

PNNL-35082

Introduction to ALERT: A User-Interface Tool for Resilient Optimization

Technical Report

October 12, 2023

Scott Upton Gwen Kidd Soumya Kundu Saptarshi Bhattacharya Yangchao (Nino) Lin Veronica Adetola Thiagarajan Ramachandran Nawaf Nazir



Prepared for the U.S. Department of Energy Under contract DE-AC05-76RL01830

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor Battelle Memorial Institute, nor any of their employees, makes **any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof, or Battelle Memorial Institute. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.**

PACIFIC NORTHWEST NATIONAL LABORATORY operated by BATTELLE for the UNITED STATES DEPARTMENT OF ENERGY under Contract DE-AC05-76RL01830

Printed in the United States of America

Available to DOE and DOE contractors from the Office of Scientific and Technical Information, P.O. Box 62, Oak Ridge, TN 37831-0062 www.osti.gov ph: (865) 576-8401 fox: (865) 576-5728 email: reports@osti.gov

Available to the public from the National Technical Information Service 5301 Shawnee Rd., Alexandria, VA 22312 ph: (800) 553-NTIS (6847) or (703) 605-6000 email: <u>info@ntis.gov</u> Online ordering: <u>http://www.ntis.gov</u>

Introduction to ALERT: A User-Interface Tool for Resilient Optimization

Technical Report

October 12, 2023

Scott Upton Gwen Kidd Soumya Kundu Saptarshi Bhattacharya Yangchao (Nino) Lin Veronica Adetola Thiagarajan Ramachandran Nawaf Nazir

Prepared for the U.S. Department of Energy Under Contract DE-AC05-76RL01830

Pacific Northwest National Laboratory Richland, Washington 99352

Acknowledgments

This research was supported by the **Resilience through Data-driven intelligently-Designed Control Initiative (RD2C)**, under the Laboratory Directed Research and Development (LDRD) Program at Pacific Northwest National Laboratory (PNNL). PNNL is a multi-program national laboratory operated for the U.S. Department of Energy (DOE) by Battelle Memorial Institute under Contract No. DE-AC05-76RL01830.

Contents

Ackr	nowledg	ments	iv
1.0	Introdu	lction	1
	1.1	Overview	1
	1.2	Report Structure	2
2.0	ALER	Algorithmic Components	3
	2.1	Robust Predictive Dispatch	3
	2.2	Resilience Verification	4
	2.3	Resilient Online Adaptation	4
3.0	ALER	User-Interface Tool	5
4.0	Conclu	isions	9

Figures

1	Basic idea of the ALERT controls.	1
2	Schematic outline of the ALERT user-interface.	2
3	Essential building blocks of the ALERT technology.	3

1.0 Introduction

Current resilience practices in cyber-physical systems (such as electrical power grid) either involve long-term, and expensive, investment decisions; or are reactive in nature, relying on predominantly ad-hoc (simulations-based) strategies that fail to provide resilience guarantees and/or requiring intervention of human operators who are prone to mistakes and introduces response delays. Moreover, it is often cost-prohibitive to redesign existing baseline controls for resilient performance. As the cyber-physical systems grow in complexity, there is a need for proactive resilience strategies such as the ones proposed here, that involve online, adaptive control actions to best prepare for any impending adversarial events. It is desirable that such a resilient control design would render an add-on layer such as the one proposed for a more preferable, easily implementable, and reconfigurable solution. Finally, system theoretical guarantees of (guantitative) resilience performance measures would not only help develop trust in the automated control algorithms and accelerate real-world deployment, such guarantees would also provide guantitative specifications of sensor/control performance for resilient co-design efforts. In this effort, the objective was to design online strategies for adaptive tuning of existing optimal control solutions in response to cyber-physical adversarial events; and assure (quantifiably) sufficient margins of resilience. The developed solution acts as a resilient add-on layer and replaces the need for cost-prohibitive redesign of existing baseline controls for assured resilience. One key outcome of this effort is a design of Adaptive Learning-Enabled Resilient Tuning (ALERT) controls for cyberphysical systems, with quantitative assurance of resilience to adversarial events, validated on (single and networked) microgrid use-cases.

1.1 Overview



Figure 1: Basic idea of the ALERT controls.

In this technical effort, the project team designed and demonstrated online strategies – henceforth referred to as ALERT controls – for proactive and adaptive tuning of existing optimal controls in a microgrid, with quantifiably assured margins of resilience to various cyber-physical adversarial events. The overall idea of the ALERT controls is summarized in Fig. 1. ALERT controls sits on top of the existing (i.e., baseline) system-level optimal controllers, and only minimally adapts (i.e., tunes) the baseline controllers' settings and its output to ascertain the satisfaction of resilience constraints. Real-time sensor updates, and time-series forecasts are fed as input to the ALERT algorithm which then adjusts the controller settings and actuator set-points to ensure that the system maintains resilience under cyber-physical adversarial events. A brief outline of the ALERT algorithms is presented in Section 2.0, with more details found in [1].



Figure 2: Schematic outline of the ALERT user-interface.

This ALERT functionality is made available to the end-users, e.g., the system operators, via an interactive user-interface, a schematic outline of which is shown in Fig.2. On this user-interface, the end-users will have the options of entering their system details (e.g., microgrid network models, information on the dispatchable resources), resilience specifications (e.g., load curtailment limits, reserve margins, voltage limits), and specify cyber-physical events of interest (e.g., physical disruptions, cyber attacks, forecast errors). The user-interface will process the visualize the entered information, along with displaying the ALERT control outcomes via time-series results, as well as novel time-varying adversarial set plots (see [1] for details). The end-users will not only be able to use the interface to visualize the system's operation under various cyber-physical adversarial perturbations of interest (e.g., malfunctioning sensors, suspected attacked measurements) via the adversarial plots. Details of the prototype user-interface and some illustrative results are discussed in Section 3.0. A current implementation of the user-interface is available at: https://devops.pnnl.gov/alrt-client.

1.2 Report Structure

In this technical report, we briefly outline the algorithmic modules of the developed ALERT control technology (in Section 2.0), and introduce the user-interface tool that allows end-users (e.g., microgrid operators) to enter their system description, specify various operational and resilience requirements, and evaluate the impact of the control decisions via illustrative plots (in Section 3.0).



2.0 ALERT Algorithmic Components

Figure 3: Essential building blocks of the ALERT technology.

A brief outline of basic work-flow of the ALERT technology is shown in Fig. 3. The core ALERT technology can be broken down into a proactive and an adaptive module. The proactive module processes as inputs user-defined resilience specifications (e.g., reserve margins, curtailment limits, voltage limits) and associated cyber analytics (e.g., likelihood of cyberattacks, likelihood of other anomalies) to output resilience-verified optimal control set-points (e.g. dispatching DERs) that are guaranteed to ensure system's resilience under the predicted (i.e., likely) adversarial scenarios. The adaptive module takes as input real-time updates (via sensor measurements) of the system's conditions under unforeseen adversarial events, and performs online adjustment of the control set-points to track the resilience specifications under evolving adversarial conditions. It has three sub-modules that implement proactive and adaptive responses:

- (Proactive) Robust Predictive Dispatch to optimally allocate set-points and reserves to distributed energy resources (DERs).
- (Proactive) Resilience Verification via bi-level optimization to quantify the tolerable adversarial set.
- (Adaptive) Resilient Online Adaption of set-points via sensitivity-based feedback control to safeguard against adversarial events.

Next we briefly describe the three sub-modules which are presented in details in [1,2].

2.1 Robust Predictive Dispatch

In this sub-module, a multi-periodic, robust, predictive optimization is solved to optimally allocate set-points and reserves to meet resilience specifications under uncertainties. In the most general form, the robust optimization problem for a system can be expressed in the following form:

$$\min_{u} \max_{w} f(u, w) \tag{1a}$$

$$s.t. \ g(u,w) \le 0 \qquad \forall w \in \Omega_W$$
 (1b)

where g(u, w) are the different system-level operational, and resilience constraints (see [1] for example). The above optimization problem (1) can be converted to a robust formulation using the *explicit maximization method* (see [3]) in the following form:

$$\min \widehat{f}(u), \quad \text{s.t. } \widehat{g}(u) \le 0 \tag{2}$$

where $\hat{f}(u) = \max_w f(u, w)$ and $\hat{g}(u) = \max_w g(u, w)$. The new model does not contain any disturbance terms and if the functions $\hat{f}(u)$ and $\hat{g}(u)$ are convex, then the optimization problem is convex, which can be solved efficiently [1]. Resilience is enforced in a robust sense via inclusion of penalties on resilience violations and/or hard constraints of resilience performance. These robust dispatch problems can also accommodate risk-based and probabilistic constraints – often reflected in estimated likelihood of cyberattacks – as shown in [2]. An outcome of the robust predictive dispatch problem is a set of set-points and reserve margins.

2.2 **Resilience Verification**

In this sub-module, candidate solutions from the robust predictive dispatch – in the form of optimal set-points and reserves – are used to quantify the largest set of w (i.e., adversarial disruption-s/perturbations) that the system can tolerate without violating critical resilience specifications. This is achieved by solving the following problem:

$$\max_{w} |w - w^*| \tag{3a}$$

subject to:
$$g(u^*, w) \le 0$$
 (3b)

$$w \in \Omega_W$$
 (3c)

where u^* are the candidate solutions (optimal set-points) from the robust predictive dispatch, w^* are the best-known estimates of the adversarial input, and $w - w^*$ are the adversarial perturbations. A polytopic inner approximation of the largest tolerable adversarial set Ω_W can be constructed via tractable optimization formulations as described in details in [1]. The calculated adversarial sets are used to inform design decisions around sizing of the dispatchable resources and/or quality of the sensors which can in turn be used to update the predictive dispatch solutions.

2.3 **Resilient Online Adaptation**

In this sub-module, online adaptive control laws are designed, which allow tapping into the available reserves to maintain resilience under adversarial events, by tuning the optimal set-points from the proactive module under unforeseen cyber-physical events. Sensitivity-based feedback control policy such as the following is used for real-time adaptation of optimal control set-points to safeguard against evolving (and largely unforeseen) adversarial events:

$$u = u^* + K y(u, w) \tag{4}$$

where u^* are the dispatched set-points from the proactive module, K is a feedback control gain, w are the actual adversarial perturbations (which are unknown), y are the sensors updates (capturing the system states under adversarial perturbations), and u are the real-time adjusted set-points. An example of the online adaptive implementation is provided in [1].

3.0 ALERT User-Interface Tool

In this section, we introduce the interactive user-interface tool for the ALERT controls. A current implementation of the user-interface is available at the PNNL GitLab page: https://devops.pnnl.gov/alrt-client. It has a set of simple instructions to install and run the user-interface:

How to Install and Run

- Clone Repo
- 🗌 Run npm install
- Add SERVER_USERNAME and SERVER_PASSWORD to the .env file. This should be your local credentials to connect to the constance server
- 🗌 Once everything is installed, run "npm run dev:backend". This will start up your node middleware to communicate with the server
- Run npm start to start the front end. This will start running the appication

Brief Tutorial. To help end-users quickly go over the available functionalities that the userinterface offers, there is a short tutorial (a collection of slides) made available on the interface. Illustrative screenshots from the tutorial are shown below.



ALERT Grid Resiliency Applics	Tutorial		×	LOGIN ()
INPUT SIMULATION PARAMETER Suncario to the total 02/17/2023 02:07 AM Decastor Bor Sar 02/17/2023 02:22 AM Soc Prints NOA car Decastor Function Soc Prints Decastor Function	CERTIFICATION ADDRESS	CLICK HERE FOR INPUT SPECIFIC TO THE VISUALIZATION ON THE DIGHT HAND SIDE		80
Voltage Lover Bound 0.95 Voltage Bound 1.05 Coment Influent Moder IEEE123	sPCOY DANT Replay Attack + Rem			

Enter and Visualize System Information. At the welcome page (or, home screen) of the userinterface ALERT tool, the end-user has access to the all the input settings for the system model, including the start and the end time of the simulations, the system information (e.g., the size and locations of the dispatchable resources), the operational limits and/or resilience specifications, as well as different cyber-physical adversarial scenarios of interest. Default input files containing IEEE 123-node microgrid network – e.g., default solar profiles, diesel generator parameters, and dispatchable load parameters – are also made available for an easy and quick set-up of the simulations.

After entering all the simulation parameters, system information, and scenarios, the user hits 'RUN ALGORITHM' and lands on the system visualization page. At this page, the entered system

is visualized along with all its controllable resources for the users to verify the accuracy of the entered information. Different types of resources are associated with different keys to clearly mark those out on the network. Zoom-in and zoom-out options are available, along with options to click on the resources (represented as nodes/circles) to see additional information about those resources. The input settings and parameters are also made accessible on the left panel, which can be modified to re-run the ALERT optimization on the selected scenario.

ALERT Grid Resiliency Application			LOGIN 🛈
MODEL INPUT VIZ SETTINGS INPUT SIMULATION PARAMETERS Simulation Start Date"	RUN OPTIMIZATION	•••••	
02/17/2023 02:07 AM	G	• • • • • •	STORAGE NODE GENERIC NODE GENERATOR NODE (PV)
Simulation End Date" 02/17/2023 02:22 AM			GENERATOR NODE (DG) UNES
Sele Prote NOA.cor Gen_parameters Better: Preventers Better: Preventers Vertage Laver Bound 0.95			
Voltage lipper Bound 1.05		•••	
Current Network Model"	-		
ATTACK PARAMETERS		SYSTEM VISUALIZATION THE SERIES RESULTS	

Visualize Simulation Outcomes. Once the back-end completes the simulation of the ALERT controls with the entered settings and parameters, the end-user is able to visualize the outcomes via two different sets of plots: *adversarial set (AS) plots* and *time-series (TS) plots*. The user may choose which AS and TS variables (up to two each at a time) are of interest for the plotting purpose, by selecting the appropriate variables from the drop-down lists, as illustrated below.

NUCL RAVIT VESTINGS NPUT ASSAULTION NAMETERS Standard Into Stand Data Q2077/2023 D222 AM Image: Standard Data Standard Data Standard Data Standard Data Standard Data Q2077/2023 D222 AM Image: Standard Standard Data Standard Data Standard Data Standard Data Quarter D	0 v 29	
Tendents Index	C * 29	
traument behaves 20/1 7/2023 202 22 AM CD Show how Show how Show		-
Adversarial Set Pior 1 Product Pior terms Series Pior 1 Product Provide Pior 1 Product Provide Pior 1 Product Pior terms Pior Pior Pior Pior Pior Pior Pior Pior		
AS X Ave Label Tene Voltage toper tourid	Plast A Plast B Plast C	
1.05 Adversarial Set Piot 2 Time Series Piot 2	Phase A Phase B Phase C	

Grid Resiliency Application							LOGIN (
MODEL INPUT VIZ SETTINGS		FILTERS AS 1 Options AS 1 Y-Asis	AS 2 Options AS 2 X-Jan	TS 1 Options Type	Das	TS 2 Options	
Simulation Start Date" 02/17/2023 02:07 AM		Load Bus -	DG Unit -	Aggregate - A	-	Battery SoC - Voltages	29 -
Simulation End Date*	-					Battery SoC Diesel Generation	
ter Prote NDA.cor Gen_parameters Gen_parameters Vib_parameters Vib_parameters Vib_parameters 0.05 votage itsper Bound		1.0.1 用用 HALL AND THEN WAS ADD THEN HALL AND THE HALL AN	Adversarial Set Plot 1	13 14 15 15 10 10 10 10 10 10 10 10 10 10 10 10 10	Time Series Plot 1	PV Solar Battery Inverter Aggrepate - Active Aggrepate - Reactive	4)
1.05 Current Network Model*	*	200 180 100 2	Adversarial Set Plot 2	000 090 094 004 0.00 0.00	Time Series Plot 2	Plase A Plase B Plase C	

Once the AS and TS options are selected, the user clicks on 'START' to view the results in a streaming fashion in the form of both AS and TS plots. As time progresses, the AS plots show the updated adversarial sets of the selected AS variables, informing the user of the time-varying tolerance of the system to adversarial perturbations in the selected variables – with larger sets demonstrating greater tolerance (and less sensitivity) to adversarial perturbations. Similarly, the TS plots show the resulting time-varying values of the selected TS variables as a result of the ALERT controls. The 'RESET' option allows the user to view the results again by selecting different sets of AS and TS variables.

MODEL INPUT VIZ SETTING				
		HESET HESET		
INPUT SIMULATION PARAMETERS		Adversarial Set Plot 1	Time Series Plot 1	
02/17/2023 02:07 AM		2000 1.500 - 1.000 -	2.5 2.0 3.0 3.0 3.0 3.0 3.0 3.0 3.0 3.0 3.0 3	
Simulation End Date"		3	Applantery (Active	
02/17/2023 02:22 AM		-100 100 -	10 mm	
Solar Profile NOA.csv		 -1000 - -2008 - -1000 - 	5 10	
Generator Parameters Gen_params_123.csv		-2.000 -1.000-dos-dos-dos -200 8 são eão são v.doo-doo-doo A5 X Aves Lebert	alon Kalimerkalasi ka ka ka ka ka sa ba kalasi kalasi ka sa ka ka ka ka ka Time	
Battery Parameters vb_params_123.csv		Adversarial Set Plot 2	Time Series Plot 2	
Voltage Lower Bound		2.000	20.000 P (37W) - Phase A	
0.95		3 200-	26.000 Planar C O (Med) - Planar C O (Med) - Planar C O (Med) - Planar C O (Med) - Planar C	8
Voltage Upper Bound		9	0 (Marc)-Phase	v
1.05		2 -1.00 - 22 -1.000 -	K0.900	
Current Network Model*		-2.000 -		
IEEE123	-	-1000	12:08 12:10 12:18 12:20 12:28 12:30 12:38 12:40 12:48	
ATTACK PARAMETERS		ADAAnsaad	SUALIZATION THE SERIES RESULTS	LOGIN ()
ATTACK PARAMETERS Nove Trace ALERT Grid Resiliency Application		ATXANLAR DISTRICT	THE LEASE HEALTS	LOGIN ()
ATTACK PARAMETERS Nove Two ALERT Grid Resiliency Application	<u> </u>		THE REAL PROCESSION OF THE REAL PROCESS	LOGIN ()
ALERT Grid Resiliency Application MODEL INVIT	- L 		THE SHOEL BALLS	LOGIN ()
ALERT Grid Resiliency Application MODELINITY V2 BITTING		Alt Xon Lear BIO Adversarial Ser Port 1	Tone Series Pert 1	LOGIN ()
ALERT Grid Resiliency Application MODELINITY V2 ETTING INNULATION PARAMETERS Stretch Text Topic	i i	Alt Annual Enter Adversarial Set Port 1	Time Series Plot 1	LOGIN 🔘
ALLERT Grid Resiliency Application MODELING CONTRACTOR MODELING CONTRACTOR MODELING M	6	Al Vociaer Altreaction Adversarial Set Pres 1	Time Series Port 1	
ALLERT Grie Reutlency Application MODEL Beutlency Application MODEL Beutlency Application MODEL Beutlency Application SHULL TON PARAMETERS Structure for Service 92/17/2033 02:07 AM Services De Cort AM		Alt Vociaer	The Series Port 1	LOGIN ()
ALLERT Grid Resiliency Application MODELINUT WIDELINUT MODELINUT WIDELINUT MANAGEMENT (2017)203203 2027 AM Tendens better (2017)20320 2027 AM Tendens better (2017)20320 2027 AM	0	All Variant Morener Adversarial Ser Port 1	Time Series Plot 1	LOGIN ()
ALLERT Gits Resiliency Application MODEL HOLD MODEL HOLD MODEL MODEL HOLD MODEL	a a	All Annual WITTER AL All Annual All Ann	THE Series Plot 1 THE Series Pl	L063N ()
ALLERT Gits Resiliency Application MODEL NUME MODEL NUME MODEL NUME MODEL NUME MODEL NUME NUM NUME NUM NUME NUME NUME NUME NUME NUME NUME NUME NUME NUME NUME NUME NUME N	C3 C3	Alt Anstant TOTO	THE SERIES POINT THE SERIES P	LOGINI ()
ALLERT GIG Sealinery Application MODEL HOLD MODEL HOLD MODEL HOLD V2 BETTHEO MODEL HOLD V2 BETTHEO V2 BETTHEO MODEL HOLD V2 BETTHEO MODEL HOLD V2 BETTHEO MODEL HOLD V2 BETTHEO MODEL HOLD V2 BETTHEO MODEL HOLD V2 BETTHEO MODEL HOLD V2 BETTHEO V2 BETH		Alt Ansister TOTO	THE SERIES PLOT THE SE	LOSIN ()
ALLERT Grid Realitery Application MODEL HOLD MODEL HOLD MODEL MODEL HOLD MODEL HOLD MODEL MODEL HOLD MODEL MODEL HOLD MODEL MODEL HOLD MODEL MO		Alt Ansister TOTO	THE SERIES POINT THE SERIES P	LOGINI
ALCOR PRAMETERS Non-Tool ALCOR PRAMETERS ALCOR Resultency Application ALCOR Resultency Application ALCOR Results ALCOR Result ALCOR RESULT ALCOR RESULT ALCOR RESULT ALCOR RESULT ALCOR RESULT		At social TOTO TOTO TOTO Adversarial Set Port 1 Adversarial Set Port 1 Adversarial Set Port 1 Adversarial Set Port 1 Adversarial Set Port 2 Adversarial Set Port 2 Adversarial Set Port 2 Adversarial Set Port 2	THE SERIE PLET THE SERIE PLET	L0649 ()
Contract PRAAMETERS Known how Contract Prevailing Con		Al Social Description Adversaria de Port 1 Adversaria de Port 2 Adversaria de Port 2	THE SERIE PER 1 THE SE	LOGHN ()
ATTACK PRAAMETERS Wate here: ALLERT Gits Resiliency Application MODEL NUMP: V2 detTimed INDUITION PRAAMETERS INDUITION PRAAMET	6	Alt souther TOTO	The Series Pier 1 The Series Pi	LOGMI ()

4.0 Conclusions

In this report, we provide a brief introduction to the user-interface tool demonstrating the performance of the ALERT controls to ensure resilience of a microgrid under various cyber-physical adversarial scenarios. While the current implementation demonstrates some key functionalities of the user-interface, future developmental efforts will focus on generalizing the interface to other cyber-physical system applications, along with a deployment of the application to the cloud for wider access to users who would like to test the ALERT functionalities.

References

- [1] N. Nazir, T. Ramachandran, S. Bhattacharya, A. Singhal, S. Kundu, V. Adetola, Optimizationbased resiliency verification in microgrids via maximal adversarial set characterization, in: 2022 American Control Conference (ACC), 2022, pp. 2214–2220. doi:10.23919/ACC53348. 2022.9867826.
- [2] N. Nazir, T. Ramachandaran, S. Kundu, V. Adetola, Improved microgrid resiliency through distributionally robust optimization under a policy-mode framework, in: 2024 IEEE PES General Meeting (available online at: arXiv preprint arXiv:2210.12586), 2024 (Submitted).
- [3] X. Bai, L. Qu, W. Qiao, Robust AC optimal power flow for power networks with wind power generation, IEEE Transactions on Power Systems 31 (5) (2015) 4163–4164.

Pacific Northwest National Laboratory

902 Battelle Boulevard P.O. Box 999 Richland, WA 99352 1-888-375-PNNL (7675)

www.pnnl.gov