WHITE PAPER

Railway Data Security: Building a Durable NVR Platform

KW Chou

Product Manager

Bruce Chen and **Kyle Pearson**

Technical Writers

Moxa Inc.

Overview

Whether nationally or locally, a railway is always critically important infrastructure, particularly in its role as public transport. Increasingly, digital solutions are required to supplement every level of railway operations, both in day-to-day customer service and minute-by-minute management, maintenance, and oversight.

To better serve passenger safety and logistical efficiency, in the coming decade digital technology systems will be commonly found on every railway. Such solutions include (but are not limited to) devices like network video recorders (NVRs) and passenger information systems, and will require powerful computing hardware to support them. Because of the special, ever-present environmental challenges that railways create, commercial hardware is unacceptable. Instead, digital devices on railways must be industrial grade, to ensure durability and resiliency. Take networked video recorders as an example: an NVR is a software package, typically one that runs on a dedicated, embedded device. When paired with an NVR, the computing platform is primarily tasked with receiving video streams and saving them in a conveniently retrievable format. An NVR deployed on a suitably robust computing platform may share the hardware resources with other applications, like passenger information systems, which provide real-time information to mass transit passengers, and are another example of software that will be commonly deployed on railways. Just as NVRs will require high performance hardware, so too these wireless systems will require a powerful, sturdy computing platform with large capacity storage devices.

The Challenges of Train and Trackside

Commercial computing platforms are unfit for these applications because railway solutions involve massive, constantly moving vehicles operated by crews of only one to three individuals. This presents several key challenges:

1. Unless manageable from a centralized, single switch, restarts and shutdowns are a tremendous problem. Railway computers will be installed in cabinets, perhaps one to a carriage; each cabinet may well contain an uninterruptible power supply (UPS) alongside one or more devices. Verifying that these discrete, onboard systems are each either off or on, as intended, will be laboriously time consuming and error prone if executed car-by-car, cabinet-by-cabinet. Railway computers must, therefore, be conveniently linkable to a centralized, single-switch power management system.

Released on January 15, 2013

How to contact Moxa

Tel: 1-714-528-6777
Fax: 1-714-528-6778
Web: www.moxa.com
Email: info@moxa.com

2. Another critical challenge is temperature tolerance, which must be capable of enduring greater extremes than commercial devices can. Due to space limitations, railway computers are installed in unventilated cabinets, usually with no climate controls. In these confined spaces, heat can become a serious problem, so making sure the computers will work reliably in extreme temperatures is an imperative.

3. On any moving vehicle—but particularly on trains—vibration and shock are critical issues that will easily and quickly cause serious damage to stock digital storage platforms.

4. Finally, power surges and brief, intermittent failures are constantly occurring on trains. Consequently, to meet the international standard for railway computers, EN 50155, all onboard computing platforms must be protected against surges and have low-level mechanical failsafes in place to protect against power hiccups and strong surges.

Four Technologies to Safeguard Railway Computers

Industrial designs overcome these challenges in the following four ways:

- Centralizing power controls using digital or serial interfaces.
- Carefully engineered temperature tolerance.
- Steady operations despite constant vibration and/or strong shocks.
- Protections from inconsistencies in the power supply such as surges and failures.

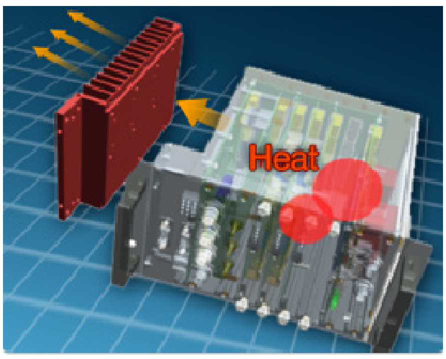
The challenge and design solution for each of these points is reviewed in detail below.

Centralized Power Controls and Failsafes

Several solutions may be used to centralize the shutdown and boot process; the most common and direct involves wiring the computer power controls to a remote switch using digital I/O, or a user-installed relay. The BIOS can be adapted so that computers automatically boot up the moment the switch receives a signal, or to cleanly shut down the OS once the signal to turn off is received. In this way, the train operator can power up (or down) all computers simultaneously, from a central control station, and always be certain that the machines are on or off, as expected. There is an additional benefit, as well: because devices may be configured to power up without physically triggering the local, individual switches, then when the ACPI is set for an automatic reboot following a power failure each offline device will, following an unexpected power failure, automatically re-boot after the power supply is re-established.

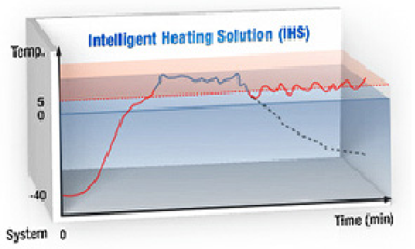
Extreme Temperature Tolerance

To say that a computer works reliably in extreme temperatures means that it will continue to function as expected under both high and low temperature extremes. Beating high temperatures is a relatively direct engineering problem: maximize heat dissipation by any and all means, and if needed (though preferably not) apply active cooling systems. Active systems typically mean fans, however, and fans introduce a considerable point of failure. By turning the entire computer into one large heat sink and giving painstaking attention to layout, materials, and components, high thermal tolerance can instead be achieved using only passive means, even to the point of eliminating fans and



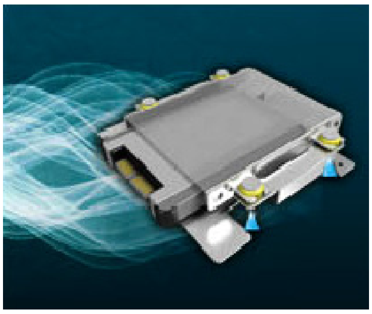
other cooling mechanisms.

Yet temperature controls should still be built into the computer. High thermal tolerance does not mean 100% tolerance for all conditions. If the device is used for long enough, eventually circumstances will arise where the environment is simply too hot for any existing computer or storage drive. For these situations, a temperature sensor should be installed to monitor ambient conditions so that failsafes can be initiated by the local operating system whenever worst-case conditions arise. For these most severe cases, power to the hard disk (the largest generator of heat after the CPU) will be cut, and any new data be recorded to a solid-state, non-volatile buffer until the temperature returns to within the operable threshold.

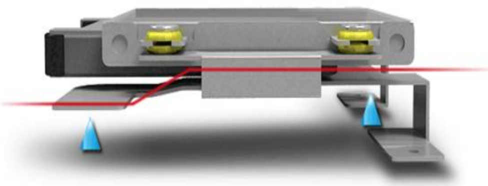


At the opposite extreme, guaranteeing a computer will still work well under extremely low temperatures means adding heat, rather than eliminating it. For climates where temperatures can drop to well below zero, an intelligent, on-board heating solution is necessary to warm the device to an operative temperature before the computer can make itself available to the network. Again, this means a sophisticated, fully automated design that combines an onboard heater with intelligent software controls.

Vibration and Shock Safeguards

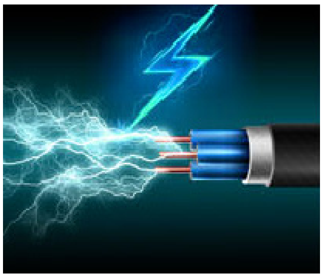


Vibration might be the biggest engineering challenge for computers designed to be used on moving trains. One important part of the solution is to use either solid state drives (which have no moving parts), or industrial-grade hard disks that have been engineered to withstand long periods of heavy vibration. By mounting these already sturdy drives on a highly shock-resistant bracket, the natural tolerances of these devices are significantly enhanced.

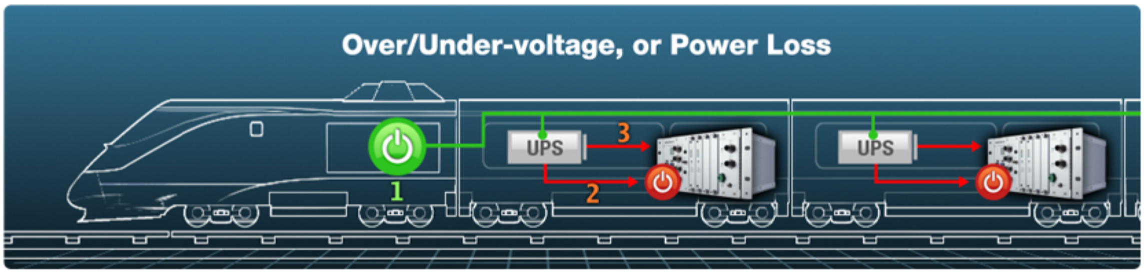


Yet these workarounds may still not be enough. The only way to ensure that a device remains unaffected by strong vibrations is to build an independent vibration sensor into the platform, one that may be directly accessed from within the operating system, so that vibration conditions may be monitored and recorded for analysis and system adjustment. With better awareness and the drive preparations mentioned above, significant increases in MTBF may be achieved even within the highly shock- and vibration-prone environment of a moving train.

Power Supply Protections



Regardless if they are on the train or at the trackside, protection of the power supply—and *from* the power supply—is the last critical problem that railway systems must overcome. To meet the EN 50155 standard, railway computers must provide a range of power inputs that includes 24, 48, 72, 96 and 110 VDC. More importantly, however, the standard also includes a stipulation for a high tolerance of intermittent power interruptions. To meet the EN 50155 Class S2 regulations—the strictest class defined—a device must be able to maintain operations through a 10ms power interruption. As above, there is more than one solution to this problem.



Step 1: The system powers down or power is lost.
Step 2: The UPS signals its client computer that it must shut down and the OS initializes the shutdown process.
Step 3: Finally, the UPS waits until the computer has powered down and powers itself down.

A UPS is the most immediate and convenient method for backing up and ensuring against power supply failures, and a reliable buffer against power spikes. A UPS may also, however, serve an additional role: by using serial or digital I/O communications, a UPS may also be set up to serve as a system monitor and local control device. The moment power is lost, the UPS can maintain normal operations while it automatically initializes a safe shutdown. In this way, computers which have been cut off from their regular power supply will still power down using the standard system shutdown process, guaranteeing your data and storage drives remain secure and properly synchronized.

However, the protections provided by a UPS may not be enough to justify the installation and configuration of an additional device. Space may be too precious, and the increase in overall costs may be prohibitive. If these are significant obstacles to system deployment, then a device fitted with on-board capacitors and optical isolation becomes very attractive. Optical isolation protects the device from electrical surges, per EN 50155. The capacitors, on the other hand, store a small power reserve which the device may call upon to act as its own internal UPS during brief interruptions in the power supply. While the computer will remain susceptible to sudden, catastrophic power failures, it will nevertheless meet the EN 50155 Class 2 specification, making it an excellent choice for systems where a UPS is too much.

Conclusion

Computers used in railway applications require more sophisticated and thoughtful designs to cope with the peculiar challenges presented by moving vehicles. Advanced technologies are needed to safeguard such computers from the conditions that will inevitably arise as they serve passengers and operators. Moxa's TC-6110 Series computers are built specifically for railway solutions, and provide users with all of the above features, and more: safe, reliable, and automated power controls; built-in temperature and vibration sensors; and protections from power surge and interruption, bringing the TC-6110 into full compliance with the EN 50155 Class 2 standard.