

CLAIMS:

1. An electronic device (108), comprising:

an embedded computer (106), comprising one or more processors configured to:

receive (302) one or more security event messages from a security appliance (102), the one or more security event messages each indicating a security event of a plurality of available security events associated with a protected component (104), an indication of a type of program logging the one or more security event messages and a native severity classification of the security event;

identify (304) a customized severity characterization of the one or more security event messages based at least in part upon the indication of the type of program logging the one or more security event messages and the native severity classification;

determine (306) one or more presentation or control actions to be performed based upon the customized severity characterization; and

perform (308) the one or more presentation or control actions.
2. The electronic device of claim 1, wherein the customized severity characterization is determined by executing a mapping script (110) that maps one or more characteristics of the one or more security event messages received by the security appliance (102) to a particular customized severity characterization expected by the embedded computer (106).
3. The electronic device of claim 2, wherein the one or more characteristics of the one or more security event messages received by the security appliance comprises a first severity level and the particular customized severity characterization expected by the embedded computer (106) is a second severity level.
4. The electronic device of claim 2, wherein the one or more processors of the embedded computer are configured to execute the mapping script.
5. The electronic device of claim 2, wherein the customized severity characterization is

received from the security appliance.

6. The electronic device of claim 1, comprising a display (406), wherein the one or more presentation or control actions comprises:

presenting, via a graphical user interface (GUI) (600, 700, 800, 900, 1000) on the display, one or more alarm banners associated with the one or more security event messages, the one or more alarm banners displayed based upon the customized severity characterization; or

presenting, via a stack light (402), one or more visual alarm indications associated with the one or more security event messages, the one or more visual alarm indications based upon the customized severity characterization; or
both.

7. The electronic device of claim 1, wherein the one or more presentation or control actions comprises modifying an operational status of the protected component.

8. The electronic device of claim 7, wherein the protected component comprises an amusement attraction.

9. The electronic device of claim 1, wherein the one or more security event messages comprise a message generated in accordance with a Syslog standard for message logging.

10. The electronic device of claim 1, comprising:

one or more input/output (I/O) devices configured to receive one or more I/O commands from an operator of the electronic device, or provide one or more output indications to the operator, or both; and

a programmable logic controller (PLC) (116) configured to:

receive I/O data indicative of the one or more I/O commands, and implement the one or more I/O commands; or

receive the one or more output indications, and present the one or more output indications via the one or more I/O devices; or
both.

11. The electronic device of claim 10, wherein the one or more I/O devices comprise a set of one or more lights (402) that provide an indication of the customized severity characterization;

wherein the set of one or more lights comprises a fault light-emitting diode (LED) that selectively indicates a critical severity security event when in a first state and a medium severity security event when in a second state; and

wherein the set of one or more lights comprises a health light-emitting diode (LED) that indicates whether all expected interfaces are communicatively coupled to the electronic device.

12. The electronic device of claim 10, wherein the embedded computer is configured to: determine when a continuously changing state of a variable of the PLC is not detected at

the embedded computer within a threshold amount of time; and

providing a fault in response to not detecting the continuously changing variable state within the threshold amount of time, the fault indicating a malfunction of the embedded computer.

13. The electronic device of claim 10, wherein the one or more I/O devices comprise a run/bypass switch that:

when in a run mode, causes logging and presentation of one or more alarm banners associated with the one or more security event messages and causes presentation of one or more alarms associated with the one or more security event messages, as they are received; and

when in a bypass mode, causes logging and presentation of the one or more alarm banners associated with the one or more security event messages, and causes refrain from presentation of the one or more alarms associated with the one or more security event messages, as they are received.

14. The electronic device of claim 10, wherein the one or more I/O devices comprise a reset switch that, when set to a reset mode, causes the embedded computer to power down, or reboot, or both.

15. A tangible, non-transitory, computer-readable medium, comprising computer-readable instructions that, when executed by one or more processors of a computer, cause the computer to:

receive (302) one or more security event messages from a security appliance (102), the one or more security event messages each indicating a security event of a plurality of available security events associated with a protected component (104), an indication of a type of program logging the one or more security event messages and a native severity classification of the security event;

identify (304) a customized severity characterization of the one or more security event messages based at least in part upon the indication of the type of program logging the one or more security event messages and the native severity classification;

determine (306) one or more presentation or control actions to be performed based upon the customized severity characterization; and

perform (308) the one or more presentation or control actions.

16. The computer-readable medium of claim 15, comprising computer-readable instructions that, when executed by the one or more processors, cause the computer to:

identify the customized severity characterization by executing a mapping script to map one or more characteristics of the one or more security event messages received from the security appliance to a particular customized severity characterization expected by the computer.

17. The computer-readable medium of claim 15, comprising computer-readable instructions that, when executed by the one or more processors, cause the computer to:

present one or more alarm banners corresponding to the one or more security event messages along with an indication of the customized severity characterization of the one or more security event messages in a graphical user interface (GUI) of the computer.

18. The computer-readable medium of claim 15, comprising computer-readable instructions that, when executed by the one or more processors, cause the computer to:

determine when a continuously changing state of a variable of a programmable logic controller (PLC) is not detected at the computer within a threshold amount of time;

and

providing a fault in response to not detecting the continuously changing variable state within the threshold amount of time, the fault indicating a malfunction of the computer.

19. A computer-implemented method, comprising:

receiving (302), via a computer, one or more security event messages from a security appliance (102), the one or more security event messages each indicating a security event of a plurality of available security events associated with a protected component (104), an indication of a type of program logging the one or more security event messages and a native severity classification of the security event;

identifying (304), via the computer, a customized severity characterization of the one or more security event messages based at least in part upon the indication of the type of program logging the one or more security event messages, the customized severity characterization comprising a severity expected by the computer identified based upon a mapping to at least the native severity classification indicated in the one or more security event messages;

determining (306) one or more presentation or control actions to be performed based upon the identified customized severity characterization; and

performing (308) the one or more presentation or control actions.

20. The computer-implemented method of claim 19, comprising:

presenting, via a graphical user interface (GUI), one or more alarm banners associated with the one or more security event messages, the one or more alarm banners displayed based upon the customized severity characterization; or

presenting, via a stack light, one or more visual alarm indications associated with the one or more security event messages, the one or more visual alarm indications based upon the customized severity characterization; or both.