Enabling Interoperability and Extensibility of Future SCADA Systems*

Wei Ye and John Heidemann
USC Information Sciences Institute

1 Challenges and Applications

Supervisory Control And Data Acquisition (SCADA) systems have been widely used in industry applications. Due to their application specific nature, most SCADA systems are heavily tailored to their specific applications. For example, a remote terminal unit (RTU) that monitors and controls a production well in an oilfield is only connected with a few sensors at the well it resides. The RTU usually collects sensor data at pre-defined intervals, and only sends data back when being polled by a central data server. A user can only access the data in one of the two ways: directly connecting to the RTU in the field or reading from the data server in the control room.

A major drawback of typical SCADA systems is their inflexible, static, and often centralized architecture, which largely limits their interoperability with other systems. Wireless sensor networking is a promising technology that can significantly improve the sensing capability of the SCADA system. Sensor networks employ large number of low-cost sensors with easy and flexible deployment, which can largely extend the sensor coverage. For example, in a SCADA system developed for oil and gas fields, the RTUs are usually places at production wells and injection wells. However, there are many other places, such as pipeline, tanks, *etc.*, that have valuable data but are too expensive (*e.g.*, cable requirement) to deploy more RTUs. In such cases, sensor networks are a perfect solution to extend the sensing capability of the SCADA system. However, it is difficult to integrate sensor networks with current SCADA systems due to their limited interoperability. We identify that enabling such interoperability is an important task for future SCADA systems.

Another drawback of the current SCADA systems is their limited extensibility to new applications. In the above oilfield monitoring example, a user in the field can only access a sensor's data by physically going to that well and connecting to its RTU. If the company wants to extend its SCADA system by adding a safety alarm system, it will be very difficult to add the new application. The original application only monitors well production at predefined intervals or on demand. The new application requires real-time interaction between sensors and mobile users in the field. The RTUs that detect a safety problem need to proactively report the problem without waiting. The rigid design of current RTUs makes it hard to extend the SCADA from one application to another.

This position paper argues that it is very important to enable the interoperability and extensibility of future SCADA systems. Our work is based on the application of oil and gas field monitoring, a collaborative effort between USC and Chevron Corporation. Deploying a SCADA system in a large field is very expensive. If the SCADA system is interoperable with new technologies, such as sensor networks, and extensible for new applications, it will be able to significantly improve the oil/gas productivity at a minimal cost.

2 Research Issues

This section identifies major research issues to enable interoperability and extensibility of future SCADA systems. We roughly classify them in three categories: flexible communication architecture, open and interoperable protocols, and smart remote terminal units. We next elaborate each of them in more details.

Flexible communication architecture. Current SCADA systems are essentially a centralized communication system, where the data server polls each remote terminal unit (RTU) to collect data. There is no data sharing and forwarding between different RTUs. Usually these RTUs only communicate with the data server. This communication architecture is not flexible to interact with other systems, such as the embedded sensor networks and mobile users in the field.

Designing a flexible communication architecture is one of the key factors to enable interoperability and extensibility. We suggest that SCADA systems should adopt the use of Internet technologies for networking, rather than proprietary or link-level approaches. Such

*This work is partially supported by the National Science Foundation (NSF) under the grant NeTS-NOSS-0435517 as the SNUSE project and by Chevron Co. through the USC Center for Interactive Smart Oilfield Technologies (CiSoft).

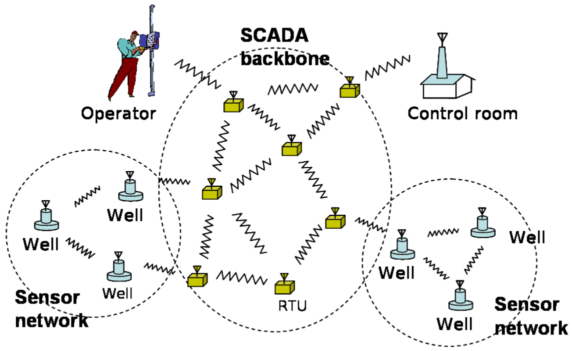

Figure 1: Two tiered architecture of SCADA with wireless sensor networks.

a scheme would make it easy to shift to a two tiered architecture, as shown in Figure 1. At the top tier is a backbone network that connects all RTUs. We expect future SCADA systems to support multi-hop data communication between different RTUs. Therefore, data sharing between RTUs becomes possible, which enables real-time interaction with mobile users, as data from a sensor far away can be forwarded to the users by multiple relaying nodes. More importantly, the use of IP decouples the physical network from the software and logical network.

The bottom tier consists of different patches of wireless sensor networks that flexibly extend the sensor coverage of the SCADA system. Each sensor network will connect with one or more RTUs. These RTUs will serve as gateways between SCADA and sensor networks, and will respond to user queries and manage data collection from its connected sensor networks.

Open and interoperable protocols. Protocols include communication protocols and data management protocols. Communication protocols need to be open and interoperable. For examples, sensor networks have their own set of protocols that mainly focus on energy-efficient data collection and communication. When working with SCADA systems, these protocols should address how to take advantage of the more powerful SCADA RTUs. On the other hand, SCADA RTUs should employ protocols that help to maximize the performance of the resource-constrained sensor networks.

Data management protocols specify how to describe, collect and manipulate different types of sensor data. It also includes how to discover and configure sensors. An open protocol should be extensible to support various types of sensors. These protocols should also address what types of data should be transmitted and to whom. For example, raw data are only sent to data server for archival. Status summaries will be sent to managers and engineers, while emergency safety alarms should be broadcast to all field operators.

Smart remote terminal units. Remote terminal units play an important role in the new communication architecture we described above. They serve as bridge points to sensor networks as well as access points to mobile users in the field. They respond to users queries and collect data from specific sensors. These RTUs should be smart enough to perform preliminary data processing. The first reason is to validate the data collected from different sensors. Sensors can give false values due to various reasons. It is important to validate them before use them to make important decisions. For example, in oilfield monitoring, a false sensor reading may result in a mistaken decision to shut in a well and lose production. The RTU is in a good position to validate sensor readings by cross checking from adjacent sensors.

Another reason of requiring smart RTUs is that they are important in changing the reactive operation to proactive operation. Current SCADA systems mainly operate in the reactive mode, where data are usually sent in response to the data server's polling. In a new class of applications, detection needs to be done in real-time, and events need to be reported immediately, such as pipeline leakage, or H_2S detection. Intelligent algorithms will run on these smart RTUs to process data in real time.

Finally, these RTUs need to be smart enough to protect data from unauthorized access and altering. Access control and security measures need to be installed to protect the sensing system from attackers and ensure data integrity.

3 Roadmap

We see the research issues in the above three areas are interrelated. To begin with, we propose to first address the issue of open and interoperable protocols. This step will establish a solid foundation for future SCADA system to inter-operate with sensor networks and mobile users, such as those using IEEE 802.11. Based on this foundation, we can further build smart remote terminals. A flexible software framework is needed to enable the integration of various intelligent algorithms. Transition from current communication architecture to the flexible two-tiered architecture may take longer time until individual components are ready. In summary, future SCADA systems with good interoperability and extensibility can greatly benefit applications such as monitoring large oil/gas fields.