# MALICIOUS ATTACK DETECTION AND ANALYSIS

## CLAIM OF PRIORITY

**[0001]** This application claims the benefit of priority of United States Provisional Application No. 61/346,787 filed on May 20, 2010, the entirety of which is hereby incorporated by reference.

## BACKGROUND

1. Field of the Invention

**[0002]** The present invention relates generally to a system and method for detecting and identifying undesired events in intelligent utility grid systems, and more particularly to a system and method for detecting and identifying malicious attacks on an intelligent utility grid system.

2. Related Art

**[0003]** The objective of Internet Protocol (IP), Industrial Control System (ICS), Physical Control System, and Supervisory Control and Data Acquisition (SCADA) attacks on the Smart Grid is to bypass the grid's normal operation by exploiting one or more weaknesses (e.g., Radio Frequency (RF) jamming wireless nodes on the grid, key derivation, flashing firmware, anonymous inputs from inappropriate entities, physical hardware tampering). Many of these risks have well-defined solutions that are addressed by either ICS/SCADA security controls, physical security controls, or enterprise information technology (IT), operational, or physical security controls. Residual Risk is the remaining risk after the security controls have been applied. Most systems are never fully secure, and residual risk always remains. When faced with the cyber-security challenges of the smart grid, a residual security risk remains that is beyond the typical risks mitigated by SCADA, enterprise IT, operational, or physical security controls.

## BRIEF SUMMARY

**[0004]** According to one aspect of the disclosure, there is provided a method of characterizing malicious activity in an intelligent utility grid system, the method executable by a computer having at least one processor and at least one memory, including: ~~may include~~ receiving, by the at least one processor, information-technology (IT) data including IT-related activity from the intelligent grid system. The method may further include receiving, by the at least one processor, non-IT data including location-specific event data from a plurality of electronic sources~~.~~, grid analog measurements including phasor measurements; and a list of high-value targets and corresponding geographic locations. The non-IT data,

as will be explained in more detail later, includes information-technology-related information (or data) that is not traditionally used by a power grid as well as information such as historical data and addresses or locations of high value targets. The method may further include pre-processing, by the at least one processor, the non-IT data including: disregarding the non-IT data failing to meet a predetermined level of relevance to one of a plurality of risk-related events. The method may further include applying, by the at least one processor, a plurality of rules to the pre-processed non-IT data including~~to~~: associating~~associate~~ an undesired event with reference to the IT-related activity; and determining~~determine~~ a probability that the undesired event is indicative of malicious activity including comparing predetermined criteria to the non-IT data to generate one of a plurality of probability levels as a sum of: (1) a product of a probability of occurrence of an intentional malicious attack and a probability of existence of a vulnerability exploitable by the intentional malicious attack; and (2) a product of a probability of occurrence of an unexpected hazard and a probability of existence of a vulnerability associated with the unexpected hazard, where the intentional malicious attack and the unexpected hazard include mutually independent events. The event may have already occurred or may not yet have occurred. The method may further include applying, by the at least one processor, a risk characterization to the undesired event based on the probability level and the IT-related activity.

**[0005]** According to another aspect of the disclosure, there is provided a system for characterizing malicious activity in an intelligent utility grid system may include a system storage in which to store a database including a plurality of rules. A collector may be operable to collect and store in the system storage information-technology (IT) data including IT-related activity from the intelligent grid system. A complex event processing (CEP) bus may be operable to receive non-IT data including location-specific event data from a plurality of electronic sources, the CEP bus further operable to disregard the non-IT data failing to meet a predetermined level of relevance to one of a plurality of risk-related events~~.~~, where the non-IT data further includes historical data retrieved from: event logs, geographical location associated with corresponding parts of the intelligent utility grid system, and from operational data. A processor may be operable to apply the plurality of rules to the relevant non-IT data including to: associate an undesired event with ~~reference to~~ the IT-related activity; and determine a probability that the undesired event is indicative of malicious activity including comparing predetermined criteria to the non-IT data to generate one of a plurality of probability levels as a sum of: (1) a product of a probability of occurrence of an intentional malicious attack and a probability of existence of a vulnerability exploitable by the intentional malicious attack; and (2) a product of a

probability of occurrence of an unexpected hazard and a probability of existence of a vulnerability associated with the unexpected hazard, where the intentional malicious attack and the unexpected hazard include mutually independent events. The processor may further be operable to apply a risk characterization to the undesired event based on the probability level and the IT-related activity. The risk characterization may include, for instance, an engineering risk for which a maintenance team may be dispatched or it may be a security risk for which law enforcement authorities are alerted.

**[0005a]** According to another aspect of the disclosure, there is provided a computer-readable storage medium including a set of instructions for characterizing malicious activity in an intelligent utility grid system executable by a computer having a processor and memory, the computer-readable medium including: instructions to receive information-technology (IT) data including IT-related activity from the intelligent grid system; instructions to receive non-IT data including location-specific event data from a plurality of electronic sources, grid analog measurements including phasor measurements; and a list of high-value targets and corresponding geographic locations; instructions to pre-process the non-IT data including: disregarding the non-IT data failing to meet a predetermined level of relevance to one of a plurality of risk-related events; instructions to apply a plurality of rules to the pre-processed non-IT data including to: associate an undesired even with the IT-related activity; and determine a probability that the undesired event is indicative of malicious activity including comparing predetermined criteria to the non-IT data to generate one of a plurality of probability levels as a sum of: (1) a product of a probability of occurrence of an intentional malicious attack and a probability of existence of a vulnerability exploitable by the intentional malicious attack; and (2) a product of a probability of occurrence of an unexpected hazard and a probability of existence of a vulnerability associated with the unexpected hazard, where the intentional malicious attack and the unexpected hazard include mutually independent events; and instructions to apply a risk characterization to the undesired event based on the probability level and the IT-related activity.

**[0006]** Other systems, methods, features and advantages will be, or will become, apparent to one with skill in the art upon examination of the following figures and detailed description. It is intended that all such additional systems, methods,

14. The system according to any one of claims 10 to 13, where the probability level is generated based on a co-existence of a threat and a corresponding vulnerability found in the IT-related or non-IT data that is exploitable by the threat.

15. The system according to any one of claims 10 to 145, where the processor applies the plurality of rules by comparing the IT-related activity to the historical data.

16. The system according to any one of claims 10 to 15, where at least part of the IT-related activity includes an event message from a smart meter; and the processor applies the risk characterization by determining an area within the intelligent utility grid system where the malicious activity is occurring.

17. The system according to any one of claims 10 to 16, where the non-IT data further includes: grid analog measurements including phasor measurements; and a list of high-value targets and corresponding geographic locations.

18. A computer-readable storage medium including a set of instructions for characterizing malicious activity in an intelligent utility grid system executable by a computer having a processor and memory, the computer-readable medium including:

instructions to receive information-technology (IT) data including IT-related activity from the intelligent grid system;

instructions to receive non-IT data including location-specific event data from a plurality of electronic sources, grid analog measurements including phasor measurements; and a list of high-value targets and corresponding geographic locations;

associate an undesired event with the IT-related activity; and

determine a probability that the undesired event is indicative of malicious activity including comparing predetermined criteria to the non-IT data to generate one of a plurality of probability levels as a sum of:

(1) a product of a probability of occurrence of an intentional malicious attack and a probability of existence of a vulnerability exploitable by the intentional malicious attack; and

(2) a product of a probability of occurrence of an unexpected hazard and a probability of existence of a vulnerability associated with the unexpected hazard,

where the intentional malicious attack and the unexpected hazard include mutually independent events; and

instructions to apply a risk characterization to the undesired event based on the probability level and the IT-related activity.

19. The computer-readable storage medium according to claim 18, where at least part of the IT-related activity includes an event message from a smart meter; and to apply the risk characterization, the instructions to determine an area within the intelligent utility grid system where the malicious activity is occurring.

2021. The computer-readable storage medium according to either claim 18 or claim 19, where the non-IT data further includes historical data retrieved from: event logs, geographical locations associated with corresponding parts of the intelligent utility grid system, and from operational data; and to apply the plurality of rules, the instructions further to compare the IT-related activity to the historical data.

21. The computer-readable storage medium according to any one of claims 18 to 20, where the risk characterization includes an engineering risk or a security risk.