BLUE-RIBBON DEVELOPMENT
FOR SECURE, RELIABLE SYSTEMS
In the investment world, we’re familiar with “blue chip stocks” – the solid, reliable choices that consistently produce good returns, outperform their competitors, and never succumb to wild dips or corrections in the market. Every industry has its blue chips, and every investor has their favorites.

In the technology world, there are also blue-chip companies that supply the most solid, reliable, and trouble-free components to their clients and customers. Intel has been one of those blue-chip vendors for more than 30 years, but its “portfolio” recently got even better. With technologies from the extended Intel family, embedded software leader Wind River* and security pioneer McAfee*, Intel delivers a one-two-three punch that is the envy of product-development teams.

**Greater Than the Sum of Its Parts**

Everyone is familiar with Intel’s role in the personal computer (PC) market, and how Intel’s breakneck pace of progress catapulted PCs into the mainstream industry they are today. Less well known is Intel’s role in embedded systems, the electronics that surround us and drive the global infrastructure. From factory automation systems, to power generation, to wireless base stations, and innumerable other ubiquitous systems, Intel chips power everything from the everyday to the exotic.

Today’s embedded systems are as complex as yesterday’s PCs. Indeed, sometimes they really are like PCs, repurposed or redesigned to accommodate different embedded, industrial, medical, or high-reliability requirements. More often, however, embedded systems are designed from the ground up and are uniquely tailored to their purpose, whether it’s monitoring a power substation or delivering individual medical care. But regardless of a system’s provenance, they all share some things in common – and not all of them are good.

As embedded systems become more complex and more ubiquitous, they also become more vulnerable to failure or attack. The rise of widespread wireless connectivity also leaves these systems more exposed to outside attacks. In short, today’s embedded systems need the same kind of cyber- and anti-hacking protection as any computer. Maybe even more so. It’s one thing to lose the data on a PC to hackers. It’s another to have a power station’s monitoring systems brought down, or to lose faith in the security of a medical device, surveillance system, or robot controller. Computer breaches can cost money; insecure embedded systems can ruin lives and careers.

That’s why Intel is at the forefront of securing embedded systems with its three-part strategy. First, there’s the secure silicon. Intel’s wildly popular microprocessors include innumerable features that make the chips themselves secure, robust, and trustworthy. Second, Wind River provides one of the industry’s most trusted real-time operating systems and embedded software, giving embedded programmers a safe and secure foundation for their products. And third, McAfee’s industry-leading security technology – which often goes far beyond the familiar antivirus products – adds a tough layer of armor around modern embedded systems. All three complement one another to provide something greater than merely the sum of their parts. The Intel/Wind River/McAfee combination delivers investment-grade components to engineering firms in any market.

**Secure Silicon**

Intel’s security suite starts with Intel chips, of course. For decades, the family of Intel® architecture (“x86”) microprocessor chips has included security features that
other microprocessors just didn’t have. It starts with Intel architecture’s four-level privilege hierarchy, which separates all software into four distinct privilege levels, or rings. Programs can’t move outside their ring, so low-privilege programs can’t interrupt or interfere with higher-privileged code. These rules are enforced in the silicon itself, so they can’t be sidestepped, ignored, or thwarted by malicious code. These privilege rings have been a part of every Intel architecture processor for 20 years, with continual enhancements and improvements over that time.

Then there’s the chips’ memory-protection units, which prevent buggy (or malicious) programs from overwriting memory, possibly corrupting data, breaching security, or causing failures. Like the privilege rings, Intel chips have offered memory protection for years, and it’s a feature that programmers have come to rely upon. Intel® processors also offer an execute-disable (XD) bit, a silicon “on/off switch” that disables the ability to run arbitrary software, one common vector for attacks. These features, and plenty more, make Intel architecture’s processor family a safe, secure, and reliable foundation for even the most mission-critical systems.

Wind River* Means Real Time
But the security features don’t stop there. Even safe and secure systems can fail. Bugs, programming mistakes, and simple software errors can bring down a system just as rapidly as a focused attack. That’s why reliable commercial-grade software with built-in security capabilities is so important for modern embedded systems across market segments.

For more than 30 years, Wind River has been the blue-chip standard with its real-time operating system (RTOS) and broad portfolio of embedded software. First with its VxWorks® product RTOS, later with its industry-leading embedded Linux®, and now with its platforms for intelligent systems, Wind River has been the preferred choice for engineering teams with an emphasis on reliability and robustness. From the early days, Wind River software has been optimized for Intel architecture processors, and that connection is even stronger today.

In addition to its runtime embedded software, Wind River also provides top-grade development tools for the programmers and engineers who have to make these systems work. Wind River’s tools for development and debugging and its simulation software can effectively make time stand still or even run backwards, allowing programmers to find and fix bugs in uniquely powerful ways. Development teams can work remotely, even across continents, and stay on the same page using full system simulators, enabling around-the-clock development before hardware is even available. It’s a whole new level of full-system design, available now through Intel and Wind River.

McAfee® Security Layer
Viruses, worms, Trojans, and assorted malware used to be just the province of networked computers. But now everyday embedded systems are subject to the same attacks, and more. That’s why industrial-grade security technology is required for every type of medical, industrial, automotive, communications, or aeronautic system. Any development team that doesn’t design-in security from the outset is likely to find itself starting over again, perhaps after a rude introduction to their product’s security holes.

Design teams can leverage McAfee’s software-based security in their own systems, hardening

“McAfee* has been the leader in computer security for years, and now that expertise is focused on Intel-based product development.”

McAfee’s software-based security helps embed embedded products against viruses, denial-of-service attacks, network scans, Trojans, to name a few. The company’s around-the-clock threat detection keeps developers apprised of the latest outbreaks. Encryption and filtering technology help keep threats from...
“The wisest investment a product team can make is to rely on the most reliable and most secure tools they can get.”

penetrating the system in the first place. It’s like having an entire company focused on protecting your system – which is exactly what they do. What embedded system isn’t important enough to warrant that kind of security?

Summary

Product development has always been tough. That’s why engineers and programmers are highly compensated, and why good program managers build good teams that are productive and efficient. But now, with always-on Internet connections, numerous wireless standards, ubiquitous connectivity, real-time demands, regulatory approval, and shorter product life cycles, those jobs became tougher still. With that solid foundation, developers can create new products and new value. They can focus on their value-add, and worry less about the basic details. Blue-chip companies always were the best investment.