CLAIMS

1. 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, ~~comprising~~including:

receiving, by the at least one processor, information-technology (IT) data including IT-related activity from the intelligent grid system;

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;

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;

applying, by the at least one processor, a plurality of rules to the pre-processed non-IT data ~~to~~including:

~~associate~~ associating an undesired event with ~~reference to~~ the IT-related activity; and

~~determine~~ determining 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

applying, by the at least one processor, a risk characterization to the undesired event based on the probability level and the IT-related activity.

2. The method ~~of~~ according to claim 1, where the undesired event has not yet occurred.

3. The method ~~of~~ according to claim 1 or claim 2, where the risk characterization ~~comprises~~ includes an engineering risk or a security risk.

4. The method ~~of claim 1~~ according to any one of the preceding claims, further including:

generating a risk characterization message having the risk characterization of the undesired event; and

sending the risk characterization message to a system administrator.

~~where applying the plurality of rules comprises comparing predetermined criteria to the non-IT data for which one of a plurality of different probability levels is generated~~.

5. The method ~~of~~ according to claim 4, 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.

6. The method ~~of~~ according to claim 4, where the ~~probability level is generated as a sum of: (1) a product of a probability of occurrence of a specific malicious attack and a probability of existence of a vulnerability exploitable by the specific 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~~ risk characterization message including the probability level and an area at risk selected from the group consisting of security, engineering and communication.

7. The method ~~of claim 1~~ according to any one of the preceding claims, 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 where applying the plurality of rules includes comparing the IT-related activity to the historical data.

8. The method ~~of claim 1~~ according to any one of the preceding claims, where at least part of the IT-related activity ~~comprises~~ includes an event message from a smart meter; and applying the risk characterization includes determining an area within the intelligent utility grid system where the malicious activity is occurring.

~~9. The method of claim 1, where the non-IT data further includes: grid analog measurements comprising phasor measurements; and a list of high-value targets and corresponding geographic locations.~~

~~109~~. The method ~~of claim 1~~according to any one of the preceding claims, where the electronic sources of non-IT data include one or a combination of the following inputs: a weather feed; a disturbance recorder feed; a digital fault recorder feed; a harmonic recorder feed; a power quality monitor feed; a device status; a connectivity state; a control limit; US CERT feeds; GPS feeds; a Power Management Unit (PMU) feed; sensor feeds; load forecasts; and renewable generation forecasts.

~~11~~10. A system for characterizing malicious activity in an intelligent utility grid system, ~~comprising~~including:

a system storage in which to store a database including a plurality of rules;

a collector 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 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 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; and

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

~~12~~11. The system ~~of~~according to claim ~~11~~10, further ~~comprising~~ including the CEP bus coupled with one or a combination of the following electronic

sources of non-IT data: a Web-crawling device; a search engine-capable computing device; a Web-access device; a GPS device; a social-media-thread monitoring device; a thermometer; and an emergency response communicator.

~~13~~12. The system ~~of~~ according to claim ~~11~~10 or claim 11, where the undesired event has not yet occurred, and where the risk characterization comprises an engineering risk or a security risk.

~~14~~13. The system ~~of~~ according to any one of claims ~~11~~10 to 12, where to apply the plurality of rules, the processor is further configured to:

generate a risk characterization message having the risk characterization of the undesired event; and

send the risk characterization message to a system administrator.

~~compares predetermined criteria to the non-IT data for which one of a plurality of different probability levels is generated.~~

~~15~~14. The system ~~of~~ according to any one of claims 10 to 13~~claim 14~~, 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.

~~16~~15. The system ~~of~~ according to any one of claims ~~11~~10 to 145, where ~~the non-IT data further includes historical data from retrieved from: event logs, geographical location associated with corresponding parts of the intelligent utility grid system, and from operational data; and where~~ the processor applies the plurality of rules by comparing the IT-related activity to the historical data.

~~17~~16. The system ~~of~~ according to any one of claims ~~11~~10 to 15, where at least part of the IT-related activity ~~comprises~~ 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.

~~18~~17. The system ~~of~~ according to any one of claims ~~11~~10 to 16, where the non-IT data further includes: grid analog measurements ~~comprising~~ including phasor measurements; and a list of high-value targets and corresponding geographic locations.

~~19~~18. A computer-readable storage medium ~~comprising~~ 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 ~~comprisingincluding~~:

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 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; and

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

~~20~~19. The computer-readable storage medium ~~of~~ according to claim ~~19~~18, where at least part of the IT-related activity ~~comprises~~ 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.

21. The computer-readable storage medium ~~of~~ according to either claim ~~19~~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.

~~22~~21. The computer-readable storage medium ~~of~~ according to any one of claims ~~19~~18 to 20, where the risk characterization ~~comprises~~ includes an engineering risk or a security risk.

~~23~~22. The computer-readable storage medium ~~of~~ according to any one of claims ~~19~~18 to 21, where ~~to apply the plurality of rules, the instructions further to compare predetermined criteria to the non-IT data for which one of a plurality of different probability levels is generated, where~~ the criteria includes one or a combination of: temperature, dollars, social networking statistics.

~~24~~23. The computer-readable storage medium ~~of~~ according to claim ~~23~~22, 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.