

# A Modular, Flexible Internet Traffic-Monitoring Solution for Networks of Today and Tomorrow

An AdvancedTCA<sup>®</sup>-Based Security Solution from RadiSys and IP Fabrics

## Table of Contents

<i>Executive Summary</i> .....	1
<i>The Challenge: Develop a Modular, Flexible, High-Performance Network Solution</i> .....	2
<i>Today's Response</i> .....	2
<i>Next-Generation Requirements</i> .....	2
<i>The Solution: Build on Modular Architecture With Off-the-Shelf Components</i> .....	3
<i>The Details: Building Blocks From RadiSys, Intel, and IP Fabrics</i> .....	3
<i>RadiSys Provides Open, Modular Architecture</i> .....	3
<i>Intel Provides Protected Content Processing</i> .....	5
<i>Intel Provides Security Software Tools</i> .....	6
<i>A Virtual Machine (VM) Model Harnesses the Power of Network Processor Units (NPU's)</i> .....	7
<i>IP Fabrics Provides Packet Processing Language (PPL)</i> .....	7
<i>The Future: Utilizing Building Blocks</i> .....	8
<i>Example: Security Gateway Platform</i> .....	8
<i>Time is Market Segment Share and Money</i> .....	8
<i>Conclusion</i> .....	10

## Executive Summary

*The proliferation of Internet, VPN, and broadband networks has heightened security awareness among network administrators. Given the essential role of the Internet in the world of business and commerce, transaction and information security is a top priority for corporations and governments worldwide.*

*As developing markets join the networked world and more networks become IP-based, potent new viruses and other security challenges are emerging. Traffic volume and the need for deep packet and sophisticated "stateful" inspections are increasing steadily.*

*To counter the escalating number and variety of security attacks, a network security solution must be scalable, flexible, easily updatable, and customizable.*

*A modular architecture like Advanced Telecom Computing Architecture (AdvancedTCA<sup>®</sup> or ATCA<sup>®</sup>) combined with off-the-shelf solutions addresses the need for high-performance security solutions that handle deep packet processing at multiple gigabit wire speeds. The solution described in this paper is based on the RadiSys Promentum\* ATCA-7010, Intel<sup>®</sup> building blocks, and IP Fabrics software and tools.*



# The Challenge: Develop a Modular, Flexible, High-Performance Network Solution

Today’s mobile, always-connected road warriors demand fast and protected connections to their mission-critical data. Service providers vying for such highly profitable business users must deploy networks that offer security and high-bandwidth connectivity.

Network systems must monitor and thwart ever-changing and increasingly complex threats to large amounts of data. As security attacks and viruses become more sophisticated, network security devices must include intelligence to adapt to the mutations of viruses and worms. The challenge does not stop here. Users have little tolerance for slow response times due to virus scanning or security authentication.

## TODAY’S RESPONSE

Network administrators and service providers have responded to security attacks by deploying discrete security devices, such as firewalls and intrusion detection services. However, because they inspect each packet that enters the network, these devices can create access bottlenecks and slow business activity.

Various network processor solutions have been employed for high-performance packet processing. The following table summarizes some of the trade-offs involved.

## NEXT-GENERATION REQUIREMENTS

As telecommunications equipment manufacturers (TEMs) implement their IP-based, next-generation architectures for 3G wireless and broadband infrastructures, they face the challenges of providing security capabilities built into their architecture. Typical security packet processing requirements for such network elements include:

- **High bandwidth**—Multi-Gigabits up to 10 Gbps to stand up to today’s needs and future growth.
- **Scalable and cost-efficient**—Scalable solution that lowers the cost of providing protected and efficient packet processing.
- **Adaptable to mutating viruses and worms**—Ability to be upgraded and evolved in the field.
- **Designed for reuse**—Flexible design that enables reuse in a multitude of network elements for different markets and applications.
- **High availability**—Carrier-grade high availability offering at least five nines (99.999 percent) of availability.
- **Fast time-to-market (TTM)**—Minimize long, expensive development cycles and address aggressive price points.

Solution	Advantages	Disadvantages
ASICs	<ul style="list-style-type: none"> <li>■ High speed</li> <li>■ High volume</li> </ul>	<ul style="list-style-type: none"> <li>■ Significant expense</li> <li>■ Expanded time-to-market (TTM)</li> <li>■ Increased risk</li> <li>■ Inflexible</li> </ul>
General Purpose Processors (NPU's)	<ul style="list-style-type: none"> <li>■ Low cost</li> <li>■ Flexible</li> <li>■ Short TTM</li> </ul>	Insufficient performance for applications needing Gigabit-class performance
Specialized merchant silicon	Some of the same benefits and costs as ASICs and general purpose processors	<ul style="list-style-type: none"> <li>■ Often have limited functionality</li> <li>■ Don't allow for sufficient end-product differentiation</li> <li>■ Markets often too small to support attractive pricing</li> </ul>
Intel® network processors	ASIC-class performance, with general purpose processor programmability, flexibility, and compatible scalability	Complex programming models; better suited to assembly language than high-level languages like C

## The Solution: Build on Modular Architecture With Off-the-Shelf Components

The most promising way to meet the challenge is to use a network processor unit (NPU)-based AdvancedTCA platform with off-the-shelf components.

The solution detailed in the rest of this paper incorporates:

- The RadiSys Promentum ATCA-7010, an NPU-based AdvancedTCA solution.
- The Intel® IXP2850 network processor for protected processing at high-data rates.
- The Intel® IXA Software Developers Kit (SDK) 4.1 to test, debug, and tune application code.
- A virtual machine (VM) model to enable application developers to focus attention on packet processing logic and not on the underlying NPU or platform architecture.
- The IP Fabrics packet processing language (PPL), a high-level, functional programming language that reduces the amount of code needed for complex networking applications.

## The Details: Building Blocks From RadiSys, Intel, and IP Fabrics

### RADISYS PROVIDES OPEN, MODULAR ARCHITECTURE

Traditionally, TEMs resorted to proprietary form factors and architectures. But competitive and TTM pressures have prompted a move to open standards-based architecture—AdvancedTCA. The RadiSys Promentum ATCA-7010, is an excellent NPU-based AdvancedTCA solution.

The true competitive advantage of the ATCA-7010 is scalability. That scalability can be harnessed to easily upgrade the product to efficiently protect Internet applications from the security vulnerabilities of the future (see Figure 1).

The ATCA-7010 boasts ten 1 Gigabit interfaces and can process up to 10 Gbps of packet processing using the dual Intel IXP2850 network processor. It is a very modular and flexible architecture with high-performance memory architecture. For demanding table look-up applications, the ATCA-7010 offers an optional ternary content addressable memory (TCAM). The

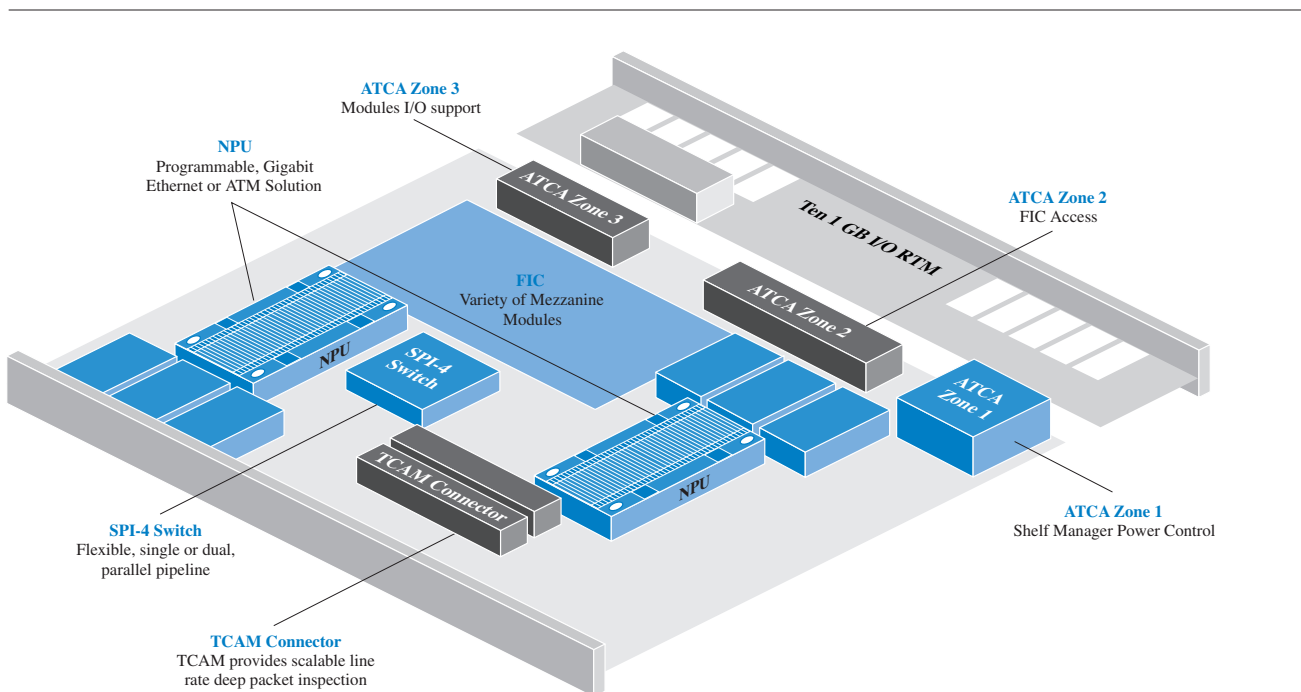


Figure 1. RadiSys Promentum\* ATCA-7010

Intel IXP2850 builds upon and extends Intel’s fully programmable, high-performance network processor architecture. The Intel IXP2850 includes hardware mechanisms that enable popular encryption and data integrity standards, such as data encryption standard (DES), triple DES (3DES) and advanced encryption standard (AES) encryption algorithms, along with secure hash algorithm (SHA-1) hashing to be implemented at speeds up to 10 Gbps. These capabilities are supplemented by comprehensive reference software and support services ranging from cryptography building blocks for IPsec and TCP/SSL to complete custom software support encompassing code design, module integration, and performance tuning.

The ATCA-7010 is highly modular with several features that increase ROI. It has:

- An SPI-4 switch between the processor that provides processor configurability.
- An I/O implementation on the rear transition module (RTM) that allows users to offer a multitude of interfaces by substituting the RTMs.

- A fabric interface that is implemented as a mezzanine to provide fabric choices—10 GE, ASI or proprietary fabrics.
- A modular memory design for the NPU, with socketed RDRAM and an optional TCAM memory module.

The combination of the Intel IXP2850 and design flexibility makes the ATCA-7010 a compelling choice for designers implementing high-performance security solutions.

Figure 2 shows the high-level architecture of the ATCA-7010. This architecture gives the ATCA-7010 the flexibility to function with multiple types of Zone 3 and Zone 2 connectors.

The modular design of the ATCA-7010 board enables it to operate on different network configurations. For example, if the ATCA-7010 Zone 3 is currently connected to an RTM with 10 ports, each with 1 Gigabit capacity, it can also function seamlessly with an RTM that has one port with 10 Gigabit capacity.

Inline accelerators offer the advantage of isolating security functions from packet processing. Unfortunately, the packet still

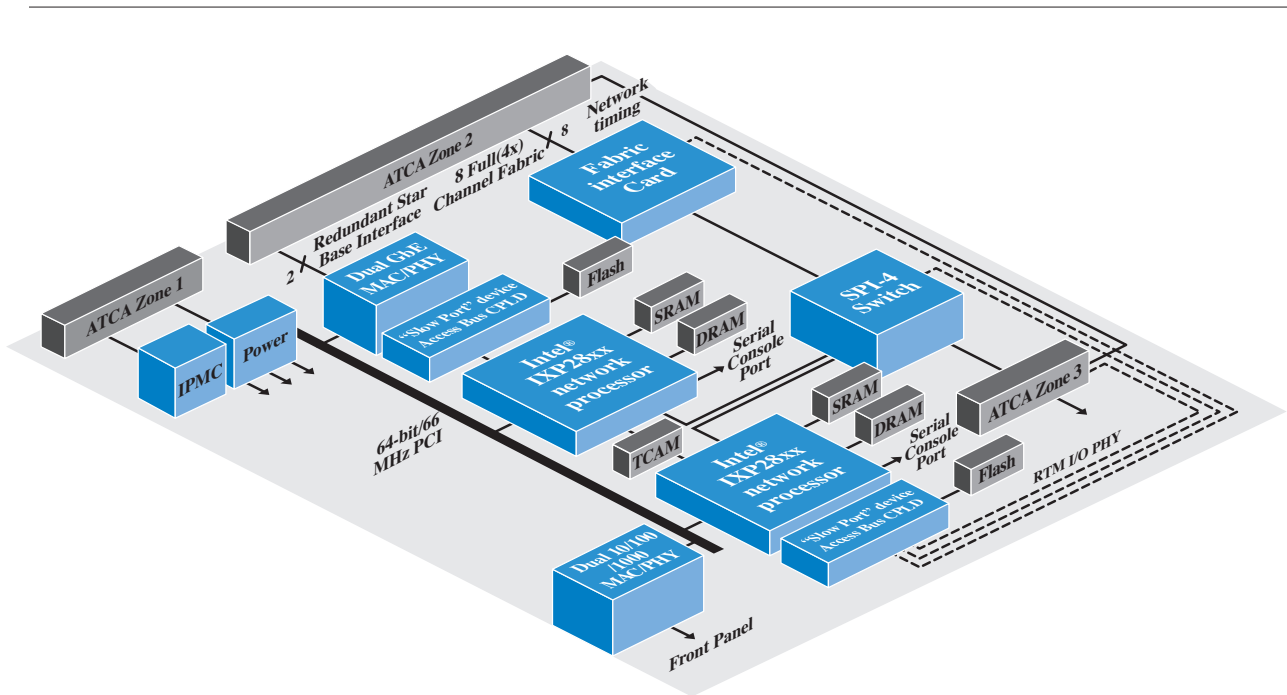


FIGURE 2.  
The ATCA-7010 Line Card Technology Highlights

requires two round trips to memory and must be reassembled twice—once in the accelerator and again in the ASIC or NPU. Though inline accelerators hold promise for higher throughput capacity, few products have been announced.

Another approach, called the flow-through model, merges the security and packet-processing features in a single chip.

Advantages of this model include:

- For some security protocols the packet data is written to memory once, which means that the impact on packet processing is limited only by the operational performance of the cryptography unit itself, and not by the imposition of additional I/O operations.
- PCI bandwidth is available for other uses, such as communication with the control-plane processor.
- By placing security operations within the NPU, instead of in a look-aside secure sockets layer (SSL) or IPSec accelerators; designers can expect lower power budgets, fewer layout constraints, and shorter integration time. An integrated security solution automatically scales to the processing capabilities of the NPU.

### **INTEL PROVIDES PROTECTED CONTENT PROCESSING**

To meet the requirements for protected processing at high data rates, Intel has added a cryptography unit to its 10 Gigabit NPU. Dubbed the Intel IXP2850 network processor, this chip is the latest addition to the Intel® IXP2XXX product line of second-generation processors. It provides on-chip support for the industry's leading bulk data encryption standards. Additionally, it is pin compatible and architecturally identical to the Intel® IXP2800 network processor, so software developed for the Intel IXP2800 will run unmodified on the Intel IXP2850.

The Intel IXP2XXX product line is a family of programmable NPUs designed to process packets at line rates up to 10 Gbps per second. Each chip is comprised of multiple RISC data-plane processors, called microengines, plus an Intel XScale® core for control plane functions, such as exception handling. The micro-engine design incorporates hardware multi-threading with non-pre-emptive context switching. The processors support a set of industry-standard busses that include PCI, SPI-4.2, UTOPIA, POS-PHY, QDR\* SRAM, and the Network Processing Forum's Look Aside-1 (LA-1) coprocessor interconnect.

The Intel IXP2850 cryptography unit implements the DES, 3DES, and AES encryption algorithms along with SHA-1 hashing. Intel selected these algorithms because of their use in the industry's predominant security standards, namely IPSec, SSL, and TLS. Each of these protocols specifies DES, 3DES, and AES algorithms for encryption and SHA-1 for authentication. Additionally, protected ATM devices use DES or 3DES for encrypting cells.

The Intel IXP2850 is designed using the flow-through security architecture. This technique enables software designers to combine security with packet processing software. For network layer security protocols, such as IPSec, encryption and hashing operations are applied as packets are received or transmitted rather than as a secondary step as with look-aside or inline approaches. This feature enables the Intel IXP2850 to protect continuous flows of packets at sustained maximum line rates.

The Intel IXP2850 offers hardware designers advantages over using a standalone accelerator in a protected processing card. The cryptography unit does not require dedicated memory units or a TCAM to hold security state information. Instead, the microengine software maintains the state along with all other packet information in Intel IXP2850 memory. Additionally, the cryptography unit is a low-power feature, consuming about 2 watts more power than the Intel IXP2800.

Figure 3 shows a sample application using the Intel IXP2850. The ten-port Intel® IXF1110 Gigabit Ethernet MAC on the front end exchanges packets with the Intel IXP2850 via an SPI-4.2 interface. On the back end, the NPU communicates with another MAC/Framer or a switch fabric interface. A general purpose processor, such as the Intel® Pentium® 4 processor, typically resides on the board to perform configuration and management functions and to execute control-plane signaling.

The Intel IXP2850 cryptography unit is designed with bulk encryption in mind. But, as with many security applications developed today, a separate means of managing key exchanges may be necessary. The solution shown here is to add a public key accelerator by means of the PCI bus to perform either SSL or IPSec key exchanges when security associations or handshakes are established. The software that implements the key exchange protocol, such as Internet key exchange (IKE), can be implemented on either the microengines or the Intel XScale® core.

Many of the baseline security protocols, as well as protected application standards, are still evolving. With the security algorithms implemented in hardware and security protocols implemented in software, designers can stay current with state-of-the-art protected application standards through software enhancements. Changes in protocol software can be downloaded to the Intel IXP2850 on the communications board.

This is true whether the board is still being designed in the lab or is deployed and running within a customer's network.

Intel's fully programmable NPU architecture is appropriate for use in a variety of network-based applications, including wireline data and voice, wireless, video, and storage networking. The Intel IXP2850 network processor offers a choice to designers who require encryption and authentication services as part of a rich set of packet processing applications.

### INTEL PROVIDES SECURITY SOFTWARE TOOLS

The Intel® IXA Software Developers Kit (SDK) 4.1 includes compilers, assemblers, debuggers, libraries, and simulation tools used to create software for the Intel IXP2XXX product line. A principal component of the SDK is the Transactor, a cycle- and data-accurate software model of the NPU. It is used with the SDK's graphical interface to test, debug, and tune application code.

The Transactor incorporates a model of the Intel IXP2850 cryptography unit, so designers can create and test security applications in a simulation environment in parallel with hardware development.

The security algorithms implemented in the Intel IXP2850 cryptography unit represent the state-of-the-art in encryption and authentication technology. The U.S. National Institute of Standards and Technology (NIST) has standardized 3DES,

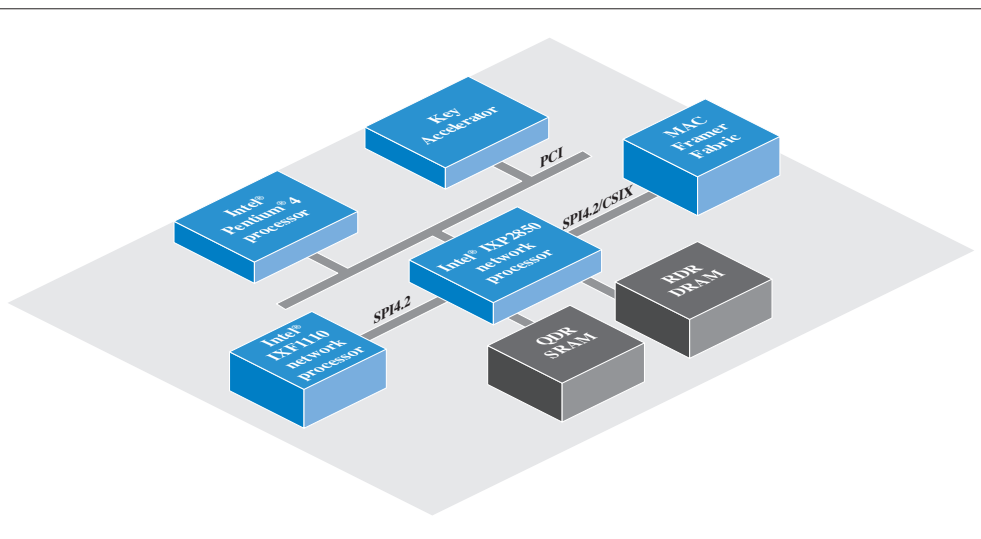


FIGURE 3. IMS AdvancedTCA Building Blocks to Applications

SHA-1, and most recently, AES. However, many security applications must be compatible with legacy algorithms—specifically RC4 encryption which is widely used in SSL, and MD5 hashing, which is specified as an option to SHA-1 in HMAC.

### A VIRTUAL MACHINE (VM) MODEL HARNESSSES THE POWER OF NPUs

A solution using sophisticated packet processing subsystems, such as the ATCA-7010, is highly complex. The ATCA-7010 incorporates multiple NPUs, pluggable I/O and fabric options, a flexible data path switch, and optional accelerators, such as TCAMs. A key challenge is to find a way to harness the power of the hardware system.

The answer to this challenge is to abstract the underlying NPU hardware by creating an application-specific programming model implemented as a VM.

The VM approach gives programmers a functionally-oriented programming environment that is machine-independent and designed to take advantage of proven parallel programming optimizations and highly optimized “built-in” functions. Using the VM approach enables application developers to focus on packet processing logic and not on the underlying NPU or platform architecture.

Although it is feasible to compile a higher level language directly into machine code for the NPU, the VM approach has compelling advantages:

- **Portability**—Applications can be ported across successive generations of NPUs and can also be mapped to physical machines with very different anatomy.
- **Scalability**—Complexity and performance level increase as the physical machine capabilities increase.
- **Robustness**—The syntax and semantics of the VM programming model are focused on packet processing, eliminating many of the programming errors associated with low-level, machine-dependent functional languages. Also, the VM implementation is rich with built-in runtime error checking.

### IP FABRICS PROVIDES PACKET PROCESSING LANGUAGE (PPL)

The IP Fabrics VM architecture is programmed by the PPL, a high-level, functional programming language for describing the types of packet processing found in many of today’s networking applications. The primitives of this language include fundamental network-processing capabilities, such as tracking connections, removing an outer header, translating IP addresses, encrypting a packet, scanning the payload for a regular expression, and so on. Such high-level abstractions enhance productivity, enforce consistency and reuse of code modules (see Figure 4).

PPL is oriented toward layer 3 IP packets, toward specific protocols at layer 4, such as TCP and UDP, and toward deep packet processing at layers 5 through 7. PPL can also easily integrate and interoperate with external programs, such as user-

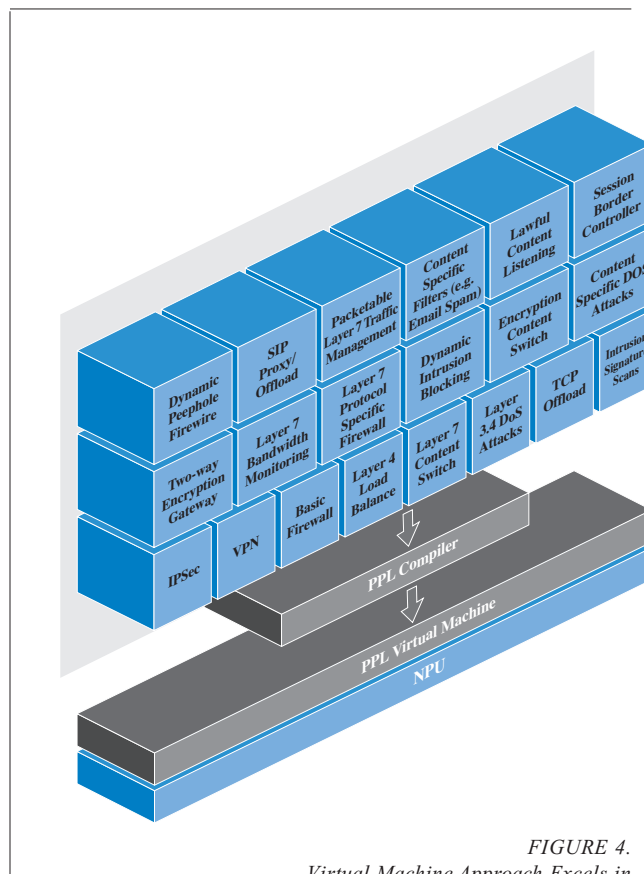


FIGURE 4. Virtual Machine Approach Excels in Scalability, Portability and Robustness

written microcode, control plane code, and protocol stacks, as well as external application processors such as DSPs.

Perhaps the best way to understand the power of this approach is to look at a specific example like the “bump in the wire” NPU coding benchmark. (For more information, visit [www.ipfabrics.com](http://www.ipfabrics.com).) The program counts TCP/IP packets (Web traffic) destined for port 80. The PPL implementation is just three lines of source code—one-twentieth the size of programs in other functional languages and less than one two-hundredth the size of an assembly language implementation. PPL program code savings are shown in Figure 5.

The implications are clear. The use of a high-level functional programming language significantly reduces the amount of code required for complex networking applications. It also reduces TTM and cuts the cost and complexity of debugging and maintaining programs. As with other programming tasks, high-level languages are clearly the best path. However, the complex architectural features of NPUs make a functional language a superior alternative to traditional programming languages like C.

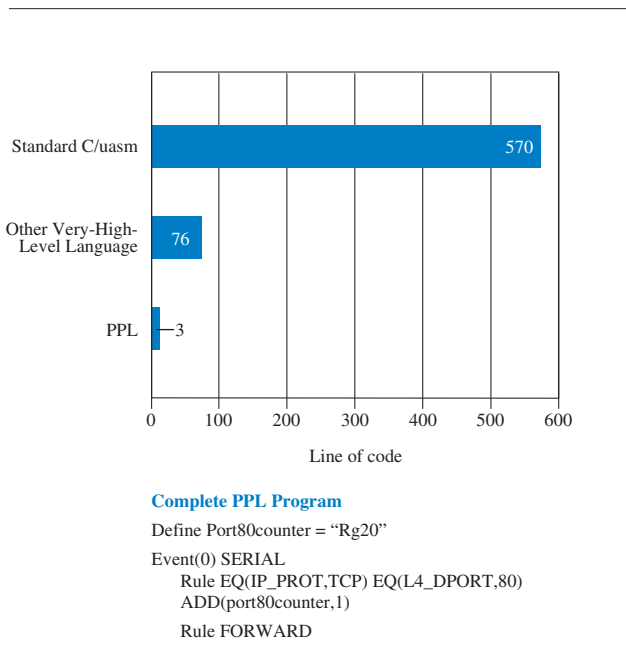


FIGURE 5. Code Savings Through Reuse of Code Modules

It should be noted that PPL and its VM implementation are far more than a simple productivity tool, but a complete software subsystem. For example, the scope of PPL software encompasses standard transmit and receive functions, IP forwarding, and interfaces to control plane IP stacks—all of which are included with the PPL software. Systems designers can create flexible systems by optionally including hardware accelerators like TCAMs, installation-dependent I/O interfaces, and application-dependent NPU configurations (such as ingress/egress, parallel, and so on) without costly software efforts. Ultimately, this allows systems designers to focus 90 percent of their time on the packet processing application, as opposed to underlying hardware and detailed programming.

## The Future: Utilizing Building Blocks

As the NPU market matures and AdvancedTCA adoption increases, systems designers can utilize existing building blocks to create a complete packet processing solution. Figure 6 shows a typical packet processing subsystem architecture.

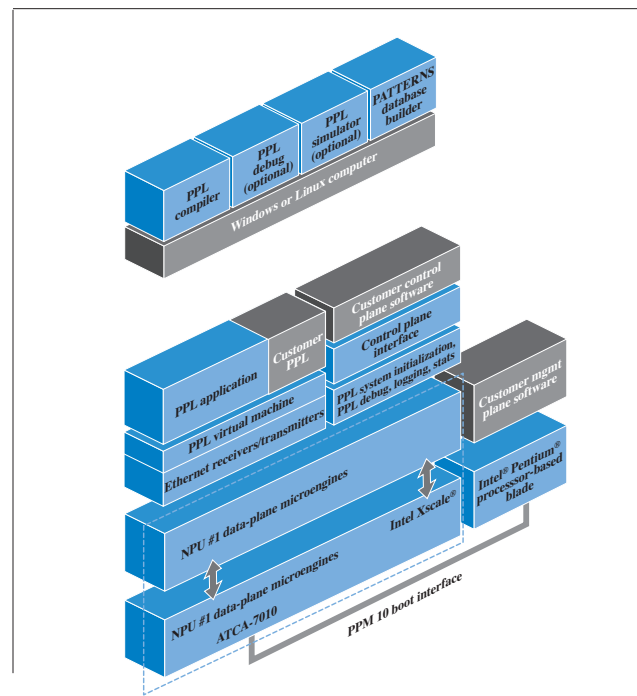


FIGURE 6. Packet Processing Subsystem

### EXAMPLE: SECURITY GATEWAY PLATFORM

Using an off-the-shelf AdvancedTCA platform like the RadiSys Promentum SYS-6000, it is possible to get a significant head start on developing the complete solution. The RadiSys Promentum family is a suite of carrier-grade platforms addressing blade server and network element applications designed to offer industry-leading price/performance and unparalleled flexibility. RadiSys delivers Promentum systems consisting of RadiSys and third-party components that are validated through proven hardware and software validation procedures. The RadiSys validation program is based on RadiSys system engineering and integration experience and provides complete, functional, parametric, and limit testing for turn-key platforms. Validation of platforms at these levels means customers can confidently and quickly deploy Promentum solutions in their networking systems.

### TIME IS MARKET SEGMENT SHARE AND MONEY

Perhaps the most important byproduct of utilizing hardware and software building blocks is the reductions in TTM, software development expense, and lifecycle development expense. Figure 7 looks at these factors at the system level for a typical development project. The charts compare the economic results of development using conventional software development methods with development using the IP Fabrics PPL and off-the-shelf hardware, such as the ATCA-7010. The results pertain to a complex IP-based product like a wireless base station controller/3G-Node B, or an Internet security appliance. They assume 24,000 lines of handwritten microcode versus 2,000 lines of PPL code (a conservatively high estimate for PPL), and a three-year active product lifetime.

Aside from the obvious value in being a more economical and faster-to-market approach, there are other points to note. First, the PPL approach allows for a much faster proof-of-concept and/or prototype. This is often crucial for initial customer engagements, to obtain future project funding, and for system-wide performance analysis. Second, using PPL greatly reduces the financial risk in a speculative project, since the initial software development expense is far lower than developing all NPU software in microcode.

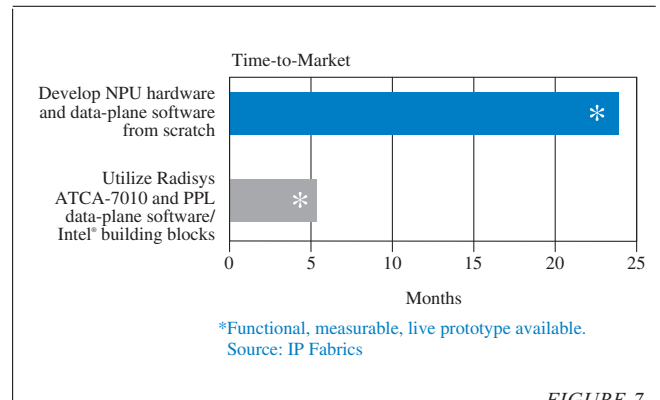


FIGURE 7.  
*Utilizing Building Blocks Translated to Time and Expense at System Level*

### COST OF ESCALATING SECURITY ATTACKS

*A recent survey by Cybertrust's ICSA Labs found that the frequency of security attacks and resulting costs climbed significantly in 2004.<sup>1</sup> This was the 10th consecutive year of increases in such attacks. The same survey also found that in 2004, computer virus incidents grew by 50 percent over the previous year even in the absence of a major new attack. The recovery time and costs from such virus attacks rose 25 percent from 2003. According to some estimates, nearly \$17.5 billion were lost to various attacks on the Internet in 2004.*

### AdvancedTCA

*The Advanced Telecom Computing Architecture, or AdvancedTCA, defines a new industry-wide architecture for telecommunications. Developed by over 100 companies in the PCI Industrial Computer Manufacturers Group, AdvancedTCA provides a framework for high-performance, standard modular building blocks—ideal for next-generation network platforms. As a platform architecture that spans hardware, interconnect, and management, AdvancedTCA enables modular reuse for network infrastructure platforms.*

*Based on industry standards, AdvancedTCA products offer carrier-grade, high-density computing solutions that feature high availability, hot-swappable components, computer telephony capabilities, and are designed to be NEBS-3/ETSI-compliant. Processor boards, switches, and accessories support powerful, cost-effective computing solutions for a diverse set of network elements, such as RNC, SGSN, GGSN, media gateways, and other server/database elements like CSCF, VLR, and media servers.*

## Conclusion

The security challenges that IP-based networks face today present significant business opportunity for TEMs. In order to gain advantage in such a competitive landscape, TEMs must utilize commercial off-the-shelf solutions.

Solutions using the RadiSys Promentum family with the ATCA-7010, Intel® building blocks, and the IP Fabrics PPL software solution enable application-ready platforms to build advanced NPU solutions for the security problems. With this application-ready platform, it is far easier to create, model, debug, and modify packet processing logic by utilizing building block software and writing new code in a functional language like PPL rather than in a low-level language. The optimization burden is shifted to the VM software, which is highly optimized for complex, parallel hardware platforms.

Using the PPL building block hardware, such as the ATCA-7010, developers can prototype new applications rapidly, assess architectural bottlenecks before investing significant software development resources, reduce schedule risk, and accelerate completion of product milestones. The result is accelerated TTM and lower lifecycle costs for NPU applications.

Modular platform architecture, using AdvancedTCA products, provides benefits for TEMs and service providers alike:

### TEMs:

- **Lower development costs and decreased TTM**—TEMs can focus on platform differentiation, cutting development time and delivering solutions with increased value-add.
- **Supply chain flexibility resulting from a broad vendor ecosystem**—Hardware and software products can be delivered at every level of integration.
- **Solid platform strategy**—Building with industry-standard components enables flexibility and easy scalability.

### SERVICE PROVIDERS:

- **Realize fast time-to-revenue with new, innovative services**—When TEMs build on a modular infrastructure based on industry standards, they can rapidly deliver a broad range of feature-rich solutions to service providers.
- **Increase flexibility and scalability of networks**—Modular platforms built on industry standards make it possible to quickly respond to dynamic customer requirements.
- **Manage network evolution with confidence**—Moving to a converged, all-IP network requires the flexibility that industry standard, modular network elements deliver.

Intel was able to work with IP Fabrics and other Intel Communications Alliance members to easily complete the solution.

### TO LEARN MORE ABOUT THIS INNOVATIVE SOLUTION, VISIT THE FOLLOWING WEBSITES:

[www.intel.com](http://www.intel.com)

[www.radisys.com](http://www.radisys.com)

[www.ipfabrics.com](http://www.ipfabrics.com)

*Sources*

<sup>1</sup> March 2005, ICSA Labs

<http://www.icsalabs.com/html/communities/nips/pressreleases/20050329.pdf>

# The Intel® Communications Alliance

## **A TRUSTED SUPPLY LINE FOR NEXT-GENERATION SOLUTIONS**

Radisys and IP Fabrics are members of the Intel Communications Alliance, a global community of communications and embedded developers and solutions providers committed to the development of modular, standards-based solutions using Intel® technologies. With well over a hundred members worldwide, the alliance is delivering economies of scale to the communications industry, accelerating the development of optimized, multi-vendor solutions based on industry-standard technologies and Intel communications building blocks.

Intel® Communications Alliance members have a close working relationship with Intel and have demonstrated the high levels of design expertise, research capabilities and manufacturing capacity required to deliver high value to customers in the communications and embedded markets. Combined with Intel's communications and silicon expertise and high-volume manufacturing capabilities, this broad community helps to ensure very rapid innovation on a consistent architecture. It also helps to ensure the wide availability of interoperable solutions at every level of integration, so TEMs, carriers and service providers have a trusted supply line for deploying and supporting next-generation services.

**For more information about the Intel Communications Alliance, visit: [www.intel.com/go/ica](http://www.intel.com/go/ica).**

## **ABOUT INTEL CORPORATION**

By advancing silicon technologies and driving industry standards, Intel is leading the convergence of computing and communications to provide new ways for people to gain value from technology and transform their world. Intel is meeting the expanding need for innovative, cost-effective and standards-based building blocks in wired and wireless networking and communications infrastructure. Intel's strength in silicon design, integration and high-volume manufacturing delivers high-performance, low-power components at lower costs that provide the flexibility and faster time-to-market necessary in today's communications industry.

## **ABOUT RADISYS CORPORATION**

RadiSys, a premier member of the Intel Communications Alliance, was founded in 1987 and successfully operates as an extension, or virtual division, of its customers' organizations. With expertise in architecture and integration, embedded operating systems, ASIC design, middleware and software, RadiSys collaborates with in-house engineering groups to successfully integrate custom building blocks into larger systems that power next-generation products. By incorporating RadiSys' proven technology into their designs, customers can focus on what matters: developing IP that differentiates their products from the competition. RadiSys also provides long-life support for its products. This not only protects OEMs' initial investment, but also allows them to easily upgrade their

products as customer needs change. RadiSys is a part of the PCI Industrial Computer Manufacturers Group (PICMG), and the SAForum. Radisys has played a leading role in the development and adoption of specifications, including AdvancedTCA. The company's AdvancedTCA strategy is based on its success as a strategic supplier of proven, tested, modular platforms that help TEMs reduce costs and development time associated with designing next-generation communications equipment.

The RadiSys integrated platforms make extensive use of common architectural and component designs, and integrate carrier-grade operating systems and middleware, reducing development costs and enhancing application portability. The Promentum SYS-6000 is an application-ready, highly configurable, integrated Linux\* blade server for control and services plane applications. These common platforms help TEMs reduce costs, shorten development time and realize economies of scale, and flexibility, from platform application reuse.

## **ABOUT IP FABRICS**

IP Fabrics, an affiliate member of the Intel Communications Alliance, empowers a new era of networked systems by breaking down the software barriers to using network processor silicon. The company is venture-capital financed by Ignition Partners, Intel Capital, Frazier Technology Ventures, and Northwest Venture Associates. IP Fabrics is a member of the Network Processing Forum, Intel Communications Alliance, and RadiSys Alliance Program.

© 2005 Intel Corporation. All rights reserved. Intel, the Intel logo, Intel XScale® and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Performance tests and rating are measured using specific computer systems and/or components and reflect the 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.

Information in this document is provided in connection with Intel products. No license, express or implied, by estoppel or otherwise, to any intellectual property rights is granted by this document. Except as provided in Intel's Terms and Conditions of Sale for such products, Intel assumes no liability whatsoever, and Intel disclaims any express or implied warranty, relating to sale and/or use of Intel products including liability or warranties relating to fitness for a particular purpose, merchantability, or infringement of any patent, copyright or other intellectual property right. Intel products are not intended for use in medical, life saving, life sustaining, critical control or safety systems, or in nuclear facility applications.

AdvancedTCA and the AdvancedTCA logo are the registered trademarks of the PCI Industrial Computers Manufacturers Group.\*

© 2005 RadiSys Corporation. RadiSys is a registered trademark of RadiSys. Promentum and Procelerant are trademarks of RadiSys. All other products are trademarks or registered trademarks of their respective companies.

© 2005 IP Fabrics, Inc. All company and/or product names may be trade names, trademarks and/or registered trademarks of the respective owners with which they are associated. Features, pricing, availability, and specifications are subject to change without notice.

\*Other names and brands may be claimed as the property of others.

Printed in USA/0605/PM/PMS/PDF Order Number: 308191-001US