

Your White Collars Could Use Some Starch
Are standard laptop PCs durable enough for your mobile workforce? It depends on how much failure you can tolerate.

Integrated Solutions, March 2003

Written by [Tom von Gunden](#)

If your goal is to expand your mobile enterprise, it doesn't matter what color of collar your employees are wearing - blue, white, or whatever. If you attempt to equip an increasing - and increasingly mobile - workforce simply with consumer-grade laptops, you can expect frequent hardware breakdowns, repairs, and replacements. Even your white collar employees can do plenty of damage - both to their machines and to the bottom line for your mobile computing budget. As Rance Poehler, president of mobile hardware vendor Panasonic Computer Solutions (Secaucus, NJ), explains, "Studies from industry analysts show that plastic retail notebooks can have you facing up to a 20% annualized failure rate. When workers regularly grab those notebooks from their desktops and head outside the building, that rate can jump to as high as 30%." According to Poehler, rugged notebooks and tablets, by contrast, can push those failure rates way down - to below 10%. "Imagine the productivity gains you would realize if you could improve your uptime from, say, 70% to over 90%," he says.

So, even if workers aren't carrying their mobile devices into dust-laden manufacturing sites or cold storage facilities, they're moving - and bumping, banging, and dropping - their machines. "Mobile professionals doing a lot of traveling typically don't expose their computers to a wide range of environmental challenges, but they do need their computers to meet rugged mobility requirements," explains Richard Perley, senior VP for mobile computing provider Xplore Technologies Corp. (Austin, TX).

In upgrading your mobile workforce to rugged notebooks or tablets, consider two key factors: 1) What kinds of environments will users be taking the devices into? 2) Does the device need to have real-time wireless access to the home office? (The answer to #2 is almost certainly "yes.") The first factor will help you evaluate a device's ability to withstand environmental or movement-based threats to its operation. The second will help you determine which network connectivity capabilities the unit must have.

What Makes 'Rugged' Rugged?

Rugged mobile computers come in three broad categories: semi-rugged (sometimes referred to as "enhanced commercial-grade"); rugged; and ultra-rugged (or, "military-hardened"). To verify vendors' claims about a unit's level of ruggedness, check for documentation showing the unit has been tested for various specifications under the military 810F standard. The 810F specifications cover environmental engineering concerns, such as resistance to humidity, sand and dust, extreme temperatures, immersion, vibration, and shock. Devices marketed as semi-rugged should meet one or two of the specifications. Rugged devices should meet several. And, ultra-rugged devices should meet all military 810F criteria. Of course, you'll want to ensure the unit you are considering has passed tests for the environmental or mobility factors your mobile workforce is most likely to encounter.

Despite the differing degrees of ruggedness, there are common design features distinguishing even semi-rugged notebooks and tablets from their non-rugged counterparts. Metal enclosures (commonly including magnesium in their composition) protect internal components against vibration and shock. In addition to protecting the outer shell, magnesium may be used inside the unit - for example, as a supplemental layer around the hard drive. External components, such as the LCD, are often protected with bumpers made of special damping materials for added resistance to vibration and shock.

Rugged mobile computers may also be equipped with suppression devices that control levels of

disrupting or being disrupted by other electronic devices in the local environment.

The evaluation of hardware features should take into account the ever-diminishing intervals between computer sessions. For many employees, a workday is best described not as a series of isolated computing events but rather as a nearly seamless event that shifts from place to place. According to Dale Szymborski, president of rugged hardware vendor Kontron Mobile, Inc. (Eden Prairie, MN), companies should consider what a single user's mobile computing experience might entail from moment to moment. "Workers know what they need the computer to do to bring efficiency to their jobs," he says. "They may need to be able to read the display indoors and outdoors. They may need the device to have long battery life, and they may need to hot swap the battery. They may need to use the computer as they drive and have a reliable way to get the computer in and out of a vehicle. Or, they may need it to do all of these things."

Protect Wireless Transmissions

Most mobile computing deployments require real-time wireless data transmission. Quickly receding into the "remember when" category are applications that had mobile workers doing end-of-day data dumps back at the home office. In response to the need for reliable real-time service, rugged computer manufacturers build into their devices specific protections for the physical components that enable wireless communications.

First and foremost is the location of the radio antenna. Non-rugged laptops typically transmit wirelessly via PC Card-based antennas inserted into the devices. Those exposed antennas are highly vulnerable to damage. Even rugged units may have externally mounted, rod-shaped antennas - less vulnerable but still not immune. "Imagine a plastic notebook with a PC Card with an antenna on it sticking out of the side of the unit," says Poehler. "Sometime during frequent mobile use, that antenna is going to break. Annualized failure rates as high as 80% to 90% have been reported for that kind of design." By contrast, the trend in antenna design for rugged notebooks and tablets is to integrate the antenna as part of the unit - building it into the casing and protecting it with metal enclosures or damping bumpers.

Beyond the reliability of the physical antenna, wireless communications depend on the rugged device's ability to accommodate current and emerging data transmission standards and protocols. And, it can't rely on handling only one. "To give the user optimal mobility, the device will have to be able to work in diverse network environments," says Matt Gerber, VP of marketing for rugged hardware manufacturer Itronix (Spokane, WA). "A utility worker, for example, may begin the day with a wired connection in the home office's briefing room. Then, that worker may move across the corporate campus and jump to an 802.11-enabled wireless LAN connection or onto a Bluetooth infrastructure. Out in the field, that worker may need to establish communications via multiple radio technologies and transmit data over CDMA [code division multiple access] or GPRS [general packet radio service] wireless protocols."