the performance-time chart into three charts. The cumulative performance level of these three charts represents the system performance level. In Figure 1, the provided service for each user group is illustrated by F^{p}*: priority;* F^{u}*: urgent;* and F^{r}*: routine,* and the overall system performance level is the sum. Although these three charts represent pre- and post-incident performance in a general format, an incident may only impact one or two demand categories. An example of such a case is a targeted cyber-attack against the *urgent* demand category. Alternatively, an incident such as a natural disaster may have a similar negative impact on all demand categories. After an incident, and during the recovery process, a system may allocate all of its resources to one end-user category at each time-frame (i.e., first *urgent* category and then *priority* category), or the resources may be distributed among all three end-user types. The three key points in the performance-time chart (Figure 1) are:

F_{Start} (F_s) - the stable system performance level just before the incident,

$F_{Disrupted}$ (F_d) - the stable performance level immediately after the incident (disrupted), and

$\mathrm{F_{Finish}}$ $(\mathrm{F_F})$ - the performance level at the new stable level. The recovery reaches its final stage, and the system satisfies the required service.

For each end-user group, three control points F_1, F_2, and F_3 define when the recovery process completes for the first, second, and third end-user types, respectively. The presented order of the three control points ($F_1, F_2, and\ F_3$) illustrated in Figure 1 may differ by system or incident. After the Tōhoku earthquake and tsunami in Japan in 2011 the recovery process of the Daiichi nuclear power plant (priority category) took much longer than the other demand categories [38].

While in Figure 1, the system performance-levels (control points), are connected with lines to provide a visual aid, in a real-world scenario, system performance is not necessarily linear. This does not affect the computation of the resilience capacity, because in the proposed framework the values of system performance at each control point are required as the input variables. This approach is also employed in the previous studies discussed in the literature review section.

3.2. Resilience Metric

We apply the concept of resilience with four dimensions: *robustness, redundancy*, *resourcefulness,* and *rapidity* plus the adaptation capacity of the system to its new environment, post-incident, which we call the *readjust-ability* capacity. The performance levels and the associated time-stamps are the input variables for the resilience measurement formulas. Based on which demand category the DG systems serve, their capacity is divided into priority ($F^{(priority)}_{DG}$), urgent ($F^{(urgent)}_{DG}$), and routine ($F^{(routine)}_{DG}$).

Let R1 represent *robustness*, R2 *redundancy*, R3 *resourcefulness*, R4 *rapidity*, and R5 *readjust-ability*, we define the resilience (*R)* as the weighted average of these five resiliency dimensions (Equation (1)). The weights can provide system-specific requirements. If all resilience dimensions are equally important, the weighted average can be then simplified to an average of the five dimensions. All five resilience dimensions are unit-less and bound to zero. The upper bound of all five dimensions (robustness, resourcefulness, and rapidity) is 1.

The system *robustness* ($R1$), presented by Equation (2), is a characteristic of a system during the incident, and it defines how much a system can absorb turbulence and continue to deliver stable service. Throughout an incident, a robust system absorbs all the negative shocks and maintain an optimum service level, at which $F_s = F_d$ and $R1 = 1$. To formulate the *robustness* capacity of a system, we modified the sigmoid function – a monotonic function – to bound between 0 and 1.

Equation (3) defines the system *redundancy* capacity ($R2$) as the ratio of DG systems' capacity (temporarily resources) to the grid capacity (primary system during normal operation). The capacity of the DG system can range between zero and total consumption of end-users in each category. We also assume the service (electricity) provided by the DG system has the same characteristics as the primary service provided by the electric infrastructure system. This assumption is necessary to have a unitless value for R2, bounded between 0 and 1.

The third dimension of the resilience capacity, *resourcefulness* ($R3$), is computed based on how, during the recovery process, the system mobilizes its resources to serve the end-users' needed-service based on their priority category (end-user type) (Equation (4)). A resourceful system, through its recovery process, mobilizes all of its resources to restore the required services for the end-users at the highest priority category. The formulation defines the resource mobilization capability as the ability of the system to mobilize its resources for recovery according to the priority list. If end-users in the first category (*priority*) are not impacted by the mishap ($F^p_s = F^p_d$), $R3_1$should be excluded from the calculation of *resourcefulness* capacity. The same rule governs for the exclusion of R 3_2 in the case of the second category (*urgent*) does not experience a power outage ($F^u_s = F^u_d$). The upper boundary of the *resourcefulness* capacity ($R3 = 1$) represents a system that allocates its resources to recover the service for the end-users at the highest priority list. The lower bound of the *resourcefulness* capacity ($R3 = 0$) represents a system with poor resource allocation and inefficient service mobilization.

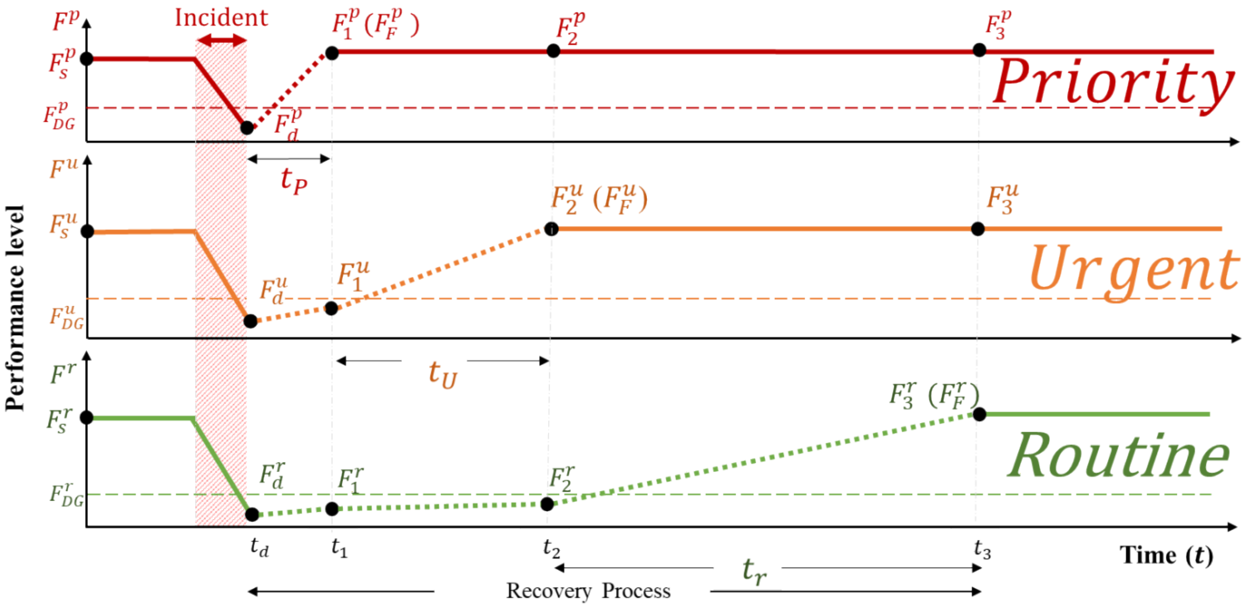


Figure 1 - Performance level over time: system, and demand types: priority, urgent, and routine.

$$\boldsymbol{Resilience(R)} = \boldsymbol{Weighted\ Avg}.\ [\ \mathbf{R1}, \mathbf{R2}, \mathbf{R3}, \mathbf{R4}\ ] \tag{1}$$

$$\boldsymbol{R1} = \ Weighted\ average \left(\frac{2}{1 + exp\left(\frac{F_s - F_d}{F_d}\right)} \right)_i \tag{2}$$

$$i = priority, urgent, routine$$

$$\boldsymbol{R2} = Weighted\ average \left(\frac{F_{DG}}{F_s}\right)_i \tag{3}$$

$$i = \ priority, urgent\ , routine$$

$$\boldsymbol{R3} = \ Weighted\ Avg.\ (R3_p, R3_u) \tag{4}$$

$$\boldsymbol{R4} = \ Weighted\ avg \left(\frac{1}{1 + exp\left(\frac{\Delta t_i - t_{\delta_i}}{ɣ}\right)} \right)_i \tag{5}$$

$$i = priority, urgent, routine$$

$$\boldsymbol{R5} = \ Weighted\ Avg. \left(\frac{F_F}{Fs}\right)_i \tag{6}$$

$$i = \ priority, urgent, routine$$

where

$$R3_p = \max\ [1 - \left(\frac{\Delta F_I^u + \Delta F_I^r}{\Delta F_I^p}\right), 0\ ]$$

$$R3_u = max\ [1 - \left(\frac{\Delta F_{II}^u}{\Delta F_{II}^r}\right), 0\ ]$$

$\Delta F_I^u = \ F_1^u - F_0^u$

$\Delta F_I^p = \ F_1^p - F_0^p$

$\Delta F_{II}^u = \ F_2^r - F_1^r$

$\Delta F_I^r = \ F_1^r - F_0^r$

$\Delta F_{II}^u = F_2^u - F_1^u$

$F_0^{(i)} = \ F_d^{(i)} + \ F_{DG}^{(i)}, \ \ i = p,u,r$

ɣ: $time\ scale\ factor,$

and

$$Constraints \begin{cases} F_{DG} = \sum_i F_{DG}^i \\ F_s = \sum_i F_s^i \end{cases}$$

$i = p, u, and\ r.$

Rapidity$(R4)$ evaluates how fast the system recovers. The formulation (Equation (5)), separately assesses the *rapidity* for each end-user category and computes the overall *rapidity* capacity of the system as their weighted average. The variable Δt_i represents the recovery time for each group of end-users. The clock for the recovery process starts immediately after the incident occurs. However, based on the prioritization of end-users by the system manager, the resources are allocating to each category of end-users. The recovery process finishes when for each end-user, the system reaches the system performance-level prior to the incident, for that group of users. We define slack time t_δ separately for each end-user type, as the maximum allowance time for a system to perform recovery process, without major consequence due to lack of the electricity power. The time scale ɣ defines how sensitive the end-users in each category are to power loss. We explain the effect of time-scale (ɣ) on the *rapidity* capacity in the sensitivity analysis section. The coefficient in the weighted average is defined based on the end-users in each category. Some factors to determine this weight coefficient are fatalities, financial loss, and negative environmental impacts. The upper bound of the *rapidity* capacity represents a well-prepared system with a rapid inflow of resources. Such a system has an instant recovery. A slower initial recovery shows that the system lacks optimal recovery actions, and if the recovery process takes twice the slack time or longer, the system does not have a *rapidity* capacity. An intense and widespread hazardous incident may delay the start of the recovery and create a shortage of support of recovery services. An example is the Nisqually Earthquake in the Olympia-Seattle area [39].

The last dimension of the resilience capacity, *readjust-ability* ($F5$), represents the capacity of a system to plan, prepare, and implement an adaptation plan after an incident occurs. The *readjust-ability* capacity shows the capability of the system to adapt in a situation in which it cannot absorb a stress, and is a complementary process to the mitigation [40].

3.3. Sensitivity analysis

To determine the impact of each variable in the proposed metric of the resilience in a system, we run a sensitivity analysis on our proposed metric. Immediately prior to the incident, the system performance is set to 100% as the reference point. Figure 2 illustrates a summary of the ranges of the first three capacity factors, with respect to change in input variables. Assuming prior to the incident the system has a non-zero performance level, a case of blackout represents no *robustness* capacity. At the upper bound, if the system can absorb the shock from an incident without deviating from its original performance level, the r*obustness* capacity is 100%. The proposed formulation does not suggest a one-to-one relation between proportion of power lost and *robustness.* This is aligned with the concept of resilience, that is to design a system with some level of resistance to a mishap but avoid over spending money and workforce to resist against any mishaps. At the upper bound, the system will penalize less if it fails to provide electricity to only a small fraction of end-users. At the lower boundary, in which the system provides service to a low number of end-users, the proposed formulation suggests the system has almost no *robustness* capacity.

The sensitivity assessment for *redundancy*, based on the assumption the electricity provided by the DG systems is a perfect substitute for grid electricity, is linear with a one-to-one relation of the sources of electricity. This model includes DG systems that generate reliable and steady electricity during the recovery process. This can be achieved by coupling PV systems with a storage system, or for diesel generators adequate fuel provided by reserve fuel tanks.

Resourcefulness is at its highest level (R3=1) when all the required resources for conducting the recovery process are allocated to end-users at the highest category. At the lower boundaries, a system allocates most of its resources for the recovery of its lower priorities end-users.

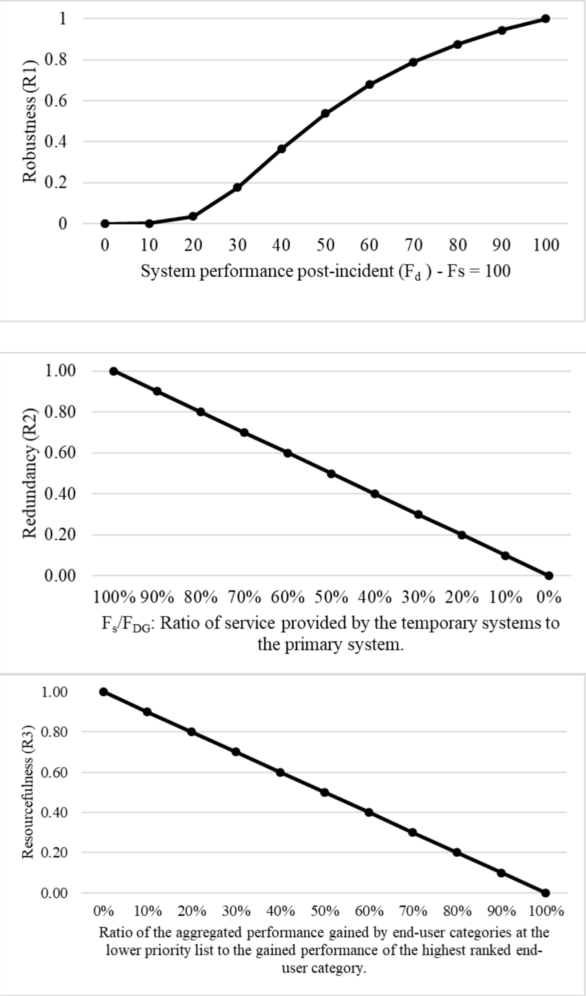


Figure 2 - Sensitivity analysis: robustness, resourcefulness, and redundancy.

Readjust-ability value depends on the ratio of performance-level after the recovery process finish to its value prior to a major incident. If the performance-level prior to an incident be at 100%, the maximum value of *Readjust-ability* capacity is 1, in which the recovery brings back the system to 100% level. In a special case, if the electric infrastructure system performs above 100% level at the end of the recovery process, defining a case in which either the recovery process consists of the repair of the existing system and expansion of service to new areas and end users, Readjust-ability capacity (R5) can reach a value higher than 1. However, in such a case the new system does not have the same characteristics, such as end-user types and population and service coverage, as the original system. To overcome this issue, any expansion of the system during a recovery process is excluded from the analysis, and the fifth dimension of the resilience (R5) is also bounded to one. However, the initial performance-level cannot be zero, meaning the grid prior to an incident should provide electricity to some end-users. Figure 3 illustrates how changes in performance-level after the recovery (F_F), affect the *Readjust-ability* capacity.

Finally, in Figure 4 the sensitivity analysis of the *rapidity* dimension shows if a system recovers immediately, it has the highest level of rapidity capacity (R4 = 1). While the slack time is defined as the allowable time to recover, the recovery process time equal to the slack time results in *rapidity* capacity equal to *50%.* This means if a recovery process takes as much time as the maximum allowable pre-defined allowable recovery duration, the R4=0.5, our system provides an average recovery capacity. If the recovery process lasts two times the slack time or longer, the system has low rapidity capacity.

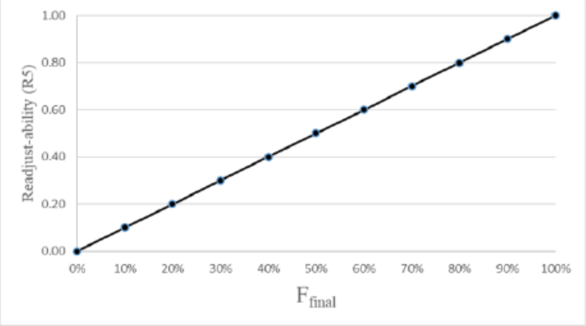
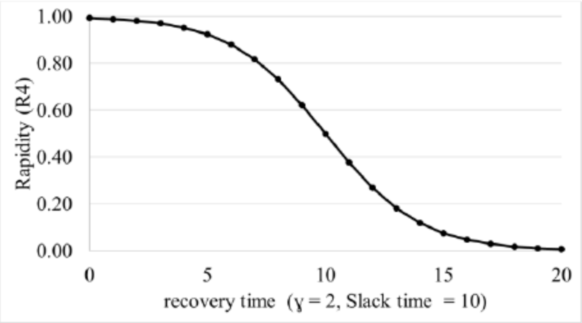


Figure 3 - Sensitivity analysis: readjust-ability.



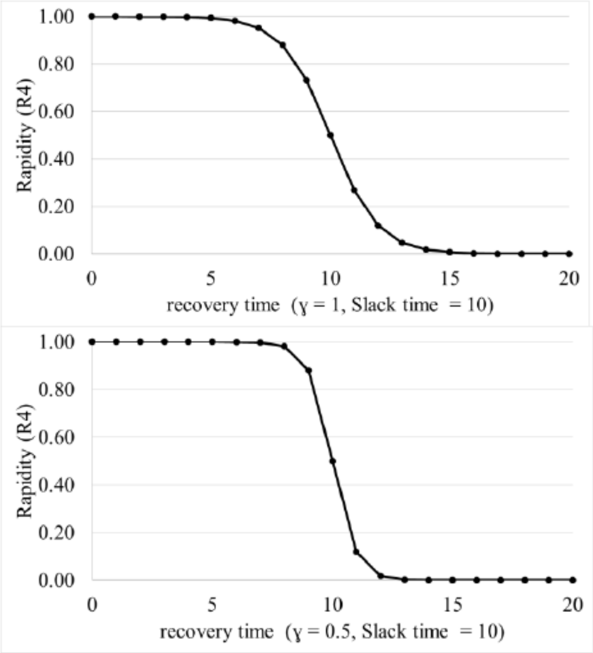


Figure 4 - Sensitivity analysis: rapidity.

The time scale, □, controls the slope of the sensitivity curve, and is defined based on the vulnerability of end-users to power outage. The scale factor provides an additional customization capability in the proposed formulation. It differentiates among different proportion of end-users in each category. Refer to section 3.1 (Demand types) each end-user category consists of a range of end-users. Considering two regions, each with equal total nominal electricity consumptions in the urgent category (Table 1). Assume in one region, a high proportion of consumption be allocated to the *food and agricultural industries*, such as rural areas dominated by agricultural industries, and in the other region a higher proportion of consumption be allocated to financial industries, such as a business district in an urban area. These two regions, despite having same total electricity consumption, differ in their sensitivity to the duration of power-loss (recovery duration). A lower scale factor (□=0.5) represents a system with end-users who are more vulnerable to power loss. In this scenario, if the recovery time exceeds the slack time, end-users are not able to tolerate and the rapidity capacity drops to zero. Scalar factor with higher values (□=2) represents a scenario, in which the end-users can tolerate a longer recovery duration, without financial or fatality consequences.

In all cases, the upper bound of the *Rapidity* dimension is bounded to one, expressing a system with immediate recovery. Such a system provides an instant recovery and brings the system performance-level back to the pre-incident level.

4. Notional examples

Through two notional examples, we demonstrate the proposed framework. The first notional example, the blackout example, shows how the framework captures the contribution of DG systems to improve the resilience capacity. The result is compared with a previously proposed metric system. The second notional example, targeted end-users example, illustrates how separating end-users by type enables more specific investigation of the resilience capacity of a system.

While these are fictional examples, the aftermath of recent hurricanes shows there exists a potential risk of blackout in large scale in the U.S.

Figure 5 illustrates hurricane Florence's path and the impacted areas, which caused a power outage for 890,000 customers in 2017 [41].

4.1. Blackout example

Table 2 illustrates three scenarios of the first example. The initial system performance level in all scenarios is set to 100%, which indicates the grid system provides electricity service to all end-users. Scenario *blackout* can be a representative of urban areas in the coastal line, which are directly impacted by hurricane Florence. Scenario *partial blackout* can demonstrate those areas with RADII 34 (Figure 5) in which power outage affects only a portion of end-users.

The first scenario (*Blackout*) in this example represents a complete interruption of power generation and distribution. There is no active DG system available in this scenario. While the second scenario also represents a power blackout, there are several DG systems that are spread equally across the end-user categories, which generate electricity with the accumulated generation equal to 30% of the total initial needed electricity. The third scenario represents a partial blackout, in which the grid system loses 70% of its performance level with no active DG systems. The recovery process in the two blackout scenarios is assumed to be similar. The recovery process in the partial blackout scenario, compared with the first two scenarios, takes 30% less time.

Table 2 – Notional blackout-example scenarios.

	Scenarios		
	I	II	III
	Blackout	Blackout + DG systems	Partial Blackout
Power loss	100%	100%	70%
DG systems*	0%	30%	0%
* capacity as the % of primary system capacity			

The remaining input variables are provided in the Appendix I. We assume the recovery process in the partial blackout is 20% faster than the complete blackout scenario. In this example, we make the following simplifying assumptions:

- In all three scenarios, the system after the recovery process returns to 100% performance-level.
- The weighted factors for all the computation are equal to 1.
- The capacity of DG systems is equal among the end-users.

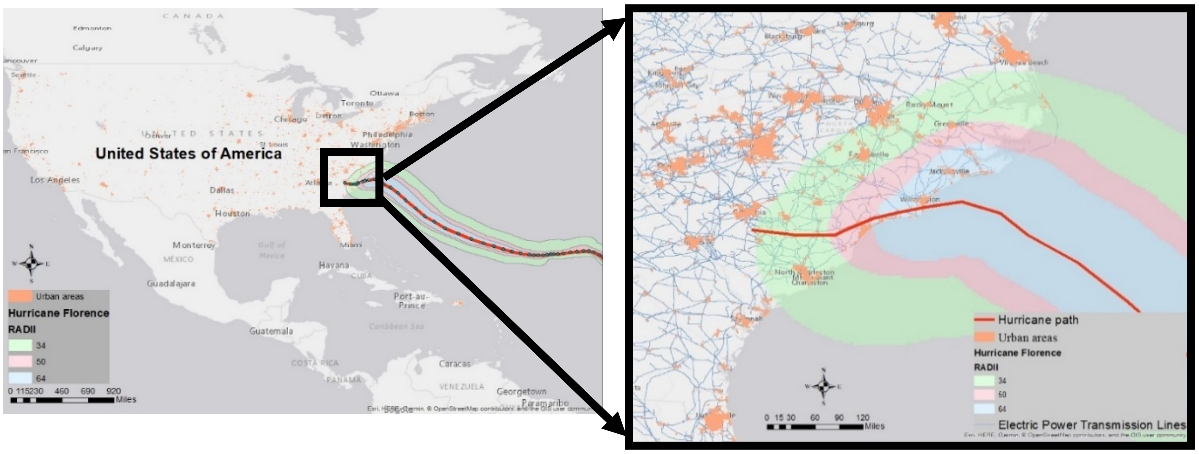
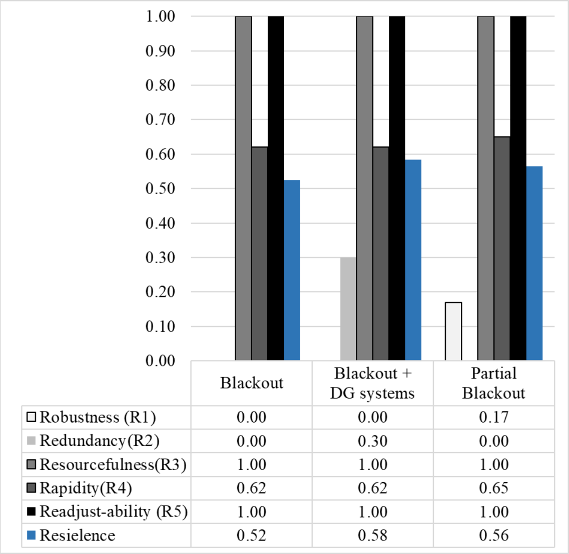


Figure 5 - Hurricane Florence and impacted areas.



	Blackout	Blackout + DG systems	Partial Blackout
□ Robustness (R1)	0.00	0.00	0.17
■ Redundancy(R2)	0.00	0.30	0.00
■ Resourcefulness(R3)	1.00	1.00	1.00
■ Rapidity(R4)	0.62	0.62	0.65
■ Readjust-ability (R5)	1.00	1.00	1.00
■ Resielence	0.52	0.58	0.56

Figure 6 – Results: blackout example.

We develop an application (Toolkit for Resilience Measurement: TIM) to facilitate the computation of the resilience and its dimensions (Appendix II). The TIM software was developed as an enhancement to the proposed metric system, and facilitate the computation of the resilience capacity of a system. This tool uses only the explained framework and formulation to generate the results. Employing the TIM, we compute the results for each scenario. Figure 6 illustrates the calculated resilience capacities. The blackout scenario shows the poorest resilience capacity, although the system shows some level of resiliency. This is due to a fast recovery process and ability to recover 100% and provide electricity to all end-users when the recovery process is complete.

The results of the second scenario show how the DG systems, by providing electricity up to 30% of the capacity of the grid, can improve resilience capacity by 10%. However, the DG systems only increase the *redundancy* dimension and have no effect on the other dimensions. Unlike the first two scenarios in which the system shows no Robustness capacity (blackout), the system under the third scenario (partial blackout) shows some level of Robustness. The resilience capacity of the system in the third scenario is slightly less than the second scenario; even though the system has some level of Robustness and recovers faster than the second scenario.

The fatality and cost impact of power failures adds another angle to the resilience assessment of a system. To address this, we introduce weight factors for each end-user groups and each resilience dimension. These weight factors can be calculated based on the results from a lifecycle cost analysis of both system components and consequences of a power outage.

A comparison between the method presented by Francis and Bekera (2014), and the method developed here is shown in Table 3. In the case of a blackout, even for a short time, the proposed metric provides informative results by computing the resilience dimensions (*Table 3*). In addition to presenting a metric to assess the resilience capacity of a system, Francis and Bekera propose a probabilistic approach to compute the probability of hurricane occurrence, which prior to computing the resilience dimensions can also be applied to the framework proposed in this study.

Table 3 – Results: comparison between metric frameworks.

	Resilience Capacity		
	Blackout	Blackout + DG systems	Partial Blackout
Proposed metric	100%	100%	70%
Francis and Bekera [25]	0%	30%	0%

4.2. Incident-based example

Not only should an electric infrastructure system be enhanced with a level of resilience against natural disasters, but also it needs to be resilient against focused incidents with high intensity and small effective range. The second notional example demonstrates how separating the end-users by type results in an informative assessment of resilience for a targeted incident. In this example, two scenarios are compared: 1- a targeted incident which impacts the priority end-user category with minimal damage to end-users in the other categories, and 2- scattered incidents which damage all types of end-users. In this example, we assume the share of end-user consumption out of total grid capacity is 20% for *priority*, 40% for *urgent* and 40% for *routine* categories.

Table 4 – Notional incident-based scenarios.

		Scenarios	
	Type	Targeted incident	Scattered incident
Power outage	Priority	100%	25%
	Urgent	12.5%	25%
	Routine	25%	50%
DG systems*	Priority%	50%	50%
	Urgent	50%	50%
	Routine	20%	20%
* capacity as the % of the consumption in each category			

In the *targeted* incident scenario, the incident causes complete power outage for the *priority* end-users, and the DG systems provide up to 50% of the required electricity to the end-users in this category. In this scenario, a small percentage of other end-users, mainly those adjacent to the incident, lose power. In the second scenario, *scattered* incidents, a partial power outage occurs for all customers. The DG systems have the same capacity in both scenarios. *Table 4* outlines the power outage DG systems' capacity for both scenarios.

While the power outage for each end-user category is not similar, the power outage of the grid system in both systems is equal to 35% (*Table 5*). If a framework only computes the resilience capacity based on the system performance level, the results for the *robustness* dimension will be equal for both scenarios.

Table 5 – System power outage: incident based example.

		Scenarios	
	Type	Targeted incident	Scattered incident
Consumption as a proportion of grid capacity	Priority%	20%	20%
	Urgent	40%	40%
	Routine	40%	40%
Power outage as a proportion of grid capacity	Priority%	20%	5%
	Urgent	5%	10%
	Routine	10%	20%
	Sum	**35%**	**35%**

To illustrate application of the framework, we make some assumptions for this example. In the *targeted* scenario, we assume the system will partially recover up to 90% in the *priority* category due to the high intensity of the incident. In case of a high intensity incident, inability to conduct the recovery in the contaminated areas may prevent the recovery process to bring the system performance-level back to its pre-incident level. We assume the recovery process for the other two categories, *urgent and routine*, starts at the same time as the *priority* category. Appendix II provides a detailed list of input variables for this example.

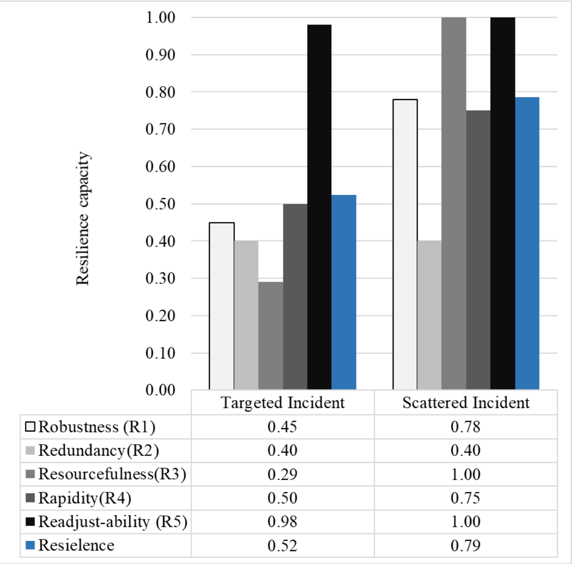
The *scattered* scenario represents a range of random incidents in which power outage spreads across all end-users. This scenario can represent a natural disaster such as Hurricane Maria. In 2017, Hurricane Maria caused the largest blackout in the U.S. history, leaving more than 1.5 million residents in Puerto Rico without power [42,43]. In this example, we applied weight factors, according to the end-user categories: priority = 3, urgent =2, and routine =1. In a real world scenario, the weight factors could be developed from of a life cycle cost analysis and risk assessment.

For consistency between the two scenarios, the recovery process time is calculated based on a similar rate of recovery per unit of time for each end-user type (*Table 6*). In the targeted-incident scenario, the recovery processes for all end-users start at a same time after the incident. The recovery process in the second scenario is a consecutive process based on the prioritization of end-users by type. The total recovery process time in the first scenario is 40 (units of time), because the recovery process is started at the same time, it is equal to the longest recovery process. The recovery process time in the second scenario is 30 (units of time), the sum the recovery processes for each end-user category. Appendix I presents the inputs in this scenario.

Table 6 – Recovery rate.

	End-user category		
	Priority	Urgent	Routine
Rate (unit of time per 1% recovery of grid capacity)	2	1	0.5
	Recovery time (unit of time)		
Targeted incident	40	5	5
Scattered incident	10	10	10

Employing the TIM, we compute the resilience capacities of the two scenarios. Figure 7 illustrates the results. The system under the scattered incident shows a higher resilience capacity. This is due to a combination of factors. The targeted-incident scenario has a lowest *robustness* capacity. The higher weight-factor for the *priority* end-users magnifies the importance of this category in the computation of resilience dimensions. Both scenarios have alike DG capacity, which results in equal *redundancy* capacity in both scenarios. The *resourcefulness* capacity in the targeted-incident scenario is much lower than the scattered-incident scenario, because the system allocate its resources to the recovery process of all end-users concurrently. In a real-world scenario, this may slow down the rate of recovery, which we ignored in this example. The lower *rapidity* capacity in the targeted-incident example is due to the higher recovery time for the *priority* end-users. The *readjust-ability* capacity in the targeted scenario is less than 1, because the system could not reach a 100% performance level at the end of the recovery process.



	Targeted Incident	Scattered Incident
□ Robustness (R1)	0.45	0.78
■ Redundancy(R2)	0.40	0.40
■ Resourcefulness(R3)	0.29	1.00
■ Rapidity(R4)	0.50	0.75
■ Readjust-ability (R5)	0.98	1.00
■ Resielence	0.52	0.79

Figure 7 - Results – incident-based example.

Employing the previously proposed metrics of resilience, the resilience capacity of both scenarios would have a similar result. This is because in both scenarios the system loses 35% of its capacity. Also, while the overall recovery time in the targeted-incident scenario is 30% higher than the scattered-incident scenario, the low slack-time minimizes the impact of this difference on the results of the *rapidity* capacity.

Employing the proposed framework provides insight into the resilience of the system. The low resilience score in the targeted-incident scenario may lead the decision makers to provide higher capacity dedicated emergency generators a for the *priority* end-users, in addition to an onside repair facility to boost the recovery process. Furthermore, a micro smart-grid system enhanced with damage detection features can improve the *rapidity* and *resourcefulness* capacities. In the *scattered-incident* scenario, the system shows a low redundancy capacity. The adoption of EVs and PV systems provides potential for increasing alternative electricity generation after the incident and during the recovery process.

5. Conclusion

The electric infrastructure system faces many natural and man-made threats. To maintain a stable flow of service, electric infrastructure must be resilient and able to reduce its vulnerability to hazardous incidents. This paper develops a quantitative method of examining the resilience capacity of an electric infrastructure system that includes ancillary service providers and different customer types. Through two examples, we show how the proposed framework evaluates the resilience capacity. The proposed framework allows policy makers and system designers to evaluate and improve the resilience capacity of an electric infrastructure system based on system specific characteristics.

Evaluation of the resilience capacity is one step toward improving resilience. Additional steps can evaluate how each component of the system can contribute to improving the resilience capacity. This study introduces new avenues to improve resilience capacity through the adoption of decentralized renewable technologies such as PV systems. Future work can consider extension of this approach to additional infrastructure systems, and to broader system contexts.. Furthermore, a complementary life-cycle analysis has a merit in the resilience engineering process, and expands the scope of the resilience assessment framework. From the management perspective, the first step of improving the resilience capacity of a system is to measure the current state of the system and define a goal for the desired resilience capacity according to the needs of stakeholders. The proposed framework provides a means to measure and evaluate the resilience capacity of a system at each point in time. Application experience and further studies can illustrate how the resilience goals can be defined, and propose actionable plans to achieve those goals.

Acknowledgements

This material is based upon work supported by the National Science Foundation under Grant No. 1441208.

References

[1] Chertoff M. National infrastructure protection plan. Dep Homel Secur (DHS), Washington, DC 2009:175.

[2] Spitzer A, Armstrong T, Lucas B. Transmission &amp; Distribution Infrastructure. 2014.

[3] ASCE. A Comprehensive Assessment of America’s Infrastructure. 2017.

[4] Roege PE, Collier ZA, Mancillas J, McDonagh JA, Linkov I. Metrics for energy resilience. Energy Policy 2014;72:249–56. doi:10.1016/j.enpol.2014.04.012.

[5] Office E, August P. Economic Benefits of Increasing Electric Grid Resilience To Weather Outages. Exec Off Pres 2013:1–28.

[6] Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector Mission Support Center Analysis Report. 2016.

[7] Patriarca R, Bergström J, Di Gravio G, Costantino F. Resilience engineering: Current status of the research and future challenges. Saf Sci 2018;102:79–100. doi:10.1016/j.ssci.2017.10.005.

[8] Carayon P, Hancock P, Leveson N, Noy I, Sznelwar L, van Hootegem G. Advancing a sociotechnical systems approach to workplace safety – developing the conceptual framework. Ergonomics 2015;58:548–64. doi:10.1080/00140139.2015.1015623.

[9] Bakx GCH, Nyce JM. Risk and safety in large-scale socio-technological (military) systems: a literature review. J Risk Res 2017;20:463–81. doi:10.1080/13669877.2015.1071867.

[10] Nemeth CP, Herrera I. Building change: Resilience Engineering after ten years. Reliab Eng Syst Saf 2015;141:1–4. doi:10.1016/j.ress.2015.04.006.

[11] Woods DD. Four concepts for resilience and the implications for the future of resilience engineering. Reliab Eng Syst Saf 2015;141:5–9. doi:10.1016/j.ress.2015.03.018.

[12] Hollnagel E, Woods DD, Leveson N. Resilience engineering : concepts and precepts. Ashgate; 2006.

[13] Faturechi R, Miller-Hooks E. Measuring the Performance of Transportation Infrastructure Systems in Disasters: A Comprehensive Review. J Infrastruct Syst 2015;21:04014025. doi:10.1061/(ASCE)IS.1943-555X.0000212.

[14] Hosseini S, Barker K, Ramirez-Marquez JE. A review of definitions and measures of system resilience. Reliab Eng Syst Saf 2016;145:47–61. doi:10.1016/j.ress.2015.08.006.

[15] Robbins J, Krishnan K, Allspaw J, Limoncelli TA. Resilience Engineering: Learning to Embrace Failure. Queue 2012;10:20. doi:10.1145/2367376.2371297.

[16] Yang Y. Power Line Sensor Networks for Enhancing Power Line Reliability and Utilization. 2011.

[17] Bruneau M, Chang SE, Eguchi RT, Lee GC, O'Rourke TD, Reinhorn AM, et al. A Framework to Quantitatively Assess and Enhance the Seismic Resilience of Communities. Earthq Spectra 2003;19:733–52. doi:10.1193/1.1623497.

[18] Henry D, Emmanuel Ramirez-Marquez J. Generic metrics and quantitative approaches for system resilience as a function of time. Reliab Eng Syst Saf 2012;99:114–22. doi:10.1016/j.ress.2011.09.002.

[19] Cimellaro G, Villa O, Bruneau M. Resilience-Based Design of Natural gas distribution networks. J Infrastruct Syst 2014;21:1–14. doi:10.1061/(ASCE)IS.1943-555X.0000204.

[20] Enhancing the Resilience of the Nation's Electricity System. Washington, D.C.: National Academies Press; 2017. doi:10.17226/24836.

[21] Hart D, Birson K. Deployment of Solar Photovoltaic Generation Capacity in the United States. 2016.

[22] USA DOE. Enhancing Grid Resilience with Integrated Storage from Electric Vehicles, Recommendations for the U.S 2018:1–13.

[23] Berkeley Iii AR, Wallace M. A Framework for Establishing Critical Infrastructure Resilience Goals: Final Report and Recommendations. Final Rep Recomm by Counc 2010:1–73.

[24] Cimellaro GP, Reinhorn AM, Bruneau M. Framework for analytical quantification of disaster resilience. Eng Struct 2010;32:3639–49. doi:10.1016/j.engstruct.2010.08.008.

[25] Francis R, Bekera B. A metric and frameworks for resilience analysis of engineered and infrastructure systems. Reliab Eng Syst Saf 2014;121:90–103. doi:10.1016/j.ress.2013.07.004.

[26] Molyneaux L, Wagner L, Froome C, Foster J. Resilience and electricity systems: A comparitive analysis. Energy Policy 2012;47:188–201.

[27] Atkinson G, Dietz S, Neumayer E. Handbook of sustainable development. Edward Elgar; 2007.

[28] Yodo N, Wang P. Resilience Modeling and

Quantification for Engineered Systems Using Bayesian Networks. J Mech Des 2016;138:031404. doi:10.1115/1.4032399.

[29] Holling CS. Resilience and Stability of Ecological System. AnnuRevEcolSyst 1973;4:1–23. doi:10.1146/annurev.es.04.110173.000245.

[30] Youn BD, Hu C, Wang P. Resilience-Driven System Design of Complex Engineered Systems. J Mech Des 2011;133:101011. doi:10.1115/1.4004981.

[31] Meerow S, Newell JP, Stults M. Defining urban resilience: A review. Landsc Urban Plan 2016;147:38–49. doi:10.1016/j.landurbplan.2015.11.011.

[32] EXECUTIVE SUMMARY Organizational Resilience A summary of academic evidence, business insights and new thinking by BSI and Cranfield School of Management 2 ORGANIZATIONAL RESILIENCE | BSI AND CRANFIELD SCHOOL OF MANAGEMENT ORGANIZATIONAL RESILIENCE | BSI AND CRANFIELD SCHOOL OF MANAGEMENT 3. n.d.

[33] Gaitanidou E, Tsami M, Bekiaris E. ScienceDirect. Transp Res Procedia 2017;24:26–7. doi:10.1016/j.trpro.2017.05.113.

[34] Cimellaro GP, Reinhorn AM, Bruneau M. Seismic resilience of a hospital system. Struct Infrastruct Eng 2010;6:127–44. doi:10.1080/15732470802663847.

[35] Department of Energy. Energy Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan 2010.

[36] Security Committee I. Presidential Policy Directive 21 Implementation: An Interagency Security Committee White Paper. 2015.

[37] Department of Homeland Security U. Critical Infrastructure Resilience, Final Report and Recomendations. 2009. doi:59972.000117 EMF_US 28318682v2.

[38] Dunbar P, McCullough H, Mungov G, Varner J, Stroker K. 2011 Tohoku earthquake and tsunami data available from the National Oceanic and Atmospheric Administration/National Geophysical Data Center. Geomatics, Nat Hazards Risk 2011;2:305–23. doi:10.1080/19475705.2011.632443.

[39] Kafali C, Grigoriu M, California SEA of. Rehabilitation Decision Analysis Toolbox. Structural Engineers Association of California,; 2005.

[40] Rose A. Economic resilience to natural and man-made disasters: Multidisciplinary origins and contextual dimensions. Environ Hazards 2007;7:383–98. doi:10.1016/j.envhaz.2007.10.001.

[41] Hurricane Florence: Power outages top 890,000, could reach 3 million n.d. https://www.usatoday.com/story/news/nation/2018/09/14/hurricane-florence-power-outages/1301060002/ (accessed April 10, 2019).

[42] Puerto Rico power: Why the blackout is the largest in US history - Vox n.d. https://www.vox.com/2018/2/8/16986408/puerto-rico-blackout-power-hurricane (accessed April 10, 2019).

[43] Puerto Rico power restored 11 months after Hurricane Maria - Vox n.d. https://www.vox.com/identities/2018/8/15/17692414/puerto-rico-power-electricity-restored-hurricane-maria (accessed April 10, 2019).

Appendix I

Input variables: blackout example

The following table represent the input variables for the first example.

Description	End-user type	Variables	Scenario		
			Blackout	Blackout+ DG systems	Partial Blackout
Performance level pre-incident	priority	F_s^p	100%	100%	100%
	urgent	F_s^u	100%	100%	100%
	routine	F_s^r	100%	100%	100%
Capacity of DG systems as a percentage of the F_s		F_{DG}	0	30%	0
Performance level after incident before the recovery process	priority	F_d^p	0	0	30%
	urgent	F_d^u	0	0	30%
	routine	F_d^r	0	0	30%
Performance level after the recovery process	priority	F_F^p	100%	100%	100%
	urgent	F_F^u	100%	100%	100%
	routine	F_F^r	100%	100%	100%
Time scale factor		□	1	1	1
Slack time	priority	Δt_I	8	8	8
	urgent	Δt_{II}	24	24	24
	routine	Δt_{III}	120	120	120
Recovery duration	priority	Δt_I	6	6	4.8
	urgent	Δt_{II}	18	18	14.4
	routine	Δt_{III}	168	168	134.4

Input variables: incident-based example

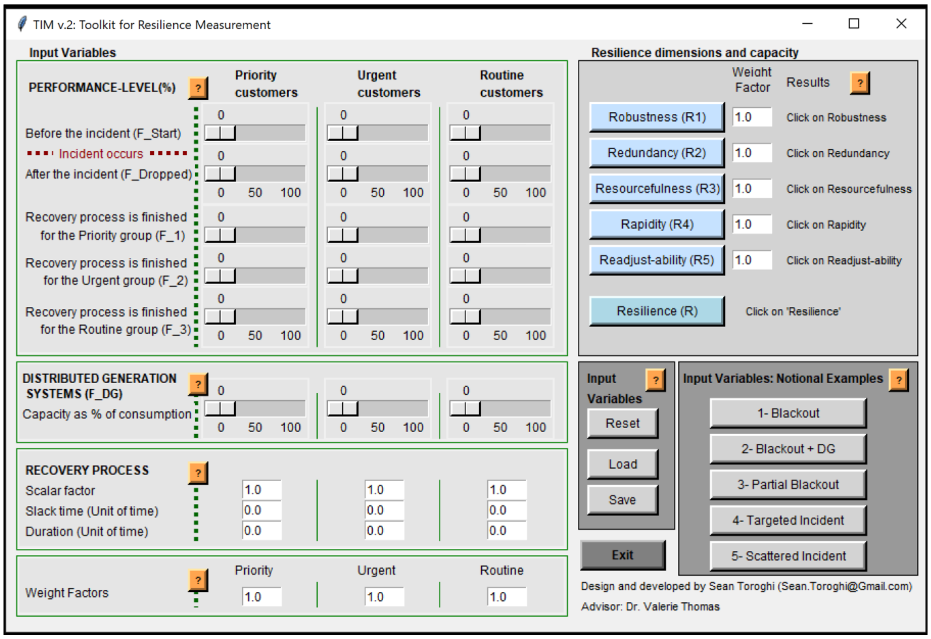
The following table represent the input variables for the second example.

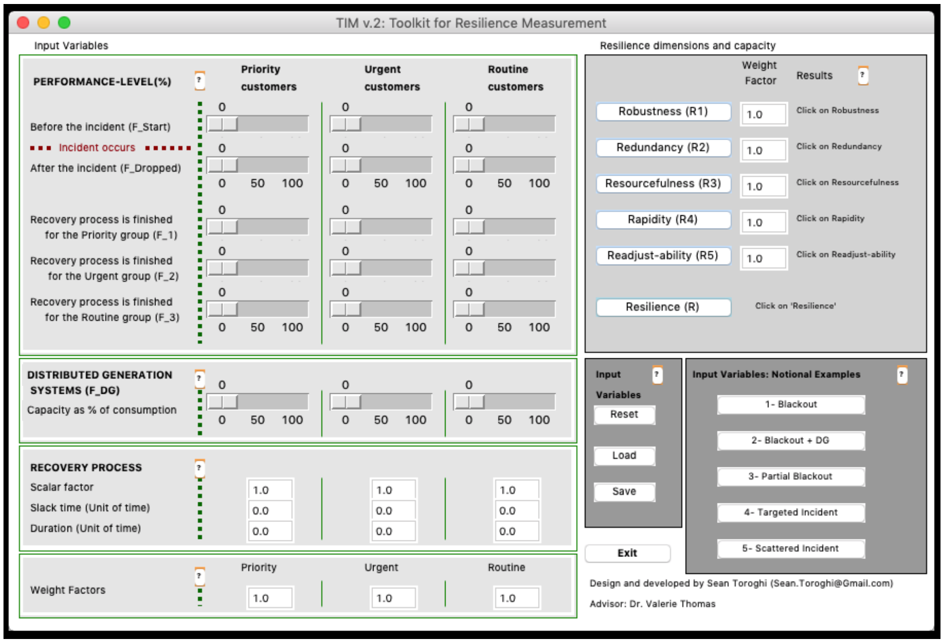
Description	End-user type	Variables	Scenarios	
			Targeted incident	Scattered incident
Performance level pre-incident	priority	F_s^p	100%	100%
	urgent	F_s^u	100%	100%
	routine	F_s^r	100%	100%
Capacity of DG systems as a percentage of the F_s	priority	F_{DG}^p	50%	50%
	urgent	F_{DG}^u	50%	50%
	routine	F_{DG}^r	20%	20%
Performance level after incident before the recovery process	priority	F_d^p	0%	75%
	urgent	F_d^u	87.5%	75%
	routine	F_d^r	75%	50%
Performance level after the recovery process	priority	F_F^p	90%	100%
	urgent	F_F^u	100%	100%
	routine	F_F^r	100%	100%
Time scale factor		□	2	2
Slack time	priority	$t_{\delta I}$	10	10
	urgent	$t_{\delta II}$	24	24
	routine	$t_{\delta III}$	48	48
Recovery duration	priority	Δt_I	40	10
	urgent	Δt_{II}	5	10
	routine	Δt_{III}	5	10

Appendix II – TIM application

To facilitate the computation of resilience, we developed the TIM (Toolkit for Resilience Measurement) application. The proposed framework requires computation of five dimensions of resilience for a system with 35 inputs. The TIM application only employs the proposed formulation to compute the resilience capacity. A detailed explanation of each formula and input variables are presented in section 3. TIM is a stand-alone executable application that is developed in two versions for Windows and MacIintosh operating systems. Both versions shares a similar user interface (Figure II- 1).

To run TIM, there is no need to pre-install any other application. Users can enter all required input variables into the TIM and get the results. TIM computes the resilience capacity of the system as well as the fiv resilience dimensions. TIM is divided into three sections: input variables, results, and Other features. This appendix provides a brief manual for using the TIM to compute the resilience dimensios and capacity. Readers can access TIM via the Github depository at www.github.com/Sean-Toroghi/TIM.




TIM v.2: Toolkit for Resilience Measurement
Input Variables
PERFORMANCE-LEVEL(%)
?
Priority customers
Urgent customers
Routine customers
Before the incident (F_Start)
Incident occurs
After the incident (F_Dropped)
Recovery process is finished for the Priority group (F_1)
Recovery process is finished for the Urgent group (F_2)
Recovery process is finished for the Routine group (F_3)
0
0 50 100
DISTRIBUTED GENERATION SYSTEMS (F_DG)
Capacity as % of consumption
RECOVERY PROCESS
Weight Factors
Priority
Urgent
Routine
Resilience dimensions and capacity
Weight Factor
Results
Click on Robustness
Click on Redundancy
Click on Resourcefulness
Click on Rapidity
Click on Readjust-ability
Click on 'Resilience'
Input Variables
Reset
Load
Save
Input Variables: Notional Examples
1- Blackout
2- Blackout + DG
3- Partial Blackout
4- Targeted Incident
5- Scattered Incident
Exit

	Priority	Urgent	Routine
Scalar factor	1.0	1.0	1.0
Slack time (Unit of time)	0.0	0.0	0.0
Duration (Unit of time)	0.0	0.0	0.0
Weight Factors	1.0	1.0	1.0

	Weight Factor
Robustness (R1)	1.0
Redundancy (R2)	1.0
Resourcefulness (R3)	1.0
Rapidity (R4)	1.0
Readjust-ability (R5)	1.0
Resilience (R)	

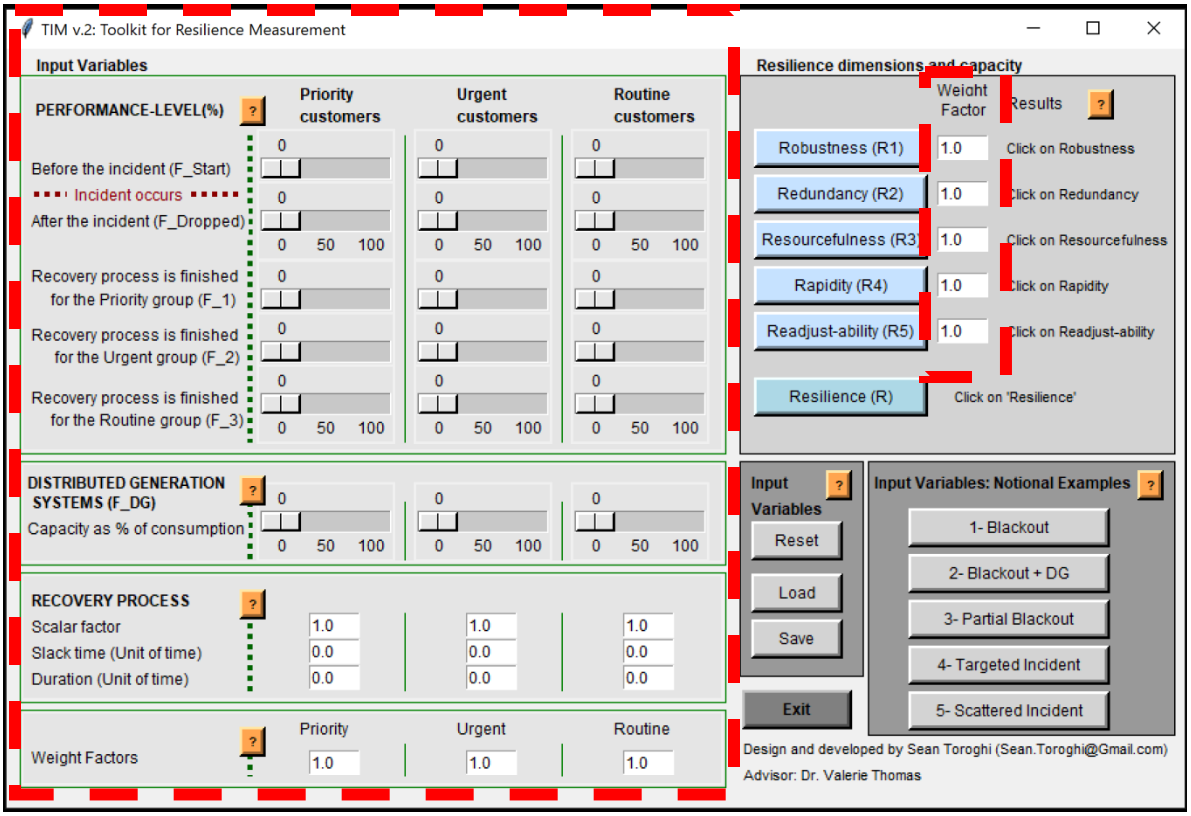
Design and developed by Sean Toroghi (Sean.Toroghi@Gmail.com)

Advisor: Dr. Valerie Thomas

Figure II- 1 - TIM user interface (Top: Windows Operation System, and Bottom: MacintoshOperation System).

In the input variables section, users can enter the information required for computing the resilience dimensions and capacity. Figure II- 2 illustrates the TIM interface with red dashed rectangles highlighting the input section. The system performance level contains five variables in three groups. The performance-level prior to an incident indicates the system performance level under normal operation conditions. The performance level after the incident indicates the system performance level immediately after the incident when it reaches a stable level. The recovery process has not yet started at this point. The three control points, (F_1, F_2, and F_3) represent the system performance level for each end-user type at the time the recovery process is finished for the priority, urgent, and routine categories, respectively. If there exist DG systems in the region under investigation, the users can enter the capacity of the DG systems as a percentage of consumption for each end-user category.

To compute the Rapidity capacity, users are required to enter the variables in the recovery process section. The unit of time for the three variables in this section (tim scale factor, slack time, and duration of the recovery process) should be consistent. Finally the weight factors for both the end-user types and resilience dimensions provides the capability for user to apply any prioritization according to the results of other complimentary analysis such as life-cycle cost analysis.



TIM v.2: Toolkit for Resilience Measurement

Input Variables

PERFORMANCE-LEVEL(%)	Priority customers	Urgent customers	Routine customers
Before the incident (F_Start)	0	0	0
After the incident (F_Dropped)	0	0	0
Recovery process is finished for the Priority group (F_1)	0	0	0
Recovery process is finished for the Urgent group (F_2)	0	0	0
Recovery process is finished for the Routine group (F_3)	0	0	0

DISTRIBUTED GENERATION SYSTEMS (F_DG)			
Capacity as % of consumption	0	0	0

RECOVERY PROCESS			
Scalar factor	1.0	1.0	1.0
Slack time (Unit of time)	0.0	0.0	0.0
Duration (Unit of time)	0.0	0.0	0.0

	Priority	Urgent	Routine
Weight Factors	1.0	1.0	1.0

Resilience dimensions and capacity

	Weight Factor	Results
Robustness (R1)	1.0	Click on Robustness
Redundancy (R2)	1.0	Click on Redundancy
Resourcefulness (R3)	1.0	Click on Resourcefulness
Rapidity (R4)	1.0	Click on Rapidity
Readjust-ability (R5)	1.0	Click on Readjust-ability
Resilience (R)		Click on 'Resilience'

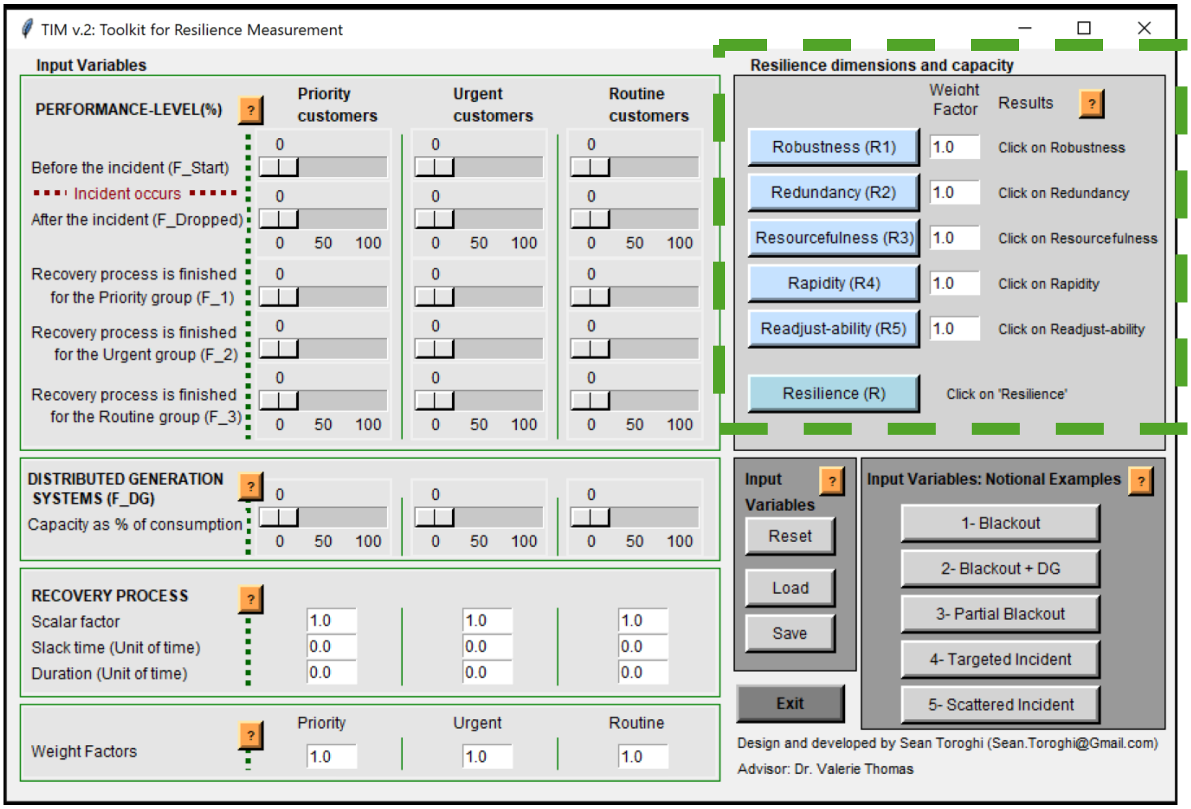
Design and developed by Sean Toroghi (Sean.Toroghi@Gmail.com)

Advisor: Dr. Valerie Thomas

Figure II- 2 – TIM application: input variables.

To compute the results, users need to click on the associated buttons in the resilience dimensions and capacity section, highlighted by the green dashed rectangle in Figure II- 3. The computation of results is based on the formulation presented in this paper. Five buttons are allocated to compute the five resilience dimensions, separately. The resilience (R) button computes the system resilience capacity and five resilience dimensions together.

The TIM application is enhanced with some other features to facilitate and aid users' interaction. Users can reset the input variables to default values by clicking on the reset button. Also at any point, users can save the input variables by clicking the save button and save the input data in the computer. The user can later retrieve the saved data by clicking on the load button. Also, the input data of the notional examples (the three scenarios of the first example and two scenarios of the second example) in this article are provided through the "input variable: notional examples" section, in which the user can click on any of the five buttons representing the associated scenario and the application will automatically change the input variable to the ones used for that particular scenario. Figure II- 5 through II-8 illustrate the input variables of the five scenarios. A brief description of each section is available to the users by clicking on the question mark orange buttons.



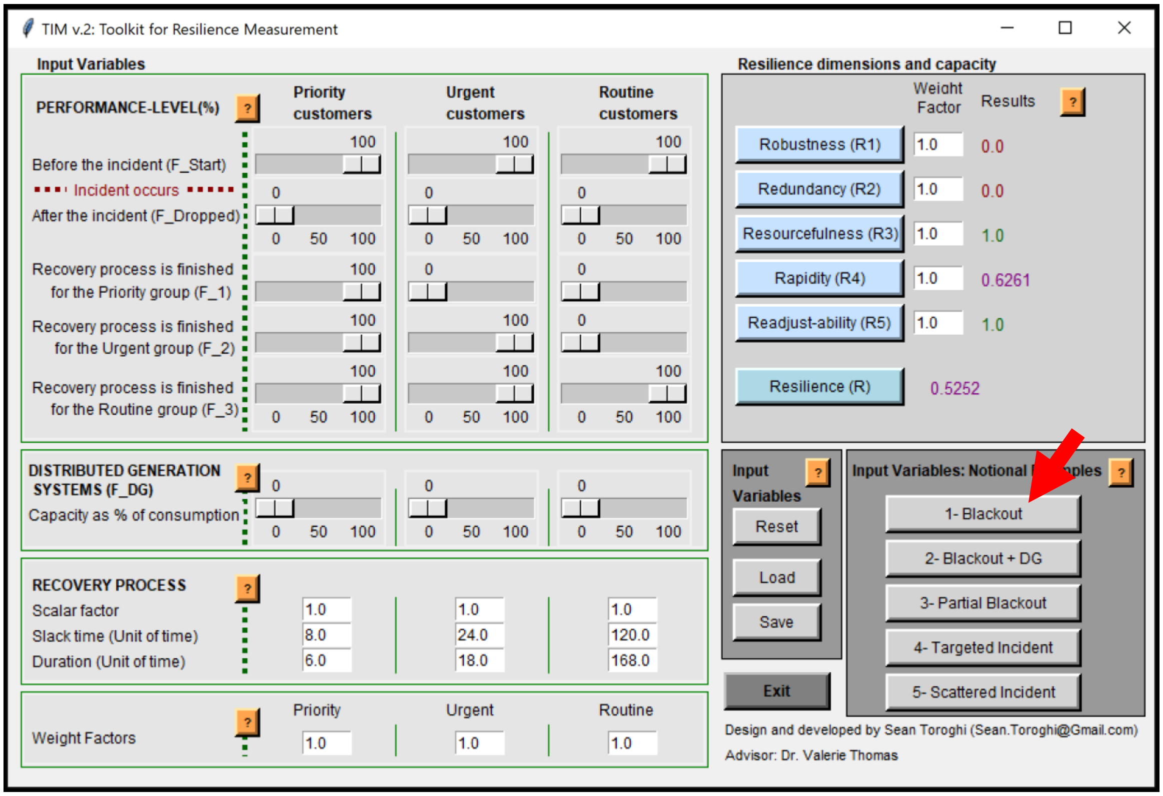
	Priority	Urgent	Routine
Scalar factor	1.0	1.0	1.0
Slack time (Unit of time)	0.0	0.0	0.0
Duration (Unit of time)	0.0	0.0	0.0
Weight Factors	1.0	1.0	1.0

Resilience dimension	Weight Factor
Robustness (R1)	1.0
Redundancy (R2)	1.0
Resourcefulness (R3)	1.0
Rapidity (R4)	1.0
Readjust-ability (R5)	1.0

Design and developed by Sean Toroghi (Sean.Toroghi@Gmail.com)

Advisor: Dr. Valerie Thomas

Figure II- 3 - TIMapplication: compute the results.

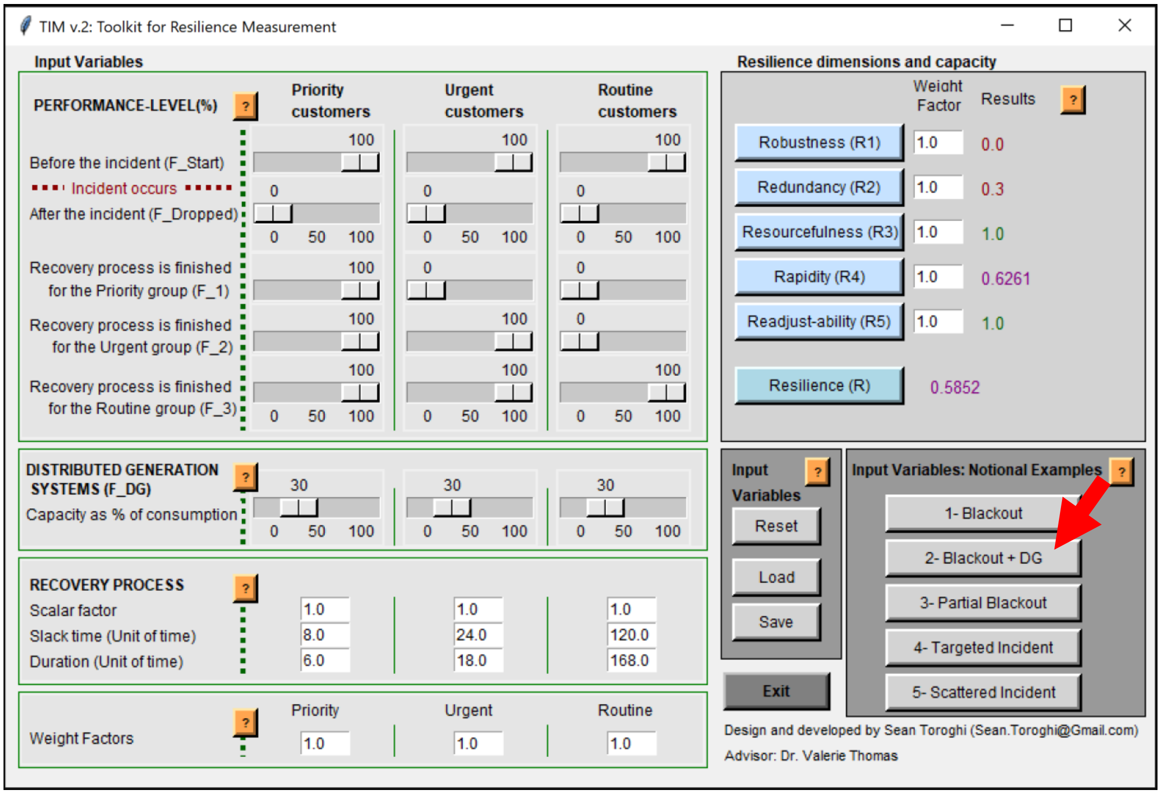


PERFORMANCE-LEVEL(%)	Priority customers	Urgent customers	Routine customers
Before the incident (F_Start)	100	100	100
Incident occurs			
After the incident (F_Dropped)	0	0	0
Recovery process is finished for the Priority group (F_1)	100	0	0
Recovery process is finished for the Urgent group (F_2)	100	100	0
Recovery process is finished for the Routine group (F_3)	100	100	100
DISTRIBUTED GENERATION SYSTEMS (F_DG) Capacity as % of consumption	0	0	0
RECOVERY PROCESS			
Scalar factor	1.0	1.0	1.0
Slack time (Unit of time)	8.0	24.0	120.0
Duration (Unit of time)	6.0	18.0	168.0
	Priority	Urgent	Routine
Weight Factors	1.0	1.0	1.0

	Weight Factor	Results
Robustness (R1)	1.0	0.0
Redundancy (R2)	1.0	0.0
Resourcefulness (R3)	1.0	1.0
Rapidity (R4)	1.0	0.6261
Readjust-ability (R5)	1.0	1.0
Resilience (R)		0.5252

Design and developed by Sean Toroghi (Sean.Toroghi@Gmail.com)
Advisor: Dr. Valerie Thomas

Figure II- 4 -TIM: input variables of the blackout scenario.

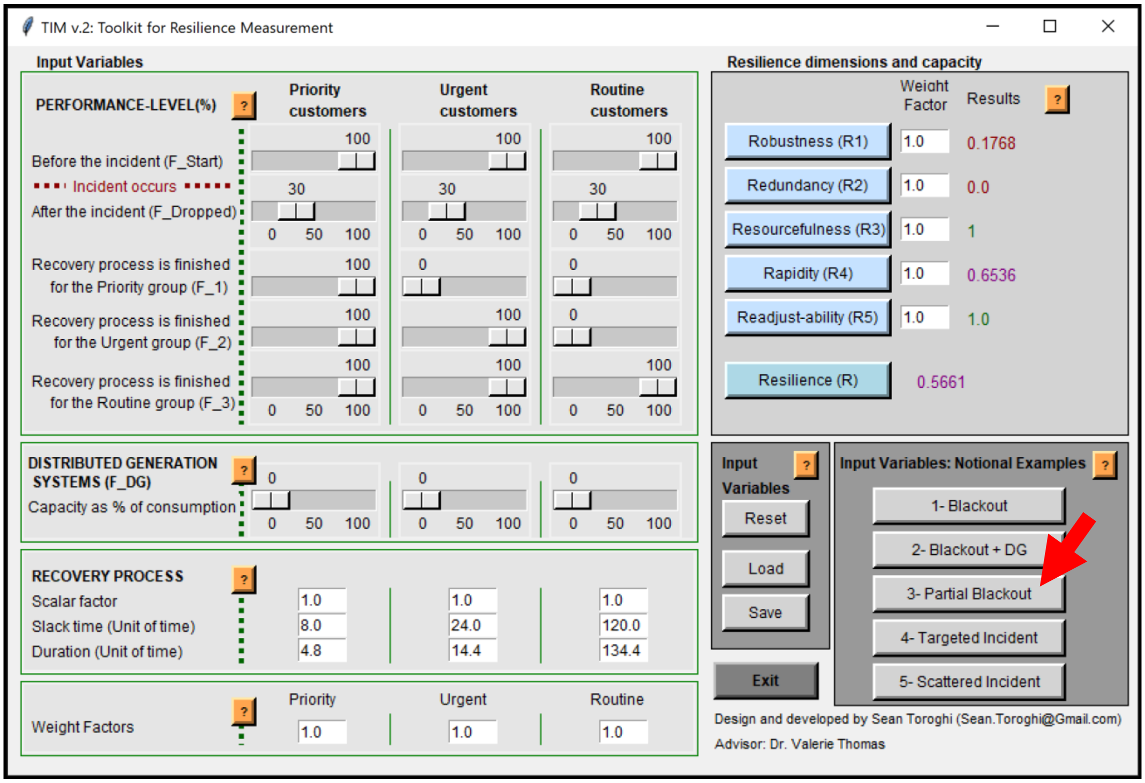


PERFORMANCE-LEVEL(%)	Priority customers	Urgent customers	Routine customers
Before the incident (F_Start)	100	100	100
Incident occurs			
After the incident (F_Dropped)	0	0	0
Recovery process is finished for the Priority group (F_1)	100	0	0
Recovery process is finished for the Urgent group (F_2)	100	100	0
Recovery process is finished for the Routine group (F_3)	100	100	100
DISTRIBUTED GENERATION SYSTEMS (F_DG) Capacity as % of consumption	30	30	30
RECOVERY PROCESS			
Scalar factor	1.0	1.0	1.0
Slack time (Unit of time)	8.0	24.0	120.0
Duration (Unit of time)	6.0	18.0	168.0
	Priority	Urgent	Routine
Weight Factors	1.0	1.0	1.0

	Weight Factor	Results
Robustness (R1)	1.0	0.0
Redundancy (R2)	1.0	0.3
Resourcefulness (R3)	1.0	1.0
Rapidity (R4)	1.0	0.6261
Readjust-ability (R5)	1.0	1.0
Resilience (R)		0.5852

Design and developed by Sean Toroghi (Sean.Toroghi@Gmail.com)
Advisor: Dr. Valerie Thomas

Figure II- 5 - TIM: input variables of the blackout plus DG scenario.



TIM v.2: Toolkit for Resilience Measurement

Input Variables

PERFORMANCE-LEVEL(%)	Priority customers	Urgent customers	Routine customers
Before the incident (F_Start)	100	100	100
After the incident (F_Dropped)	30	30	30
Recovery process is finished for the Priority group (F_1)	100	0	0
Recovery process is finished for the Urgent group (F_2)	100	100	0
Recovery process is finished for the Routine group (F_3)	100	100	100

DISTRIBUTED GENERATION SYSTEMS (F_DG)			
Capacity as % of consumption	0	0	0

RECOVERY PROCESS			
Scalar factor	1.0	1.0	1.0
Slack time (Unit of time)	8.0	24.0	120.0
Duration (Unit of time)	4.8	14.4	134.4

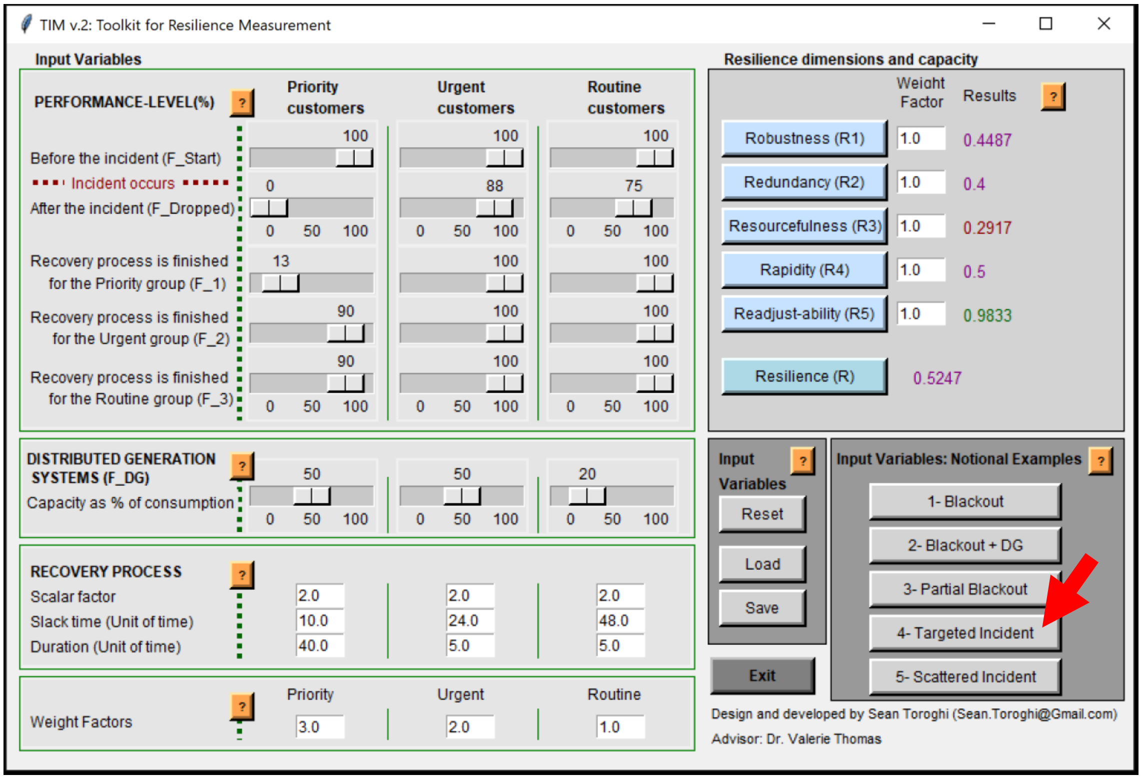
	Priority	Urgent	Routine
Weight Factors	1.0	1.0	1.0

Resilience dimensions and capacity

	Weight Factor	Results
Robustness (R1)	1.0	0.1768
Redundancy (R2)	1.0	0.0
Resourcefulness (R3)	1.0	1
Rapidity (R4)	1.0	0.6536
Readjust-ability (R5)	1.0	1.0
Resilience (R)		0.5661

Design and developed by Sean Toroghi (Sean.Toroghi@Gmail.com)
Advisor: Dr. Valerie Thomas

Figure II- 6 - TIM: input variables of the partial blackout scenario.



TIM v.2: Toolkit for Resilience Measurement

Input Variables

PERFORMANCE-LEVEL(%)	Priority customers	Urgent customers	Routine customers
Before the incident (F_Start)	100	100	100
After the incident (F_Dropped)	0	88	75
Recovery process is finished for the Priority group (F_1)	13	100	100
Recovery process is finished for the Urgent group (F_2)	90	100	100
Recovery process is finished for the Routine group (F_3)	90	100	100

DISTRIBUTED GENERATION SYSTEMS (F_DG)			
Capacity as % of consumption	50	50	20

RECOVERY PROCESS			
Scalar factor	2.0	2.0	2.0
Slack time (Unit of time)	10.0	24.0	48.0
Duration (Unit of time)	40.0	5.0	5.0

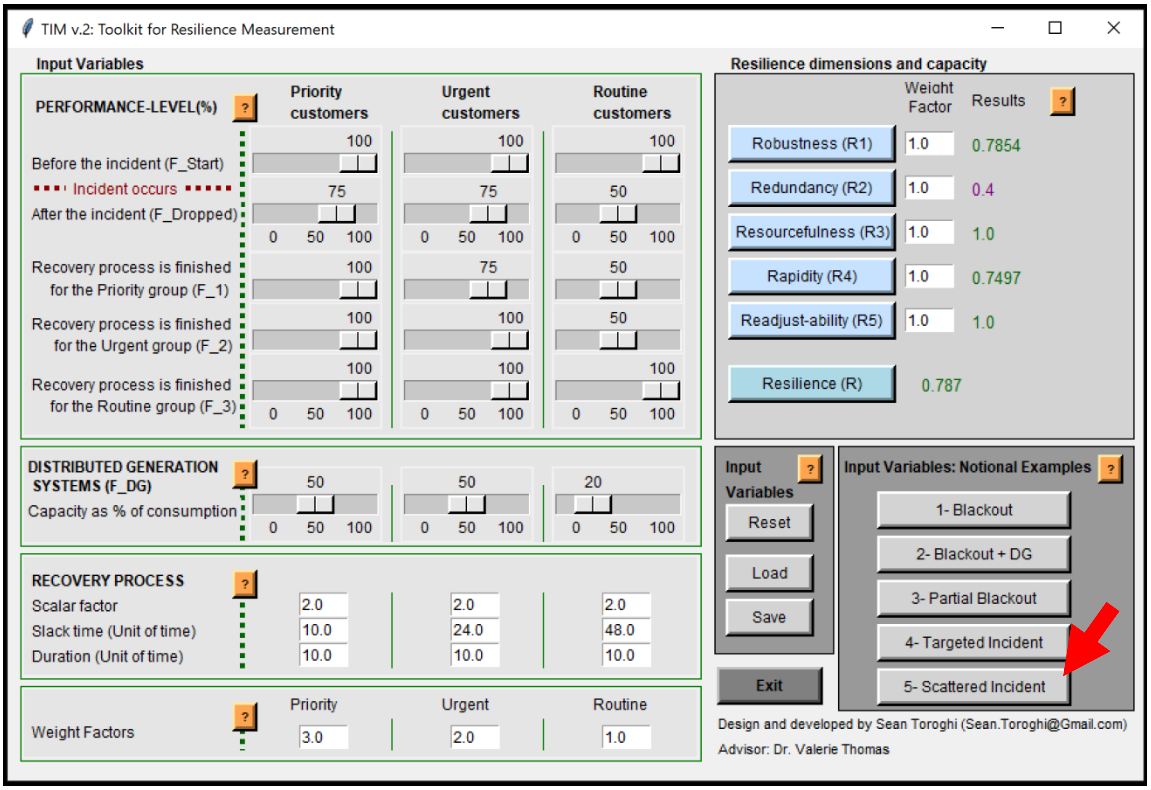
	Priority	Urgent	Routine
Weight Factors	3.0	2.0	1.0

Resilience dimensions and capacity

	Weight Factor	Results
Robustness (R1)	1.0	0.4487
Redundancy (R2)	1.0	0.4
Resourcefulness (R3)	1.0	0.2917
Rapidity (R4)	1.0	0.5
Readjust-ability (R5)	1.0	0.9833
Resilience (R)		0.5247

Design and developed by Sean Toroghi (Sean.Toroghi@Gmail.com)
Advisor: Dr. Valerie Thomas

Figure II- 7- TIM: input variables of the targeted incident scenario.



PERFORMANCE-LEVEL(%)	Priority customers	Urgent customers	Routine customers
Before the incident (F_Start)	100	100	100
After the incident (F_Dropped)	75	75	50
Recovery process is finished for the Priority group (F_1)	100	75	50
Recovery process is finished for the Urgent group (F_2)	100	100	50
Recovery process is finished for the Routine group (F_3)	100	100	100

DISTRIBUTED GENERATION SYSTEMS (F_DG)			
Capacity as % of consumption	50	50	20

RECOVERY PROCESS			
Scalar factor	2.0	2.0	2.0
Slack time (Unit of time)	10.0	24.0	48.0
Duration (Unit of time)	10.0	10.0	10.0

	Priority	Urgent	Routine
Weight Factors	3.0	2.0	1.0

	Weight Factor	Results
Robustness (R1)	1.0	0.7854
Redundancy (R2)	1.0	0.4
Resourcefulness (R3)	1.0	1.0
Rapidity (R4)	1.0	0.7497
Readjust-ability (R5)	1.0	1.0
Resilience (R)		0.787

Design and developed by Sean Toroghi (Sean.Toroghi@Gmail.com)
Advisor: Dr. Valerie Thomas

Figure II- 8 TIM: input variables of the scattered incident scenario.