TECHNICAL ARTICLE

SCADA Data Verification for Commissioning & Operations

By Graham Nasby, City of Guelph Water Services

With any computerized data collection system, it is important to ensure that the data being collected and recorded matches the data being read in from the field instruments by the system.

Data verification is the process of checking that the data that is collected, stored, and reported matches the data from the instrument being monitored.

Data Verification vs. Validation

It is important to make the distinction between "data verification" and "data validation." Data verification is the process of checking that data values match from end-to-end from a technical perspective. Data validation is checking that data values are correctly collected from a regulatory compliance perspective. Though the terms are very similar, it is important to differentiate between them. The most important difference is that validation is a standardized continuous work process that is continually used to prove regulatory compliance for the water utility. Verification on the other hand is usually only done as part of system commissioning, or as part of an infrequent preventative maintenance procedure.

Another difference is that the time-consuming process of doing data validation is usually only done on a smaller subset of "regulated" parameters (or other parameters of interest) in the system. Data verification, when carried out, is usually done on all data points in the part of the system being checked over.

System Commissioning

During system commissioning, the field vs. displayed/logged value of every new and upgraded data point needs to be checked as part of a "data verification" work process. This involves checking the data value of each point from the originating instrument up to into the SCADA systems HMI screen, historian, and reporting functions.

When data verification is performed, it is usually done in the form of either a single pass or double-pass I/O check.

In a single pass I/O check, the value on the originating instrument is compared to the value that is shown on the screen / historian / reporting interface. Thus, the value is checked all the way up from the originating instrument up to the SCADA systems HMI.

In a double-pass I/O check, the transmission of the value from the originating instrument to the PLC Input card's memory address is first checked, and then as a second separate check is done to verify the value from I/O card up to the SCADA systems HMI.

Depending on the project type, it may be more efficient to do either a single-pass or double-pass I/O check -- each is functionally equivalent and equivalently valid. No matter which type of I/O check is done, the testing should be documented on a signed and dated I/O check test form, with any anomalies noted for further follow up.

Also, when doing the "data verification" for an analog data point, it is ideal if more than just than just one value is checked. Often, the values at 0%, 25%, 50%, 75% and 100% of an instruments range, plus one live value, will be checked as part of a "data verification" I/O check.

When designing or upgrading instrumentation, such as process analyzers or transmitters, the use of "blind" instruments (instruments with no local display) should be avoided as much as possible. Having a local display on an instrument makes doing I/O checks on measurement values much easier, as the local instrument reading can readily be seen and checked.

During system commissioning, both regulated and non-regulated parameters will be tested using data verification

System Operation – Periodic Data Verification Checks

As a best practice, the value of data points in the system should be subjected to data verification on a scheduled periodic basis. Often a 1-, 2-, or 5-year verification cycle is used, so that all data points are periodically checked during the operation of the system.

For regulated parameters, it is best practice to do a data verification at least once a year. Often, this periodic data verification can be done in conjunction with the annual calibration activities of field instruments, to avoid having to make additional site visits.

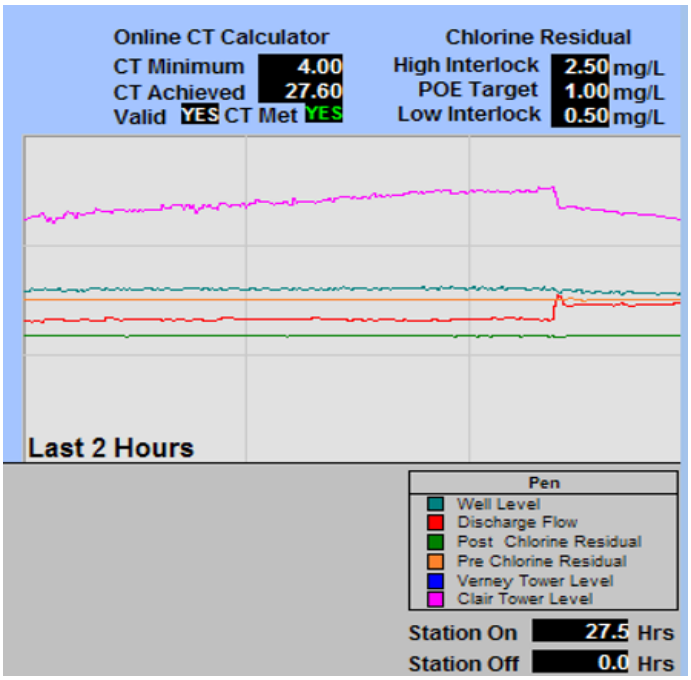

Figure 1- Example of screen indicators and trend lines that will need to have their data links checked and verified when a new site is being added to a SCADA system

System Operation – Data Verification & Data Validation

From an operations point of view, both data validation, and a limited version of data verification, should be carried out on a periodic basis.

From a data validation perspective, in most water districts the water regulator will require certain types of process data be reviewed every so many hours, the check be documented in a log book, and then any data anomalies followed up on. For example, in Ontario Canada, all data for regulated parameters must be checked at least every 72 hours (O.Reg. 170, Sched 6, Section 6.5 Continuous Monitoring under the Safe Water Drinking Act, Ontario Canada)

From a regulatory perspective, the types of data validation checks which are done usually include identifying if/when values drop below regulatory minimums and maximums; missing data, signal dropouts, data gaps, signal outliers, and other data that appears to be out of normal. Checks are also usually done to ensure that data is being logged on at least the minimum intervals specified by the regulator as well. (For example, in Ontario Canada, chlorine values for primary disinfection must be logged every 5 minutes.) Operators will also note in the log when equipment has been taken out of service, so that any false readings from associated instrumentation can be ignored from a regulatory perspective.

At the same time, it is advisable that operations staff also keep an eye on any datapoints they encounter in the SCADA system from a "data verification" perspective. Any data points that are not working properly should be noted, so they can be followed-up on and fixed as needed. Since this is an ad-hoc verification, it does not need the same rigor as the regulation-prescribed data validation work process.

Summary

Data verification is the activity of checking that data from the source instruments up into the SCADA system is being recorded correctly from a technical perspective. Data verification is typically first done as during initial system commissioning and periodically during the lifetime of the system to ensure system integrity.

Data validation is a separate regulatory compliance activity to check that logged process data can be used to prove regulatory compliance and that the process data has been logged in accordance with regulations under the local drinking water regulations and associated license and/or permit conditions.

About the Author

Graham Nasby, P.Eng., PMP has worked in the municipal water sector for 15+ years in a variety of roles, including consulting, operations, and capital projects. Since 2015, he has held the role of Water SCADA & Security Specialist at City of Guelph Environmental Services. He is also co-chair of the ISA112 SCADA systems management committee. Graham lives in Guelph, Ontario. Contact: graham.nasby@grahamnasby.com .

NEW ISA LEARNING MODULES

ISA Launches New Micro-Learning Modules for CSIOs (Chief Security Information Officers)

From ISA news release

As a senior-level executive, the chief information security officer (CISO) plays a pivotal role in establishing and maintaining programs that ensure information technology (IT) and operational technology (OT) assets are adequately protected. This means data protection, risk assessment, cyber incident response, and adherence to standards, policies, and procedures are top priorities. Aside from these responsibilities, keeping up with a cyber landscape that is constantly moving remains at the forefront of many executives' minds. A recent Proofpoint study discovered that roughly 64% of CISOs around the world suspect a material cyberattack will hit their organization within the next 12 months. Based on these findings, the majority of CISOs believe their organizations are unprepared to fend off potential cyberattacks.

With this in mind, ISA is introducing a new set of microlearning modules (MLMs) focused on specific areas of industrial cybersecurity. ISA microlearning modules consist of short, 5- to 10-minute videos that address cybersecurity challenges and help viewers better understand the purpose of the ISA/IEC 62443 series of standards. The first set of MLMs consists of three videos on cybersecurity awareness and three on cyber use-cases.

The awareness videos, entitled, "IACS Cybersecurity for Chief Information Security Officers (CISOs)," are designed to help CISOs gain more insight and understanding of the ISA/IEC 62443 series of standards. With this newfound knowledge, executives can be better prepared when collaborating with automation engineering colleagues to ensure the improved safety, reliability, and performance of physical process operations.

Executives can expect to learn more about:

- The differences between IT and OT systems
- Industrial cybersecurity terminology
- How IT and OT should work together, what should be protected in each environment, and the associated risks
- Consequences of implementing a disjointed cybersecurity program (or not having a program entirely)
- Benefits of implementing ISA/IEC 62443 standards

The use-case MLMs review two cyberattacks on Ukraine in 2015 and 2016, and an attack on a wastewater plant in the United States. These videos examine the causes of the attacks, the ramifications of the attacks, and how a cybersecurity program would have prevented the attacks or mitigated the consequences.

Learn more by visiting the IACS Cybersecurity for CISOs MLM visit: www.isa.org/training-and-certification/isa-training/microlearning-modules/iacs-cybersecurity-for-cisos

To learn about ISA's new Microlearning Modules Program, visit www.isa.org/training-and-certification/isa-training/microlearning-modules