Aging and Rejuvenation Models of Load Changing Attacks in Micro-Grids

Ricardo M. Czekster
School of Computing, Newcastle University
Newcastle upon Tyne, United Kingdom
ricardo.melo-czekster@ncl.ac.uk

Alberto Avritzer
eSulab Solutions
Princeton, New Jersey, USA
beto@esulabsolutions.com

Daniel Sadoc Menasché
Institute of Computing, UFRJ
Rio de Janeiro, Brazil
sadoc@dcc.ufrj.br

***Abstract*—Recent cyber-attacks in critical infrastructures have highlighted the importance of investigating how to improve Smart-Grids (SG) resiliency. In the future, it is envisioned that grid connected micro-grids would have the ability of operating in 'islanded mode' in the event of a grid-level failure. In this work, we propose a method for unfolding aging and rejuvenation models into their sequential counterparts to enable the computation of transient state probabilities in the proposed models. We have applied our methodology to one specific security attack scenario and four large campus micro-grids case studies. We have shown how to convert the software aging and rejuvenation, with cycles, to its unfolded counterpart. We then used the unfolded counterpart to support the survivability computation. We were able to analytically evaluate the transient failure probability and the associated Instantaneous Expected Energy Not Supplied metric, for each of the four case studies, from one specific attack. We envision several practical applications of the proposed methodology. First, because the micro-grid model is solved analytically, the approach can be used to support micro-grid engineering optimizations accounting for security intrusions. Second, micro-grid engineers could use the approach to detect security attacks by monitoring for unexpected deviations of the Energy Not Supplied metric.**

***Index Terms*—Cyber-security, survivability, aging and rejuvenation, Markovian processes.**

I. Introduction

Over the years, attacks to Smart-Grid power control components, such as, the Stuxnet worm [1], Black Energy 3 [2], Crashoverride [3], and Trisis [4], were able to significantly damage Industrial Control Systems (ICS) [5]. In the first quarter of 2021 the US' East Coast oil supply chain, provided by Colonial Pipeline, was the target of a serious attack. This ransomware attack caused service interruptions in several US states with significant impact to oil prices. To mitigate these problems, an alternative approach is to isolate ICT and power networks, and to design micro-grids [6], [7], which would retain the connection to the conventional power grid, but could also operate in islanded mode, when faulty conditions are detected. The expected benefit from using this architecture is the use of distributed micro-sources that can effectively sustain Demand Response (DR) mechanisms according to load demands. Managers segment these so-called "grid-connected micro-grids" into smaller independent units. One of the objectives of this segmentation is to mitigate the impact of single points of failure [8], [9].

We model Load Changing Attacks (LCA) in micro-grids using software aging and rejuvenation techniques [10]. We analyze the survivability of the grid-connected micro-grid in islanded mode. Survivability-related metrics capture the ability of a system to retain its operating features under duress, i.e., during failures or disturbances [11]–[13][1]. Here, we are interested in analyzing the effects of LCA and its mitigation to avoid the impact of cascading failures.

Our main contributions in this paper are as follows:

1. Aging and rejuvenation model for micro-grid attacks: we show that classic aging and rejuvenation models can be used to capture LCA attacks and to model its mitigation (Sections III and IV).

2. Bridging aging, rejuvenation with survivability models through unfolding: we unfold the considered aging and rejuvenation model, whose Markov chain contains cycles, into a survivability model, captured by a Directed Acyclic Graph (DAG). In the realm of micro-grids, this corresponds to allowing up to a finite fixed number of attack events before ultimately reaching the stable state (Section V).

3. Implementation of unfolding at PRISM: we show that a model implementation to evaluate the proposed Markov chain unfolding can be used to replicate elements over time, e.g., multiple attack trials towards a micro-grid and cyber-attack scenarios (Section VI and Appendix).

II. Related work

The US micro-grid initiative [14] document discussed grid modernization and listed ongoing projects in the US. The National Electric Sector Cybersecurity Organization Resource (NESCOR) conducted cyber-security assessment and grid failure scenarios for increase SG resilience [15] and Jauhar et al. (2015) proposed model-based techniques [16] for its study. One could use reported vulnerability incidents and detailed cyber-attack vectors using MITRE's ATT&CK framework[2], combining with databases provided by NVD[3] or CVE[4].

Dabrowski et al. (2017) [17] commented on "Grid-shock", i.e., the problem of synchronizing attacks to destabilize the

[1]As termed by the ANSI T1A1.2 committee.

[2]Adversarial Tactics, Techniques, and Common Knowledge framework: https://attack.mitre.org/

[3]National Vulnerability Database: https://nvd.nist.gov/.

[4]Common Vulnerabilities Exposures Database: https://cve.mitre.org/.

power grid. Soltan et al. (2018) [18] discussed BlackIoT where a swarm of malicious infected IoT could imbalance the power provision. The same authors have discussed attacks known as Manipulation of Demand (MAD) in smart infrastructure and their potential to harm the Smart Grid [19]. In contrast to that result, Huang et al. (2019) [20] have discussed that the grid is resilient enough to withstand a large magnitude power surge or drop due to the security contingencies that offers customers.

Micro-grids offer higher flexibility for power managers. However, since the same level of protections are not present, it makes the solution highly susceptible for cyber-attacks. Let us suppose, for instance, that even a small number of malicious software are present in high-wattage devices. Adversaries could remotely command those compromised devices to impair the micro-grid operation, imbalance the frequency out of nominal levels, and promote black-outs that could impact both the critical infrastructure, and the power utility customers.

Frequency control services are crucial for power managers to deliver reliable power [21]. Mana et al. (2020) [22] simulated a micro-grid and studied resiliency employing telecommunication over diesel generators and batteries. Czekster et al. (2021) [23] have surveyed power simulation to extract features for modelling the Smart-Grid whereas Arnaboldi et al. (2020) [24] applied Continuous Time Markov Chains (CTMC) to model LCA by analyzing the balance between Supply-Demand under normal and attack situations.

In our previous research [25]–[28], we have introduced Markov models with rewards to support survivability metrics. We have shown that these models could be efficiently applied for the optimization a Smart-Grid. To address the complexity of its distribution networks, the analytical model applied three key modelling principles: state space factorization, state aggregation, and initial state conditioning. We extend the approach introduced in [25]–[28] to model LCA in micro-grids.

III. Problem

A grid-connected micro-grid operates in two modes: i) connected; and ii) islanded. On the one hand, in *connected* mode, it powers the infrastructure and enjoys power quality (frequency and voltage regulation) provided by the grid. Another feature of this mode is to offer a series of security contingencies to customers, where secondary and tertiary power reserves are present to stabilize frequency as required (or load-shedding mechanisms that disconnect power in selected regions), according to Supply-Demand needs. Even if an elevated number of customers was to turn on or off their devices simultaneously, due to these protections in place, the grid would withstand these peak demands or the lack of power and adjust its mode accordingly.

Fig. 1 shows an overview of the main components under consideration. It encompasses *generic* elements, i.e., they could be a healthcare facility, or a power supplier. The "Households" element is abstracted and may represent a small neighborhood with particular energy profiles. It is worth noticing that power elements do not necessarily overlap with telecommunications.

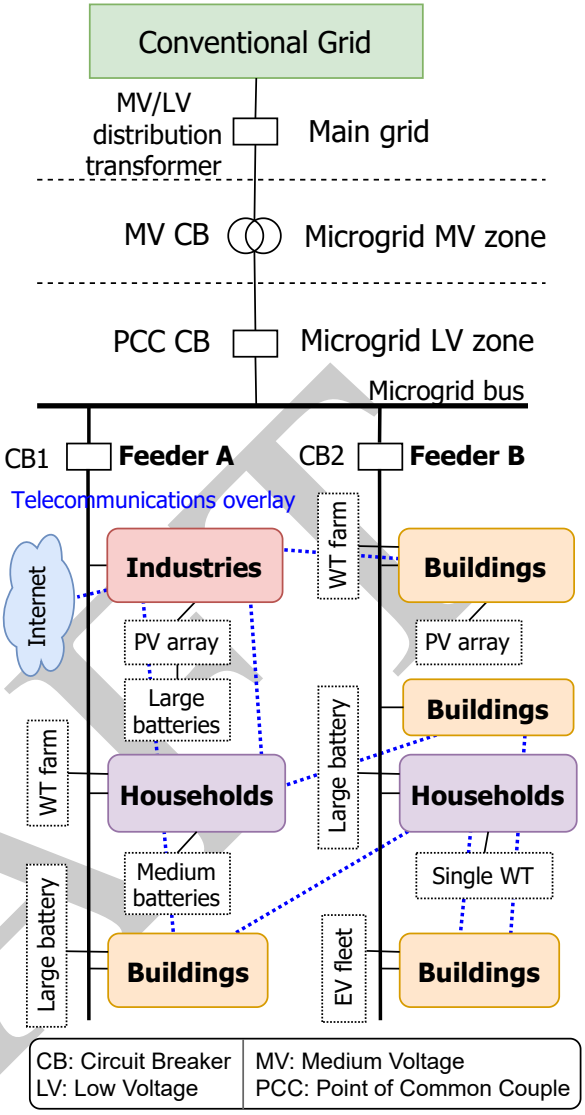


Fig. 1: High-level grid-connected micro-grid system overview.

On the other hand, in the *islanded* mode, it operates disconnected from the power grid. However, this mode is highly susceptible to cyber-attacks. Adversaries may install malware in the grid components such as Smart Meters or any other IoT device connected to high-wattage appliances to direct attacks. As stated earlier, in LCA, malicious actors synchronize turning on or off a large number of compromised high-wattage devices to imbalance frequency regulation. As the frequency ramps up or down very quickly, it may cause the micro-grid to black-out (or brown-out), since it is not prepared for such occurrence. In the micro-grid, the buses could prioritize powering-up critical infrastructure (e.g., a hospital), choosing to disconnect (load-shedding) a less important bus as deemed necessary.

Fig. 2 details the balancing conditions as performed by the Load Frequency Control (LFC) mechanism, showing the cases where Supply-Demand equilibrium conditions are not met.

An example of this modelling set-up is illustrated in Fig. 3

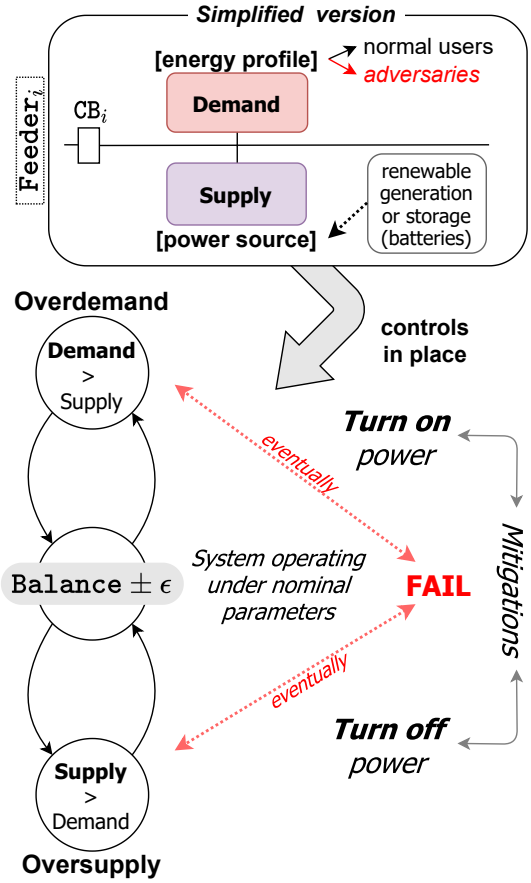


Fig. 2: Supply-Demand imbalances may lead to failure requiring timely repair to resume operations to nominal levels.

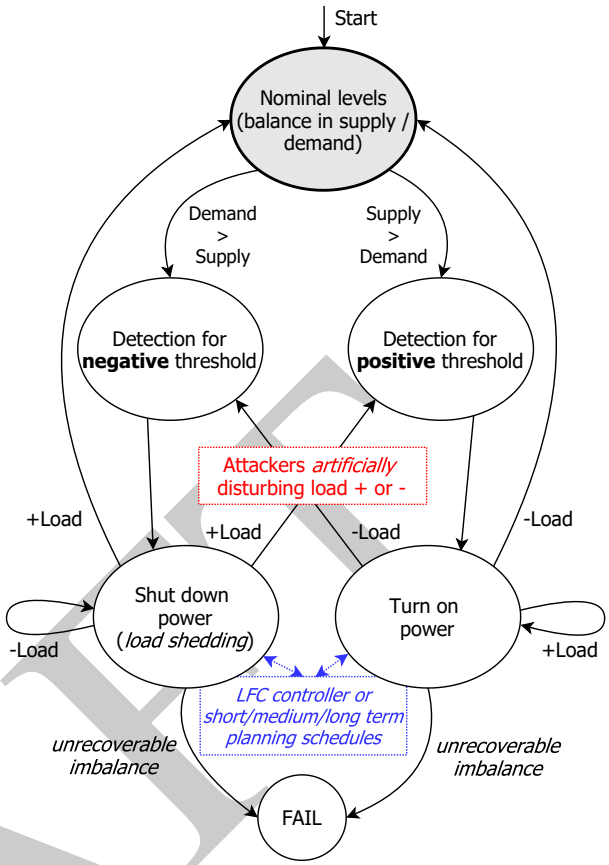


Fig. 3: Aging model (LFC perspective) – *original* model.

showing the LCA problem with transitions that return to the 'Nominal levels' state (original model with cycles). Specifically, measurement apparatuses scattered across the infrastructure can measure instantaneous frequency and respond to changes to implement frequency control within the required nominal values. Some measures that can be implemented are: (1) disconnections; or (2) turning on power assist on the balance, since it is easier to shut down than to power up due to inertia or other considerations set by energy operators.

Fig. 4 demonstrates the proposed approach, where we have unfolded the Markov chain removing self-loops and cycles into new states named 'Fixed'. Our assumption is that attackers will choose a given strategy and persist on it until the system eventually collapses ('Fail' state) or gets patched for security ('Fixed' state).

Our goal is to develop an approach to bridge between aging and rejuvenation models and survivability models. We apply our approach to a known cyber-security attack.

IV. Micro-grid Case Studies

Table I summarizes the power assessments and resiliency features of the micro-grids described in this section. In the following, we describe the micro-grid features found in a few selected case studies.

TABLE I: Selected micro-grid assessments (in the US).

Micro-grid	Supply (MW)	% Demand	Resiliency Features
Princeton	20.5	100%	Optimized
UCSD	42	85%	60 MW Diesel
IIT	9	90%	50% DR
NYU	13.4	100%	Optimized

A. Princeton University[5]

The distributed energy resources supply side consists of a solar array, a gas turbine, and a steam turbine. These are used to supplement purchases of grid power and natural gas.

In addition, heating and cooling operations are managed by the co-generation plant, which consists of chilled water for cooling and steam for heating. Cooling electricity operations is based on off-peak cost, during the night, and stored as chilled water to be used for daytime air conditioning. Steam is produced in the co-generated plant and is used for campus-wide heating using a network of underground pipes. Therefore, the co-generation plant is used to centralize heating and cooling operations, which allows for fuel cost optimization. The co-generations plan has a supply capacity of 15 MW

[5]https://tiger-energy.appspot.com/home

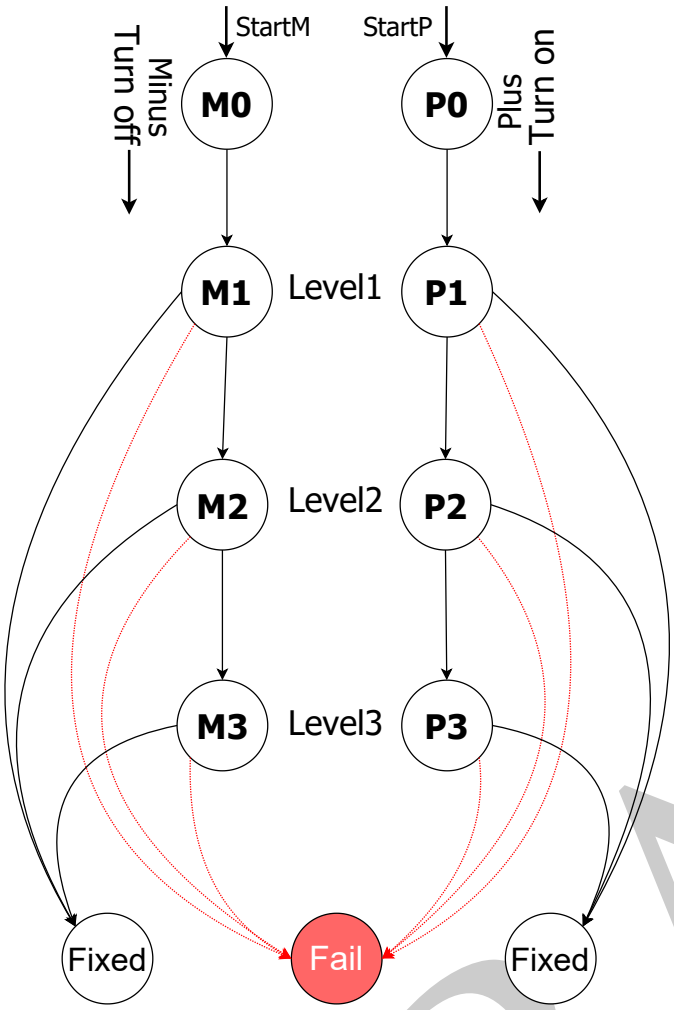


Fig. 4: Aging model (LFC perspective) – *unfolded* model. Each level is associated with contingencies in place to avoid load-shedding such as starting *spinning reserves* or aggregate/disconnect power to meet frequency balance.

and can operate in island mode to supply 100% of Princeton micro-grid demand. It consists of steam boilers, water chillers, electric generators and an energy storage tank. Energy Demand in the Princeton University's campus can be categorized into laboratories, housing building, academic buildings, other buildings, and sports facilities.

B. The University of California, San Diego[6]

The distributed energy resources supply side consists of two 13.5 MW gas turbines, one 3 MW steam turbine, 1.2 MW generated using solar panels, and a 2 MW fuel cell power that is powered by methane produced in a wastewater treatment facility, and other distributed generation facilities for a total supply of 42 MW. These can be used in island mode or integrated into the power grid.

[6]https://the-atlas.com/projects/uc-san-diego-microgrid

UCSD micro-grid uses a co-generation facility composed of two 13 MW natural gas turbines. In addition, turbine exhaust heat is used for water chilling, which is stored in very large water tanks with 3.8 million gallon capacity. In addition, solar power is integrated with battery storage to provide a 3 MW solar network. A 60 MW emergency backup power, supplied by diesel generators, can be activated for emergency recovery.

C. Illinois Institute of Technology[7]

The Illinois Institute of Technology has implemented a smart micro-grid distribution system with the objective of demonstrating advanced Smart Grid features. Among them, (1) automated loop with system breakers and switches to support automated fault detection, isolation, and recovery; (2) a software controller to support distributed generation; (3) sensing distribution to support active and reactive power management; (4) advanced smart-metering to support demand response; (5) large scale batteries to support daily peaks, load shedding, and intermittent integration with wind, solar, and EV charging; and (6) advanced ZigBee wireless technology.

Campus power demand is 10 MW and distributed generation using two 4 MW gas-powered generators supplemented by wind, solar PV, and one 500 kWh battery. The total distributed generation of 9 MW allowing the micro-grid to operate in islanded mode.

D. New York University[8]

The NYU micro-grid uses similar architecture features as Princeton's. Specifically, natural gas-powered turbines with hot waste recovery is used to produce both electricity and steam. Hot water and chilled water are stored for later use in heating and cooling devices.

The NYU micro-grid incorporates a Combined Heat and Power supply power generator with a total generation capacity of 13.4 MW. It contains two 5.5 MW gas powered generators with heat recovery of steam coupled to a 2.4 MW steam turbine, which allows the NYU micro-grid to operate in islanded mode.

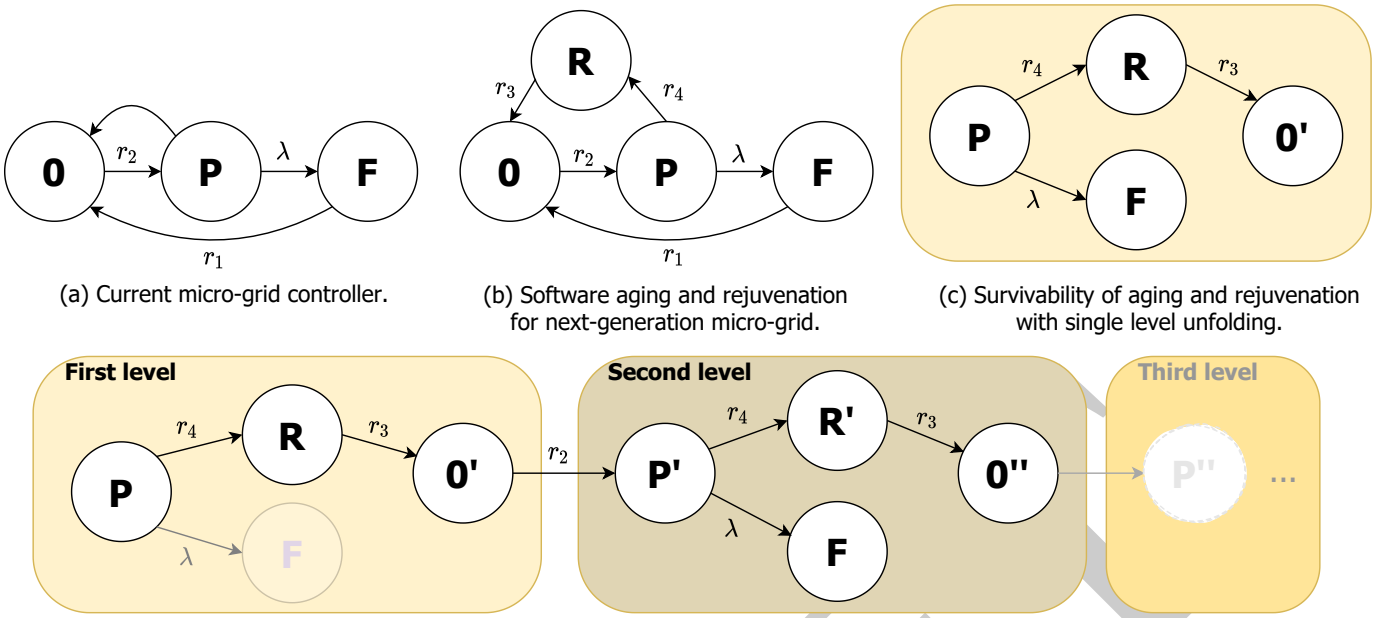
The application of the proposed methodology to the described Micro-grids is presented in Section VI and illustrated in Table III.

V. Aging, Rejuvenation and Survivability

Aging and rejuvenation models typically account for failures and recovery in an integrated fashion. Survivability modelling, in contrast, aims at characterizing the system from a prone to failure state up to recovery.

[7]https://microgrid-symposiums.org/microgrid-examples-and-demonstrations/illinois-institute-of-technology-microgrid

[8]https://microgrid-symposiums.org/microgrid-examples-and-demonstrations/new-york-university-microgrid, https://www.nyu.edu/about/news-publications/news/2011/january/nyu-switches-on-green-cogen-plant-and-powers-up-for-the-sustainable-future.html



(a) Current micro-grid controller.

(b) Software aging and rejuvenation for next-generation micro-grid.

(c) Survivability of aging and rejuvenation with single level unfolding.

(d) Survivability of aging and rejuvenation with two level unfolding. Note that there is only one state F per model.

Fig. 5: Software aging and rejuvenation: (a) classical aging and rejuvenation Markov chain [29]; (b) micro-grid power generator states extracted from [24]; (c) extending micro-grid controller states to account for a rejuvenation state wherein next-generation strategies, such as demand response, can be used to defer demand; (d) two level unfolding, extending previous model in (c). In (d), it also shows possible subsequent levels as levels progresses (state P" onward).

A. *Unfolding an aging and rejuvenation model yields a survivability model*

In this research, we extend the survivability models presented in [25]–[28] to account for LCA in grid-connected micro-grid systems shown in Figure 1, and to evaluate the survivability metrics of interest. In order to bridge aging and rejuvenation models, and survivability models, we propose to unfold aging and rejuvenation models, starting from the prone to failure state and accounting for up to a given number of tentative attacks, each of which may lead to a failure, before either ultimately reaching the failure state or, alternatively, the recovery state. Fig. 5 illustrates our methodology where we produce from the baseline model (which may involve cycles among states) a DAG corresponding to the states visited by the system after it reaches the prone to failure state.

In Fig. 5a we consider a classical micro-grid controller, and in Fig. 5b, we explicitly account for the rejuvenation time due to demand-response to react against load changes. Fig. 5c explicitly indicates that the attacker competes against rejuvenation. Whichever event occurs first, attack or rejuvenation, will determine whether the system will ultimately fail before reaching its stable state. In Fig. 5c we account for a single competitive round, i.e., we assume the attacker will try an LCA only once, whereas in Fig. 5d, we assume that the attacker will modulate its attack and try twice to adapt to grid responses. In that case, the system will move to the final stable state before failure if rejuvenation occurs twice before failure.

Table II shows the parameters employed in previous aging and rejuvenation research [29] used to calibrate our models. We used PRISM Probabilistic Model Checker [30] to create our aging and rejuvenation model that leverages a modular approach as shown in Appendix.

TABLE II: Parameters as defined in Huang et al. (1995) [29] (Illustrative example A) – Fig. 5b.

Transition	Rate	Description
P to F*	$\lambda = \frac{1}{1\times30\times24}$	Mean time between two consecutive failures (MTBF), i.e., one month.
F to 0**	$r_1 = 2$	Time to recover from an unexpected failure, i.e., 30 min.
0 to P	$r_2 = \frac{1}{7\times24}$	Base longevity interval, i.e., 7 days.
R to 0	$r_3 = 3$	Mean repair time after rejuvenation, i.e., 20 min.
P to R	$r_4 = \frac{1}{(14-7)\times24}$	Rate of rejuvenation after the application goes into failure state. Set here once every two weeks.

*Only one occurrence of P to F transition per model, on the last level.
**This transition is only used for Fig. 5a and Fig. 5b.

B. *Numerical evaluation*

First, we consider how the probability of failure varies after the system reaches the prone to failure state. Fig. 6 illustrates numerical results obtained using the proposed analytical model. It shows the probability of failure by a given time t, accounting for various values of maximum number of attack trials. The transient failure probability shown in the figure illustrates that after a certain time t, as a potential adversary keeps trying malicious attempts, eventually the attack will succeed, reaching the failure state.

Then, we consider how the maximum number of attack trials impacts the probability of failure by 8,000 hours after the system reaches the prone to failure state. Fig. 7 shows the obtained results. It indicates that as the maximum number of attack trials increases, the probability of failure also increases. Note, however, that this is subject to light-weight countermeasures, e.g., which do not decrease the probability of an attack being successful as the number of attempts increases. We further discuss countermeasures as follows.

C. Countermeasures

Our model relates aging and rejuvenation to security incidents. While it captures how adversaries try to invade systems or deplete resources (causing degradation), it is instrumental to cyber-security analysts deploying mitigation and containment mechanisms to thwart attacks (rejuvenation).

The attack vector in LCA consists of a synchronized increase in power demand, which triggers one or more circuit breakers. Possible countermeasures to address LCA involve the use of the following SG features:

- *FDIR* fault detection isolation, recovery (back-up power).
- *DR* use of demand response feature to provide varying local load limit per smart-meter that is based on estimation of total load level in the micro-grid.
- *Segmentation* - fine grain feeder segmentation to increase the effectiveness of FDIR and DR features.

We present next several versions of the survivability model accounting for the LCA phases (aging) and the corresponding countermeasures (rejuvenation).

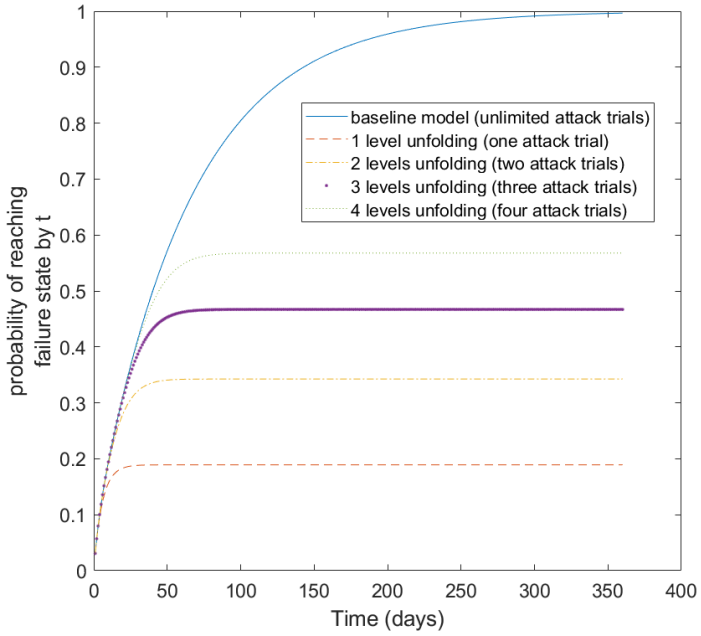


Fig. 6: Probability of failure by time t, after reaching prone to failure state, for the baseline model, and 1 to 4 trials.

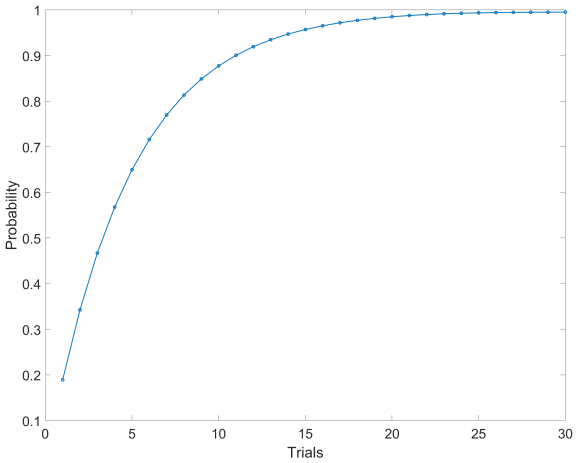


Fig. 7: Probability of failure by 8,000 hours (around 333 days), after reaching prone to failure state, as a function of the number of trials (a trial represents a model unfolding).

VI. Cyber-attack scenarios

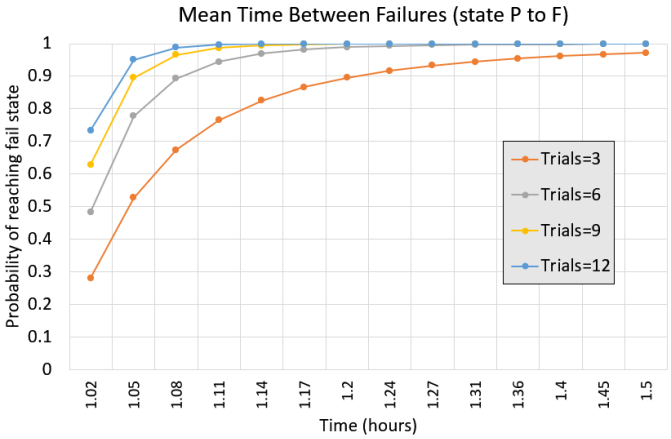
We conducted a series of scenarios and representations of different micro-grids to showcase our approach. Fig. 8 shows three experiments varying λ, r_2, and r_4 parameters in the model for number of attack trials varying among values 3, 6, 9, 12 and we measure our time in hours.

Fig. 8a shows that as time progresses, the probability of reaching the failed increases with the increase in the number of trials. Fig. 8b shows the impact of varying the residence time in state Z, where it represents the rejuvenation states, and P the prone to failure states.

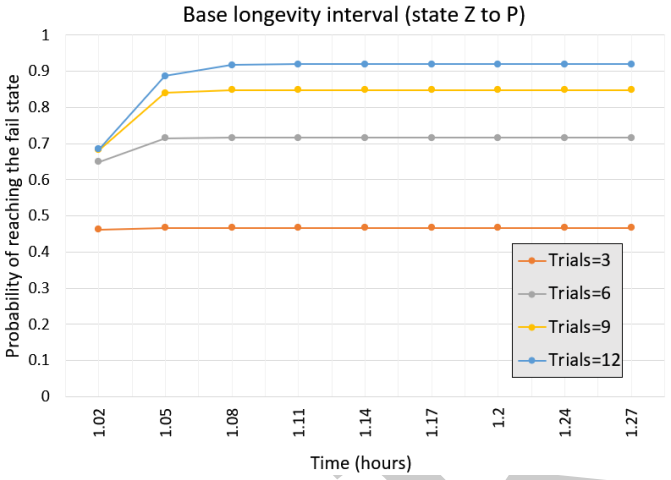
Fig. 8c shows the impact of varying the residence time in state P. The failure probability increases with the increase in the residence time in state P as the number of trials increases. The number of trials needed to effectively conduct an attack is an indication of the necessary adversarial capabilities required to circumvent protections, at the same time where cyber-security defences are enacted to thwart and contain malicious incursions. The plots show that as the number of trials increases, the probability of reaching the 'fail' state tends to 100%. In our modelling approach reaching the fail state represents a successful attack.

Our approach can be used by micro-grid engineers to support the computation of metrics affecting the power utility income. For example, the Instantaneous Expected Energy Not Supplied (IEENS) by time t, can be computed from the fail state probability. Table III shows an analysis for the IEENS metric computed at instant 1.2 hours by varying the number of maximum attack trials. We compute the value of IEENS by multiplying state failure probability by the energy supplied.

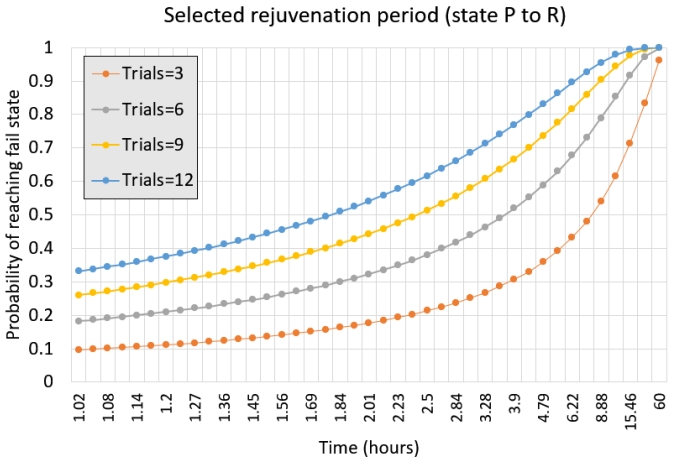
In the event of failures, quick responding to cyber-attacks has substantial effects on IEENS. If security officers manage to detect and then thwart attacks as fast as they are identified, they could protect critical resources from harmful incursions.



(a) Varying residence time in state P, transition $P \rightarrow F$ (λ).



(b) Varying residence time in state Z, transition $Z \rightarrow P$ (r_2).



(c) Varying residence time in state P, transition $P \rightarrow R$ (r_4).

Fig. 8: Experiments on PRISM varying selected parameters.

TABLE III: IEENS analysis for P to R (t=1.2h), Fig. 8c.

Micro-grid	**Energy Supplied (MW)**	**IEENS (MW) at $t = 1.2$h** *Maximum Attack Trials*			
		3	6	9	12
Princeton	20.5	2.3	4.4	6.2	7.9
UCSD	42	4.8	9.0	12.8	16.1
IIT	9	1.0	1.9	2.7	3.5
NYU	13.4	1.5	2.9	4.1	5.1

VII. Conclusions

Cyber-attacks have devastating consequences to a non-negligible number of stakeholders in critical infrastructures. In Smart-Grids, energy spikes, brown-outs, and black-outs may cascade and impact large portions of the power network, causing significant damage and financial losses. It is thus crucial to investigate means to improve resiliency and address those shortcomings in a timely, safe, and secure fashion.

This work has shown a modelling proposition of combining classical aging and rejuvenation models into unfolded counterparts that may be used to compute survivability metrics. We applied our novel technique to a cyber-security attack known as LCA, where malicious actors synchronize compromised resources to artificially imbalance the power system frequency aiming to disrupt the infrastructure until it collapses. We have shown how to convert the software aging and rejuvenation model, with cycles, to its unfolded counterpart that can be used to support the survivability computation.

We envision several practical applications of the proposed methodology. First, because we solved the micro-grid model analytically, the approach can be valuable when supporting micro-grid engineering optimizations accounting for security intrusions. Second, they could use the approach to detect security attacks by monitoring for unexpected deviations of the Energy Not Supplied metric.

As future work we aim to refine our model by including other types of security attacks, and extending the unfolded Markov chain to include rewards for energy not supplied and other factors impacting the utility company's income.

Acknowledgments

Ricardo M. Czekster acknowledges funding from the Industrial Strategy Challenge Fund and EPSRC grant EP/V012053/1, for The Active Building Centre Research Programme (ABC RP).

References

[1] J. R. Lindsay, "Stuxnet and the limits of cyber warfare," *Security Studies*, vol. 22, no. 3, pp. 365–404, 2013.

[2] M. Geiger, J. Bauer, M. Masuch, and J. Franke, "An Analysis of Black Energy 3, Crashoverride, and Trisis, Three Malware Approaches Targeting Operational Technology Systems," in *2020 25th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)*, vol. 1. IEEE, 2020, pp. 1537–1543.

[3] J. Slowik, "Anatomy of an attack: Detecting and defeating crashoverride," *VB2018, October*, 2018.

[4] Y. Mekdad, G. Bernieri, M. Conti, and A. E. Fergougui, "A threat model method for ics malware: the trisis case," in *Proceedings of the 18th ACM International Conference on Computing Frontiers*, 2021, pp. 221–228.

[5] B. Wang, X. Li, L. P. de Aguiar, D. S. Menasche, and Z. Shafiq, "Characterizing and modeling patching practices of industrial control systems," *Proceedings of the ACM on Measurement and Analysis of Computing Systems*, vol. 1, no. 1, pp. 1–23, 2017.
[6] P. Asmus, "Microgrids, virtual power plants and our distributed energy future," *The Electricity Journal*, vol. 23, no. 10, pp. 72–82, 2010.
[7] I. Series, "Microgrids and active distribution networks," *The institution of Engineering and Technology*, 2009.
[8] T. Zhu, Z. Huang, A. Sharma, J. Su, D. Irwin, A. Mishra, D. Menasche, and P. Shenoy, "Sharing renewable energy in smart microgrids," in *2013 ACM/IEEE International Conference on Cyber-Physical Systems (ICCPS)*. IEEE, 2013, pp. 219–228.
[9] S. Lee, P. Shenoy, K. Ramamritham, and D. Irwin, "Autoshare: Virtual community solar and storage for energy sharing," *Energy Informatics*, vol. 4, no. 1, pp. 1–24, 2021.
[10] A. Avritzer, R. M. Czekster, S. Distefano, and K. S. Trivedi, "Software aging and rejuvenation for increased resilience: modeling, analysis and applications," in *Resilience assessment and evaluation of computing systems*. Springer, 2012, pp. 167–183.
[11] P. E. Heegaard and K. S. Trivedi, "Network survivability modeling," *Computer Networks*, vol. 53, no. 8, pp. 1215–1234, 2009.
[12] J. C. Knight and K. J. Sullivan, "On the definition of survivability," *University of Virginia, Department of Computer Science, Technical Report CS-TR-33-00*, 2000.
[13] Z. Ma, "Towards a unified definition for reliability, survivability and resilience (i): the conceptual framework inspired by the handicap principle and ecological stability," in *2010 IEEE Aerospace Conference*. IEEE, 2010, pp. 1–12.
[14] D. T. Ton and M. A. Smith, "The us department of energy's microgrid initiative," *The Electricity Journal*, vol. 25, no. 8, pp. 84–94, 2012.
[15] A. Lee, "Electric sector failure scenarios and impact analyses," *National Electric Sector Cybersecurity Organization Resource (NESCOR) Technical Working Group*, vol. 1, 2013.
[16] S. Jauhar, B. Chen, W. G. Temple, X. Dong, Z. Kalbarczyk, W. H. Sanders, and D. M. Nicol, "Model-based cybersecurity assessment with NESCOR smart grid failure scenarios," in *2015 IEEE 21st Pacific Rim International Symposium on Dependable Computing (PRDC)*. IEEE, 2015, pp. 319–324.
[17] A. Dabrowski, J. Ullrich, and E. R. Weippl, "Grid shock: Coordinated load-changing attacks on power grids: The non-smart power grid is vulnerable to cyber attacks as well," in *Proceedings of the 33rd Annual Computer Security Applications Conference*, 2017, pp. 303–314.
[18] S. Soltan, P. Mittal, and H. V. Poor, "BlackIoT: IoT botnet of high wattage devices can disrupt the power grid," in *27th {USENIX} Security Symposium ({USENIX} Security 18)*, 2018, pp. 15–32.
[19] ——, "Protecting the grid against MAD attacks," *IEEE Transactions on Network Science and Engineering*, vol. 7, no. 3, pp. 1310–1326, 2019.
[20] B. Huang, A. A. Cardenas, and R. Baldick, "Not everything is dark and gloomy: Power grid protections against iot demand attacks," in *28th {USENIX} Security Symposium ({USENIX} Security 19)*, 2019, pp. 1115–1132.
[21] D. Greenwood, K. Y. Lim, C. Patsios, P. Lyons, Y. S. Lim, and P. Taylor, "Frequency response services designed for energy storage," *Applied Energy*, vol. 203, pp. 115–127, 2017.
[22] P. T. Mana, K. P. Schneider, W. Du, M. Mukherjee, T. Hardy, and F. K. Tuffner, "Study of microgrid resilience through co-simulation of power system dynamics and communication systems," *IEEE Transactions on Industrial Informatics*, 2020.
[23] R. M. Czekster, C. Morisset, J. A. Clark, S. Soudjani, C. Patsios, and P. Davison, "Systematic review of features for co-simulating security incidents in cyber-physical systems," *Security and Privacy*, vol. 4, no. 3, p. e150, 2021.
[24] L. Arnaboldi, R. M. Czekster, C. Morisset, and R. Metere, "Modelling Load-Changing Attacks in Cyber-Physical Systems," *Electronic Notes in Theoretical Computer Science*, vol. 353C, pp. 39–60, 2020.
[25] A. Avritzer, S. Suresh, D. S. Menasché, R. M. M. Leão, E. de Souza e Silva, M. C. Diniz, K. Trivedi, L. Happe, and A. Koziolek, "Survivability models for the assessment of smart grid distribution automation network designs," ser. ICPE '13. New York, NY, USA: Association for Computing Machinery, 2013, pp. 241—252. [Online]. Available: https://doi.org/10.1145/2479871.2479905
[26] D. S. Menasché, A. Avritzer, S. Suresh, R. M. Leão, E. de Souza e Silva, M. Diniz, K. Trivedi, L. Happe, and A. Koziolek, "Assessing survivability of smart grid distribution network designs accounting for multiple failures," *Concurrency and Computation: Practice and Experience*, vol. 26, no. 12, pp. 1949–1974, 2014.
[27] A. Koziolek, A. Avritzer, S. Suresh, D. S. Menasche, K. Trivedi, and L. Happe, "Design of distribution automation networks using survivability modeling and power flow equations," in *2013 IEEE 24th International Symposium on Software Reliability Engineering (ISSRE)*, 2013, pp. 41–50.
[28] A. Avritzer, L. Carnevali, H. Ghasemieh, L. Happe, B. R. Haverkort, A. Koziolek, D. Menasche, A. Remke, S. S. Sarvestani, and E. Vicario, "Survivability evaluation of gas, water and electricity infrastructures," *Electronic Notes in Theoretical Computer Science*, vol. 310, pp. 5–25, 2015, proceedings of the Seventh International Workshop on the Practical Application of Stochastic Modelling (PASM).
[29] Y. Huang, C. Kintala, N. Kolettis, and N. D. Fulton, "Software rejuvenation: Analysis, module and applications," in *Symposium on Fault-Tolerant Computing*. IEEE, 1995, pp. 381–390.
[30] M. Kwiatkowska, G. Norman, and D. Parker, "PRISM 4.0: Verification of probabilistic real-time systems," in *International Conference on Computer Aided Verification*. Springer, 2011, pp. 585–591.

APPENDIX

Next, we introduce the PRISM model representing the behavior described in Fig. 5d.

```
ctmc

// TRIALS: undefined constant (experiment)
const int TRIALS;
// MAX: set the number of local states
const int MAX = (TRIALS=0 ? 3 : TRIALS*3);

const double r_PF = 1/(30*24); // lambda
const double r_ZP = 1/(7*24);  // rate r2
const double r_RZ = 3;         // rate r3
const double r_PR = 1/(7*24);  // rate r4
const int SF = 0;              // fail state

module M1
    x : [0..MAX] init 1;
    [] (mod((x-1),3)=0) -> r_PR:(x'=x+1);
    [] (mod((x-2),3)=0) -> r_RZ:(x'=x+1);
    [] (mod((x-3),3)=0 & x!=0 & x!=MAX)
                        -> r_ZP:(x'=x+1);
    // only used when TRIALS=0
    [] (mod((x-3),3)=0 & x!=0 & TRIALS=0)
                        -> r_ZP:(x'=1);
    // P-->F
    [] (mod((x-1),3)=0) -> r_PF:(x'=SF);
endmodule
```

The maximum number of attack trials is set according to our experimental goals, e.g., varying among values 3, 6, 9 and 12. The rates between states are determined through the four constants set at the beginning of the code.

The implementation of the model is modular where each module contains a set of states. We use the *modulo* (`mod`) operator (integer remainder of division) to compute state indices within the module.

To produce Figure 7, for instance, we verified the following property: `P=? [ F=8000 x=0 ]` (*'what is the probability of reaching the fail state (SF=0) in 8,000 hours (333 days)?*).