GENERAL DYNAMICS | intel

# Essential Technologies for Vehicle-Rugged Notebooks

IT managers, equipping employees whose offices are on wheels, must determine which computers can survive the demanding vehicle environment without carrying the cost premium associated with fully-rugged systems. For many professions, such as law enforcement, public safety and telecom, notebooks are docked in either vehicles or offices and aren't exposed to the harshest conditions, like a rainstorm. The mobile workforce needs a notebook with the right mix of durability, performance, security and cost, somewhere between commercial-grade and fully-rugged. A new category of notebooks, called "vehicle-rugged," meets these requirements.

This white paper reviews leading-edge technologies that IT managers should evaluate and consider when selecting a vehicle-rugged notebook. These technologies provide durability for the road, office-level computing performance, and added security to protect confidential data.

## Working On The Road

Everyday, millions of workers are dispatched in vehicles to provide essential services such as emergency response, line outages and installation requests, as shown in Figure 1. Although they represent a diverse collection of governmental and commercial entities, these workers have similar in-vehicle computing requirements.

The vehicle-based workforce requires durable computer systems that can withstand extreme environmental conditions with respect to lighting, vibrations, bumps, temperature range and space constraints. Computing performance requirements of vehicle and business-office users are comparable, both running multiple applications and processing different types of media. For example, law enforcement officers use notebooks for dispatching personnel, mapping locations, identifying who to call, looking up vehicle licenses and criminal history, and ticketing. When writing reports, they include pictures and videos that must be edited, cut and pasted. Over the entire shift, vehicles are recording video and generating huge amounts of data that's eventually downloaded over wireless networks at the precinct.

In the field, workers also need access to all sorts of confidential information in order to do their jobs. Since their computers aren't protected by bricks and mortar, notebooks need to safeguard data using the best available security technologies. And because these systems are used outside the office, they should have a display that's easy to read in all outdoor lighting conditions. Table 1 summarizes mobile worker notebook requirements and expectations, which are addressed by the innovative technologies described in the following sections.


**Figure 1.** Examples of Vehicle-Rugged Notebook Deployments

**Table 1.** Key Requirements: Vehicle-Rugged Notebook

| Requirement | Expectation |
|---|---|
| Durability | • Survive bumpy rides, vibration, temperature extremes, drops, spills, humidity and dust |
| Computing Performance | • Deliver business-class computing performance and high-speed wireless throughput |
| Security | • Protect against unauthorized system usage, data accesses and theft |
| Viewability | • Integrate a display that's easy to read in all indoor and outdoor lighting conditions |

**Table 2.** Durability Test

| | Drop | Moisture |
|---|---|---|
| **Vehicle-Rugged** | 30-inch drops | Spill-resistant keyboard |
| **Fully-Rugged** | 36-inch drops | Seven gallons of water blown at 40 miles per hour for 60 minutes |

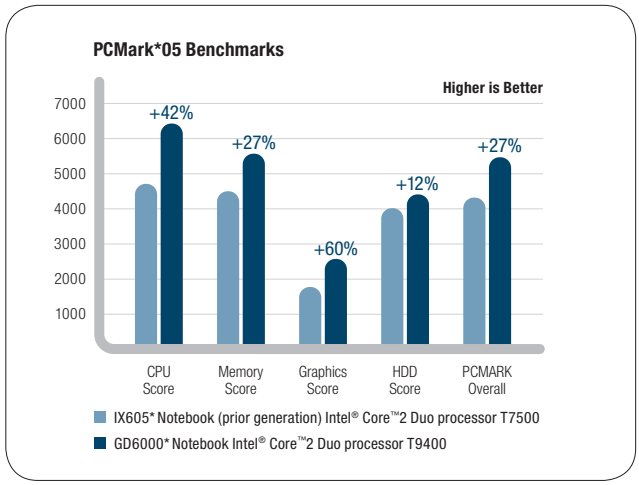


**Figure 2.** PCMark*05 Performance Benchmarks

## Durability Technologies

Vehicle-rugged notebooks are designed to handle more punishment than consumer notebooks. They are more susceptible to abuse, like getting knocked around when moved between offices and vehicles or spilled on when workers drink beverages in the vehicle. To achieve a level of industrial-grade toughness and reliability, vehicle-rugged notebooks are nearly fully-rugged, passing most every mil spec test. Vehicle-rugged notebooks are typically not tested under all fully-rugged conditions (e.g., drop and moisture) as shown in Table 2.

The majority of notebooks docked in vehicles won't experience the severest conditions, and as a result, vehicle-rugged notebooks can be produced less expensively than their fully-rugged counterparts. Still, vehicle-rugged notebooks require special durability technologies, performing consistently over a wide range of use conditions to protect components from dust, drop, vibrations and humidity. For instance, it's not acceptable for a sealant that successfully keeps water out at -10 degrees Fahrenheit to become porous at 145 degrees because of its expansion properties.

It's possible for a technology to be effective for one condition, like vibrations, yet detrimental for another condition, like drops. For example, a super spongy material that prevents damage from a 10-meter drop may not be rigid enough to protect against vibration, where a more rigid material is preferable. In this case, two distinct technologies are needed to temper vibration and drop; they must work the same way across the temperature range and withstand huge spikes of energy as well as subtle energies.

## Computing Performance Technologies

"The introduction of mainstream multi-core processors signals a major shift in the 'shape' of all computing platforms," says Markus Levy, President of EEMBC and the Multi-core Association. Multi-core architecture is now the vehicle for delivering higher computing performance, yielding processors with significantly higher raw performance and performance per watt than prior single-core processors. With greater power efficiency, docked notebooks consume less battery power and dissipate less heat, which is known to improve reliability.

Delivering greater CPU performance has traditionally been accomplished by cranking up the CPU clock speed at the expense of greater power dissipation, sometimes north of 150 watts. Today, chip makers are increasing computing performance by adding more processor cores that consume less power because they are clocked at slower speeds and supplied with lower voltage. And with more cores, users can run multiple applications simultaneously (e.g., up-load data and edit video) and experience faster system response.

Advances in processor technology are driving large performance gains, as demonstrated by the benchmark results for two General Dynamic Itronix notebooks shown in Figure 2.[1] The CPU score for the GD6000* is approximately 42 percent higher than its predecessor, the IX605.* Much of this performance improvement is attributable to the Intel® Core™2 Duo processor T9400$^{\Delta}$ used in the GD6000, which enhances system performance by improving key features such as core frequency, front side bus speed and

cache size. It can outperform its predecessor, the Intel® Core™2 Duo processor T7500,[A] without increasing power consumption by taking advantage of Intel's 45nm process technology and advanced power management technologies that regulate power consumption of the two processor cores.

It's a good idea to save power when a notebook is idle or lightly loaded. This can be accomplished by allowing users to turn devices on and off or throttle devices with the power management software. The software gives users more granular control over power consumption and battery runtime. Management software can also transition the processor and peripherals into different power-saving states, like "hibernate," when processing demand is low. This is done using an industry-standard protocol called ACPI (Advanced Configuration and Power Interface) to communicate with the operating system, which manages the power states of the processor.

## Security Technologies

Vehicle-rugged notebooks should incorporate multiple security features, perhaps even more than commercial-grade systems, to protect users, information and networks. Because vehicle-based systems are often multi-user, vulnerable to theft and access privileged information, a greater level of protection could be warranted. There are many security technologies worthy of consideration and several are described in the following.

- **Trusted Platform Module (TPM):** TPM is implemented via a microcontroller with cryptographic functionality used to generate unique RSA keys, which create an extra layer of authentication. In effect, TPM pushes security down to the hardware level and, in conjunction with software-level solutions, offers more robust security. The security keys are used for a variety of functions, including: verifying the identity of a PC; signing, encrypting, and decrypting e-mails and digital documents; managing full-drive encryption; and helping to assess the security and integrity of the host device.
- **High Security BIOS:** Passwords are used to restrict unauthorized data access and transfer, but those that are entered post-boot may be vulnerable to potential operating system security holes. A high-security BIOS solves this problem by requiring users to enter a pre-boot password, an additional layer of security, which is relatively tamper-proof.

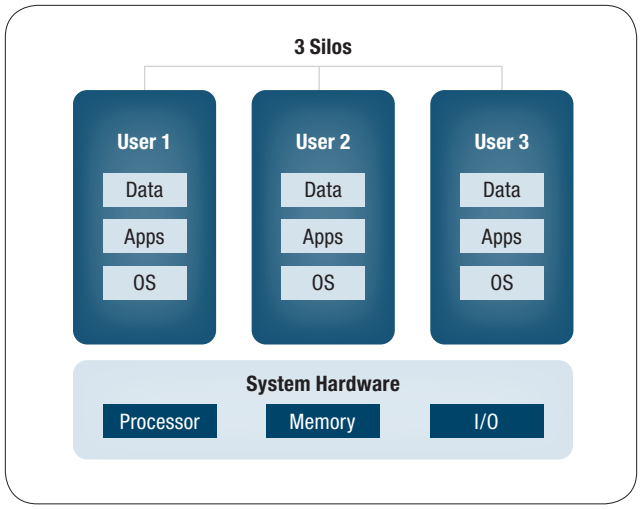


**Figure 3.** Virtualization Creates Separate Computing Environments

- **Virtualization Technology:** Virtualization can be used to set up secure computing environments, or silos shown in Figure 3, for each user in a multi-user environment. These silos protect user data and applications from being accessed by others and enable the enforcement of various data confidentiality and permission levels. When users check out the notebook and enter their credentials (e.g., password or fingerprint), they have access to everything in their enclave, but no one else's. Users are prevented from going outside of the computing environment defined by their silos.
- **Computer Tracing Agent:** In the event of theft, a notebook can be protected against unauthorized access with a computer tracing agent and special functionality deployed in the BIOS software. As soon as a stolen notebook accesses the Internet, a service provider sends a message to lockdown the system; the BIOS responds by shutting down the system and preventing any future system reboots, which renders the system inoperable.
- **Stealth Control:** To make notebooks less intrusive or detectable, stealth control, implemented in BIOS, provides greater flexibility to control the boot process, such as disabling speakers and wireless antennas or controlling screen brightness.
- **Removable Hard Disk Drive (HDD):** During a compromising situation (e.g., battlefield), users can protect their data and move faster by carrying only the HDD, not the entire notebook.

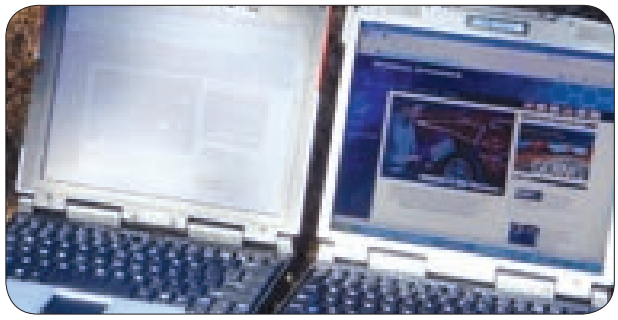

**Figure 4.** Visibility Comparison: DynaVue* on the right-hand side

## Durability, Performance, Security and Viewability

Vehicle-rugged notebook is a new category of computing systems for workers on the road, as demonstrated by the GD6000 from General Dynamics Itronix. The only notebook optimized for vehicle deployments, it provides users all the durability, computing performance and security features at a price point that is significantly less than fully-rugged systems. The GD6000 is nearly fully-rugged, designed to pass almost every mil spec test. Workers moving from vehicles to more ergonomic environments, on company premises or at home, will benefit from office docking stations with external keyboards, mice and displays.

Equipped with the Intel Core 2 Duo processor, the GD6000 supplies office-level computing performance and is virtualization-ready. The notebook supports a rich set of security features that establish extra layers of protection to overcome the additional risks associated with working outside the office. The GD6000 also incorporates industry-leading touchscreen display technology, called DynaVue,* which optimizes viewability in all lighting conditions, including direct sunlight, as shown in Figure 4. DynaVue is based on filtering technology that achieves a dramatically improved contrast ratio to provide rich color and sharp images. Since DynaVue does not rely on adding light to improve visibility, it consumes less power than standard displays, which extends battery runtime.

IT managers can lower notebook total cost of ownership (TCO) by using Intel® technologies[2] that increase the level of computing performance, security and management, including:

- Intel® Virtualization Technology[3] (Intel® VT) – enables high system performance, even when multiple operating systems and applications are running simultaneously.
- Intel® Trusted Execution Technology (Intel® TXT) – complements security software by creating another layer of protection using hardware-based security features.
- Intel® Active Management Technology[4] (Intel® AMT) – allows IT to scan and fix a computer that has crashed or is powered off.

Now IT managers can provide mobile workers with all the benefits of a fully-rugged computer they need, while at the same time reducing capital expense.

For more information on the General Dynamics Itronix GD6000 vehicle-rugged notebook, please visit **www.gd-itronix.com/index.cfm?page=Products:GD6000**.

Additional information about Intel® embedded products can be found at **www.intel.com/products/embedded/index.htm**.

GENERAL DYNAMICS | intel

[Δ] Intel processor numbers are not a measure of performance. Processor numbers differentiate features within each processor family, not across different processor families. See www.intel.com/products/processor_number for details.

[1] Performance tests and ratings are measured using specific computer systems and/or components and reflect approximate performance of Intel® products as measured by those tests. Any difference in system hardware or software design or configuration may affect actual performance. Buyers should consult other sources of information to evaluate the performance of systems or components they are considering purchasing. For more information on performance tests and on the performance of Intel products, visit www.intel.com/performance/resources/benchmark_limitations.htm.

[2] In addition to an Intel technology-ready computer, like the GD6000, these technologies require software that is available through a number of commercial vendors.

[3] Intel® Virtualization Technology requires a computer system with an enabled Intel® processor, BIOS, virtual machine monitor (VMM) and, for some uses, certain platform software enabled for it. Functionality, performance or other benefits will vary depending on hardware and software configurations and may require a BIOS update. Software applications may not be compatible with all operating systems. Please check with your application vendor.

[4] Intel® Active Management Technology (Intel® AMT) requires the computer system to have an Intel® AMT-enabled chipset, network hardware and software, as well as connection with a power source and a corporate network connection. Setup requires configuration by the purchaser and may require scripting with the management console or further integration into existing security frameworks to enable certain functionality. It may also require modifications of implementation of new business processes. For more information, see www.intel.com/technology/platform-technology/intel-amt/.



Printed in USA 0309/TB/OCG/XX/PDF 321602-001US