CLAIMS

1. A method of detecting an anomaly in operation of an industrial control system (ICS), the method comprising:

    a) by a signal monitoring device operably connected to an input/output (I/O) line carrying signaling between a logic controller (LC) and a sensor or actuator,

    measuring one or more of:

    a. voltage on the I/O line,

    b. current on the I/O line,

    thereby giving rise to data indicative of a voltage-to-time and/or current-to-time measurement of:

    a signal of a sensor or actuator to an LC, and/or

    a signal of an LC to a sensor or actuator;

    b) receiving, by a processing circuitry, first data, the first data being derivative of the voltage-to-time and/or current-to-time measurement ,;

    c) receiving, by the processing circuitry, second data derivative of at least one of:

    i) one or more ICS network control packets,

    ii) one or more statuses logged by an ICS application, and

    iii) one or more commands entered to an ICS application; and

    d) determining, by the processing circuitry, whether there is inconsistency between the first data and the second data.

2. The method of claim 1, additionally comprising:

e) responsive to whether the processing circuitry determined inconsistency, performing, by the processing circuitry, an alert action.

3. The method of claim 1, additionally comprising:

e) responsive to whether the processing circuitry determined inconsistency, determining, by the processing circuitry, whether the inconsistency is indicative of a cyber attack; and

f) responsive to whether the processing circuitry determined that the inconsistency is indicative of a cyber attack, performing, by the processing circuitry, an alert action.

4. The method of claim 1, wherein the determining whether there is inconsistency between the first data and the second data comprises:

a) decoding at least part of first data, thereby giving rise to, at least, data indicative of a first sensing/actuating event;

b) determining one or more correlated ICS network events from the second data; and

c) determining whether the one or more correlated ICS network events are inconsistent with the first sensing/actuating event.

5. The method of claim 1, wherein the determining whether there is inconsistency between the first data and the second data comprises:

a) determining a first ICS event from the second data;

b) determining one or more correlated sensing/actuating events from the first data; and

c) determining whether the one or more correlated sensing/actuating events are inconsistent with the first ICS event.

6. The method of claim 1, wherein the second data comprises data derivative of one or more ICS control packets which comprise supervisory control and data acquisition (SCADA) data.

7. The method of claim 1, wherein the second data comprises data derivative of status information logged by a SCADA human-machine interface (HMI) system.

8. The method of claim 1, wherein the second data comprises data derivative of commands entered to a SCADA human-machine interface (HMI) system.

9. A system of detecting an anomaly in operation of an industrial control system (ICS), the system comprising a processing circuitry configured to:

a) receive first data, the first data being derivative of a voltage-to-time and/or a current-to-time measurement of:

a signal of a sensor or actuator to an LC, and/or
a signal of an LC to a sensor or actuator,

the voltage-to-time and/or current-to-time measurement having been measured by a signal monitoring device operably connected to an input/output (I/O) line carrying signaling between a logic controller (LC) and a sensor or actuator;

b) receive second data derivative of at least one of:

i) one or more ICS network control packets,

ii) one or more statuses logged by an ICS application, and

iii) one or more commands entered to an ICS application; and

c) determine whether there is inconsistency between the first data and the second data.

10. A computer program product comprising a computer readable non-transitory storage medium containing program instructions, which program instructions when read by a processing circuitry, cause the processing circuitry to perform a method detecting an anomaly in operation of an industrial control system (ICS), the method comprising:

a) receiving first data, the first data being derivative of

a voltage-to-time and/or a current-to-time measurement of:

a signal of a sensor or actuator to an LC, and/or
a signal of an LC to a sensor or actuator,

the voltage-to-time and/or current-to-time measurement having been measured by a signal monitoring device operably connected to an input/output (I/O) line carrying signaling between a logic controller (LC) and a sensor or actuator;

b) receiving second data derivative of at least one of:

i) one or more ICS network control packets,

ii) one or more statuses logged by an ICS application, and

iii) one or more commands entered to an ICS application; and

c) determining whether there is inconsistency between the first data and the second data.