

Claims

1. A defense system for defending a utilities system against cyber-physical attacks associated with anomalies in a physical process operative in the utilities system, the defense system comprising:

a set of sensors configured for collecting physical data associated with the physical process;

a set of controller devices configured for receiving the physical data from the sensors and for monitoring process states of the physical process based on the physical data ~~from the sensors~~;

a set of verification devices configured for receiving the physical data from the sensors independently of the controller devices and for monitoring the physical process based on the physical data ~~from the sensors, the physical data enabling the verification devices to~~ said monitoring comprising detecting the one or more anomalies in the physical process based on the physical data and a set of invariants predefined for the physical process; and

a set of actuators selectably controllable by the controller devices or verification devices to remedy the anomalies and regulate the physical process, thereby defending the utilities system against the cyber-physical attacks.

2. The system according to claim 1, wherein the verification devices comprise a number of global verification devices programmatically integrated with the controller devices, the global verification devices configured for receiving the physical data from the sensors and for detecting the anomalies based on the physical data and the invariants.

3. The system according to claims ~~1 or~~ 2, wherein the verification devices comprise a number of local verification devices communicatively isolated from the controller devices, the local verification devices configured for receiving the physical data from the sensors and for detecting the anomalies based on the physical data and the invariants.

4. The system according to claim 3, wherein the verification devices comprise a number of independent global verification devices communicatively connected to the local verification devices and communicatively isolated from the controller devices,
5 the independent global verification devices configured for receiving the physical data from the sensors via the local verification devices and for detecting the anomalies based on the physical data and the invariants.

5. The system according to claim 4, wherein the independent global verification devices are communicatively connected to local verification devices associated with
10 other physical processes operative in the utilities system, the independent global verification devices configured for monitoring all the physical processes operative in the utilities system.

6. The system according to claims ~~4 or 5~~, wherein each of the local verification devices and independent global verification devices is configured to assume control
15 of the actuators in response to the local verification devices detecting the anomalies.

7. The system according to claim 6, wherein the local verification devices are configured to determine which one of the local verification devices and independent
20 global verification devices assumes control of the actuators.

8. The system according to ~~any one of claims 4 to 7~~, wherein the independent global verification devices are communicatively connected to actuators associated with other physical processes operative in the utilities system.
25

9. The system according to ~~any one of claims 3 to 8~~, wherein each local verification device comprises only one communication input that is a wired communication for receiving the physical data from the sensors.

10. The system according to claim ~~8~~1, wherein ~~the communication input is a wired communication~~ one or more anomalies in the physical process are detectable based on comparison between the physical data received by the controller devices and the physical data received by the verification devices.
30

11. The system according to ~~any one of claims 3 to 10~~, wherein: ~~an input communication attempt from the controller devices to the local verification devices is detected as an anomaly~~

5 ~~the controller devices are configured for communicating the physical data to a set of supervisory devices;~~

~~the verification devices are configured for communicating the physical data to the supervisory devices bypassing the controller devices; and~~

10 ~~wherein the one or more anomalies in the physical process are detectable based on comparison of the physical data by the supervisory devices.~~

12. ~~The system according to any one of claims 1 to 11, wherein the utilities system is configured for operating multiple physical processes, each physical process associated with corresponding sets of the sensors, controller devices, verification devices, and actuators.~~

1312. A defense method for defending a utilities system against cyber-physical attacks associated with anomalies in a physical process operative in the utilities system, the defense method comprising:

 collecting, by a set of sensors, physical data associated with the physical process;

~~receiving, by a set of controller devices, the physical data from the sensors;~~

25 ~~monitoring, by a set of~~the controller devices, process states of the physical process based on the physical data ~~from the sensors;~~

~~monitoring~~receiving, by a set of verification devices, the physical data from the sensors independently of the controller devices;

30 ~~monitoring, by the verification devices, the physical process based on the physical data from the sensors, the physical data enabling the verification devices to detect the anomalies based on a set of invariants predefined for the physical process;~~

detecting, by the verification devices, ~~the one or more~~ anomalies in the physical process based on the physical data and a set of invariants predefined for the physical process; and

selectably controlling, by the controller devices or verification devices, a set of actuators to remedy the anomalies and regulate the physical process, thereby defending the utilities system against the cyber-physical attacks.

~~44~~13. The method according to claim ~~43~~12, wherein the verification devices comprise a number of global verification devices programmatically integrated with the controller devices, the method comprising receiving, by the global verification devices, the physical data from the sensors and detecting the anomalies based on the physical data and the invariants.

~~45~~14. The method according to claims ~~13~~ or 14, wherein the verification devices comprise a number of local verification devices communicatively isolated from the controller devices, the method comprising receiving, by the local verification devices, the physical data from the sensors and detecting the anomalies based on the physical data and the invariants.

~~46~~15. The method according to claim ~~45~~14, wherein the verification devices comprise a number of independent global verification devices communicatively connected to the local verification devices and communicatively isolated from the controller devices, the method comprising receiving, by the independent global verification devices, the physical data from the sensors via the local verification devices and detecting the anomalies based on the physical data and the invariants.

~~47~~16. The method according to claims ~~15~~ or 16, further comprising assuming, by one of the local verification devices and independent global verification devices, control of the actuators in response to the local verification devices detecting the anomalies.

~~18~~17. The method according to claim ~~17~~16, further comprising determining, by the local verification devices, which one of the local verification devices and independent global verification devices assumes control of the actuators.

5 ~~19~~18. The method according to ~~any one of claims 15 to 18~~14, further comprising communicating the physical data from the sensors to the local verification devices via a wired communication.

~~20~~19. The method according to ~~any one of claims 15 to 19~~12, further comprising:

10 comparing the physical data received by the controller devices and the physical data received by the verification devices; and
 ~~detecting as an anomaly in response to an input communication attempt from the controller devices to the local verification devices~~one or more anomalies in the physical process based on said comparison of the physical
15 data.

20. The method according to claim 19, comprising:

communicating the physical data from the controller devices to a set of supervisory devices;
20 communicating the physical data from the verification devices to the supervisory devices bypassing the controller devices;
 comparing, by the supervisory devices, the physical data received from the controller devices and the physical data received from the verification devices; and
25 detecting one or more anomalies in the physical process based on said comparison of the physical data by the supervisory devices.