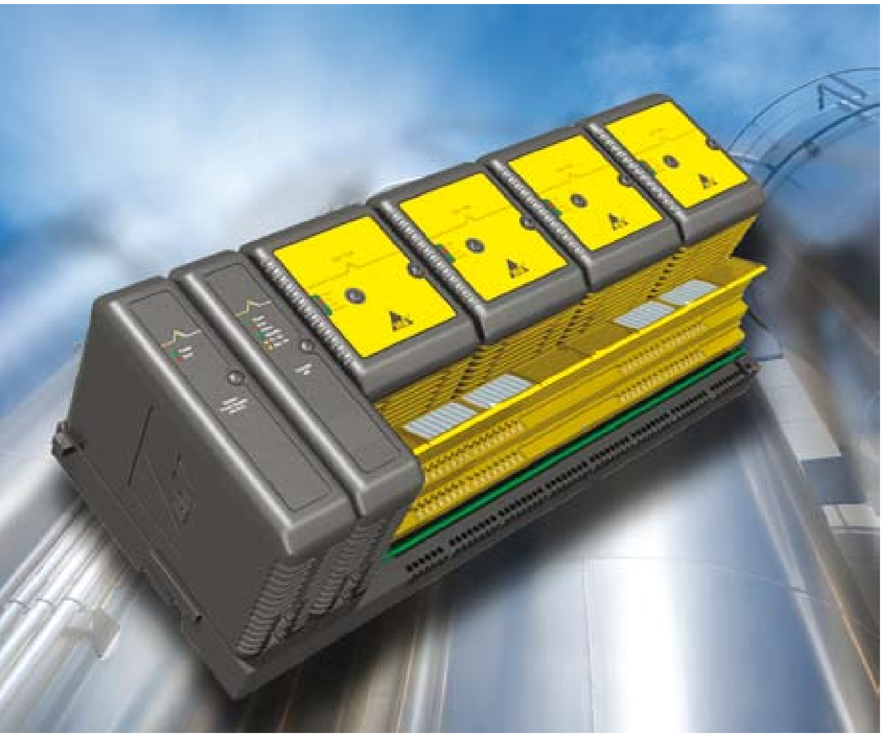
Safety the Smart Way

***Jonas Berge* explains how a smart safety instrumented system (SIS) with integrated HART capability can boost diagnostics capability and increase process availability.**

A smart safety instrumented system (SIS) emphasizes an architectural capability rather than an individual technology or component. It spans the safety instrumented function (SIF) as a whole, from sensor to final control element, including signal wires, not just the logic solver.

HART in combination with enhanced Electronic Device Description Language (EDDL) enables predictive device diagnostics integrated with operator displays, where device and signal faults are seen in time to make a difference. SIS field device problems can be captured and fixed before causing a trip, thus improving process availability.

In a smart safety instrumented system (SIS), communication from HART field devices goes beyond passing data to an isolated device maintenance system. The HART protocol provides a secondary signal from each transmitter, enabling previously undetected faults to be detected and alarmed.



Since modern transmitters, logic solvers, and valve controllers are digital, it makes sense to use digital communications to provide an integrated approach to complete safety loops - from sensor to logic solver to final control element. Integrated HART capability in a smart SIS is used in new ways that increase process availability by avoiding spurious trips.

Hardening the link

Given that signal cables deteriorate and intermediate connections can corrode over time, it is possible for the resistance of the 4-20 mA current loop to increase to a point where the transmitter output voltage may saturate with current limited below 20 mA. In this case, the transmitter may be unable to produce sufficient output to tell the logic solver the actual process value, and the logic may not trip when it should.

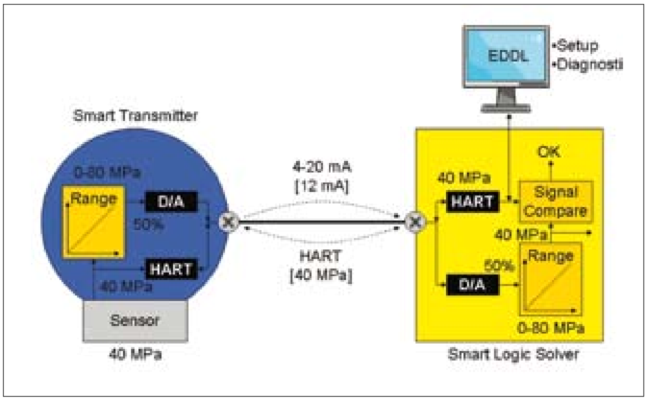
A shorted or open 4-20 mA loop is easy to detect; all logic solvers can do it. However, detecting an untrue signal in an analog system is not so easy. As long as the current is anywhere between 4 and 20 mA, it appears valid and will not arouse suspicion. For example, if transmitter output current should be 18 mA but saturates at 16 mA, the fault is not detected because the signal is still valid.

A conventional SIS would need to have at least two transmitters and be programmed to trip or alarm on excessive deviation between the two inputs to detect this problem. If there is just one transmitter, the problem would not be detected.

However, a second signal path is provided from smart HART transmitters. A smart logic solver (SLS) with embedded HART circuitry communicates digitally with transmitters simultaneously with the analog 4-20 mA signal. A diagnostics function embedded in the smart logic solver compares the digital value communicated using HART against the ranged analog value received as the 4-20 mA input. A mismatch reveals a distorted current.

When this disparity is detected, an alarm is sent to maintenance to take corrective action and optionally to operations. This is how a smart SIS uses HART to uncover faulty analog signals that previously went undetected.

Legacy SIS logic solvers without HART communication as well as systems using external



To detect a distorted current, a diagnostics function embedded in the smart logic solver compares the digital value communicated using HART against the ranged 4-20 mA analog value.

HART multiplexers do not have this ability. Many logic solvers have HART I/O for pass-through of device information to an asset management system, but that is not sufficient. The HART signal must be accessible in the smart logic solver itself in order to achieve integrated signal diagnostics.

Other potential problems may include transmitter 4-20 mA signal current diverted to ground due to ground loop. For example, if transmitter output current is 18 mA, but a ground loop diverts part of the current to ground with only 16 mA going to the logic solver input, this would not be detected in a traditional logic solver. But in a smart logic solver with signal diagnostics, this disparity is uncovered and alarmed.

Device faults unmasked

Devices in direct contact with extreme pressures and temperatures, vibration, corrosive and abrasive fluids, although reliable, will eventually fail. The analog signal conveys only the value, without indicating its validity or status. The way a transmitter with a 4-20 mA output flags a fault is by driving the output above 20 mA – for example, to 21 mA (or just below 4 mA in some applications).

However, to a logic solver, a high current looks just like a high process value. For example, over-pressure causes a trip even though pressure is not high. In other words, a device fault masquerades as a process problem. With an analog signal, a logic solver has no means to distinguish between a process problem and a device problem and therefore must shut down. This type of spurious trip reduces process availability.

A smart logic solver continuously communicates digitally with the transmitter to determine the latter's health from the HART status information. If the transmitter self-diagnostics detects a failure, the smart logic solver knows about it and invalidates the analog signal because it is not a true process signal, again avoiding a spurious trip. Voter logic can be degraded automatically upon detection of a device failure, allowing the process to continue running while the device is repaired during the specified mean time to repair (MTTR), per the IEC 61511 process safety standard.

When maintenance and operations personnel are alerted to the device problem, they use intelligent device management software, part of the Asset Management Solution (AMS), to diagnose the device to pin-point the issue.

EDDL is the technology embedded with the HART protocol used by device manufacturers to define how the device shall be displayed by the system, including the layout of the diagnostics pages in order to make troubleshooting easy for technicians. Each device manufacturer provides an EDDL file for each device type. This file contains setup and diagnostics help text with know-how from the product expert guiding the technician toward the appropriate action

In a smart SIS, HART is used by the smart logic solver to tell the difference between a process problem and a device problem. The smart logic solver makes the decision to not shut down on device problems, only on real process problems, thus reducing process downtime. What formerly caused a spurious trip is now just an alarm, which thanks to EDDL can be acted upon faster.

Legacy SIS logic solvers do not have this ability. The HART communication must be integrated within a smart logic solver for the device status information to validate the voting. Other device integration solutions are not suitable for operator station integration.

When it comes to loop testing, all HART transmitters support a fixed current mode, which is a useful feature enabling any output from 4 to 20 mA to be simulated for loop testing. The danger is that the transmitter may by mistake be left in this simulation mode, in which case the transmitter output remains constant regardless of the process input. If the logic solver is not receiving the measurement, it is unable to perform its function.

A smart logic solver continually checks transmitter status using HART communication. If the transmitter is in fixed current mode, the smart logic solver alarms maintenance and operations to take corrective action.

Smart diagnostics

Most SIF failures in the field occur because the transmitters and valves are in a harsh plant environment in direct contact with the unforgiving process, while the logic solver is indoors in a climate controlled room. Therefore, special attention must be given to the field instrumentation.

Displaying device diagnostics in a dedicated maintenance console for technicians has a drawback; the technicians are usually in the field, rarely in front of a computer, so the diagnostics do not reach them in a timely manner.

A better way is to display critical device alerts on the operator stations as well, because they are always manned, and alerts will quickly be seen. Filtering is critical so only high priority alerts are shown to ensure operators are not overwhelmed, as per EEMUA (Engineering Equipment & Materials Users' Association) 191 alarm system requirements. Devices used in a SIF are usually considered high priority.

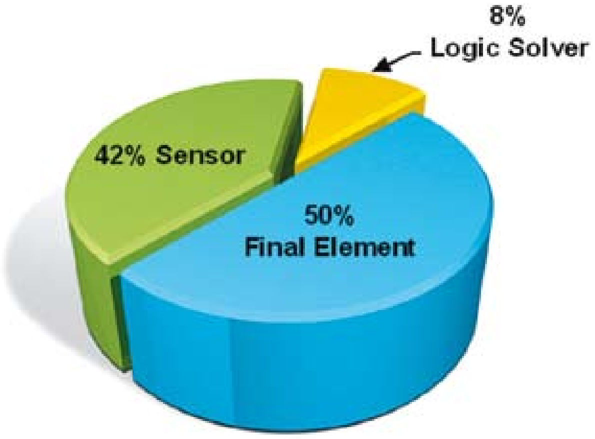
The operators cannot fix the devices, but when receiving a device alert they can decide on appropriate action to prevent the device problem from escalating into a plant shutdown. Then, they can radio the technicians to fix the problem. For this reason, diagnostics from SIF devices must go directly to those on the watch who can act quickly on device faults without first having to go to another computer and login.

In many cases, it is advisable to alert all safety personnel to every safety alert. Operator access is only to view diagnostics, so changing device configuration from the operator console is prevented.

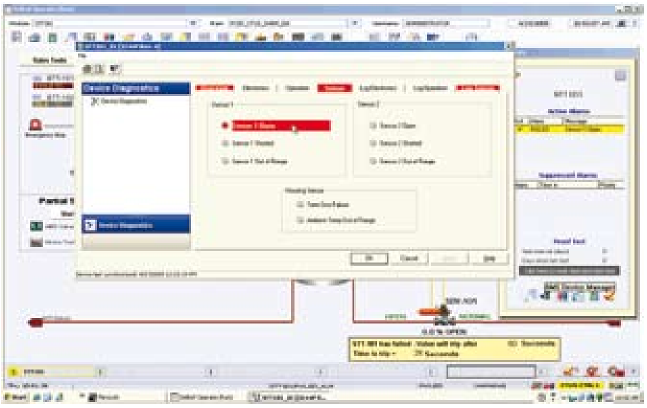
With a HART interface built into the smart logic solver, there is no need for external HART multiplexers with additional networking and interfaces. A smart SIS uses HART and EDDL to get device diagnostics to the right person in time to make a difference.

This level of visibility to SIS device problems is possible only if device diagnostics are integrated with the control and safety system. EDDL makes integration of diagnostics on operator consoles possible because the EDDL file from the device manufacturer loaded on the system is a non-intrusive, compressed text file.

Third-party device driver software would typically not be permitted on a system because it might interfere with system operation. On such a system, the diagnostics would have to be monitored from a separate, often unattended, maintenance station. EDDL does not have this limitation since the files are not programs.



Most SIF failures because the transmitters and valves are in a harsh plant environment, whereas the logic solver is indoors in a climate controlled room.



integration of diagnostics on operator consoles is possible because the EDDL file from the device manufacturer loaded on the system is a non-intrusive, compressed text file.

Smart changes

Management of change is an important part of the SIS lifecycle, which is very procedural, but where smart technology can help and save time by adding automation to some procedures.

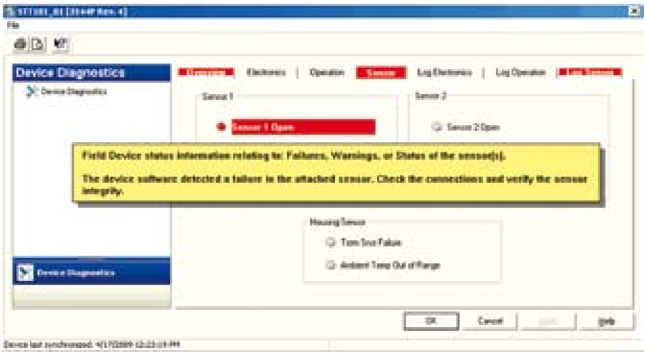
Apart from making changes to smart transmitter configuration from the device management software part of the smart SIS, changes can also be made using a handheld field communicator or from the local display on the device, although rare. The changes must be deliberate, because write protection jumpers will prevent inadvertent changes. However, all changes to devices should be logged in an audit trail.

A traditional logic solver using only 4-20 mA is unaware of configuration changes made to devices, so the traditional SIS audit trail covers only the logic solver, not changes made to the devices. A smart SIS, however, uses HART to automatically check if a device configuration, such as transmitter range, has been changed. EDDL interoperability enables the audit trail functionality to work for different types of devices from multiple manufacturers, not just some. Device failures are also logged.

Device configuration is not permitted from an operator console, only from the intelligent device management software. Even then, the technician needs a higher level authorization to access SIS devices. That is, a smart SIS uses HART and EDDL to automatically log changes to any part of the SIF to maintain an audit trail which is a complete picture of logic solver changes and field device changes. This automated audit trail saves time, improves accuracy of the record, and makes compliance with IEC 61511 easier for the user.

If a device fails because of harsh plant conditions, a failed device is typically replaced by an identical spare. In fact, a device may inadvertently be replaced by a different device type which may not have the same safety certification, PFD (probability of failure on demand), SFF (safe failure fraction), etc. But a traditional logic solver using only 4-20 mA has no way of knowing what device is connected to it, so an altered model goes undetected.

A smart logic solver uses HART to automatically detect what type of device is connected, and it raises an alarm if the wrong type of device is used. That is, a smart SIS uses HART to help sustain the



Field Device status information relating to: Failures, Warnings, or States of the sensor(s).

The device software detected a failure in the attached sensor. Check the connections and verify the sensor integrity.

Device last synchronized: 4/17/2009 12:23:19 PM

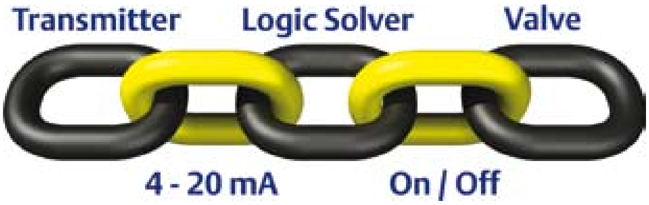
SIS transmitter diagnostics displayed based on EDDL, including manufacturer's help text.

rating of the SIS over time. This automatic check complements manual procedures that may already be in place.

Smart deployment

Another benefit of a smart SIS is the extended proof test interval for shutdown valves using the partial stroke test (PST) procedure in the digital valve controller. The PST capability is built into modern digital valve controllers; no special system configuration is required. This test can be automatically initiated by a system timer on a periodic basis, on demand from the device management software, from a local control panel in the field, or even by a command sent from an operator station.

The operator command is sent using HART communication,



A smart SIS is able to monitor the health of the entire SIF, not just the logic solver.

eliminating the need for additional PST wiring from the logic solver. Lastly, simulation enables more extensive operator training.

A smart SIS is an integral part of the digital plant architecture that uses the power of field intelligence to improve plant performance. It is not unusual to find a modern system that does control using Foundation fieldbus along with an SIS using HART to improve process availability. The fieldbus and HART devices can be integrated into the same device management software because EDDL is an integral part of both protocols.

A smart SIS makes use of existing device intelligence to reduce spurious trips, and HART is used to improve process availability. For safety, 4-20 mA is still used, but a smart SIS is able to monitor the health of the entire SIF, not just the logic solver. This includes the transmitter, the shut-down valve, and the signal path. **CEA**

Jonas Berge is Director of PlantWeb Consulting, Emerson Process Management.