

Detecting SCADA Sensor Signal Manipulations in Nonlinear Chemical Engineering Processes

Thomas Richard McEvoy¹ Stephen D. Wolthusen^{1,2}

¹Information Security Group
Department of Mathematics
Royal Holloway, University of London, UK

and

²Norwegian Information Security Laboratory
Department of Computer Science
Gjøvik University College, Norway

March 16, 2010

- Recent research on the vulnerability of SCADA systems has focused mainly on protocol-level effects as modernisation has increased interconnections
- Existing and novel vulnerabilities may be exploited at network, host and control level we concentrate on the latter
- We note that attacks need not necessarily be immediately spectacular to succeed: Degradation or clandestine attacks on products of control processes
- We have previously addressed the potential effects of sensor manipulation and the need for cost effective solutions
 - Here we present a detection model based on process control techniques as opposed to classical intrusion (anomaly) detection techniques which are less than effective against RTU, PLC, and sensor manipulation

Problem and Assumptions

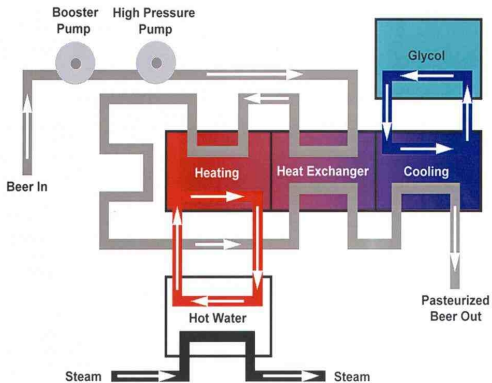
- We assume the attacker may gain unauthorised supervisory access to the system and be able to alter setpoints and sensor readings, while disguising this fact from operators
- We assume the attacker cannot take real time control of the system due to communication latency
 - However, an attacker **can rewrite processes so as to falsify signals**
 - This is an intuitive rather than a formal model of adversary capability; a formal model is addressed in ongoing work
- Our problem is to detect (and possibly prevent) this manipulation either by using or introducing sensors which can provide independent corroboration of process state
 - Sensor placement and computational complexity must be considered

Approach

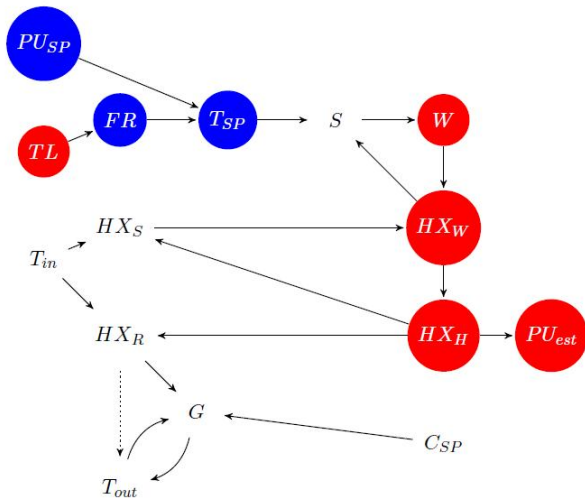
- We use a *functional causal model* to map the system
 - This must be considered an informal model
- The aim is to identify potentially independent sensors or points where such sensors could be placed
 - Systems are simulated using differential equations and block diagrams
 - This allows evaluation of further sensor placements
- In practical terms, this usually means emplacing new sensors on an OOB network to take readings and compare these with actual process state under control using real time numerical simulation to flag up anomalies
 - Confidence levels will vary depending on process disturbances and physical sensor placement
 - We use the example of a basic heat exchange process (pasteurisation)

Pasteuriser: Engineering Viewpoint

Pasteurizer Block Diagram



Pasteuriser: Causal Map



Using the Causal Map

- Blue nodes are **potentially controllable**
- Red nodes are likely to be concealed by the attacker or their readings obfuscated by taking advantage of process “noise” (i.e. natural variation in signals)
- All other nodes are potentially readable and might be useful in determining process state
 - In particular, we need to find readings which directly relate to the equational model of the process in control terms
 - We build a simulation of the pasteuriser using ODEs and take readings at various locations to discover candidate sensor emplacement points

Heat Exchange Equations

$$\dot{q} = UA(T_{in,s} - T_{out,c}) \quad (1)$$

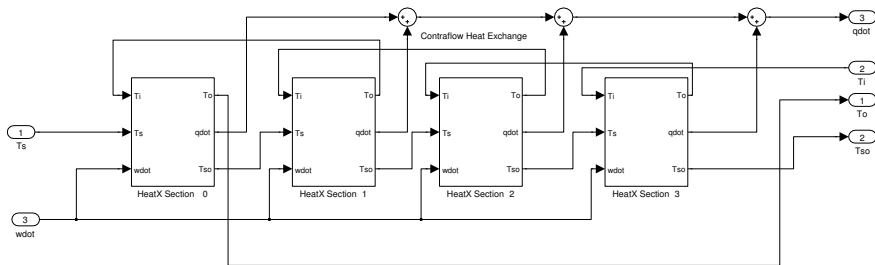
$$wCp \frac{dT}{dt} = \dot{w}Cp(T_{in,c} - T_{out,c}) + \dot{q} \quad (2)$$

$$uCp \frac{dT_s}{dt} = \dot{u}CP(T_{in,s} - T_{out,s}) - \dot{q} \quad (3)$$

In **equation 1** \dot{q} is the rate of heat exchange, U is the coefficient of heat exchange for the construction material and A is the area, $T_{in,s}$ is the initial hot-side temperature (C°), $T_{out,s}$ is the final hot side and $T_{in,c}$ the initial product temperature and $T_{out,c}$ is the final product temperature

Equations 2 and 3 represent the respective energy balances of the cold and hot sides where \dot{w} , \dot{u} represent the hot-side and cold-side flow rates respectively, w , u the liquid volume (m^3), and Cp is the specific heat capacity ($kJ/kg - K$) of the product

Block Diagram Example: Contraflow Heat Exchange



Pasteurisation

Pasteurisation units PU are derived from flow rate and temperature values using

$$PU = \frac{w}{\dot{w}}(60)(1.393^{(T-60)}) \quad (4)$$

where w is the holding volume (HL), \dot{w} is the flow rate (HL/HR) and T is the temperature

- This is a oddly dimensioned measure which was derived empirically by Dayharsh *et al.*

We observe the non-linear relationship between flow rates, temperature and pasteurisation values

Hence pasteurization, *like heat exchange*, depends on both flow rate and temperature

We show that the end products (hot and cold) of the contraflow heat exchange can be used to detect anomalies caused by sensor manipulation

Three Claims

Based on the preceding models we can state three verifiable claims:

- 1 We can detect flow rate manipulation from the cold side temperature
- 2 We can detect pasteurisation (hot side temperature rate manipulation) using hot (temperature) and cold side (flow rate) temperatures as indicators
- 3 We can detect attempts to hide changes to pasteurisation rates in process “noise”

(1) Cold-Side Temperatures indicate Flow Rates

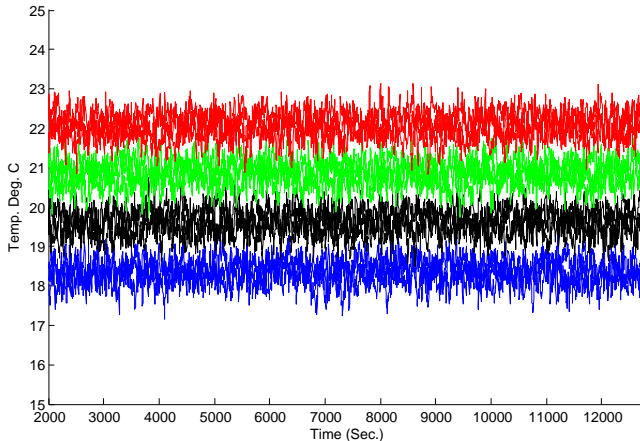


Figure: Temperature Differences for Distinct FRs [180:20:120]

(2) Hot-Side Temperatures v. Flow Rate

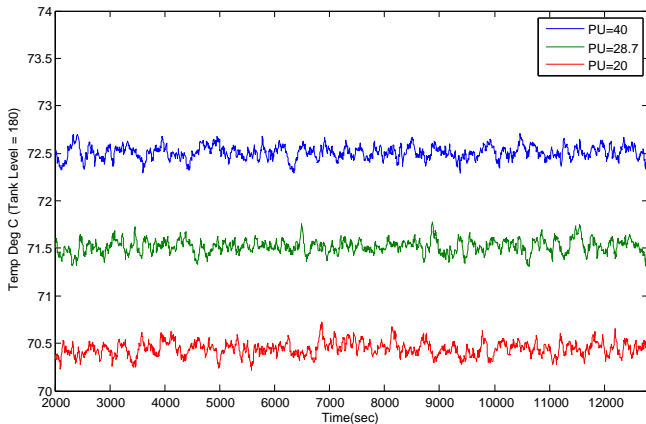


Figure: Temperature Differences for PU Changes (FR = 180)

(3) Hiding Changes in PU Using Temperature

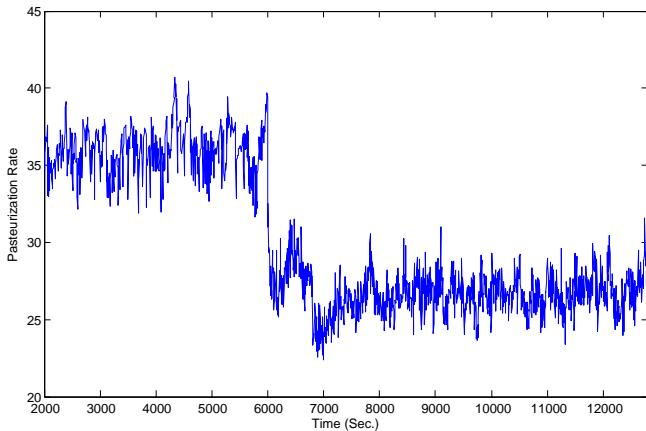


Figure: Change in PU

(3) Hiding Changes in PU Using Temperature

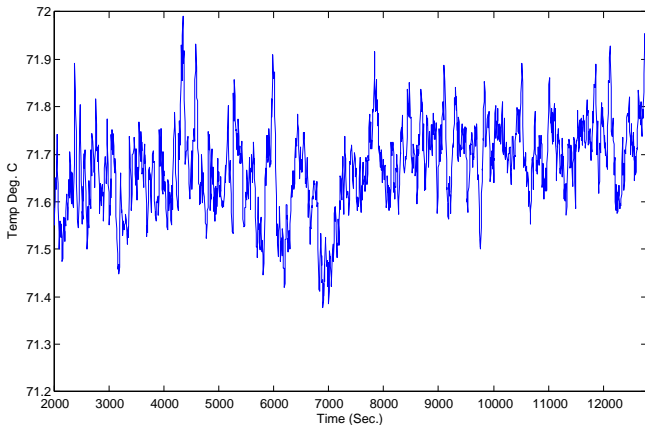


Figure: Obfuscation Using Hot-Side Temperature

(3) Detection

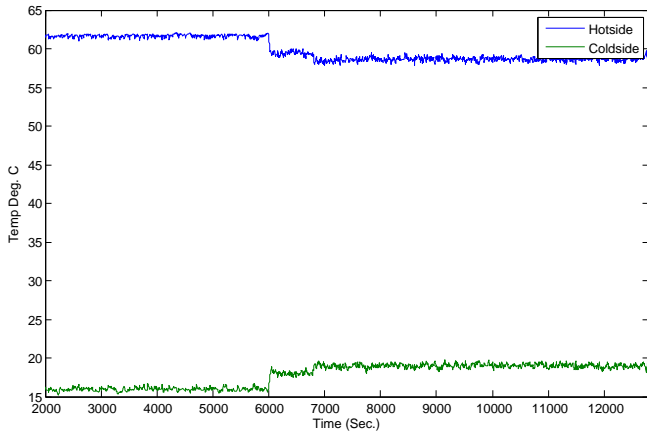


Figure: Detection using Contraflow HX Products

Discussion and Future Work

- The modernisation of SCADA systems makes them more vulnerable to attack at both network and control level
- We have shown that we can use process control techniques to detect anomalies at control level by considering potential proxy signals
- Our technique minimizes the number of sensors required to give an independent view
- Signature-based approaches are not useful here whilst anomaly-based approaches can potentially lead to model explosion to account for process variability: Real time numerical simulation provides a cheap computational way forward
- Ongoing work requires a more formal adversary capability model
- Further studies based on different control laws are also under investigation

Contact information: Stephen D. Wolthusen

Norwegian Information Security Laboratory
Department of Computer Science
Gjøvik University College
P.O. Box 191
N-2818 Gjøvik, Norway

Information Security Group
Department of Mathematics
Royal Holloway, University of London
Egham, Surrey TW20 0EX
United Kingdom

`stephen.wolthusen@{hig.no} | {rhul.ac.uk}`

- The increasing vulnerability of SCADA systems is well observed in the literature [16, 11, 8, 3]
- Interest in SCADA security including intrusion detection has risen in response [13]
- ID has been applied using signatures at the perimeter and anomaly detection against insider threats and attacks at DCS level [7, 17, 9]
- The limitations of conventional anomaly detection in the face of process disturbance have been shown [15, 14, 4]
- We argue this weakness highlights the requirement for a different model which will frequently require the use of additional, independent sensors [14, 2, 5, 10]
- To build this model we make use of causal maps [12] and classical process control techniques [1]



B. W. Bequette.

Process Control: Modeling, Design and Simulation, volume 7 of *Prentice Hall International Series in the Physical and Engineering Sciences*.

Prentice-Hall, Upper Saddle River, NJ, USA, 2002.



J. Bigham, D. Gamez, and N. Lu.

Safeguarding SCADA Systems with Anomaly Detection.

In V. Gorodetsky, L. Popyack, and V. Skormin, editors, *Proceedings of the Second International Workshop on Mathematical Methods, Models, and Architectures for Computer Network Security (MMM-ACNS 2003)*, volume 2276 of *Lecture Notes in Computer Science*, pages 171–182, St. Petersburg, Russia, September 2003. Springer-Verlag.



E. Byres and D. Hoffman.

The Myths and Facts behind Cyber Security Risks for Industrial Control Systems.

Technical report, Department of Computer Science, University of Victoria, Victoria, BC, Canada, April 2004.



Alvaro A. Cardenas, Tanya Roosta, and Shankar Sastry.

Rethinking security properties, threat models, and the design space in sensor networks: A case study in scada systems.

Ad Hoc Netw., 7(8):1434–1447, 2009.



M. P. Coutinho, G. Lambert-Torres, L. E. B. da Silva, J. G. B. da Silva, J. C. Neto, E. Bortoni, and H. Lazarek.

Attack and Fault Identification in Electric Power Control Systems: An Approach to Improve the Security.

In *Proceedings of Power Tech 2007*, pages 103–107, Lausanne, Switzerland, July 2007. IEEE Press.



C. A. Dayharsh and H. W. Del Vecchio.

Thermal Death Time Studies on Beer Spoilage Organisms.

Proceedings of the American Society of Brewing, II:48–52, 1952.



D. Gamez, S. Nadjm-Tehrani, J. Bigham, C. Balducelli, K. Burbeck, and T. Chyssler.

Dependable Computing Systems: Paradigms, Performance Issues, and Applications, chapter Safeguarding Critical Infrastructures.

John Wiley & Sons, New York, NY, USA, 2005.



R. L. Krutz.

Securing SCADA Systems.

John Wiley & Sons, New York, NY, USA, 2006.



O. Linda, T. Vollmer, and M. Manic.

Neural Network based Intrusion Detection System for Critical Infrastructures.

In *Proceedings of the 2009 International Joint Conference on Neural Networks (IJCNN 2009)*, pages 1827–1834, Atlanta, GA, USA, June 2009. IEEE Press.



T. R. McEvoy and S. Wolthusen.

Using Observations of Invariant Behavior to Detect Malicious Agency in Distributed Control Systems.

In R. Bloomfield and E. Rome, editors, *Proceedings of the 4th International Workshop on Critical Information Infrastructures Security (CRITIS 2009)*, vol. 6027 of Lecture Notes in Computer Science, Bonn, Germany, September 2009. Springer-Verlag, pages 62–72.
(in press).

 P. S. Motta Pires and L. A. H. G. Oliveira.

Security Aspects of SCADA and Corporate Network
Interconnection: An Overview.

In *Proceedings of the 2006 International Conference on
Dependability of Computer Systems (DepCos – RELCOMEX
2006)*, pages 127–134, Szklarska Proeba, Poland, May 2006.
IEEE Press.

 J. Pearl.

Causality: Models, Reasoning, and Inference.

Cambridge University Press, Cambridge, United Kingdom, 2nd
edition, 2009.



J. Rrushi and K.-D. Kang.

Detecting Anomalies in Process Control Networks.

In C. Palmer and S. Shenoj, editors, *Critical Infrastructure Protection III*, pages 151–165, Hanover, NH, USA, March 2009. Springer-Verlag.

(Proceedings of the Third Annual IFIP WG 11.10 International Conference on Critical Infrastructure Protection).



N. K. Svendsen and S. D. Wolthusen.

Modeling and Detection of Anomalies in Critical Infrastructure Networks.

In M. Papa and S. Shenoj, editors, *Critical Infrastructure Protection II*, pages 101–107, Arlington, VA, USA, March 2008. Springer-Verlag.

(Proceedings of the Second Annual IFIP WG 11.10 International Conference on Critical Infrastructure Protection).



J. Verba and M. Milvich.

Idaho National Laboratory Supervisory Control and Data Acquisition Intrusion Detection System (SCADA IDS).

In Proceedings of the 2008 IEEE Conference on Technologies for Homeland Security, pages 469–473, Waltham, MA, USA, May 2008. IEEE Press.



D. Watts.

Security & Vulnerability in Electric Power Systems.

In Proceedings of the 35th North American Power Symposium (NAPS 2003), pages 559–566, Rolla, MI, USA, October 2003. IEEE Press.



D. Yang, A. Usynin, and J. W. Hines.

Anomaly-Based Intrusion Detection for SCADA Systems.

In Proceedings of the 5th International Topical Meeting on Nuclear Plant Instrumentation, Control, and Human Machine Interface Technologies (NPIC&HMIT 06), Albuquerque, NM, USA, November 2006. American Nuclear Society.