CLAIMS

1. A method, implemented in at least one computer processor, for detecting anomalies in an industrial control system, the method comprising:

obtaining, from one or more sensors of the industrial control system, a plurality of sensor measurements of at least one parameter characterising a physical process in the industrial control system, the physical process having a current process state;

determining, based on a model of the physical process, a corresponding plurality of estimated values for the at least one parameter;

determining residuals between the estimated values and the sensor measurements;

determining a cumulative sum (CUSUM) of normalised residuals, wherein the normalised residuals are computed according to a difference between the residuals and a historical average of the residuals for the current process state;

based at least on the CUSUM, detecting whether there is an anomaly in the current process state; and

responsive to detection of an anomaly, generating an alert.

2. A method according to claim 1, wherein the detection is based on a comparison of the CUSUM with a threshold.

3. A method according to claim 1, wherein the model is based on system identification.

4. A method according to claim 3, wherein the model is an autoregressive model or a linear dynamical state space (LDS) model.

5. A method according to claim 1, wherein the detection is based on the output of a trained classifier, and wherein the inputs to the trained classifier comprise one or more features generated from the CUSUM and at least one of: the residuals; a physical status of one or more devices implementing the physical process; a transition between physical statuses of the one or more devices; and one or more network traffic parameters of network traffic in the industrial control system.

6. A method according to claim 5, wherein the classifier is a decision tree-based classifier.

7. A method according to claim 5, wherein the one or more network traffic parameters are derived from network packets at both level 0 and level 1 devices of the industrial control system.

8. A system for detecting anomalies in an industrial control system, comprising at least one processor configured to carry out the method according to any one of claims 1 to 7.