Automating the Process to Quantify Cyber-Physical Risk with Contingency Analysis and User Input

Hao Huang, *Student Member, IEEE,* Dustin Gray, Juan Mendoza, Katherine Davis, *Senior Member, IEEE*
Department of Electrical and Computer Engineering Texas A&M University, College Station, TX, USA
Email: hao_huang@tamu.edu, blake1227@tamu.edu, juaners98@tamu.edu, katedavis@tamu.edu

2021 North American Power Symposium (NAPS) | 978-1-6654-2081-5/21/$31.00 ©2021 IEEE | DOI: 10.1109/NAPS52732.2021.9654646

***Abstract*—Obtaining enough situational awareness is a critical task for power system security and reliability. With thousands of devices and various adversaries, it is hard to assess the impact of those devices under adversaries on power systems. The lack of enough situational awareness can lead the operators to misunderstand the system and make inappropriate decisions. Thus, this paper presents a framework to consider different types of contingencies for a comprehensive device-oriented risk assessment.**

The proposed framework considers three aspects, including the *Steady State Contingency*, *Transient State Contingency*, and *Device Model Validation*. Corresponding metrics have been utilized to evaluate the power system elements with respect to power system security. With the input information, the proposed framework streamlines and automates the process of quantifying the risk of different devices through different types of contingency analyses and metrics. In this way, operators can get comprehensive situational awareness to ensure the security of the system and avoid potential cascading failures. This paper uses the synthetic 200-bus case (ACTIVSg200) to illustrate the process of quantifying cyber-physical risk using the proposed framework.

***Index Terms*—Cascading failure, Power system contingency analysis, Power system transient stability**

I. Introduction

Modern power grids consist of thousands of cyber and physical devices. The integration of intelligent electronic devices (IEDs) and communication networks improves power systems' observability, controllability and efficiency. Meanwhile, there are also increasing cyber and physical adversaries that can cause the malfunction of those devices, making the system vulnerable and fail to deliver energy properly. Any misoperation of either the cyber or the physical device can reduce the system's reliability and cause disturbances to the whole grid. For example, the 2003 North America Blackout is because of the insufficient reactive power supply causing multiple relays tripped and lost over 400 transmission lines and 500 generating units [1]. The 2016 Ukraine cyber attack is due to the compromised communication network, allowing outsiders to control and isolate the substation [2]. Such incidents highlight the importance of the power system cyber-physical situational awareness. It is essential to identify the critical elements and assess their impact on the whole system if they are compromised or out of control.

A lot of works have been done to identify the critical contingencies from both steady and transient state. The most common steady state contingency analysis is the *N-1* contingency analysis, which considers the loss of one element in the system and solve the power flow equations to check whether the system is within operating limits. This is a basic guideline for reliable power system planning and operation [3]. In [4], Fu and Bose present several ranking indices for power system dynamic security analysis based on coherency, transient energy conversion, dot products, and their composite. In [5], Deuse *et al.* introduce a dynamic security assessment tool to comprehensively analyze the dynamic contingencies within a network to identify its weak, critical or vulnerable elements. Besides, with the integration of IEDs, several works have been done to identify the critical cyber-physical elements in the system based on both cyber and physical data [6]–[9]. Even though these emerging indexes are proposed to rank power system elements from both cyber and physical domains, they are still based on contingency analysis, power flow equations, and energy functions to capture the cyber adversaries' impact in power systems. Thus, the contingency analysis is still useful and necessary for capturing and quantifying the impact of different adversaries.

With the increasing number of devices in modern power grids, various approaches have been proposed to identify the critical elements efficiently. In [10], Davis and Overbye propose a method to efficiently determine double contingencies that can cause system violations. In [11], Mittal *et al.* propose a scalable parallel implementation of a probabilistic contingency analysis scheme only for most severe and most probable contingencies. In [12], Yan *et al.* utilize the self-organizing map and electrical charateristics to assess the vulnerability and cascading effects of multiple component sets in the power grid. In [13], [14], authors proposed a graph theory based approach to identify critical *N-x* contingencies using line outage distribution factors (LODFs). However, those approaches are focused on identifying critical elements but not assessing their impact. For operators, it is essential to obtain information of critical elements and their impact to power systems so that they can better allocate their resource to protect them against cyber and physical adversaries.

The challenge of the risk assessment for cyber-physical power systems associates is the immense potential outcomes from cyber and physical adversaries. The adversaries can influence the power systems operation, the transient stability, devices' functionality, etc. To quantify the impact, it is necessary to utilize contingency analysis with specified considerations. Thus, this paper proposes a framework that streamlines the process of performing device-oriented contingency analyses, including the *Steady State Contingency*, *Transient State Contingency*, and *Device Model Validation*. It quantifies the cyber-physical risk to power systems with corresponding metrics.

The main contributions of this paper are as follows:

1) This paper presents a framework to streamline the process of steady and transient state contingencies for

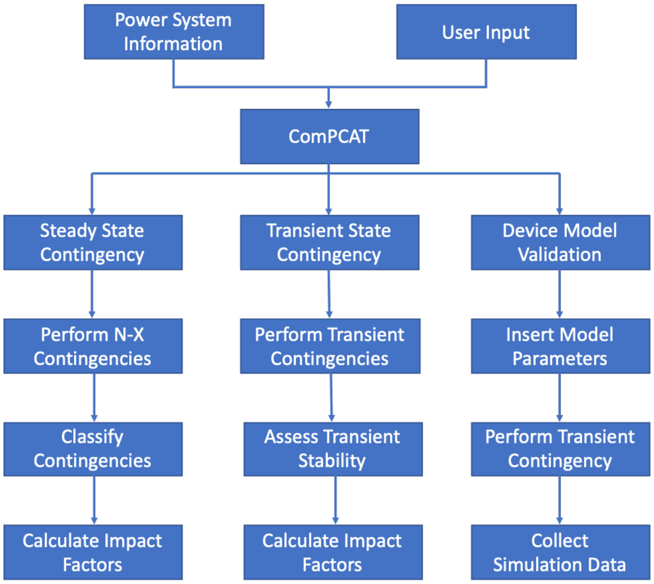


Figure 1. The framework Device-Oriented Power System Contingency Analysis (DOCAT).

different power system devices to assess their impact in power systems under different adversaries.

2) A tool, called *DOCAT*, has been developed based on the proposed framework and its use to automatically quantify the cyber-physical risk is presented with a synthetic 200-bus case (ACTIVSg200). The code is available at *https://github.tamu.edu/hao-huang/DOCAT*.

The paper is organized as follow. Section II presents the framework of device-oriented contingency analysis to evaluate the risk of power system devices with specific considerations. Section III shows the *N-3* contingency analysis with *DOCAT* for the ACTIVSg200 case. Section IV shows the *Transient State Contingency* analysis to assess all branches' critical clearing time and transient impact index in the ACTIVSg200 case. Section V demonstrates the relay model (**TIOCR1**) validation for one branch in the ACTIVSg200 case.

II. Framework of Device Oriented Contingency Analysis

Figure 1 shows the framework of device-oriented power system contingency analysis that considers three types of contingency analysis, including the **Steady State Contingency**, **Transient State Contingency**, and **Device Model Validation**. For **Steady State Contingency** and **Transient State Contingency**, it performs analysis and provides different indexes to rank contingencies. **Device Model Validation** focuses on validating the model parameters with corresponding contingencies to evaluate the performance.

Based on the proposed framework, authors have built a tool, *Device-Oriented Contingency Analysis Tool (DOCAT)*, to streamline and automate the process of quantifying cyber-physical risk with contingency analysis and user input. With PowerWorld Simulator [15] and Easy SimAuto (ESA) [16], the *DOCAT* automatically generates Auxiliary Files (.aux) and performs all analyses based on users' input information. Then, it collects and organizes the results for users to better understand the impacts of the corresponding element(s). Moreover, the *DOCAT* utilizes different indexes to evaluate corresponding element(s) from both steady and transient contingencies regarding to their functionality.

For **Steady State Contingency Analysis**, the *DOCAT* automatically performs *N-x* contingencies based on the case information and user's input of device type and x. Based on the results, it will classify the contingencies into *Violations*, *Reserve Limit*, *Unsolved*, *Load Isolation* and *Generator Isolation*. For the contingencies that cause violations with overflows and voltage over limits, we use an *Impact Factor* to evaluate their composite impact by summed up normalized values of violations. If the case is large, making it hard to perform all *N-x* contingencies, the *DOCAT* would ask the information of specific device(s) the user wants to consider to reduce the total number of contingencies to analyze. This is a practical consideration. When a certain device is suspected as compromised by cyber or physical adversary, the *DOCAT* can generate all related contingencies instead of a full contingency list, which maintains the target of evaluating suspected element(s) and also improves efficiency.

As for **Transient State Contingency**, the *DOCAT* focuses on the assessment of critical clearing time (*CCT*) and related metric for buses and branches when there are physical faults in the system. The *CCT* is the maximum fault duration time the system can have without causing violations on the transient stability requirement [17]. It represents the importance of each element's protective relay in the system. Besides, in [18], Huang and Davis propose a transient impact index (*TII*) with *CCT* to quantify the impact of a compromised protective relay in the system if it clears a fault after the *CCT*. The *DOCAT* would request the information of *Device Type*, *Clear Fault Action*, and *Perturbation* for calculating *TII*. With the information, the *DOCAT* can generate corresponding *Transient State Contingency* and perform the analysis automatically.

Regarding to **Device Model Validation**, the *DOCAT* analyzes the functionality of different devices. In this paper, the *DOCAT* focuses on the protective relay model of **TIOCR1**. With *User Input* of the relay model parameters, the *DOCAT* will generate corresponding contingency to validate the input's parameters and its functionality with transient state analysis. The *DOCAT* would generate the contingency of physical fault at a specified branch and examine whether the relay can fulfill its function satisfying the requirements. *DOCAT* will inform the users how the relay's performance is based on the specified transient limit monitors.

The following sections present the details of the algorithms and indexes for each type analysis.

III. Steady State Contingency Creation and Analysis

This section shows the algorithm and indexes that are used in **Steady State Contingency**. Algorithm 1 shows the algorithm of how the *DOCAT* generates the contingencies and processes the results. For different scenarios, users can specify device type: branch, bus, generator, or substation. With specified x, the *DOCAT* automatically generates all contingency combinations. As mentioned earlier, if the total number of contingencies is too large, it will take a long time to finish all contingency analysis. Thus, there is a pre-defined limit of the total number of contingencies to make the analysis more efficiently. The *DOCAT* will ask for more information to reduce the number of contingencies need to be analyzed at one time. The extra information can be specified elements that must be included in the contingencies. In this way, when some elements have been identified as compromised, the *DOCAT* can generate all related contingencies to efficiently assess the impact. It ensures the efficiency of performing contingency analysis and also maintain the effectiveness of assessing critical elements.

Algorithm 1 Steady State Contingencies Based on User's Input

```
Input = Device Type, X
Calculate all $N - X$ Contingencies
while the number of contingency is over 10000 do
    Ask User to Add n Elements (n<X)
    Specific the new elements
    Get reduced $N - X$ Contingencies
end while  Generate Aux File for Steady State Contingency Analysis
Run Contingency Analysis
Collect the results
Classify the results into Violations, Unsolved, Reserve Limit, Load Isolation, and Generator Isolation
Compute Violation Impact Index as Equation (1)
Identify the most critical contingency for overflow and voltage instability respectively
```

After obtaining the analysis results, the *DOCAT* classify the contingencies into: *Violations*, *Unsolved*, and *Reserve Limit*, *Load Isolation*, and *Generator Isolation*. The *Violations* has all contingencies that can cause the system's operation under stress. It specifies the number of violations regarding to voltage and power flow violations that the bus voltages and branch power flows are over their required operating limits. To better compare the contingencies' violations with both voltage and overflow violation, the *DOCAT* also generates *Impact Factor* based on a security index from [19] as shown in Equation (1). This metric uses normalized value of voltage and power flow violation to quantify the impact of the contingency since voltage and overflow violations associate with the distribution of real and reactive power over the system. Because the voltage violation can be either over voltage or under voltage and the normal voltage p.u. is 1, the normalized value of voltage impact is the absolute value of voltage instability minus 1. To equally consider the impact of overflow, Equation (1) uses the overflow percentage, which is over 100%, minus 1.

$$\begin{aligned} Impact\ Factor = &\sum(overflow\ percentage - 1) + \\ &\sum abs(voltage\ instability - 1) \end{aligned} \tag{1}$$

The *Unsolved* has all contingencies that can cause the power flow cannot be solved, and *Reserve Limit* has all contingencies that islands do not have enough makeup generation capacity. The load and generator connection is critical for energy supply. Thus, the *DOCAT* also provides the *Load Isolation* and *Generator Isolation* specifying all contingencies that can cause load and generator are disconnected from the main grid, respectively.

The **Steady State Contingency Analysis** has been tested with ACTIVSg200 [20] to run *N-3* contingency analysis for all buses. However, the total number of contingency is 161700, which is over the predefined limit of 100000. Thus, the *DOCAT* requests more elements to include. We specify two buses must be included, which are *Bus 1* and *Bus 2*. After the analysis is done, there are 4 contingencies cause violations, 1 contingency causes the power flow unsolved, 3 contingencies cause reserve limit, 196 contingencies have load isolated and 55 contingencies have generator isolated (All *N-3* contingencies must have *Bus 1* and *Bus 2*).

Table I, II, and III shows *N-3* contingencies that cause *Violations*, *Unsolved*, and *Reserve Limit* in the system respectively. For all tables, *DOCAT* provides the *Contingency* and *Contingency Elements* so that users can quickly identify what combination of elements are critical. In Table I, it provides the total number of violations and the number of violations for branch power flows and bus voltages respectively. With the *Impact Factor*, we can see the *Contingency N-3_130*, when *Bus 1*, *Bus 2*, and *Bus 133* are out, cause the most number of violations in the system, making its *Impact Factor* the highest. Table II shows the only *N-3* contingency that can cause the system unsolved, which is when *Bus 1*, *Bus 2*, and *Bus 149* are out of service. Table III shows *N-3* contingencies cause the reserve limits. From the tables, we can see the *Contingency N-3_130* and *Contingency N-3_186* appear in both Table *Violations* and *Reserve Limit*. With *DOCAT*, users can obtain such information in an efficient and clear manner. There are also other tables for *Load Isolation* and *Generator Isolation*. Due to the page limit, they are not shown here.

Table I
N-3 CONTINGENCIES WITH *Bus 1* AND *Bus 2* THAT CAUSE VIOLATIONS

Contingency	Contingency Elements	Total Violations	Impact Factor	Flow Violations	Voltage Violations
Contingency N-3_120	['Bus 1', 'Bus 2', 'Bus 123']	7	0.766	0	7
Contingency N-3_125	['Bus 1', 'Bus 2', 'Bus 128']	1	0.101	0	1
Contingency N-3_130	['Bus 1', 'Bus 2', 'Bus 133']	31	3.813	1	30
Contingency N-3_186	['Bus 1', 'Bus 2', 'Bus 189']	1	0.012	1	0

Table II
N-3 CONTINGENCIES WITH *Bus 1* AND *Bus 2* THAT CAUSE POWER FLOW UNSOLVED

Contingency	Contingency Elements	Lable
Contingency N-3_146	['Bus 1', 'Bus 2', 'Bus 149']	Unsolved

IV. TRANSIENT STATE CONTINGENCY CREATION AND ANALYSIS

Transient Contingency Analysis associates with the small signal perturbation analysis and see how the system reacts in transient state. Different devices have different levels of tolerance to the perturbation for their safety and the system's stability. With the transient contingencies, *DOCAT* utilizes the

Table III
N-3 CONTINGENCIES WITH *Bus 1* AND *Bus 2* THAT CAUSE RESERVE LIMITS

Contingency	Contingency Elements	Label	LoadMW	GenMW
Contingency N-3_130	['Bus 1', 'Bus 2', 'Bus 133']	RESERVE LIMITS	10.82	418.97
Contingency N-3_184	['Bus 1', 'Bus 2', 'Bus 187']	RESERVE LIMITS	10.82	0
Contingency N-3_186	['Bus 1', 'Bus 2', 'Bus 189']	RESERVE LIMITS	10.82	0

CCT to evaluate each device's ability to withstand physical fault. It also uses the *TII* [18] to evaluate the impact to the system if the fault stays longer than *CCT*, as follow:

$$TII(r(i)) = \min\{(f_{max-c} - f_{max-o}), 5\} \tag{2}$$

where the $r(i)$ represents the digital relay in the system. The f_{max-c} is the maximum frequency in the system if the digital relay is compromised and clear the fault after the *CCT*. The f_{max-o} is the maximum frequency in the system when the fault is cleared at the *CCT*. If the difference is bigger than 5Hz, there will be a cascading event making the system completely unstable. Thus, the TII has a maximum value of 5.

Algorithm 2 shows the process of how the *DOCAT* generates transient contingencies and how to calculate the metrics. The input requires *Device Type*, *Element Identifier*, *Clear Fault Action*, and *Perturbation*. Currently, the device type has two options, branch and bus, to assess their *CCT* and *TTI*. The running time of the transient contingency analysis depends on the case, thus the *DOCAT* allows run the analysis for all buses or branches at one time or choose a specific device with its identifier, such as the bus number. For large systems, it is suggested to run the analysis for a particular device due to the computation time. The *Clear Fault Action* has two options as well, *Clear Fault* and *Open the Faulted Element*. The *Clear Fault* simply removes the fault from the system without changing the system's topology. The *Open the Faulted Element* will open the faulted device, which removes the fault from the system and changes the system's topology.

Algorithm 2 Transient State Contingencies Based on User's Input

```
Input = Device Type, Element Identifier or All, Clear Fault
    Action, Perturbation
Generate Aux File for CCT function
Generate Aux File for Transient Contingency Analysis
Load WECC transient reliability requirement
Run Transient Contingency Analysis
Get the CCT result for corresponding elements
Generate Transient Contingency Analysis with 3 Phase
    Solid Fault with for the device based on Input information
Clear Fault at CCT and collect frequency result
Clear Fault at CCT with Perturbation and collect fre-
    quency result
Calculate TII as Equation (2)
Run Contingency Analysis
Collect the results
```

In this section, we run the **Transient State Contingency** for all branches in the ACTIVSg200 and calculate the *CCT* and *TII* with a perturbation of 0.02 seconds. The evaluation of *CCT* is based on the bisection method [21], so it is necessary to load the *Transient Limit Monitor* to define what time to clear the fault can keep the system stable and satisfy the limit monitor. Currently, the tool utilizes the *WECC* reliability requirement [22] as limit monitor, which monitors the *Non-Load Bus Voltage Dip*, *Load Bus Voltage Dip*, *Load Bus Voltage Dip Duration*, and *Bus frequency* during transient contingency.

In Table IV, it shows five branches with 5 highest *TTI* in the system. From the Table, it has *Branch*, *Critical Clearing Time*, *Perturbation*, *Clear Fault Action*, *TII*, and *Comment*. *Branch* shows the element information with *From Bus Number*, *To Bus Number*, and *Circuit ID*. *Critical Clearing Time* is the CCT results based on the user's input of *Clear Fault Action*. The *Perturbation* is for calculating *TII*. The *Comment* is an extra note for the *TII*. If the *TII* is over 5, which means the system will be *Unstable* when the fault is cleared after CCT plus *Perturbation*. If the *TII* is less than 5, then the system will be *Stable*. There is another *Comment*, *Unavailable*, which happens when the CCT information is not available. For a particular device, if it connects to an important generator, the fault happens to that branch/bus can cause the system unstable without the value of CCT.

From Table IV, the *Branch {'66','158','1'}* has the shortest *CCT* and largest *TII*. However, the second important branch, *Branch {'53','48','1'}*, has longer *CCT* than the other three branches, which means it can withstand the fault longer without causing system unstable. While, with a small perturbation of clearing fault, the fault at that branch can even cause more instability to the system than others. This shows the importance of assessing elements with further consideration.

Table IV
TRANSIENT STATE CONTINGENCY ANALYSIS

Branch	CCT (second)	Perturbation (second)	Clear Fault Action	TTI	Comment
Branch '66' '158' '1'	0.118	0.02	CLEARFAULT	0.259	Stable
Branch '53' '48' '1'	0.305	0.02	CLEARFAULT	0.203	Stable
Branch '73' '66' '1'	0.268	0.02	CLEARFAULT	0.194	Stable
Branch '123' '133' '1'	0.136	0.02	CLEARFAULT	0.183	Stable
Branch '48' '5' '1'	0.296	0.02	CLEARFAULT	0.168	Stable

V. PROTECTIVE RELAY PARAMETERS VALIDATION

The idea of *TII* originates from a *'What If'* question that the protective relay's settings are falsified by adversaries. Protective relay is a critical cyber-physical device in power systems that connects the cyber and physical networks. Its function is to protect the system against faults in the system by clearing fault based on its parameters. With the analysis in Table IV, a slightly delay on the relay operation can cause big disturbances in power systems. It is essential to study it based on the mathematical model. Thus, the *DOCAT* has a specific function of **Device Model Validation** for protective relay studies. Currently, *DOCAT* supports the analysis of **TIOCR1**.

The **TIOCR1** is a time inverse line overcurrent relay. The *TimeToClose* varies according to the piece-wise linear function of per unit current as shown in the Figure 2 and as specified by the input values *Threshold*, *m1...m5*, and *t1...t5*. If m1 is greater than 1.0, then an additional point at the *Threshold* current of 1 hour (3600 seconds) is added to the curve [15]. The Equation (3) and (4) show the relay operation and reset based on the *Threshold Current*, *TimetoClose* and *TReset*. Figure 3 shows an example of **TIOCR1** time-overcurrent curve, where the blue curve is the reset curve and the red curve is the operate curve. The Equation (3) is used to decide when the relay will close if the fault current is over the *Threshold Current*. Based on the **TIOCR1** model and fault current, there is a corresponding *TimeToClose* value. With the Equation (3), when θ equals to 1, the relay will close and trip the circuit breaker after the *Breaker Time* (seconds) have elapsed. The Equation (4) is to reset the relay if the fault current is under the threshold current. With the **TIOCR1** model, there is also a reset curve. If the *TReset* is 0, then the relay will be reset, and not trip the circuit breaker after the fault current is under the *Threshold Current*. Otherwise, based on the fault current and *TimeToClose* value, when θ equals to 1 based on the Equation (4), the relay will close.

$$\theta = \int \frac{1}{TimetoClose}\, dt \tag{3}$$

$$\theta = \int [1 - (\frac{Icurrent}{Threshold})^2][\frac{-1}{TReset}]\, dt \tag{4}$$

Algorithm 3 Protective Relay Model Validation

```
Input = Device Type, Element Identifier, Relay Model Parameter
Generate Aux File for the Device for the Case
Generate Aux File for Transient Contingency Analysis with 3 Phase Solid Fault with for the device based on Input information
Run Transient Contingency Analysis
Get the results
Check whether the voltage and frequency satisfy the requirement
Provide feedback about the Relay Model Parameter
```

Algorithm 3 shows the process of how the *DOCAT* generates the relay model and analyzes whether the input from users satisfies the requirement. Since **TIOCR1** is a line overcurrent relay, *Device Type* in this paper is *Branch*. The user needs to specify the *Element Identifier* for the branch and the relay model parameters. Then, the *DOCAT* generates the aux file for transient analysis with fault for the target branch. Based on the result from transient analysis, *DOCAT* can check whether the relay clears the fault within the reliability requirement. Here, we still use the *WECC* reliability requirement as a reference.

From the transient analysis in Table IV, *Branch {'66', '158','1'}* has the largest *TII* and shortest *CCT*, which shows its importance. Thus, we insert the **TIOCR1** model for that branch using the following parameters: *Relay Place: From*, *Threshold: 1.02*, *Reset Time: 5*, *m1,...,m5: 1.05*, *1.1*, *1.15*, *1.2*, *8*, and *t1,...,t5*: *0.04*, *0.03*, *0.02*, *0.01*, *0.001*. Based on Algorithm 3, we apply a three phase fault at *Branch {'66', '158','1'}* and check whether it is satisfied with *WECC* transient reliability. From the requirement of *WECC*, this fault causes the bus voltage of some load bus reduced over 30%. However, other requirements are satisfied.

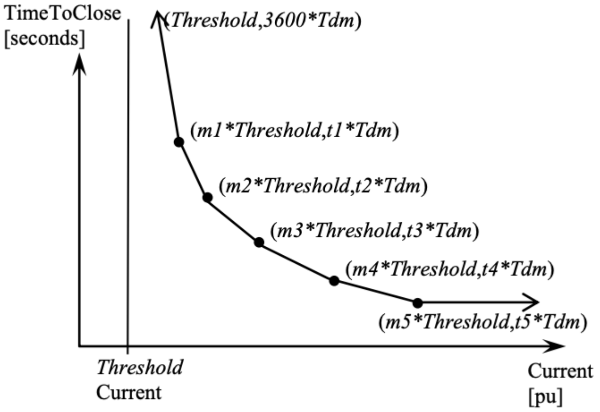


Figure 2. PSS/E TIOCR1 Model [23].

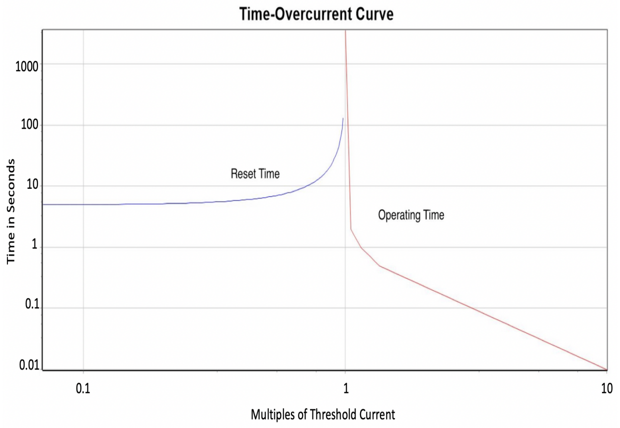
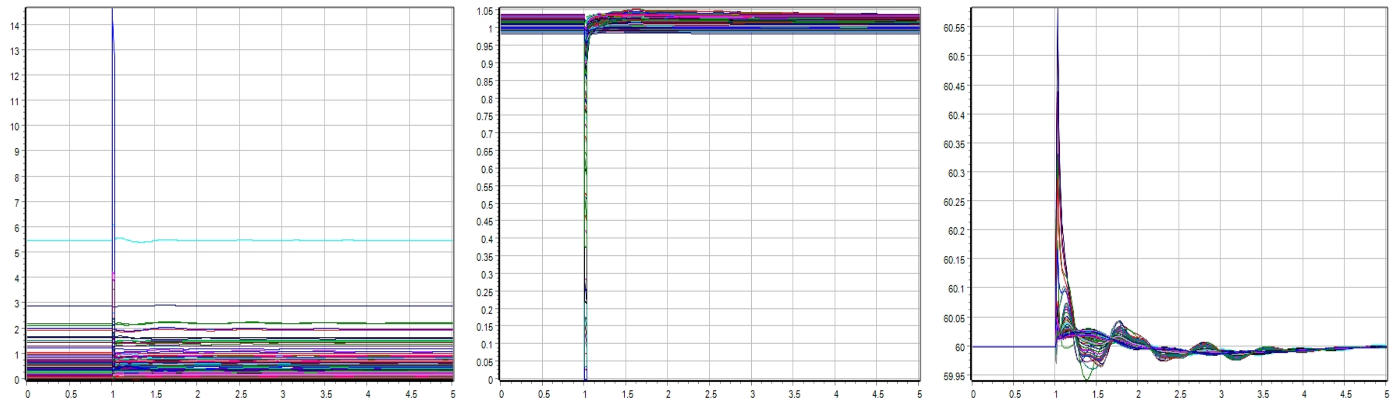


Figure 3. **TIOCR1** Diagram with User's Input (Blue Curve is the reset curve; Red Curve is the operate curve.)

To better analyze the relay operation, Figure 4 shows the transient analysis for **TIOCR1** with above parameters when there is a three phase fault in *Branch {'66', '158','1'}* at 1 seconds. From Figure 4, we can see that the fault is cleared at 1.024 seconds (0.024 seconds to clear the fault), which is less than the critical clearing time. The system keeps stable without any frequency violation and the low voltage duration is also within *WECC* requirement. However, there are still some load buses' voltage reduced over 30% during the fault period, and that is because the fault directly impacts the connected load buses. It shows the relay settings can be applied to ensure the system stability despite some load buses need further protection, such as the load relay.

VI. Conclusion and Future Work

This paper presents a framework to streamline the process for device-oriented contingency analysis in both steady and transient states to quantify the cyber-physical risk to power systems. Based on the framework, authors have developed a tool, *DOCAT*, for operators to automatically perform the analysis based on their needs. With different metrics deployed in *DOCAT*, users can obtain a comprehensive situational



(a) Current p.u. in all branches

(b) Voltage p.u. in all buses

(c) Frequency in all buses

Figure 4. Transient Analysis of Relay Operation in Branch {'66', '158', '1'} with **TIOCR1** relay model.

awareness if a certain device/certain type of device is compromised. With the ACTIVSg200, this paper demonstrates different functionalities of *DOCAT*. The code of *DOCAT* is available at *https://github.tamu.edu/hao-huang/DOCAT*.

In future work, we will incorporate more types of devices in **Transient State Contingencies** based on their functions. Besides, we will also add more relay models in **Device Model Validation** to expand the analysis from branch to bus, load, and generator. Last but not least, the real industrial relay settings and mathematical relay models are different. It is also important to build a function to map them for a more convenient application in the field.

VII. Acknowledgement

The work described in this paper was supported by funds from the US Department of Energy under award DE-OE0000895, the National Science Foundation under Grant 1916142, and Undergraduate Research Scholars.

References

[1] G. Andersson, P. Donalek, R. Farmer, N. Hatziargyriou, I. Kamwa, P. Kundur, N. Martins, J. Paserba, P. Pourbeik, J. Sanchez-Gasca *et al.*, "Causes of the 2003 major grid blackouts in north america and europe, and recommended means to improve system dynamic performance," *IEEE transactions on Power Systems*, vol. 20, no. 4, pp. 1922–1928, 2005.

[2] D. U. Case, "Analysis of the cyber attack on the ukrainian power grid," *Electricity Information Sharing and Analysis Center (E-ISAC)*, vol. 388, 2016.

[3] (2006, mar) The north american electric reliability corporation (nerc). [Online]. Available: https://www.nerc.com/Pages/default.aspx

[4] C. Fu and A. Bose, "Contingency ranking based on severity indices in dynamic security analysis," *IEEE Transactions on power systems*, vol. 14, no. 3, pp. 980–985, 1999.

[5] J. Deuse, K. Karoui, A. Bihain, and J. Dubois, "Comprehensive approach of power system contingency analysis," in *2003 IEEE Bologna Power Tech Conference Proceedings,*, vol. 3. IEEE, 2003, pp. 6–pp.

[6] S. Zonouz, C. M. Davis, K. R. Davis, R. Berthier, R. B. Bobba, and W. H. Sanders, "Socca: A security-oriented cyber-physical contingency analysis in power infrastructures," *IEEE Transactions on Smart Grid*, vol. 5, no. 1, pp. 3–13, 2013.

[7] C. Vellaithurai, A. Srivastava, S. Zonouz, and R. Berthier, "Cpindex: Cyber-physical vulnerability assessment for power-grid infrastructures," *IEEE Transactions on Smart Grid*, vol. 6, no. 2, pp. 566–575, 2014.

[8] K. R. Davis, C. M. Davis, S. A. Zonouz, R. B. Bobba, R. Berthier, L. Garcia, and P. W. Sauer, "A cyber-physical modeling and assessment framework for power grid infrastructures," *IEEE Transactions on smart grid*, vol. 6, no. 5, pp. 2464–2475, 2015.

[9] A. K. Srivastava, T. A. Ernster, R. Liu, and V. G. Krishnan, "Graph-theoretic algorithms for cyber-physical vulnerability analysis of power grid with incomplete information," *Journal of Modern Power Systems and Clean Energy*, vol. 6, no. 5, pp. 887–899, 2018.

[10] C. M. Davis and T. J. Overbye, "Multiple element contingency screening," *IEEE Transactions on Power Systems*, vol. 26, no. 3, pp. 1294–1301, 2010.

[11] A. Mittal, J. Hazra, N. Jain, V. Goyal, D. P. Seetharam, and Y. Sabharwal, "Real time contingency analysis for power grids," in *European Conference on Parallel Processing*. Springer, 2011, pp. 303–315.

[12] J. Yan, Y. Zhu, H. He, and Y. Sun, "Multi-contingency cascading analysis of smart grid based on self-organizing map," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 4, pp. 646–656, 2013.

[13] M. R. Narimani, H. Huang, A. Umunnakwe, Z. Mao, A. Sahu, S. Zonouz, and K. Davis, "Generalized contingency analysis based on graph theory and line outage distribution factor," *arXiv preprint arXiv:2007.07009*, 2020.

[14] H. Huang, Z. Mao, M. R. Narimani, and K. R. Davis, "Toward efficient wide-area identification of multiple element contingencies in power systems," in *2021 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT)*. IEEE, 2021, pp. 01–05.

[15] "PowerWorld Simulator," 2020. [Online]. Available: https://www.powerworld.com/

[16] B. L. Thayer, Z. Mao, Y. Liu, K. Davis, and T. J. Overbye, "Easy simauto (esa): A python package that simplifies interacting with powerworld simulator," *Journal of Open Source Software*, vol. 5, no. 50, p. 2289, 2020. [Online]. Available: https://doi.org/10.21105/joss.02289

[17] T. Miki, D. Okitsu, E. Takashima, Y. Abe, and M. Tano, "Power system transient stability assessment using critical fault clearing time functions," in *IEEE/PES Transmission and Distribution Conference and Exhibition*, vol. 3. IEEE, 2002, pp. 1514–1517.

[18] H. Huang and K. Davis, "Power system equipment cyber-physical risk assessment based on architecture and critical clearing time," in *2018 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*. IEEE, 2018, pp. 1–6.

[19] H. Huang, M. Kazerooni, S. Hossain-McKenzie, S. Etigowni, S. Zonouz, and K. Davis, "Fast generation redispatch techniques for automated remedial action schemes," in *2019 20th International Conference on Intelligent System Application to Power Systems (ISAP)*. IEEE, 2019, pp. 1–8.

[20] A. B. Birchfield, T. Xu, K. M. Gegner, K. S. Shetye, and T. J. Overbye, "Grid structural characteristics as validation criteria for synthetic networks," *IEEE Transactions on Power Systems*, vol. 32, no. 4, pp. 3258–3265, July 2017.

[21] S. Aboreshaid, R. Billinton, and M. Fotuhi-Firuzabad, "Probabilistic transient stability studies using the method of bisection [power systems]," *IEEE Transactions on Power Systems*, vol. 11, no. 4, pp. 1990–1995, 1996.

[22] Western Electricity Coordinating Council, "WECC Reliability Criteria," 2004.

[23] P. Siemens, "Pss/e 32 model library," *PSS/E Manual*, 2009.