

Fieldbus 202

Reliability and redundancy

- Overview
- Wiring reliability
- Segment reliability
- Total system reliability
- How much redundancy is enough?
- Transmitter redundancy
- Valve and piping redundancy
- Control redundancy
- Host redundancy options
- Other redundancy options
- Link active scheduler and backup LAS

Overview

Can I really put all those devices on one pair of wires?

This is often the first question asked by those new to the fieldbus world. That's not surprising: After years of "one set of wires for each device," at first you might wonder about the reliability of using one wire pair for several devices.

But the wires themselves are only a minor factor in overall reliability. With good design and installation practices, FOUNDATION fieldbus actually offers significant advantages in total system reliability.

This course examines the issue of reliability, along with methods for improving it -- including redundancy.

Hint: As you go through the topics in this course, watch for answers to these questions:

- *What are the major external factors affecting fieldbus network stability?*
- *What parts of a fieldbus system can be made redundant?*
- *Where is control most reliable, in a field device or in the host system?*

Wiring reliability

The major concern with wiring is not failure of the media itself, but external factors that affect the wiring.

Fewer wires mean faster repairs. Consider the damage if a physical event affects an entire wire bundle. In the world of analog point-to-point wiring, this catastrophe could involve hundreds, maybe thousands, of severed wires.

In the digital fieldbus world, however, where many devices can be connected to the same set of wires, the same number of I/O points would be on far fewer wires.

Service would be interrupted in either case. But the time to repair would be significantly less in the fieldbus scenario because there are fewer wires, and wiring checkout is faster for each wire pair. And the faster the repair, the sooner production resumes.

Reasons for assurance. Excluding external events, wire reliability is determined by the reliability of the physical wire itself -- and wire has the lowest complexity level of the system and generally the lowest failure rate.

The reliability of the wire can be greatly enhanced by following installation and maintenance procedures that avoid accidental **shorting** or **grounding**. Those are the most common causes of wiring failures.

You can also enhance reliability by selecting the wire, cable routes, and connectors that shield exposed media from physical contact with electrical discontinuities. In addition, fieldbus junction boxes are available that isolate a short-circuit to a single drop on a segment.

Segment reliability

The total fieldbus network is divided into **segments** for the purpose of aligning sections of the network with process, hazardous, or geographic areas, or with specific device combinations.

From a reliability standpoint, each segment can be treated as a separate entity, and thus can be handled separately. If a host H1 interface card connects to more than one segment, and represents a failure point that could impact more than one segment, then all segments attached to that interface card should be considered as a whole.

Segment reliability depends upon several factors such as

- Segment power and power conditioners
- Segment terminators
- The segment wire itself
- Various connectors
- Field devices connected to the segment
- The segment host (if present).

The greatest threat to overall segment reliability is loss of power, which affects the entire segment. One way to counter this threat is redundant segment power, coming from different sources.

Another threat to segment power involves electrical transients such as

- Lightning
- Solar storms
- Electrical noise.

Good installation practices, backup power with uninterruptible power suppliers (UPSs), and surge suppressors minimize disruption from these electrical transients.

Proper installation can also reduce the chances of improper grounding -- another major cause of reliability problems.

Total system reliability

A system's reliability is only as good as the reliability of each of its parts. So it makes sense that the fewer the parts, the higher the potential reliability of the system.

Fieldbus allows the control "system" to have fewer parts because control can now be done in the field.

That is, control does not have to go through all the host system's terminations, input cards, controllers, output cards, and so on — each a potential failure point.

With control in the host system, all these parts must be working properly for the control loop to be working. Failure of any of these components in a non-redundant system will cause loop failure. The number of loops affected can range from 8-16 for an I/O card failure to hundreds or even more if a controller or controller power fails.

In a FOUNDATION fieldbus environment using control in the field, however, the entire host system can fail without loss of control. That's because control is being done in the field devices. The host system is being used as the interface to a truly distributed "field control system."

Closing the loop in the field can be much more reliable than through the host.

How much redundancy is enough?

How much redundancy to have in the plant, and how to provide it, depends on the situation. It's based on things like mean-time-between-failure, system availability -- and experience. It's also based on how critical particular devices, loops, and processes are to safe and effective plant operation.

Options range from redundant measurements to redundant process streams and everything in between.

The next five topics describe some of these options.

Transmitter redundancy

Transmitter redundancy in a fieldbus environment is implemented basically the same way as in a traditional, analog environment. The primary difference is that FOUNDATION fieldbus provides additional information that improves the reliability of the measurement.

Analog transmitter redundancy. Analog transmitter redundant schemes often require triple redundancy. When two of the transmitters report different values, the value from the third transmitter "breaks the tie." All three measurements are sent to an input selector which chooses the input that gets sent to the PID. Sometimes the operator receives all three values and manually chooses the value that "looks best."

The FOUNDATION fieldbus input selector block available in some transmitters supports a broad range of input selection criteria -- from selecting the high, low, or middle value, to calculating the average of the three inputs, to eliminating the reading with the greatest deviation from the others.

FOUNDATION fieldbus transmitter redundancy. FOUNDATION fieldbus provides status information that helps automatically identify if a measurement is good, bad, or uncertain. A bad or uncertain quality reading can be eliminated from consideration before it's presented to the operator.

This capability may even eliminate the need for triple redundancy, since the third device is no longer needed to determine which signal is the bad one.

FOUNDATION fieldbus H1 does not support redundant media. Redundant transmitters are either on the same wires, or on different segments.

Valve and piping redundancy

Like transmitter redundancy, valve redundancy in a fieldbus environment is implemented basically the same way as in a traditional, analog environment. The theory is the same: two valves are more reliable than one. And the issues are the same: how much redundancy do I really need?

Best case/downside. The most reliable redundancy scheme would put redundant valves installed in parallel piping in the process. But double the valves and piping, and you double the installation cost.

So if redundancy in a fieldbus world isn't any cheaper than in the analog world, where's the advantage?

Information makes the difference. The advantage is in the information a fieldbus valve instrument provides.

Valves are mechanical devices subject to harsh process environments and wear of moving parts and are thus points of maintenance and potential failure in the process loop.

Because an analog valve controller (or redundant valve pair with analog controllers) has no way of determining valve health, it may fail without warning.

The PlantWeb advantage

Emerson's DVC 5000 fieldbus Digital Valve Controller (and thus a redundant valve pair with such controllers) has the intelligence to diagnose its own health. It can predictively and proactively indicate if it's having health problems so you can deal with them before they result in a failure.



Fewer failures, lower maintenance cost, less lost production. *There's the advantage*

Control redundancy

Typical DCS and PLC control system failures can affect a large number of loops. The loss of control, and possible equipment failure or plant shutdown, can carry an extremely high price.

The traditional method of avoiding such problems involves duplicating parts of the host control system. This redundancy means potentially a lot of extra equipment — input and output cards, terminations, power, controllers, etc. — at a lot of extra cost.

As you learned earlier in this course, control in the field allows the control function to continue even if the host system fails — potentially reducing the need for costly redundant host components.

It is worth noting, however, that when the host is lost, the operator can no longer see what's happening or control it manually from the operator console. Data will also not be available to alarm and event logs and historians. Also, the PID block in a host may offer features (such as autotuning) not available in the device's PID function block. And although regulatory control is maintained in the field devices, host resident advanced control is lost until the host connection is re-established.

You should therefore use this approach only where you can do without these capabilities until the host is available again. Until then, the field device can maintain safe, effective, on-spec control to prevent a process upset or unscheduled shutdown.

Host redundancy options

As explained earlier, control in the field will provide regulatory control in the event the host or host connection is lost. But it won't provide operator visibility, host-based advanced control, or alarm, alert, or historian data. To ensure these are available, host redundancy is needed.

Host redundancy philosophy. Many plants have standard practices for redundancy. These frequently include redundant communications, operator interface, power, controllers, and I/O. Specific implementations of redundancy depend on the requirements of the process. FOUNDATION fieldbus redundancy should conform to these practices.

Redundant host H1 interface cards. Although the fieldbus specification does not require H1 interface card redundancy, a backup H1 card will allow the operator continued visual access to the process should the primary H1 card fail. It will also provide process information needed for functions such as validation or quality systems, plus uninterrupted advanced control. If your plant or process requires these things, redundant H1 cards should be used.

Another common criterion is that redundant I/O is required if I/O modularity exceeds a certain level -- for example, 8 points per card. If redundant H1 cards aren't available, plant practices may require that the loading of an H1 segment be reduced to a level below the threshold required for redundancy.

Finally, if no device on the segment is a link master, capable of taking over the function of link active scheduler, redundant H1 interface cards may provide this capability.

The PlantWeb advantage

Emerson now offers redundant H1 interface cards in the DeltaV system that serves as the host system in a PlantWeb architecture. These cards can be removed and replaced under power.



In addition, each H1 interface card has LAS capability, providing backup LAS in the interface card.

Other redundancy options

In making the control system more reliable through redundancy, we've covered the major elements of the control loop — transmitters, valves, and host control systems. Now let's take a look at other areas of the automation architecture that can be redundant.

Custom redundancy block. This software option is a custom function block, residing in the valve, designed specifically for redundancy. The valve function block passes an output from the primary (host) PID to the valve's analog output. If the primary PID fails, the backup PID (in the valve) sends its output to the valve's AO.

Redundant air and power. Since actuators, transmitters, valves, and control systems all depend on air or electrical power to operate, making these sources redundant, or having a reliable backup, will go a long way toward ensuring a safe plant.

FOUNDATION fieldbus power redundancy includes redundant, isolated bulk power, and redundant power conditioners to the segment. This level of power redundancy provides reliable power even if a power failure occurs.

Redundant media (wire). As mentioned previously, the wire in general is the most reliable part of the control architecture. Adding a backup wire segment may make sense only if it is part of a completely redundant process stream with redundant instruments, valves, process piping, and host elements. This is implemented by having one set of valves and instruments on one segment, and the second set on a second segment. Each device is connected to only one segment and one set of physical media. In this case, a link must exist between the two segments to ensure status information is continually exchanged.

Link active scheduler and backup LAS

Link Active Scheduler. In a host control system, the control strategy generally dictates the execution of function blocks as well as communication between the blocks themselves. On a fieldbus segment, this task is the responsibility of the Link Active Scheduler, or LAS.

As the name implies, the LAS actively schedules communication and function block execution on the segment. If there is no LAS running on the segment, function block execution and communication on the segment cease.

Because the LAS often resides in the host system, the most probable cause of an inactive LAS is the loss of the host. A host-based LAS is also unavailable in the case of stand-alone loops, where a host is used for configuration and then disconnected.

Backup Link Active Scheduler. A backup LAS, usually not residing in the host, coordinates block execution and communication on the running segment when the primary LAS is lost or unavailable.

A backup LAS should be used in a host-plus-control-in-the-field scenario so that control can be maintained even after the host is lost.

If control is performed strictly in the host, that is, no control-in-the-field, then the loss of the host means loss of control, even if a backup LAS is present. The exception occurs when the host has redundant controllers and FOUNDATION fieldbus H1 interface cards, configured to take over control if the primary components fail. In this case, the backup LAS would usually be in the host system rather than a field device.

Regardless of where control resides, it's still important to make sure final control elements are selected to fail to the proper failsafe positions if automatic control is lost.

The PlantWeb advantage

Most fieldbus field devices from Emerson Process Management have backup LAS capability, which can be used without affecting device performance.

Configuring a backup LAS in PlantWeb is as simple as checking a box at device commissioning time.

