Chapter 10

USING PHYSICAL MODELS FOR ANOMALY DETECTION IN CONTROL SYSTEMS

Nils Svendsen and Stephen Wolthusen

Abstract Supervisory control and data acquisition (SCADA) systems are increasingly used to operate critical infrastructure assets. However, the inclusion of advanced information technology and communications components and elaborate control strategies in SCADA systems increase the threat surface for external and subversion-type attacks. The problems are exacerbated by site-specific properties of SCADA environments that make subversion detection impractical; and by sensor noise and feedback characteristics that degrade conventional anomaly detection systems. Moreover, potential attack mechanisms are ill-defined and may include both physical and logical aspects.

This paper employs an explicit model of a SCADA system in order to reduce the uncertainty inherent in anomaly detection. Detection is enhanced by incorporating feedback loops in the model. The effectiveness of the approach is demonstrated using a model of a hydroelectric power plant for which several attack vectors are described.

Keywords: SCADA systems, anomaly detection, hydroelectric power plant

1. Introduction

Most critical infrastructure components rely on supervisory control and data acquisition (SCADA) systems or distributed control systems for operations and maintenance. This situation, in combination with the desire for higher efficiency and centralized operations, have contributed to the increased threat levels encountered in critical infrastructure components from cyber and cyber-physical attacks [19].

The detection of intrusions and subversion attacks is becoming as important for SCADA systems as it has been for traditional computer networks. However, we argue that several properties of SCADA systems, particularly the

uncertainty of measurements and actuator status induced by interactions with the physical environment make signature-based attack detection problematic. In particular, large error margins must be included, which reduce signature specificity. Moreover, the general problem of signature-based systems being able to detect only variations in known or expected attacks is exacerbated by the fact that the configuration of SCADA systems at a given facility is unlikely to be replicated elsewhere. As a result, the creation and replication of signature patterns can be very problematic.

We argue that anomaly detection provides a better match with the constraints found in SCADA environments. While the specificity of anomaly detection techniques can be inadequate, the problem space may be reduced considerably by imposing constraints on the variables based on the knowledge of the modeled system (e.g., minimum and maximum sensor values and gradients), and the margins of error for sensors and actuators; and, especially, by modeling the correlations between components. One area in which an explicit control system model is critical is in the incorporation of feedback loops as these would otherwise result in correlated variables not being detected by most pattern classification and correlation mechanisms.

This paper analyzes selected aspects of the control systems used in a hydroelectric power plant with particular emphasis on the effects induced by the feedback loops that occur at several different time scales. A hydroelectric power plant was chosen for the study because it contains a limited number of well-defined, albeit nested, feedback control loops, and characteristics of feedback itself. In addition, hydroelectric power plants are of particular relevance due to their role as stabilizing (and, in some cases, sustaining) entities for the electric power grid, and also for the potential physical damage that can result from some failure modes. Moreover, the observations and mechanisms described in the context of control systems for hydroelectric power plants are applicable to other control system environments as well.

2. Hydroelectric Power Plants

Hydroelectric power plants convert hydrological power in a waterfall via mechanical power on a machine shaft to electrical power in a generator. This section briefly describes the structure of a simple hydroelectric power plant without the additions required by pumped storage. The description does not address specific installations or turbine variants that are described in the literature (see, e.g., [12]).

The water intake for a hydroelectric plant is normally constructed with an accumulation dam in a river course. Depending on the formation of the dam, the intake can be of a shallow water or deep water kind. In both cases, a physical rack or sump is installed to protect the intake from debris and biological material. The intake is also equipped with one or more valves that control water flow.

A conduit system channels water from the intake to the turbine. This can be an open channel, tunnel, penstock or pressure shaft, or a combination of

these systems. In Norwegian installations, which are frequently constructed as high head power plants, the conduit system consists of a head race tunnel of low inclination where sand traps are installed for sedimentation of suspended particles. A surge chamber system is installed at the downstream end of the head race tunnel to reduce water hammer pressure variations and to keep mass oscillations caused by load changes within acceptable limits. At the same location, there may exist a fine trash rack and a valve that enables the penstock to be emptied upstream of the turbine without having to empty the head race tunnel; this valve also serves as a security feature in case of pipeline rupture. The conduit system often ends with a lined or unlined steel penstock that connects the shaft with the valves in the machine hall.

Turbines convert hydrological power to mechanical power, the most popular being the Pelton, Francis and Kaplan turbines. The type of turbine used depends on the penstock profile and vertical drop. The (usually adjustable) guide vane cascade in a turbine gives the water flow the velocity and direction required for the inlet to the runner. The hydraulic power is then converted to mechanical power on the turbine shaft to which the runner is fixed. The turbine shaft is guided in a radial bearing and an axial bearing that is loaded with the axial force from the runner, which is caused by the water pressure and impulse from the flow and the weight of the rotating parts. The scroll case in the turbine conducts the water flow into the guide vane cascade. The draft tube conducts the water flow from the turbine outlet into the tail race canal.

The mechanical energy from the turbine is transferred to a generator via the generator shaft. The generator produces electrical power by the process of electromagnetic induction. An excitation system provides the DC voltage to the field winding of the generator and modulates this voltage for control purposes (see, e.g., [7, 17]). The excitation power may be provided by a rotating exciter or by controlled rectifiers supplied from the generator terminals. The excitation system includes several subsystems designed to protect the generator and excitation system from excessive duty under abnormal operating conditions.

Hydroelectric power plants are responsive in nature, meaning that they can respond quickly to changes in load demand. These plants can be started and shut down much more quickly and economically than coal-fired plants, let alone nuclear plants. Nevertheless, due to the nature of hydroelectric power plant operations, control systems should be able to implement both long-term and short-term actions. Numerous sensors are positioned to gather data used by automatic control systems to perform the appropriate control actions, and by human operators to run the plant in a safe, reliable, secure and economical manner.

The protection system of a hydroelectric plant has two main elements: (i) an electrical protection system responsible for the major electrical apparatus and auxiliary systems, and (ii) mechanical protection systems for the hydraulic turbine, generator and mechanical systems. Both the elements of the protection system employ large numbers of electronic sensors and actuators. The supervisory process involves comparing plant and equipment operating values against

limits, requirements and projections. Typically, the control process monitors hard and soft limits in a hysteresis band and compensates for overshoot, also issuing alarms as control actions. Other activities involve the monitoring of equipment status and the status of sensors and actuators. We only provide a qualitative overview of the control system elements that are relevant to the attack vectors considered in this paper. Readers are referred to [8, 9] for additional details related to the control of hydroelectric power plants.

3. Attack Vectors

Transient failures of individual power plants are, of course, undesirable, but they do not pose a threat to the overall stability of the electric grid. Therefore, from a critical infrastructure point of view, they are only of limited interest.

Failures resulting in physical damage, however, are relevant to the stability of the power grid. Taking a power plant off the grid for a long period (several months) limits the overall generation capacity and, depending on the demand and grid topology, can weaken the overall grid. Also, inducing coordinated failures across multiple plants, even if they are only transient in nature, can affect the infrastructure as a whole. We concentrate on attack vectors that can lead to either type of failure. Note that these attack vectors are not exhaustive and should not be considered to represent a full attack taxonomy, which is beyond the scope of this paper.

3.1 Components from Dam to Turbine

The geospatial extent of hydroelectric power plants makes it difficult to provide adequate physical security for sensors and actuators located outside the turbine and generation complex (unlike those situated within the reservoir itself or at the penstock). Physical attacks (including manipulations) of these sensors and actuators must be considered along with attacks that target the control networks.

Sensors in or near the reservoir are used to assess the state of the reservoir such as water level and flow rates. Other sensors may monitor hydrological and geological features as well as the dam itself. Of particular interest, however, is the penstock in which a number of valves for normal operation and emergencies must be monitored and operated. Rapid closure of the emergency valves can result in penstock collapse [20]. Operating other valves can result in damage to turbine and generator equipment; control actions based on flow rates that are not measured or reported correctly can induce water hammer or cavitation effects [21]. Likewise, misreported valve settings and flow rates can result in damage to turbine blades or buckets depending on the turbine type and configuration. This can occur during shutdown if the protective closure of guide vanes or needles is not performed within the required time, or in overspeed conditions where bearings could be damaged. Static overspeed conditions and dynamic oscillations can also result in excessive stress on turbine casings and the anchoring of the turbine to its supports.

In addition to the components related to power generation, bypass mechanisms are exist to regulate flow that cannot be handled by the turbine pathways (e.g., during turbine failure or maintenance, or when the influx exceeds capacity). While these mechanisms are not very time-critical and do not have an immediate impact on the generation pathway, manipulations of their sensors and actuators can still result in severe damage, especially if there is a failure to relieve pressure when water levels exceed the designed capacity.

3.2 Generator Components

Attacks on the generator and its components primarily seek to create overload conditions. For the purposes of studying these attacks, the clutches, generator, exciter and governor can be considered together. Voltage and current sensors and the control loops associated with these sensors have tight timing requirements, rendering the introduction of delays into control loops an attractive attack strategy. Moreover, unlike the components discussed in the previous section, these components are not easily inspected visually and require quick feedback from the control system, making manual intervention problematic. In addition, it is possible for attackers to de-synchronize sensors or to misreport sensor readings and actuator feedback, forcing the control system to operate the generator outside its performance envelope while suppressing warnings and fault condition reports to control system operators.

When considering attacks on generator components, it is necessary to view the hydraulic and electrical systems as separate components and as a single system with interacting components. Note that feedback loop and actuator speeds for the hydraulic system are considerably lower than those for the electrical system. Interactions can arise, for example, during electrical system failures that result in load rejection. Also, transients in piezometric heads can cause significant damage that may require an emergency shutdown of a turbine.

3.3 Grid and External Control Elements

Even when the complex case of a pumped storage power plant is disregarded, the generated power is regulated externally based on the utility's load prediction system, state estimators and other factors such as requirements from grid operators. An interference with the delivery of external control messages will not, by itself, force components to operate outside their performance envelopes; however, several types of denial-of-service attacks can be executed. Depending on the security properties of the protocol, the attacks may be limited to message suppression or delay. Replay attacks are possible if freshness tests are not built into the protocol. Inadequate integrity checks can enable malleable ciphertext attacks even if the protocol data units are encrypted.

Other attack vectors can target the transformers that couple the power plant to the power grid. Possible attacks include causing generators and transformers to be out of phase, cycling circuit breakers rapidly and engaging couplers in short succession. These attacks would have to be combined with sensor data

suppression to ensure that the damage is effected before alarms can be raised or operators are able to intervene. As with the attack vectors described in the preceding sections, considerable harm can be done by de-synchronizing the internal state control systems with the ground truth, enabling the control system to cause additional damage on its own.

4. Hydroelectric Plant Control System

This section briefly describes the control system used in a hydroelectric plant.

4.1 Control from Dam to Turbine

The turbine governor is responsible for controlling and adjusting the turbine power output. The governor also evens out deviations between the power and grid load as fast as possible. In particular, the turbine governor keeps the rotational speed stable and constant for the turbine generator unit for any grid load and prevailing conditions in the water conduit. Also, it closes the turbine admission according to the acceptable limits of the rotational speed rise of the unit and the pressure rise in the water conduits using load rejections and emergency stops [12].

The penstocks connect the hydraulic turbine with the intake structure. They are equipped with piezometer taps or pressure flow instrumentation sensors near the connection to the turbine. The flow of water to the turbine is stopped by closing the inlet to the penstocks, by having gates at intermediate points, or by using guards in the penstock just upstream from the generator. The gates are either open or closed; thus, instrumentation and alarms are limited to the fully open and fully closed positions.

4.2 Control of Generating Components

The adjustment of the rotational speed of a turbine depends on the type of turbine. Impulse (Pelton) turbines are controlled by moving the needles into or out of the nozzles. During rapid load changes, water can be channeled using deflectors. Reaction (Francis and Kaplan) turbines are controlled by adjusting wicket gates. The adjustments are monitored by the turbine governor.

The turbine governor uses speed detection, acoustic, differential or Winter-Kennedy taps to measure the rotational speed of the turbine – this is the "speed signal." The speed signal and the speed reference control signal are used to determine whether the turbine is in an overspeed, underspeed or synchronous speed state. The drop/regulation control is used together with set point control to determine if there should be a speed drop or speed regulation. This is accomplished by adjusting the water flow and/or applying air brakes on the turbine shaft. The control decision is made by a PID controller based on the combined speed signals and the gate or power feedback signal. The gate limit further includes the eventual gate limit control signals and start/stop signals to determine the gate set point. 3D blade control is performed on reaction

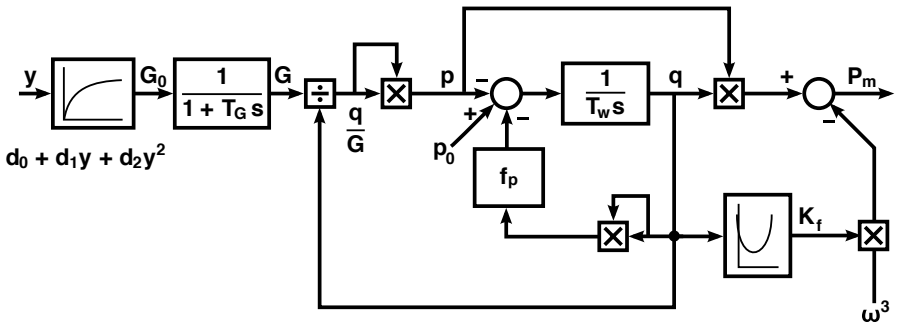

Figure 1. Non-linear model of a hydroelectric turbine [3].

turbines to optimize performance. The adjustments are made based on the gate set point and the head water and tail water levels.

4.3 Control of Grid and External Elements

The power supply to the power distribution network is dependent on numerous generators, all of which must operate in synchrony during normal and disturbance conditions. A power blackout can occur if one or more generators are out of synch. Numerous sources of instability are present in the power distribution network, including short circuits and loss of generation. Interested readers are referred to Grigsby [7] for additional information. Grigsby describes the three main types of stability in the power distribution grid: rotor angle stability, frequency stability and voltage stability; and discusses how stability can be obtained.

5. Control Models of Hydroelectric Turbines

Control system models are frequently used to represent and understand the functionality of industrial processes. This section describes two control models of hydroelectric turbines.

5.1 Non-Linear Model

Figure 1 presents a classical non-linear model of a single turbine and its water supply conduit [3]. The model illustrates the feedback and feed-forward modes involved in the interactions between the hydraulic and mechanical forces.

The valve characteristics G capture the relation between the water flow q and the pressure p in the water column. G can be expressed as a function of the gate position y. Based on experimental data, de Jaeger, *et al.* [3] have identified the function to be a combination of y and a first-order filter. This is one source of non-linearity in the model. The other non-linear component is due to the friction factor K_f, which is a second-order function of the flow q. Readers are referred to [3] for additional details about the non-linear model.

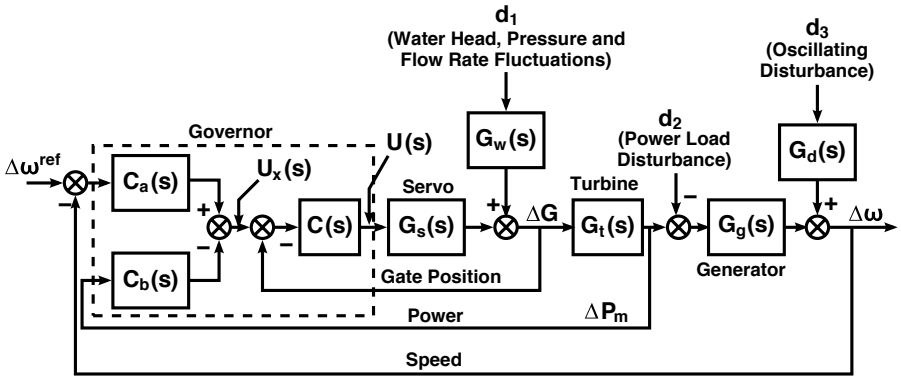

Figure 2. Multi-loop cascade control model [5].

This model can capture some of the attack vectors described above. In particular, deviations in the expected correlations between variables in the model can be used to detect direct manipulations of sensors. However, all the control elements in the model act on the same time scale, which makes it difficult to detect short-term and long-term fluctuations.

5.2 Multi-Loop Cascade Control Model

Hydro governor design has been revisited lately due to the deployment of large generating units, higher transmission voltages, higher power demands and increased complexity in the interactions between generating facilities and the distribution network. This situation is discussed by Eker [5]. Eker also provides a detailed description of a multi-loop cascade control model for hydraulic systems, which is shown in Figure 2.

The advantage of multi-loop cascade control models is that plant parameter uncertainties can be used to investigate stability and robustness. Robustness measures the ability of a plant to realize its full potential in a wide range of operating conditions [5]. The multi-loop cascade control model in Figure 2 shows the relation between the set point of the incremental speed $\Delta\omega^{\text{ref}}$ and the incremental speed $\Delta\omega$. The parameters included in the feedback to the controller in the case of Eker's model are the incremental speed $\Delta\omega$, the incremental power ΔP_m and the incremental gate position ΔG.

Eker's model captures the generator components, the components from dam to turbine, and the effects on multiple time scales. Thus, the model is able to express key aspects of the attack vectors discussed earlier.

5.3 Control System Design Challenges

Control theory provides guidance on adjusting the available degrees of freedom with the goal of achieving acceptable operation of a system (see, e.g., [18]). The task of designing a control system for a hydroelectric power plant involves

teams of engineers, the intent being that their common understanding of plant behavior is reflected in the final design.

The control system should also reflect the designers' understanding of relevant threats and disturbances. A traditional reliability approach is likely to be applied where natural exposures to the plant are considered. An essential step in the definition of a control system is the scaling of variables [18], during which time assumptions on parameters such as the largest expected change in disturbance, largest allowed input change, largest allowed control error and largest expected change in reference values are determined. The assigned values have a large impact on system behavior. From a security perspective, this is a challenge because the thresholds are different when the existence of an active adversary is taken into account.

6. Related Work

Early investigations of the effects of cyber attacks on critical infrastructure assets indicated that physical destruction was a real possibility [13]. However, subsequent research has moderated this view to a large extent.

Gonzalez-Perez and Wollenberg [6] studied interactions of the measurement infrastructure and state estimator accuracy on grid stability; their results indicate a large-scale vulnerability in the case of coordinated attacks. Other researchers have focused specifically on real-time control systems. Oman, *et al.* [15] examined the security and survivability of control systems used in power grid substations. Bigham, *et al.* [1] investigated the applicability of anomaly detection systems in SCADA environments. Oman and Phillips [16] studied intrusion detection and event monitoring in SCADA environments.

Most of the efforts related to intrusion and anomaly detection in SCADA systems have concentrated on the information system component with some exceptions (see, e.g., [10]). The problem of detecting anomalies in noisy SCADA environments has been discussed at a general level [19]. However, we are not aware of research that explicitly includes the control system model and its state prediction mechanisms, especially the consideration of feedback behavior and coupling at different time scales in baseline and anomaly models. Cheung, *et al.* [2] and Valdes and Cheung [22] describe explicit static models as a foundation for anomaly detection, but they concentrate on the control protocols rather than on the underlying system. In some domains, detailed models allow the analysis of specific control-system-dependent infrastructures and their interactions; for example, Nicolet, *et al.* [14] describe a numerical system that can provide predictive abilities beyond those discussed in this paper.

7. Conclusions

Most research on SCADA security has focused on protecting information and communication systems or the SCADA protocols themselves (see, e.g., [4, 11]). However, analyzing the physical system being controlled is useful for detecting anomalies that might indicate potential intrusions and manipulations

of the control system; for examining the implications of shutting down affected components when an attack or successful subversion attempt is detected; and for assessing the potential damage to the physical system in the event of a successful attack.

Control systems in critical infrastructures, such as the hydroelectric power plant considered in this paper, are characterized not only by the potential for direct and indirect damage but also by the delays in feedback control loops. Even if it is known that a system is compromised and can no longer be operated safely, an orderly shutdown may require an extended period of time so as not to cause damage. Delays can lead to non-intuitive behavior in the case of nested feedback loops, where, even after a primary fault has been repaired, secondary effects can lead to cascading failures.

Based on these observations, we have identified the requirements for basing anomaly detection on models of the physical system; otherwise, non-linear dependencies and anomalies are not detectable. Avenues for future research include refining the underlying models, investigating approaches that dynamically derive parameter values for use in anomaly detection, and generating explicit non-linear pattern hypotheses based on control system models.

References

[1] J. Bigham, D. Gamez and N. Lu, Safeguarding SCADA systems with anomaly detection, *Proceedings of the Second International Workshop on Mathematical Methods, Models and Architectures for Computer Network Security*, pp. 171–182, 2003.

[2] S. Cheung, B. Dutertre, M. Fong, U. Lindqvist, K. Skinner and A. Valdes, Using model-based intrusion detection for SCADA networks, *Proceedings of the SCADA Security Scientific Symposium*, 2007.

[3] E. de Jaeger, N. Janssens, B. Malfliet and B. van de Meulebroeke, Hydro turbine model for system dynamics studies, *IEEE Transactions on Power Systems*, vol. 9(4), pp. 1709–1715, 1994.

[4] J. Edmonds, M. Papa and S. Shenoi, Security analysis of multilayer SCADA protocols, in *Critical Infrastructure Protection*, E. Goetz and S. Shenoi (Eds.), Springer, Boston, Massachusetts, pp. 205–221, 2007.

[5] I. Eker, The design of robust multi-loop cascaded hydro governors, *Engineering with Computers*, vol. 20(1), pp. 45–53, 2004.

[6] C. Gonzalez-Perez and B. Wollenberg, Analysis of massive measurement loss in large-scale power system state estimation, *IEEE Transactions on Power Systems*, vol. 16(4), pp. 825–832, 2001.

[7] L. Grigsby (Ed.), *Electric Power Engineering Handbook*, CRC Press, Boca Raton, Florida, 2007.

[8] IEEE, IEEE Standard 1249-1996: IEEE Guide for Computer-Based Control for Hydroelectric Power Plant Automation, Piscataway, New Jersey, 1996.

[9] IEEE, IEEE Standard 1010-2006: IEEE Guide for Control of Hydroelectric Power Plants, Piscataway, New Jersey, 2006.

[10] P. Isasi, J. Molina-Lopez and A. Sanchis de Miguel, Unsupervised neural network for forecasting alarms in a hydroelectric power plant, *Proceedings of the International Conference on Artificial and Natural Neural Networks*, pp. 1298–1306, 1997.

[11] E. Johansson, T. Sommestad and M. Ekstedt, Security issues for SCADA systems within power distribution, *Proceedings of the Nordic Distribution and Asset Management Conference*, 2008.

[12] A. Kjolle, Hydropower in Norway: Mechanical Equipment, Technical Report, Norwegian University of Science and Technology, Trondheim, Norway, 2001.

[13] National Security Telecommunications Advisory Committee, Electric Power Risk Assessment, Technical Report, Washington, DC, 1997.

[14] C. Nicolet, P. Allenbach, J. Simond and F. Avellan, Modeling and numerical simulation of a complete hydroelectric production site, *Proceedings of the IEEE Lausanne Power Tech Conference*, pp. 1044–1048, 2007.

[15] P. Oman, A. Krings, D. Conte de Leon and J. Alves-Foss, Analyzing the security and survivability of real-time control systems, *Proceedings of the Fifth Annual IEEE SMC Information Assurance Workshop*, pp. 342–349, 2004.

[16] P. Oman and M. Phillips, Intrusion detection and event monitoring in SCADA networks, in *Critical Infrastructure Protection*, E. Goetz and S. Shenoi (Eds.), Springer, Boston, Massachusetts, pp. 161–173, 2007.

[17] T. Short, *Electric Power Distribution Handbook*, CRC Press, Boca Raton, Florida, 2004.

[18] S. Skogestad and I. Postlethwaite, *Multivariable Feedback Control: Analysis and Design*, Wiley, Chichester, United Kingdom, 2005.

[19] N. Svendsen and S. Wolthusen, Modeling and detecting anomalies in SCADA systems, in *Critical Infrastructure II*, M. Papa and S. Shenoi (Eds.), Springer, Boston, Massachusetts, pp. 101–113, 2008.

[20] A. Tijsseling, Fluid-structure interaction in liquid-filled pipe systems, *Journal of Fluids and Structures*, vol. 10(2), pp. 109–146, 1996.

[21] A. Tijsseling, Water hammer with fluid-structure interaction in thick-walled pipes, *Computers and Structures*, vol. 85 (11-14), pp. 844–851, 2007.

[22] A. Valdes and S. Cheung, Intrusion monitoring in process control systems, *Proceedings of the Forty-Second Hawaii International Conference on System Sciences*, pp. 1–7, 2009.