Engineers’ Guide to VME, VPX, VNX & VXS

Strategies for Successful VPX System Design

VITA-74/VNX System Prototyping

Tracing into the Model: Using Requirements Traceability with Model-Driven Development

As IoT Expands, Automotive Software Innovates to Ensure Functional Safety

www.EmbeddedSystemsEngineering.com/vme
OpenATR - SigPro1 Platform
OpenVPX™ Based Signal Acquisition System

Description
The SigPro1 OpenATR box is an OpenVPX™ based signal acquisition system intended for use in signal processing and recording applications such as data acquisition, radar, beamforming, and other high speed signal processing applications.

Based on a Virtex™-6 series FPGA with high performance A/D front end, the system runs on a 2nd generation Intel® Core i7™ processor and includes a two-TB storage subsystem with room to expand. For high bandwidth data collection applications, the system can operate in dual channel record and playback mode, with two 16-bit 200 MS/s A/D converters and an 800 MS/s 16-bit D/A converter.

The complete payload is a truly interoperable, multi-vendor OpenVPX platform. The OpenATR is highly configurable, accepting different FPGA cards and firmware. It also runs Pentek’s Talon® series data acquisition and recording system architecture and application software.

Features
This version is intended for use in high shock and vibration and extended temperature.

• Intel Core i7 single board computer
• High performance acquisition and FPGA processor
• Dual 2.5-inch, SLC or MLC solid state flash drives
• Multiple I/O ports brought out via rugged MIL-C-38999 connectors
• Intended for use in extended temperature, shock and vibration applications

Benefits
• Small form factor (SFF) meets SWaP requirements
• Truly interoperable OpenVPX platform is open architecture compliant
  o Multi-vendor implementation minimizes overall risk and user dependence on single sourced systems
• FPGA offloads I/O processing for faster overall system performance
• Can be configured to meet a wide range of high performance I/O processing applications

Applications and Related Products

Today’s mission critical defense systems demand high bandwidth data processing and storage. The system can be used for data acquisition, radar, beam forming and other signal processing applications in the most harsh environments.

• Other chassis and board combinations can be configured to meet different defense or industrial applications such as:
  o High definition video
  o Engine control systems data
  o Mission data storage
  o SigInt, C4ISR

• Intel & Freescale Single Board Computers
• Blade level networking boards (Ethernet, PCI Express)
• FPGA configurable I/O solutions
• Rackmount, desktop, and ATR chassis platforms
• Ruggedization programs

Elma Electronic Inc. • 510.656.3400 • sales@elma.com • www.elma.com
Introducing
GraphiteVPX/CPU

GraphiteVPX/CPU
- Intel® Atom™ E3845 (Bay Trail) Quad Core processor
- Supports 3U VPX profiles: MOD3 PAY-2F2T-16.2.5-2,3 and MOD3-PAY-2F2U-16.2.3-2,3
- Operating Supply from VS1 or VS3 or both
- Fully Loaded with Wide Variety of I/O Interfaces

CTI, your Embedded Computing Experts and Source for COTS or Custom Solutions
For more details on this and other CTI products visit, www.connecttech.com/products

sales@connecttech.com
(519) 836-1291
(800) 426-8979

www.connecttech.com
If you’re a telecom equipment manufacturer (TEM), you’re seeing a business growth slowdown in every geographic region, says InfoTrends Research in its latest Global Telecom and Datacom Market Trends and Drivers report (1-12-15). But if your company deals with datacom—and specifically mobile datacom—you’re having a very good year despite a forecasted overall slowdown in capital expenditures ahead.

Instead of yakking over traditional telecom lines, users are talking over VoIP via Google Voice or Apple’s FaceTime. They’re streaming movies on-the-go or posting to social media online. They’re data users, not audio channel users.

As applied to embedded, data devices and infrastructure, handsets and their high-performance SoCs, IoT sensors, Intelligent Gateways, or the Smart Connected Car are all consumers of terrestrial or mobile data. That means VoIP and Netflix will be competing for bandwidth against the potential “tens of billions” of IoT devices shown at last week’s Consumer Electronics Show (like Chamberlain’s Notifi porch cam or Intel’s Nixie wearable drone).

According to the report, “Europe’s 5 largest service providers...continue to experience declining revenues.” The report also says that warring US mobile carriers have been affected. But mobile data services “rose again in every region in 1H14” driven by smartphones; mobile broadband grew an astounding 26 percent year-over-year.

Depending on your vantage point—selling telecom or datacom infrastructure, or using these pipes to service your equipment as an end user—embedded is affected either way. My view is that cloud services, IoT sensors, and the meteoric rise of app-enabled, consumer smart home doodads are all going to benefit greatly from these price wars. Consequently, cheaper mobile Internet and more available pipes (wired or wireless) will accelerate connecting all kinds of IPv6-equipped devices onto the Internet. That is: in the limit, it’s a good thing.

Where the misfortune of one man is a treasure to another, using Connected Cars or the IoT to drive today’s technology markets is way better than relying on growth in the telecom and datacom industries. There are relatively few suppliers (and innovation) in the latter, while the former—the IoT and overall embedded—is experiencing innovation and wild ideas not seen since the PC brought power to your desk.

Who’d a thunk I could buy Internet-controllable, multicolored LED lights and strips for only a few dollars, or use a personal drone to stream stabilized video images in 720p of my family playing rugby on a sunny day? Gosh, I love this stuff. Sorry, TEMs: without your pipes we wouldn’t be here. But we have to move ahead!
AppliPaks
Application Development Packs

Elma’s AppliPak (Application Development Pack) is a fully integrated embedded computing solution combining a single board computer based on open architectures (VME, VPX, cPCI, etc.) with your choice of state of the art storage and/or I/O mezzanine cards, operating systems support and device drivers.

Staying on schedule is more important now than ever. For over 20 years, Elma’s AppliPaks have addressed critical board level integration issues where a tech refresh or an entirely new board set for a custom or existing platform is needed.

AppliPaks range in complexity from off-the-shelf systems with simple operating system and device driver load to fully ruggedized assemblies with custom OS and driver integration.

Features:
- A Single Board Computer from our wide range of Intel and Freescale CPU options
- Choice of mezzanine based I/O and storage options including serial, audio, video, Ethernet, FPGA I/O, solid state or rotating drives and more
- VxWorks, Linux or Windows OS, and drivers with kernel configuration, optional tools and boot file
- Rear transition module (RTM) or breakout board
- Extended temperature ranges, as well as conformal coating when required
- Assembly level testing, support and life cycle management

Benefits:
- Lower support and procurement costs - each assembly is sold and supported under one model number with Elma as your single point of contact
- Concentrate your efforts on your core business
- Cost containment and risk mitigation - take the guess work out of system design time and costs and rely on Elma for all integration work and scheduling
- Fully tested and installation ready before shipment

Elma Electronic Inc. • 510.656.3400 • sales@elma.com • www.elma.com
CONTENTS

EMBEDDED SYSTEMS ENGINEERING

Features

Words Upfront: Safety Critical
By Anne Fisher, Managing Editor
6

As IoT Expands, Automotive Software Innovates to Connect, Integrate and Ensure Functional Safety
By Chris Berg, SYSGO
10

COVER STORY

VITA-74/ VNX System Prototyping and Development Considerations
By Wayne McGee and Bill Ripley, Creative Electronic Systems
15

VME

Strategies for Successful VPX System Design
By Rodger Hosking, Pentek, Inc.
12

Product Showcases

Hardware

Backplanes
SIE Computing Solutions
17

CPU or Single Board Computers
Artesyn Embedded Technologies
18

Development Boards
Pentek, Inc.
19

Enclosures
SIE Computing Solutions
20, 21

Software

Development
Teledyne LeCroy
22

Safety Critical

Trends and Drivers in Fail-Safe Architectures for Rail Systems
By Shlomo Pri-Tal, Artesyn Embedded Technologies
23

Tracing into the Model: Using Requirements Traceability with Model-Driven Development
By John Thomas and Jared Fry, LDRA
26

Departments

From the Editor
2

Last Word
30
Rugged, Reliable and Ready

Our designer friendly and flexible technology can solve many of your application problems in the design phase.

Contact Dawn to ease the design-to-production transition and reduce deployment time to enable high performance, mission critical systems. We look forward to speaking with you soon.

Dawn’s advanced backplane topology customization tools now feature OpenVPX Fabric Mapping Modules.

You need it right. You want Dawn.

(510) 657-4444
dawnvme.com
Editor’s note: Our thanks to Fabien Gaucher, CEO of Argosim. His firm makes simulation software that allows system architects to model, debug and test real-time requirements. Fabien received a PhD in computer science from the University of Grenoble, France, where he worked on the automated debugging of reactive systems. Then he worked for 10 years at Dassault Systèmes, where he developed a software tool for the modeling, simulation and code generation of embedded systems. In 2013, he cofounded Argosim.

EECatalog: Imagine Argosim did not come along. How is life different for system architects and the customers for whom they are designing products?

Fabien Gaucher, Argosim: System architects are typically senior experts who have a sound knowledge of real-time systems issues. They make important choices that will impact the whole development process and the final product quality. However, many of their requirement specifications are informal and mainly written in natural language. These high-level requirements are generally validated through manual reviews, but many ambiguities and errors remain until they are identified through the software testing and validation process. In practice, the later these errors are detected, the more expensive it is to fix the bug. The cost is even worse when third parties are involved as the extra process iterations involve specification and contractual changes. In some cases, specifications errors may extend the development delay, and hence the whole project cost, by at least a factor of two.

[Argosim’s] STIMULUS, an innovative modeling and simulation tool, enables system architects to edit, debug and test functional real-time requirements. For the first time, requirements specifications can be validated very early in the development process, before the design phase even starts, thereby limiting errors and ultimately saving cost.

EECatalog: What practices does Argosim follow in order to succeed at anticipating what market requirements will be?

Gaucher, Argosim: If we look at software development processes, plenty of tools have been proposed for many validation activities. For critical systems, the validation process may represent more than 60 percent of the whole development effort. The functional validation activity aims at checking that design is correct with respect to system requirements. Companies are investing a lot of effort into validating the system against requirements that have not been tested yet. Functionally validating system requirements at the specification stage would ensure that the system requirements were valid. Establishing this foundation would cut the time and cost of overall system development substantially.

While requirement-engineering tools exist, they mainly focus on traceability concerns (e.g. IBM Doors). Argosim STIMULUS provides the ability to edit real-time requirements in a formal yet natural language as well as provides a unique simulation feature that allows system architects to observe whether possible executions will satisfy requirements.

EECatalog: What mistakes (made either by Argosim or others) have taught Argosim the most valuable lessons?

Gaucher, Argosim: Some tools have been proposed to validate real-time requirements. Specification tools like UML do not provide simulation features, which is a major drawback to perform analysis and debug. Proof tools are typically very hard to use, and proofs cannot always be performed for both decidability and complexity reasons. Design tools define how the system is implemented and are not suited to partial specifications, which define what systems do.

To correct these challenges, Argosim provides a modeling language as close as possible to the natural language as well as providing simulation features. STIMULUS includes a powerful library of predefined sentences that fit with standard ways of writing requirements. These libraries can be extended by users in order to adhere to internal needs.
General Standards Corporation develops and manufactures the highest-performance Analog, Digital and Serial I/O products based upon a variety of buses such as PMC, PCIe, PC104Plus, VME, and cPCI.

Our extensive product line (over 100 products) includes I/O boards, cables and software drivers.

We can customize boards for your application.
Toyota’s unwanted acceleration, or the Therac radiation therapy machine. The industrial safety standards (ISO 26262, DO-178, EN 50128, IEC 61513, etc.) have been written to formalize the development processes in a way that avoids system issues that result in death.

All of these safety standards follow the IEEE 830 quality criteria for good requirements, which it states should be correct (effectively describe the system behavior), unambiguous (not subject to multiple interpretations), complete (no missing requirements), consistent (no requirement conflicts), verifiable (a test scenario can be written), modifiable (express requirements separately), and traceable.

Currently, the verification of requirements is based on methodologies rather than tools. However, the growing complexity of systems has caused vendors to adopt tools for the design and validation phases of development, but nothing has been available until now to automate and formalize the verification of requirements. STIMULUS gives engineers the first opportunity to master the complexity of the requirements specification phase.

EECatalog: Is offering the tools, for example, those that make it possible to share clear and observable requirements among engineers, enough—what should the ecosystem into which these tools are deployed look like for companies to succeed and for the industry to evolve?

Gaucher, Argosim: The classical “V” development cycle is evolving towards a test- and requirement-based focus with some companies adopting agile methodologies in order to make systems right the first time. The basic idea of such approaches is to be able to define specifications and validation tests before starting the design, and to refine specifications incrementally. As a consequence, requirements and test scenarios must be built in parallel and their maintenance becomes a crucial issue. The success of model-based approaches in the design of embedded systems is mainly related to the ease of maintenance. Therefore, requirements and tests should be supported by models and, preferably, executable models.

[It’s important to have] a way of building requirements and tests in parallel in a simulation environment. The ecosystem of STIMULUS, as well as possible tool connections, thus ranges from requirement traceability tools to testing environments, [and it] is a tool that can be shared by system architects, validation engineers and software engineers.

EECatalog: What do you recommend is a good way for a system architect to approach information about pre-certification kits? What are the questions to ask that would lead to a useful assessment of such kits?

Gaucher, Argosim: Many safety standards require the production of a given set of development documentation, such as “requirements specifications documents.” These documents are generally written in natural language, which leaves a lot of room for errors. The lack of control and verification of this first step of the development process often leads to difficulties during the certification process. STIMULUS provides a more effective support to model, verify, and document the requirements, making it easier to pass a certification process.

Anne Fisher is managing editor of EECatalog.com. Her experience has included opportunities to cover a wide range of embedded solutions in the PICMG ecosystem as well as other technologies. Anne enjoys bringing embedded designers and developers solutions to technology challenges as described by their peers as well as insight and analysis from industry leaders. She can be reached at afisher@extensionmedia.com
As IoT Expands, Automotive Software Innovates to Connect, Integrate and Ensure Functional Safety

What steps led to the creation of a heterogeneous overall system that meets the functional safety requirements defined in ISO 26262?

By Chris Berg, SYSGO

The automotive industry and its suppliers are preparing cars for the Internet of Things. In the process, they are using a system architecture that supports better integration of functions and their connectivity to the outside. Using what it calls Interior Domain Integration, Continental Automotive (Figure 1) is developing this type of integrated platform for connected vehicles. The new system is based on a hypervisor that enables applications to be arranged in a new way.

LEARNING FROM OTHER INDUSTRIES

In the 1990s, the aviation industry revolutionized aircraft electronics with Integrated Modular Avionics. This approach combined individual control units on a central platform for the first time in the Boeing 777 and Airbus A380 in order to save size, weight and power.

Today automotive electronics face challenges similar to those aviation encountered. Here, too, it is important to separate the rapidly expanding number of devices that usually have small, low-power processors from their isolated hardware and to represent their functions in software. As many as 120 processors per vehicle and 100 million lines of software code are to be combined on a powerful central processing unit. And we are only now witnessing the dawn of “intelligent” cars. A constant flow of new multimedia applications, safety functions and assistance systems are emerging all the time, which can be dynamically installed from app stores in the workshop or even by users themselves. The mobile communications industry is also pushing its way into automotive electronics and tapping into new business models such as Car-to-Go and insurance premiums based on usage and driving habits.

INTERIOR DOMAIN INTEGRATION

Continental Automotive is developing Interior Domain Integration as a central platform for a variety of functions. The Interior Domain Integration central platform that Continental is developing relies on the PikeOS hypervisor from SYSGO. Combining GENIVI, AUTOSAR, Android and POSIX applications on a single powerful ARM multicore hardware unit, this central platform links automotive electronics with consumer electronics and infotainment. This creates more space for additional applications, increases design flexibility and opens up opportunities for additional after-sales services and long-term business models over the life cycle of the vehicle. Employing such a platform also solves the associated security problems by separating the applications in the system architecture according to their security properties: untrustworthy Android applications run on the other side of the firewall, on a separate Core 4. Trusted but non-security-relevant GENIVI applications run behind the firewall, on Core 2 and 3. Both the trusted and security-relevant POSIX and AUTOSAR applications use Core 1, as Figure 2 shows.

SYSTEM ARCHITECTURE FOR A HETEROGENEOUS SOFTWARE LANDSCAPE

PikeOS hypervisor features support the pooling of a heterogeneous software landscape consisting of existing as well as new applications according to their respective safety and security relevance. First, by means of partitioning, containers are set up for the instances of different guest operating systems with their respective applications (Figure 3). Interior Domain Integration requires that the containers be separated from one another so that they cannot interfere with each other.
ENSURING FUNCTIONAL SAFETY IN VEHICLES

The adoption of ISO 26262 in 2011 was essentially an automobile-specific version of IEC 61508 to standardize the functional safety of automotive electronics. Safety risks are classified separately for each application according to the ISO 26262 standard. A distinction is made here between QM (no risk) and ASIL A through D (low to high risk). The software of each application is then certified separately according to the risk determined by independent agencies.

Because all Interior Domain Integration applications are placed in separate containers on one platform, it’s the job of the separation kernel in PikeOS to ensure that this separation actually works. The kernel’s task is to create an environment that, from the perspective of the individual application, does not differ from a physically separated system. Time and space partitioning ensures that each application is autonomous and does not “see” the other applications. It uses only the hardware resources explicitly assigned to it by the separation kernel. These include memory areas, resources and application sets at precisely specified times. The inter-partition communication controls the flow of information with other applications by way of fixed channels and limits communication to known and accepted instances.

The integrated platform from Continental can host multiple applications, which are classified according to functional safety levels: non-critical (unsafe) to highly critical (safe). The PikeOS separation kernel separates these from each other so that they do not see and interfere with one another. All applications are certified according to their individual criticality. PikeOS itself must comply with these safety criteria as well. The heterogeneous overall system therefore meets the functional safety requirements defined in ISO 26262. If, for example, a non-critical multimedia system running on Android causes an error and crashes, this will not interfere with a high-priority, critical assistance system. Instead, the critical assistance system continues running normally.

OVERCOMING VULNERABILITIES VIA SECURITY RULES

The more entertainment and infotainment electronics find their way into the vehicle, the more vulnerable the integrated platform is to malicious attacks and deliberate manipulation. For this reason, it is important to define IT security rules for applications in cars, and the underlying system software must support these rules.

For this purpose, the Multiple Independent Levels of Security (MILS) concept, which originated in military applications, has been around for a long time. MILS organizes systems into three horizontal levels with different rights and levels of trustworthiness.

The lowest level is formed by the hardware with other platform and security modules. Level 2 contains the separation kernel, which controls all communication in the system and allocates computation time and memory access to the various applications. Only the separation kernel has hardware access privileges (kernel mode) and is considered trustworthy in terms of security (trusted). All other modules of the system software on the second level are also considered trusted, but do not have hardware access privileges. This methodology helps configure, organize and monitor the functionality of the entire system. All applications are assigned to the third level, are considered not trustworthy (untrusted) and run in user mode.

The PikeOS hypervisor supports a system architecture for Interior Domain Integration, allowing a combination of heterogeneous software applications in separate containers on a single platform. The separation kernel in PikeOS enables a strict separation of applications. It provides safety and security features that ensure the overall security of the automobile system and allows for the integration of automotive and consumer electronics and infotainment.

Chris Berg is a solutions architect at SYSGO. He has been working in the embedded industry for more than 15 years. Graduating in Physics Mr. Berg initially worked as an IC design engineer at Siemens and Infineon. Prior to SYSGO Mr. Berg held a position as solutions architect at MIPS Technologies.
Strategies for Successful VPX System Design

Yes, the sheer number of OpenVPX profiles can be intimidating, but these steps can help even newbie engineers capitalize on a comprehensive, open architecture standard that satisfies ruggedization levels while delivering unprecedented backplane bandwidth for mil-aero and industrial applications.

While VPX brings unprecedented levels of performance to embedded systems, it also presents entirely new design considerations and tradeoffs not found in previous architectures. The most profound difference is the wealth of dedicated gigabit serial links between VPX modules, completely overcoming the limitations imposed by the shared parallel bus backplanes of VME and CompactPCI. Not only are these links configurable to support any connection topology, they also support a mixture of gigabit serial speeds and protocols within the same system.

VPX is designed for applications that require high performance and flexibility in a compact form factor. This makes it ideal for applications in the defense, aerospace, and industrial sectors. VPX systems are characterized by their use of backplane interconnects that support multiple high-speed serial links, allowing for efficient data transfer.

OpenVPX also categorizes the different kinds of traffic carried through the pipes as “planes.” The five planes defined are the utility, management, control, data and expansion planes.

In order to define architectural characteristics of systems, OpenVPX defines several “profiles.” A slot profile specifies the pipes and planes found on the backplane connectors of each slot. The module profile specifies the pipes, planes, fabrics and protocols implemented on each card. The backplane profile defines how the pipes connect slots to one another. And finally, the development chassis profile includes the backplane profile and defines the dimensions, power supply and cooling method.

GETTING STARTED WITH YOUR VPX DESIGN

Before searching for products, first define the physical and environmental requirements of the system, including size and weight limits of the enclosure, operating and storage temperature limits, as well as maximum levels of shock, altitude, vibration and humidity. One of the most critical results of this study will be whether the system can be air-cooled or if it must be conduction-cooled; this is obviously a

By Rodger Hosking, Pentek, Inc.
SELECTING MODULES

Another major decision is selecting a 3U or 6U form factor.

Then identify all of the critical functions of the system including processing requirements for control, graphics, communications and DSP. Determine memory speed and density and disk storage speed and capacity. Data converters such as ADCs and DACs must be defined by channel quantity, sampling rate and resolution. Other interfaces to sensors, networks, peripherals, communication links and control ports must all be listed.

Create a block diagram of these functions and draw links to show how they must connect to each other and to the outside world. Then determine the maximum data rate for each link. One great benefit of VPX is the ability to choose the appropriate “pipe” size to sustain multiple dedicated data links between components with scalable speeds.

Be sure to consider I/O connections to the system, and whether or not front panel I/O cables are allowed for critical interfaces to analog signals, networks, control, video and storage. Many VPX modules deliver at least some of these signals through backplane connectors using rear-transition modules, so be sure to identify and list all I/O requirements and restrictions before selecting modules.

SELECTING MODULES

Now, conduct an industry survey to satisfy the functions in the block diagram with candidate modules that also meet the physical and environmental constraints. One good starting point is the VPX product directory on the VITA website (www.vita.com). For each candidate module, identify the OpenVPX module profiles that will define the gigabit serial protocols, pipe sizes and data rates.

Now look for modules that have links with the same serial protocol as the modules they must connect to. Modules with wider pipes and faster data rates can often adapt to another module with narrower and slower links, as long as the protocol is the same. If so, make sure that the resulting links can sustain the required rates.

To help widen the field of choices, consider using VPX adapters or carriers that accommodate PMC, XMC or FMC mezzanine modules, effectively turning them into a VPX module. One example of a module that includes an XMC mezzanine can be seen in Figure 1. Each 3U carrier can accommodate one module, and some 6U carriers can accommodate two. Some carriers are simple adapters that bring the system interfaces of the mezzanine module out to the VPX backplane. Other carriers can include FPGAs and processors, including complete single board computers with one or more mezzanine sites.

This strategy yields a wealth of custom VPX module configurations, all based upon industry standard form factors and interfaces with offerings from many vendors.

MAKING THE CONNECTION

Each VPX backplane slot supports multiple planes implemented separately through certain size pipes defined in the slot profile. VPX backplanes connect the slots together using various topologies of point-to-point pipes between each of the connectors. Backplane profiles support a wide range of topologies including star, mesh, daisy-chain, and combinations of these.

Search through the VITA 65 standard backplane profiles best matching the interconnection requirements of the system block diagram, including specific pin assignments for the required pipes between modules. Remember, although the modules have specific fabric protocol assignments for each pipe, the slots and backplane profiles are completely fabric agnostic. As long as the backplane profile supports the required gigabit serial data transfer rate for a given link, any fabric and protocol can be used.

Often, the standard backplane profiles will support most, but not all of the required connections. There are several techniques to overcome this common obstacle. First, be sure to consider reordering module slot positions for the best fit. Then revisit the list of candidate modules to find another substitute module that has compatible backplane connections.

As a last resort, before considering the design of a custom backplane or custom module, consider using a backplane profile designed for a VPX switch module. Here, pipes from each slot are routed to a switch slot where the switch module acts as a crosspoint switch to join the pipes. The system engineer configures the switch to make the required connections between modules. Switch modules often support multiple protocols and usually include an Ethernet switch or hub for the control plane.

Using a switch module adds cost and a slot position, but offers an excellent solution for development and prototyping using standard, off-the-shelf products. To save costs and slots in a deployed
program, a custom backplane can be developed. Often the recurring cost of a custom backplane is comparable to a standard backplane.

GETTING A HEAD START
Consider a pre-configured development system from one of the module vendors (see Figure 2) to help with the topology definition, backplane selection and interconnect strategies. This can eliminate many issues if you are an engineer embarking on your first design, making it possible to choose a final configuration after gaining experience on a working system.

One example of a VPX development platform is the SPARK VPX Development Platform from Pentek. It contains an SBC, switch card and one or more Pentek VPX modules, depending on customer requirements. It is ready to start software development with Windows or Linux operating system, drivers, and application examples fully installed and tested.

Rodger H. Hosking is vice-president and co-founder of Pentek, Inc. where he is responsible for new product definition, technology development and strategic alliances. With over 30 years in the electronics industry, he has authored hundreds of articles about software radio and digital signal processing. Prior to his current position, he served as engineering manager at Wavetek/Rockland, and holds patents in frequency synthesis and spectrum analysis techniques. He holds a BS degree in Physics from Allegheny College and BSEE and MSEE degrees.

Figure 2. Pentek SPARK 3U VPX Development System with two Pentek software radio modules, one switch module, and three CPU modules with XMC sites, one with a dual 10 GbE XMC installed. Two power supply modules offer redundancy.
VITA-74/ VNX System Prototyping and Development Considerations

Let’s clear up some misunderstandings about a spec that can put you on the path to creating a small, lightweight and low-cost system for SWaP critical deployment.

By Wayne McGee and Bill Ripley, Creative Electronic Systems

This article will discuss aspects of the VITA-74 / VNX specification that are sometimes misunderstood as well as considerations for design and deployment of a VNX system.

A common misperception of the VNX specification is that chassis and external connectors are included. This is not the case. The specification details the physical size of the two standard size modules, the module connectors and the pin assignments of the signals on the module connector. How the modules are packaged into a system is up to the system designer. Part of the confusion stems from original proof of concept pictures (see Figure 1) that were used to promote how modules could fit together, and what a VNX compliant system could look like.

Going by the original proof of concept pictures, many people assumed that the four-slot backplane, transition panel, power supply and connectors were a part of the specification. They are not. Backplanes can easily range from one to eight slots (or more) and the system designer is free to choose the most appropriate chassis shape, connector style and connector placement to fit the deployment environment. In a VNX system development, the hard questions become, “How do you quickly prototype in the lab?” and “Just what are the deployment considerations?”

EARLY STAGE TIME SAVING

To address the issue of fast prototyping, a typical D38999 style circular MIL connector panel and wiring harness can take quite some time to prepare. Utilizing commercial connectors and readily available patch cables in a laboratory environment can save a lot of time in the early stages of a program when deciding on which I/O signals will be needed and what the best layout and pin assignments for the connectors will be. Figure 2 shows a transition panel set up for quick prototyping in a laboratory environment.

Once all of the required I/O signals are settled, the appropriate transition panel can be designed for the particular application. As with any system, connections to the outside world can be a source of electromagnetic interference (EMI) and electrostatic discharge (ESD) problems. The transition panel design should address these concerns by including necessary pin-hardening and filtering techniques.
Another important consideration to the system designer is the backplane. The VNX bus topology was lifted directly from VPX, specifically VITA 46. It is possible to build a backplane where VNX and VPX cards can be intermixed, and the cards will interoperate. Among the top five items on the system design checklist is the number of VNX 12.5mm and 19mm slots required for the system, as well as any requisite possible expansion capacity, and it’s just as important to consider the function of the cards. The VNX specification is topology-agnostic for the PCIe interconnect bus. The System Controller choice, coupled with standard and specialized peripheral card-to-card data transfer requirements (such as creating an FPGA-to-FPGA data path), will add to the constraints of the exact backplane topology needed.

THERMAL REQUIREMENTS
Thermal requirements are perhaps the most critical considerations for system card placement. Depending on the external cooling methodology, which will be discussed shortly, placing 19mm cards approaching the 20W suggested maximum dissipation in non-adjacent slots could be the way to go. Placing the cards in this way will improve the thermal gradient if the design is pushing the system cooling limits.

Now that we have discussed the transition panel and the backplane considerations, let’s delve into the chassis, power supply and external cooling techniques. Power supplies in VNX designs are typically mounted parallel to the cards or perpendicular to the cards, under the backplane. Shorter chassis designs with four or fewer 19mm slots are typically single-system designs. Chassis designs with six or more 19mm slots can contain one large complex system or could host two complete systems in a single chassis using either a single monolithic or split backplanes. Power Supply Units may be one large design, or be multiple power supplies, potentially mitigating the risks of a single point of failure.

The mounting and cooling of the VNX chassis demonstrates the flexibility of the systems. The cards are designed from the outset to be conduction-cooled. It is not possible or desirable to have an air-cooled module variant. Figure 3 shows the PCB with heat spreader and case assembly. Internally, the system is natively conduction cooled. If a cold plate, or a heat conducting mounting surface with a known maximum temperature is available, the system can be bolted down to that structural plate with no further considerations. Sometimes it is not that easy. An external metal wall exposed to the sun will need to be evaluated for thermal loading. For natural convection cooling, vertically oriented external fins can cool adequately, provided that the ambient air does not exceed 159.8 °F (71°C). If the mounting surface has any thermal conductivity at all, that conductivity will augment the cooling the fins offer. Enlarging the size and area of the fins, or increasing the thermal conductivity between the chassis and the mounting plate, will aid in the thermal calculations and make heat transfer more effective.

There are times when the two cooling methods just discussed are not sufficient due to the deployment environment. "Forced air conduction cooling" is a third method, whereby heat exchangers with integral fins and external coverings (or skins) are fitted to the chassis. Air is then drawn down the sidewalls of the chassis by a fan and exhausted through a plenum. This may take on the form of a box with integral fins, and with skins and plenum being connected to a central cooling duct. Similarly, the mounting tray may have a rear- or bottom-mounted cooling fan, pulling air across the integral heat exchangers.

A NATURAL FIT
The VNX module is a natural fit for use inside other types of embedded systems that do not require a conventional VME or VPX data bus. An example would be to put a VITA 74 module inside an air compressor on an aircraft. In this case, only a small processor is required to check status of the compressor subsystem and report out to a mission computer via a serial data bus. This is where a small one- or two-slot chassis embedded deep within the compressor would fit the bill perfectly.

Wayne McGee is the vice president of sales and general manager for North American Operations for Creative Electronic Systems SA. Wayne has served in various senior management positions in his career and has more than 30 years of experience in the VME, CompactPCI, ATCA and VPX markets. Wayne is also the chairperson for the VNX VITA 74 Marketing Alliance. Companies Wayne has worked for include Motorola Computer Group, VMIC, SBS Technologies and GE Intelligent Platforms. He holds a BSEE from the University of South Carolina.

Bill Ripley is the director of business development for the North American Operations of Creative Electronic Systems. Bill has served in various Consulting, Business Development, Product Management, Sales and Marketing roles in the Embedded Computing marketplace for over 15 years with Creative Electronic Systems, Themis, GE Intelligent Platforms and SBS Technologies. Prior to these, Bill spent 23 years with Bell Helicopter performing electronic design and integration of avionic, flight control, electrical and electronic warfare systems on a variety of commercial and military aircraft including the CV/MV-22 and M609 tilt-rotor aircraft, as well as the OH-58D, AH-1W, M412 CFUTTH, M407 and M222 helicopters. He holds a BSEE from the University of Texas at Arlington.
SIE Computing Solutions
VITA 46/48/65 BACKPLANES

VITA 46/48/65 Backplanes

SIE Computing Solutions VPX backplanes are designed to the latest VITA 46, 48, 65 and OPEN VPX standards. The 5-slot I/O PLUS(TM) 3U VPX Full Mesh Backplane is designed for a wide array of VPX applications. The highly configurable backplane offers high-bandwidth in a compact size and provides greater I/O flexibility through I/O PLUS(TM), an innovative use of configurable I/O daughter cards to accommodate an array of VPX applications.

SIE Computing Solutions is now a division of Atrenne Integrated Solutions.

FEATURES & BENEFITS

❖ 5 slot full mesh
❖ 2 dedicated I/O daughter card slots
❖ Over 200 watts per slot
❖ 28 layer board
❖ Supports Gen2 PCIe

TECHNICAL SPECS

❖ J1: 10 fat pipes/high-speed differential channels
❖ J2: 16 fat pipes/high-speed differential channels
❖ J2: 20 single-ended signals

AVAILABILITY

Now

CONTACT INFORMATION
SIE Computing Solutions
10 Mupac Drive
Brockton, MA 02301
USA
800.926.8722 Toll Free
508.588.8110 Telephone
508.588.0498 Fax
www.sie-cs.com
Artesyn Embedded Technologies

**MVME8100 FREESCALE P5020 QORIQ PROCESSOR VME BOARD**

**Compatible Operating Systems:** Linux, Wind River VxWorks, Green Hills Integrity  
**Compatible Architectures:** Power

The Artesyn™ MVME8100 is a high performance 6U VME/VXS SBC featuring the new Freescale P5020 QorIQ processor supporting high speed ECC DDR3-1333MHz. It offers expanded IO and memory features with PCIe and SRI0 fabric connectivity and multiple USB, Serial and Ethernet ports. Memory includes up to 8GB DDR3, 512K FRAM non-volatile memory, and 8GB eMMC NAND Flash. The MVME8100 is offered in commercial and rugged variants for extreme environments with extended shock, vibration, temperatures and conduction cooling. It is designed for a range of high end industrial control such as SPE and photo lithography and C4ISR, including radar/sonar. It will provide technology insertion to prolong current programs while providing more performance and throughput.

**TECHNICAL SPECS**
- Freescale QorIQ P5020 1.8/2.0GHz  
- 2 PMC/XMC sites  
- Optional hard drive mounting kit  
- 2x4 PCIe or 2x4 SRI0 connectivity to VXS backplane P0  
- Up to 3 USB 2.0 ports, 5 Ethernet ports, 5 Serial ports, GPIO

**CONTACT INFORMATION**
Artesyn Embedded Technologies  
2900 South Diablo Way, Suite 190  
Tempe, AZ 85282-3222  
USA  
Phone 1 602 438 5720  
TollFree 1 800 759 1107  
computingsales@artesyn.com  
www.artesyn.com

---

Artesyn Embedded Technologies

**MVME2500**

**Compatible Operating Systems:** Linux, Wind River VxWorks  
**Compatible Architectures:** Power Architecture

Artesyn Embedded Technologies’ MVME2500 series features the Freescale QorIQ™ single-core P2010 or dual-core P2020 processor. It is a cost effective migration path for older generation MVME3100, MVME4100, MVME5100 and MVME5110 boards. The MVME2500 series is ideal for automation, medical, and military applications such as railway control, semiconductor processing, test and measurement, image processing, and radar/sonar. Memory includes up to 2GB DDR3 and 512KB non-volatile MRAM. The MVME2502 variant has 8GB soldered eMMC solid state memory for additional rugged, non-volatile storage. Connectivity includes Gigabit Ethernet, USB2, serial, SATA and either one or two PMC/XMC sites. A hard drive mounting kit and conformal coating are available.

**TECHNICAL SPECS**
- 800 MHz or 1.2G Hz Freescale QorIQ P2010 or P2020 processor  
- Up to 8GB soldered memory  
- Optional rear transition module

**CONTACT INFORMATION**
Artesyn Embedded Technologies  
2900 South Diablo Way, Suite 190  
Tempe, AZ 85282-3222  
USA  
Phone 1 602 438 5720  
TollFree 1 800 759 1107  
computingsales@artesyn.com  
www.artesyn.com
Pentek, Inc.

MODEL 8267 SPARK 3U VPX DEVELOPMENT SYSTEM FOR COBALT, ONYX AND FLEXOR BOARDS

Compatible Operating Systems: Linux
Compatible Architectures: VPX

The SPARK family are fully-integrated development systems for Pentek’s software-defined radio (SDR), data acquisition and I/O boards. The SPARK series was created to save engineers and system integrators the time and expense associated with building and testing a development system.

A fully-integrated system-level solution, the SPARK family provides the user with a streamlined out-of-the-box experience. They come preconfigured with Pentek hardware, drivers and software examples installed and tested to allow development engineers to run example applications out of the box.

All SPARK development systems come with all software and hardware installed and ready for immediate operation. All necessary analog I/O cables are installed and tested, providing SMA connectivity for all analog I/O lines.

Please contact Pentek to configure a system that matches your specific requirements.

For more information or quantity pricing please visit our website: http://www.emacinc.com/products/system_on_module/SoM-9x25

FEATURES & BENEFITS

◆ 9-slot, 4U 19-inch rackmount, 12-inch deep chassis which houses 3U VPX Boards
◆ 64-bit Windows® 7 Professional or Linux® workstation
◆ Intel® CoreTM i7 3.6 GHz processor
◆ ReadyFlow® drivers and board support libraries installed
◆ Out-of-the-box ready-to-run examples

TECHNICAL SPECS

◆ Compatible Cobalt, Onyx and Flexor 3U VPX Boards
◆ SDRAM: 8 GB standard, 16 GB optional
◆ Enhanced forced air ventilation assures adequate cooling for all boards and dual 250-W power supplies guarantee more than adequate power for all installed boards.
◆ Pentek ReadyFlow drivers and board support libraries are preinstalled and tested with the 8267. ReadyFlow includes example applications with full source code, a command line interface for custom control over hardware, and Pentek’s Signal Analyzer, a full-featured analysis tool that continuously displays live signals in both time and frequency domains.
◆ All 8267 systems come with software and hardware installed and tested. Up to seven Pentek boards in the 8267 can be supported. Please contact Pentek to configure a system that matches your specific requirements.

APPLICATION AREAS

Industrial Control, Industrial Automation, Data Acquisition, Test & Measurement

AVAILABILITY

Now

www.pentek.com/go/em8267

CONTACT INFORMATION

Pentek, Inc,
One Park Way
Upper Saddle River, New Jersey
07458, USA
201-818-5900
201-818-5904
sales@pentek.com
http://www.pentek.com/go/em8267
SIE Computing Solutions

“MUPAC” 760 SMALL FORM FACTOR SERIES

Designed to deliver mission-critical computing performance in a fully portable enclosure – ideal for rugged small spaces.

Building on SIE Computing Solution’s 40-year history of design excellence in rugged electronic and embedded systems, the “Mupac” 760 Small Form Factor product line is designed for mission-and performance-critical communications and intelligence. “Mupac” 760 Small Form Factor compute platforms allow data processing in the field in a fully transportable, highly rugged computing module that improves speed and efficiency by completing processing in the machine, at the distributed level, before delivering data upstream. SIE Computing Solutions’ Small Form Factor line provides a complete distributed computing module – exceptionally powerful and fully portable in everything from a UAV to a backpack. “Mupac” 760 Small Form Factor compute modules enable the most modern technology to work in harsh conditions at a level of distributed computing never before possible. In addition to standard offerings, the “Mupac” 760 Small Form Factor line can also be customized for a wide variety of unique specifications, providing high-end compute-class performance for harsh industrial and military environments where extreme temperatures, air particulates, liquids and vibration prevent the use of standard commercial computers.

SIE Computing Solutions is now a division of Atrenne Integrated Solutions.

FEATURES & BENEFITS

◆ Extremely rugged
◆ Easily customized
◆ Dip-brazed construction
◆ Modular power supply
◆ Rated to operate in temperatures ranging from -40 to +85 degrees Celsius

TECHNICAL SPECS

◆ Two standard dimensions: 3.25” h x 6.5” w x 8.5” d or 5.25” h x 6.5” w x 8.5” d
◆ Available in an IP67 NEMA Rated Version and IP50 NEMA Rated Version
◆ Quickly deployable with Intel® Core™ i3/i5/i7 multi-core processors and up to 4 GB RAM
◆ Standard I/O includes dual DVI display: one DVI-I (DVI-D+VGA) and one DVI-D; GbE Ethernet Port, 8 x USB 2.0, 2 x RS-232, 2 x SATA 3Gb/s with RAID 0, 1 support; 1 x 6-pin header for KB/MS

ALC888 HD SUPPORTED AUDIO

◆ Enhanced configurability via a Mini PCIe Expansion Slot that can be configured by SIE for video capture, DOM, wireless and many other functions

AVAILABILITY

Now

APPLICATION AREAS

Military/Aerospace, Industrial, Transportation

CONTACT INFORMATION

SIE Computing Solutions
10 Mupac Drive
Brockton, MA 02301
USA
800-926-8722 Toll Free
508-588-6110 Telephone
508-588-0498 Fax
jtierney@sie-cs.com
www.sie-cs.com
SIE Computing Solutions

717 SERIES AIR-OVER CONDUCTION COOLED ATR ENCLOSURES

Compatible Architecture: VME, VME64x, VXS, VPX and CPCI architectures

The 717 Series is available in standard ARINC sizes that include 1/2 ATR Short to 1-1/2 ATR Long and any custom form factor. From bus standards to applicationspecific custom designs, the 717 Series provides an expansive offering of ATRs for platforms such as the VME, VME64x, VXS, VPX and CPCI architectures. The 717 Series is a member of SIE’s conduction-cooled line of ATRs. Designed specifically for rugged deployment and to direct air over the thermal conducting walls, its cooling can be configured to meet application requirements by either drawing air through the walls and out a rear exhaust plenum or forcing air down the walls and directing it away from the equipment. When configured for unpressurized environments, the 717 Series can be configured with a high-altitude cooling scheme to permit ultimate performance at altitudes up to 50,000 feet. When used in conjunction with SIE’s System Performance Monitoring technology, the 717 Series ATR can be configured to activate internal heaters in cold start-ups or control the performance outputs of the optional external cooling fan to maintain an optimal thermal environment for the circuit card assemblies. In addition, the 717 Series is sealed from the environment and meets MIL standards for up to 95% RH (humidity), 5% for 48 hours (salt fog), no fungal growth, 13.5g acceleration, and thermal shock performance. The 717 Series can be configured with an optional avionics trays for isolation from shock and vibration environments common to airborne, vehtronics and shipboard applications. For applications where stringent weight requirements are an issue, SIE Computing Solutions offers a lightweight composite solution.

SIE Computing Solutions is now a division of Atrenne Integrated Solutions.

FEATURES & BENEFITS

▶ Dip-brazed construction
▶ Expansive range of ARINC sizes
▶ Modular power supply /AC or DC filtered inputs
▶ Cold start heaters & high altitude fan offering
▶ Configurable I/O panel

TECHNICAL SPECS

▶ Storage Temp (-40°C to +85°C MIL-STD-810F)
▶ EMC (MIL-STD-461D)
▶ Input Power (28VDC, 115VAC/ 400Hz. 1Ø, 115VAC/ 400Hz. 3Ø- MIL-STD-704A Thru 704E, MIL-STD-1275A)
▶ Wiring (Low Toxicity -MIL-C-24643)
▶ Vibration (15 to 2,000Hz At 0.1g2/ Hz. (RMS~12g) MIL-STD-810F Method 514.5) & Shock (20g for 11ms MIL-STD-810F Method 516.5)

AVAILABILITY

Now

APPLICATION AREAS

Now
Teledyne LeCroy
TELEDYNE LECROY’S PCI EXPRESS® PROTOCOL ANALYSIS AND TEST TOOLS

IT’S ALL ABOUT THE TOOLS

Compatible Operating Systems: Windows XP/7/8
Specification Compliance: PCI Express Standards: 1.1, 2.0, and 3.0

Whether you are a test engineer or firmware developer, Teledyne LeCroy’s Protocol Analyzers will help you measure performance and quickly identify, troubleshoot and solve your protocol problems.

Teledyne LeCroy’s products include a wide range of probe connections to support XMC, AMC, VPX, ATCA, microTCA, Express Card, MiniCard, Express Module, CompactPCI Serial, MidBus connectors and flexible multi-lead probes for PCIe® 1.0a, 1.1 (“Gen1” at 2.5GT/s), PCIe 2.0 (“Gen2” at 5 GT/s) and PCIe 3.0 (“Gen3” at 8 GT/s).

The high performance Summit™ Protocol Analyzers feature the new PCIe virtualization extensions for SR-IOV and MR-IOV and in-band logic analysis. Decoding and test for SSD drive/devices that use NVM Express, SCSI Express and SATA Express are also supported.

Teledyne LeCroy offers a complete range of protocol test solutions, including analyzers, exercisers, protocol test cards, and physical layer testing tools that are certified by the PCI-SIG for ensuring compliance and compatibility with PCI Express specifications, including PCIe 2.0.

FEATURES & BENEFITS

◆ One button protocol error check. Lists all protocol errors found in a trace. Great starting point for beginning a debug session.
◆ Flow control screen that quickly shows credit balances for root complex and endpoint performance bottlenecks. Easily find out why your add-in card is underperforming on its benchmarks.
◆ LTSSM state view screen that accurately shows power state transitions with hyperlinks to drill down to more detail. Helps identify issues when endpoints go into and out of low power states.
◆ Full power management state tracking with Teledyne LeCroy’s interposer technology. Prevents loss of trace data when the system goes into electrical idle.
◆ Teledyne LeCroy’s Data View shows only the necessary protocol handshaking ACK/NAKs so you don’t have to be a protocol expert to understand if root complexes and endpoints are communicating properly.
◆ Real Time Statistics puts the analyzer into a monitoring mode showing rates for any user term chosen. Good for showing performance and bus utilization of the DUT.

◆ Zero Time™ Search provides a fast way to search large traces for specific protocol terms.
◆ Config space can be displayed in its entirety so that driver registers can be verified.

TECHNICAL SPECS

◆ Analyzer
  Lanes supported: x1,x2,x4,x8,x16
  Speeds: 2.5GT/s, 5GT/s and 8 GT/s
  Probes/Interposers: active and passive PCIe slot, XMC, AMC, VPX, Express card, Express Module, Minicard, Mid-Bus, Multi-lead, External PCIe cable, CompactPCI, Serial SFF-8639, M.2/NGFF and others
  Form factor: Card, Chassis

◆ Exerciser
  Lanes supported: x1,x2,x4,x8,x16
  Speeds: 2.5GT/s, 5GT/s, 8GT/s
  Emulation: root complex and endpoint emulation

◆ Protocol Test Card
  Speeds: 2.5GT/s and 5GT/s operation
  Tests: Add-in-card test
  BIOS Platform Test
  Single Root IO Virtualization Test

APPLICATION AREAS

Mezzanine Boards, Add-in Cards, Host Carrier Systems, System Boards, Chips

CONTACT INFORMATION

Teledyne LeCroy
3385 Scott Blvd.
Santa Clara, CA, 95054
USA
1 800 909-7211 Toll Free
1 408 727-6622 Fax
psgsales@teledynelecroy.com
www.teledynelecroy.com
Trends and Drivers in Fail-Safe Architectures for Rail Systems

No veering off the tracks: the means to head straight for differentiation from the other guys is here now for rail application developers.

By Shlomo Pri-Tal, Artesyn Embedded Technologies

The market for embedded computing technologies in rail applications is following a similar trend as has been seen in other embedded market spaces. A layer of the technology value chain becomes ‘table stakes’—delivering limited competitive advantage to a point that it makes sense for application providers to reallocate R&D resources to differentiating elements of the end product and buy the base technology from companies who are dedicated to that technology. We are witnessing this transition in the rail market for embedded computers that are certified to safety integrity level four (SIL4), the highest level. These embedded computers offer a certified, commercial off the shelf (COTS) generic fail-safe platform allowing rail application developers to focus their R&D resources on differentiating applications.

This trend is driven by a number of emerging trends in the global rail industry.

In the past few years we have witnessed an explosive growth in global investments in public rail transportation, in particular high-speed rail and metro, caused mainly by the effort to reduce a nation’s carbon footprint by replacing inefficient automobile-based transport with efficient mass transportation. This is particularly evident in emerging economies such as China and India, as well as established economies in the Far East, Africa and South America. While less so in Europe and North America, we do witness growth in these markets due to other factors such as pan-European rail standardization as well as modernization of the rail infrastructure to enhance safety.

However, a growing market, while creating an attractive target for COTS products, will not on its own cause an outsourcing trend. Additional safety, technical, and commercial factors come into play.

As train speed increases to 300 kilometers per hour and above, reliance on computers that control the rail infrastructure and the trains themselves increases exponentially. As an example, stopping a train that travels at 300 Km/h will only take 2 minutes or so, but during those two minutes the train will travel 10 kilometers, requiring real-time and continuous monitoring of the rail network to provide early alerts of potentially hazardous events. High-speed, high-availability, and fail-safe computer-based control equipment must be deployed to guarantee safe operation under all conditions. High-performance and high-availability computing expertise is relatively widespread, however fail-safe computing has been the domain of a few expert companies, located mostly in Europe (Alstom, Bombardier, Siemens, etc.) for SIL4 certified systems, and Japan (Nippon Signal, Hitachi, etc.) for certification to Japanese safety standards and deployed locally. Fail-safe know-how has not been prevalent in other markets that are investing in rail networks, relying on mostly European vendors for acquiring the fail-safe systems (e.g., India, Africa, South Korea) or for forming joint ventures with these same European vendors to develop fail-safe systems for the local market (e.g., China).

The demand for SIL4 certified equipment has been further fuelled by safety incidents that have driven governmental bodies to make it mandatory for all new installations to be SIL4 certified, and that non-SIL4 certified equipment in use today must be upgraded to SIL4 certified equipment. For example, the South Korean government mandated that rail equipment be upgraded to SIL4, and the Indonesian rail authorities have recently issued an RFP to upgrade their infrastructure to SIL4 certified equipment.

Another interesting trend in the global rail market is the aspirations of Asian application providers and rail integrators to expand their reach and penetrate overseas markets. Witness Hitachi’s establishment of a design center in London, recent announcements from Chinese vendors of wins in the U.S. and Africa, as well as efforts by Korean vendors to expand into ex-Soviet Union countries. Almost without exception, SIL4 certified equipment is a mandatory requirement.

A few major factors emerge from these trends that are the root cause for the emerging trend to outsource SIL4 certified application platforms:
SAFETY CRITICAL

1. The lack of SIL4 development expertise by Asian rail application providers and the barrier that poses to aspirations to expand into overseas markets.

2. The threat to western vendors posed by the entry of Asian vendors into the global rail market and the price erosion that would likely bring (witness the impact Huawei had on the global telecom market).

3. The prevalent architecture implemented by existing fail-safe computers is no longer capable of handling the required performance, requiring an expensive development effort in ‘table stakes’ base technology.

LOCKSTEP ARCHITECTURES
Most rail systems today use an architecture called hard lockstep, whereby two processors execute the same instruction at the same time and drive their respective address and data buses in synchronization.

When operating in hard lockstep, the processors’ clocks are synchronized and, before allowing a transaction to drive external equipment, all data and address bits driven by the two processors are compared. If the bits are exactly the same, then the address and data information are allowed to change the state of external equipment. If they do not compare, then a failure is declared and the system is brought to a safe state and is prevented from driving external equipment.

Since, in hard lockstep, comparison is performed at the address and data bits of the processors, a primary and mandatory requirement is that the two processors must execute the same instruction, at the same time, to the same external resources (memory, cache, I/O, etc.). To do so, the processors themselves must be deterministic. We call the boundary created by the comparators the deterministic boundary (Figure 1).

Unfortunately, hard lockstep cannot be implemented using modern processors. Multi-threading creates multiple paths for the execution of the program. Responses to soft errors in memory and I/O will cause divergent execution paths and timing. For example, errors that are caused by cosmic rays and change a bit in the register are not synchronized and not deterministic. This is more prevalent in current technologies because of the geometries of the transistors, which are so small that cosmic rays can flip bits. Also, other CPU features such as power management and cache operations introduce non-determinism.

The second problem is that it’s practically impossible to synchronize the data pairs of two different modern CPUs. The use of on-chip devices to multiply clocks prevents synchronized operation; multiple memory channels and serial peripheral interfaces also make it impossible. And it’s not practical to synchronize buses operating in excess of 1Ghz.

Another problem with a hard lockstep system is that it is fundamentally a closed system. Everything is tuned to work together, and it has to be all synchronized such that it’s very difficult to upgrade technologies without affecting the total system. So the bottom line is that hard lockstep is just not possible any more with advanced processors.

Artesyn has developed an alternative approach we call data lockstep architecture, whereby a deterministic boundary is created at the output stage of the processor board to the system data fabric that connects the processors to external devices. Before the processor boards are allowed to change the state of external equipment by driving packets on the data fabric their packets are compared to ensure that they are the same. If they are the same, then the transaction is forwarded to external equipment; if the packets do not compare, then a failure is declared, and the system fails safe; i.e., it is prevented from changing the state of external equipment.

As shown in Figure 2, the deterministic boundary is not at the processor itself but rather at the edge of the processor and before packets are placed on the data fabric.

The benefit of data lockstep is that it makes it possible to use modern processors and deliver the performance required by modern rail applications.

2oo2 or 2oo3
There are two methodologies for voting in a fail-safe system. They are called two-out-of-two (2oo2) and two-out-of-three (2oo3).
In 2oo2 voting, two computer elements compare the results of their computation and, if they compare, the transaction is driven to external equipment. If they don’t compare, a fail-safe state is entered. As shown in Figure 3, Artesyn’s ControlSafe™ Platform implements a dual 2oo2 architecture to deliver high availability. In case the first ControlSafe Computer fails, the second redundant one takes over and continues running the application.

In 2oo3 voting, three computing elements execute the application, and if the three don’t agree then the system determines which one is at fault, disables it, and continues running with two.

If the two disagree, then the system enters its fail-safe state and is prevented from changing the state of external equipment.

While both of these voting methods deliver the required safety and availability, the 2oo3 method is more complex to implement than the 2oo2 method. In the 2oo2 method, in case of a mismatch, the failed CSC enters its fail-safe state and the second CSC is enabled to run the application. No failure analysis, or fault isolation, hot-swap or re-integration is required.

On the other hand, in case there is a mismatch in a 2oo3 voting, failure analysis, fault isolation, switching to 2oo2 voting mode, module hot-swap, module reintegration, and re-enabling 2oo3 voting are all required. This is complex, and complexity leads to design errors.

For this reason, Artesyn’s ControlSafe Platform chose the 2oo2 voting method. A simple design is a safe design.

CONTROLSAFE ARCHITECTURE HIGHLIGHTS
Artesyn’s ControlSafe Platform employs data lock step synchronization and 2oo2 voting. The system runs Wind River’s VxWorks 653 operating system, which has been deployed in many fail-safe avionics-certified applications, including extensions to assure the task level synchronizations needed to implement data lockstep.

All voting is implemented by hardware using proprietary FPGAs, making it transparent to application software, and easing porting of existing applications.

The architecture is flexible and expandable. All intra system communications are over the data fabric and are based on Ethernet. All I/O modules are connected via Ethernet such that expanding the system from local to remote or expansions in the I/O environment is straightforward and scalable (Figure 6).

In conclusion, the ControlSafe Platform is a cost-effective, modular and a scalable system that is based on open industry standards. The system is future-proof and provides protection for the customer’s investment because the architecture enables upgrades to both the CPUs and the I/O modules independently of each other.

It is designed to offer a COTS SIL4 certified platform bringing to customers all the benefits of outsourcing table-stake technology—accelerated time to market, significant savings in R&D and certification costs, and the ability to focus their effort and their R&D on differentiations from their competitors.

Shlomo Pri-Tal is the Vice President of ControlSafe Platforms at Artesyn Embedded Technologies. Artesyn Embedded Technologies is the new name for the former Embedded Computing & Power business of Emerson Network Power. In his present role, Shlomo directs all activities required to develop and bring to market a SIL4 certified fault tolerant computing and communications platform targeted at safety critical applications.

<table>
<thead>
<tr>
<th>Dual Redundant 2oo2 System</th>
<th>Feature</th>
<th>Single Redundant 2oo3 System</th>
</tr>
</thead>
<tbody>
<tr>
<td>2oo2 Only</td>
<td>Voting Logic</td>
<td>Must switch from 2oo3 to 2oo2 and back to 2oo3</td>
</tr>
<tr>
<td>Box Fail-over</td>
<td>HA Model</td>
<td>Module Fail-over</td>
</tr>
<tr>
<td>Not Required</td>
<td>On-line Fault Isolation</td>
<td>Required</td>
</tr>
<tr>
<td>Not Required</td>
<td>Hot Swap</td>
<td>Required</td>
</tr>
<tr>
<td>Not Required</td>
<td>On-line Module Reintegration</td>
<td>Required and performed by User Application</td>
</tr>
<tr>
<td>Failing CSC is diagnosed off-line; low risk of total outage</td>
<td>Human Factors</td>
<td>Risk of total outage due to hot-swapping wrong module</td>
</tr>
<tr>
<td>Simplex</td>
<td>Backplane</td>
<td>Redundant</td>
</tr>
</tbody>
</table>

Figure 4. In 2oo3 voting, three computing elements execute the application, and if the three don’t agree then the system determines which one is at fault, disables it, and continues running with two.

Figure 6. All I/O modules are connected via Ethernet such that expanding the system from local to remote or expansions in the I/O environment is straightforward and scalable.

Figure 5. Voting method comparison.
Tracing into the Model: Using Requirements Traceability with Model-Driven Development

For aerospace, defense, transportation, nuclear, medical and indeed any safety-critical sector, the gains of Model-based Design cannot come at the cost of safety.

By John Thomas and Jared Fry, LDRA

Model-Driven Development (MDD) is a growing trend within the embedded computing world including safety-critical industries such as defense and avionics. While the software development process often involves some modeling work, the key differences that make MDD distinct from modeling in general are that specialized modeling tools are used and that the resulting model directly determines how the code is implemented.

For our purposes, we will define MDD as a two-step process. Firstly, a graphical representation of the software and its functionality is created. Secondly, from this model, source code is generated, either manually, automatically, or through a combination of the two methods. In the past, MDD was unable to compete in either reliability or efficiency with manually generated code. However, advances in modeling tools have reduced, and in some cases eliminated, the gaps between hand-generated code and model-generated code. In addition, supporters of MDD cite its visual approach, simplification of complex systems, potential for component reuse and overall flexibility. Despite MDD’s popularity in safety-critical industries, companies employing model-driven development often face challenges in achieving safety certification.

In part, these challenges are due to the scope of the most popular safety standards. For instance, the first version of international standards for industrial safety (IEC 61508) and its derivatives, or medical (IEC 62304) made no mention of MDD. The focus of these standards was on verification techniques and process outputs, leaving out details of particular development strategies. More recent updates incorporate guidance for MDD, providing a way for companies to assimilate industry experience and modern best practices.

These challenges pose several important questions. What are the current issues faced by developers who use model-based design but want to maintain requirements traceability for safety verification? And, how do modern requirements traceability tools assist in overcoming these challenges?

Requirements traceability connects the highest-level description of the project with lower-level implementation and design. From there the design can be linked to the implemented code and any associated testing. This enforces the idea that every requirement must be implemented and testable. For the most safety and mission critical projects, bidirectional traceability, which also links from low-level implementations to higher-level design and requirements, is recommended. This type of traceability links tests to the code to be verified and to the requirements that the code implements. If successful, bidirectional traceability illuminates many relationships between software requirements, the code that implements those requirements, and the tests that prove the requirements are met.

Requirements traceability enables software producers to “prove” to their client that:

- The requirements have been understood.
- The product will fully comply with the requirements.
- The product does not exhibit any unnecessary feature or functionality.

In the context of safety-critical software, requirements traceability takes on an added dimension of demonstrating that developers have minimized soft-
ware risks and performed all necessary verification activities. For instance, software failure for a safety-critical medical device (e.g. an implantable defibrillator) can have catastrophic effects. It’s vital to prove implementation of the requirements using concrete and verifiable evidence.

For over two decades, requirements traceability has shown itself to be an important means of collecting, organizing and connecting that evidence.

THE CHALLENGE OF MODELS AND REQUIREMENTS

Requirements traceability was originally envisioned for a traditional software lifecycle, involving either requirements database tools or textual documents. Integrating MDD into a traceability-based workflow is a relatively new challenge. A lack of guidance by safety-certification standards compounds these complications.

For example, the first editions of IEC 61508 and IEC 62304 incorporated little guidance for using MDD technologies. However, since those standards first came out, there have been many lessons learned about how MDD should be integrated with requirements traceability. The latest updates take these lessons into account and provide guidance on avoiding some of the potential dangers of incorrect integration.

RECONCILING TWO VIEWS OF MODELS

An issue that arose in many companies within the avionics industry, and which DO-178C clarified, was exactly how design models fit within the requirements traceability methodology. Models can represent a high-level overview of the project, so some companies treated them as high-level requirements. Others treated models as source-code since they can be used to generate the actual implementation.

The approach, approved for DO-178C, which makes the most sense from the viewpoint of requirements traceability, is that design models are low-level requirements. Models are treated as design documents that show how the implementation should perform.

It is important to treat design models in this manner to allow for more accurate verification. Without establishing a high-level definition of the system, it is difficult to ensure that the model is functioning as desired. It is also important to avoid treating the model as the actual implementation as this ignores possible defects introduced by the code-generation process, external code elements (hand code) added to the generated code and verification in the target environment.

Achieving traceability between the model and the higher-level requirements can be challenging, especially since the two are usually stored and presented in very different ways. High-level requirements are predominantly textual in nature, while most modeling tools provide graphic interfaces for design. Modern requirement traceability tools can bridge this gap by

For the traceability to be meaningful, the links must be between the actual model elements and the requirement from which it is decomposed. It is tempting to link all high-level requirements to an opaque model (a top-level model with no elements visible to the traceability process) See Figure 2. Doing so, however, ignores the purpose of traceability. Only the portion of the model that represents a given requirement can provide evidence that the requirement has been realized in the design. If a requirement has not been realized, it is important to be able to isolate the exact model element at fault.

Achieving traceability between the model and the higher-level requirements can be challenging, especially since the two are usually stored and presented in very different ways. High-level requirements are predominantly textual in nature, while most modeling tools provide graphic interfaces for design. Modern requirement traceability tools can bridge this gap by

For the traceability to be meaningful, the links must be between the actual model elements and the requirement from which it is decomposed. It is tempting to link all high-level requirements to an opaque model (a top-level model with no elements visible to the traceability process) See Figure 2. Doing so, however, ignores the purpose of traceability. Only the portion of the model that represents a given requirement can provide evidence that the requirement has been realized in the design. If a requirement has not been realized, it is important to be able to isolate the exact model element at fault.
Pulling high-level requirements and model elements from their respective repositories. These components can then be linked and managed alongside other traceability connections, such as those between requirements and functional tests.

PARALLEL TRACES
The central innovation of MDD is a separation between the development and coding process. This separation, however, can cause issues with requirements traceability. If the development and coding processes exist independently, establishing traceability for both can be complicated and error-prone. Requirements traceability is meant to be a continual effort spanning the entire software development lifecycle. If implementation and design are not linked, traceability work performed during design needs to be repeated during implementation.

The best-of-breed modeling tools do mitigate this danger somewhat. Many modeling tools make automatic connections between the model elements and their corresponding code possible. While that automatic mapping works in theory, often companies combine modeling tools with customized build processes, additional hand-written code and custom code generators that help obscure the connections between code and model.

Even when traceability between code and model are used, disconnects can exist between testing occurring in the model and testing source code in the target environment. In the MDD paradigm, verifying model behavior according to the high-level requirements, and making sure that tests exist to prove that model execution, are important.

To achieve this level of verification, modeling tools provide mechanisms to test the model within the modeling environment. While this testing is useful for verifying the design, it does not necessarily constitute actual executable object-code verification. This distinction between source-code level testing and model-level testing means that traceability connections between requirements and model tests does not automatically count for traceability between source-code tests and requirements. Again, the typical solution to this problem is to create parallel traceability chains for source-code tests and model-based tests, leading to redundant testing and the additional complexity of manually integrating the testing results.

It is possible to mitigate the disconnect between model-based design and source-code verification. Requirements traceability tools can be used to pull requirements and traceability evidence from multiple sources. By gathering low-level requirements that are represented as model elements and high-level requirements from external documents or databases, traceability links can go directly to the design elements linked to source code.

As well, results from both source code testing and model-based testing can also be presented together. Requirements traceability tools allow traceability evidence to be organized as one seamless flow, joining requirements, lower-level requirements, design, source code and tests. This helps to avoid the added complexity of maintaining and integrating two separate traceability efforts. [See Figure 3. Directly linking to model elements avoids duplicate links and simplifies the traceability process.]

In addition, the practice of test case reuse can reduce separate testing requirements. This involves isolating the input and output information used in the model-based testing, and then exporting it in a format that source-code testing tools can read.

With the proper verification and modeling tools, this process can even be automated. What is important from the traceability side is that traceability evidence can be re-used. If certain test case parameters are already shown to be traceable to a requirement, these parameters can then be re-used on the source-code level, and the same justifications and artifacts used in the requirements to model test linkage can be used in the requirements to source-code test linkage.

CONCLUSION
Despite its popularity, MDD has presented safety-critical applications with several new challenges. One challenge of particular importance has been reconciling requirements traceability with a model-driven development approach. MDD blurs many of the traditional lines between design, requirements and implementation, so it can be easy to misplace the model in the traceability process. In addition, model-based design removes the design process from the source-code level testing process, which creates the danger of duplicate and erroneous traceability work. Underlying these new challenges is the question of how to integrate a new software development method with critical software development practices.
The experience and practice of using model-based development and verification by the avionics community (and encapsulated as a supplement to DO-178C/ED-12C) serves as a good baseline for standards development in other disciplines. The medical and industrial safety disciplines can leverage this to develop best practices for incorporating models into lifecycle traceability. Modern traceability and testing tools are actively innovating to simplify and automate this. Requirements traceability, especially when done with an unclear understanding of the traceability process, can be painful.

When done right, requirements traceability can provide verification on all levels of the software development lifecycle. And with the proper tools, no compromise on safety is needed to access MDD advantages.

John Thomas is a field application engineer for LDRA Ltd. He graduated from Rutgers University. Before working for LDRA, John worked as a developer for several companies and was previously Project Manager for Castel Enterprises, Ltd. He joined LDRA in 2011 and has worked with LDRA clients on coverage testing, target integration and requirements traceability.

Jared Fry is a field application engineer for LDRA Ltd. He graduated from Western New Mexico University with degrees in Mathematics and Computer Science. His career began in the defense industry working for Lockheed Martin. There Jared served as a software engineer working on various projects ranging from missile and radar systems, training simulations and software testing. With LDRA he leverages these experiences as a consultant, assisting clients throughout the development process to produce a quality and certifiable product.
End of Life or Beginning a Lasting Design Win?

Designers faced with long life cycle support should investigate technology insertion as an alternative to speculative end of life component purchases.

By Wayne McGee, CES

The recently announced end of life (EOL) of the Tsi148 VMEBus Bridge chip has caused quite a stir in the embedded community. Many single board computer suppliers based their designs on this chip and are now faced with tough choices.

WEIGHING THE OPTIONS

One approach to the Tsi148 VMEBus Bridge chip EOL announcement is to make a large EOL purchase and stockpile the parts for future production. As of this writing, resellers are asking nearly $640 per device, making stockpiling the parts for future production a very expensive proposition. The finance groups at some suppliers will insist on shifting this upfront cost to their customers as well as charging annual storage fees. This approach to life cycle management places all of the financial burden and risk on the customer.

Redesigning the board to use the Tundra Universe chip, is another option, but this option has drawbacks. The Universe II is slower and does not support the 2eSST protocol. Redesigning a mature fast product to become a mature slower product probably does not make sense. Designers utilizing the PCI-X interface for the Tsi148 are faced with having to use glue logic to interface to the Universe II, which only supports PCI and operates on different voltage rails. An ugly option.

Another possibility is designing an FPGA-based VME64x bridge that is the equivalent of the Tsi148. This not only entails a board respin to accommodate the new package, but a serious amount of engineering time to design and test the functionality of the new bridge. It is unlikely to be 100 percent compatible with the software drivers for the Tsi148 and would require that the new drivers be qualified as well. For many programs, this would invalidate previous certifications and require that the system be requalified. As with the second choice, you are still dealing with a mature product, and the cost to update might very well not be justified.

MAKING THE CASE FOR NONE OF THE ABOVE

The approaches just mentioned have shortcomings not shared by a fourth option: single board computers that can be adapted to conform to most hardwired VME backplane configurations.

It is possible to choose a single board computer that does not rely on the Universe II or the Tsi148 but is instead based on an FPGA-based VME64x bridge with a proven track record and performance. But there is a real problem that emerges here. One that the single board computer suppliers have used to their advantage since the beginning days of VME. User defined I/O pin-out.

Typically once you get a design win, the customer is yours for the life of the product especially for conduction-cooled systems with no transition modules and the I/O hardwired in the backplane, leading suppliers to create families of succeeding products with identical or at least backwards compatible I/O. A supplier had to really do something awful to make the pain of changing worse than the pain of staying the same. But, as they said in the old Westerns, there's a new Sheriff in town.

Creative Electronic Systems (CES) RIO4 single board computer incorporates FlexIO technology, which allows the user I/O for P0, P2 and the PMC/XMC sites to be remapped without having to touch the base printed circuit board.

This is accomplished by routing user defined I/O lines for P0, P2, and the P4 connector for the PMC/XMC sites to a BGA site. Front panel I/O can be routed here as well. The I/O lines from the compute core are...
The compute core signals are then mapped to the appropriate external connector pins through the use of a Static Routing Module (SRM). The Static Routing Module is a printed circuit board with a BGA footprint that is compliant to the JEDEC MS-034B standard. It uses a 1mm pitch and has 676 connections available. The entire package has a 27mm square footprint. This is shown in Figure 1.

The end result is that the RIO4 and RIO6 single board computers can be adapted to conform to most hardwired VME backplane configurations.

With the Creative Electronic Systems RIOx family of single board computers the process of technology insertion and retrofit of obsolete VME boards becomes a straightforward exercise. The RIO7, the next family member, is entering the definition stage and will add further processing power and capability to this long-lived family of single board computers. Designers faced with long life cycle support should investigate technology insertion as an alternative to speculative end of life component purchases.

Wayne McGee is the vice president of sales and general manager for North American Operations for Creative Electronic Systems SA. Wayne has served in various senior management positions in his career and has more than 30 years of experience in the VME, CompactPCI, ATCA and VPX markets. Wayne is also the chairperson for the VNX VITA-74 Marketing Alliance. Companies Wayne has worked for include Motorola Computer Group, VMIC, SBS Technologies and GE Intelligent Platforms. He holds a BSEE from the University of South Carolina.
Nürnberg, Germany
February 24 – 26, 2015

embedded world 2015
Exhibition & Conference
... it’s a smarter world

THE gathering for the embedded community!
The world’s largest event for embedded technologies brings together all the players in the embedded sector for a productive conversation.

Make sure you are there when contacts and networks are being cemented on the international level and new trends are being set.

Media partners
elektroniknet.de
computer-automation.de
energie-und-technik.de
MEDIZIN-elektronik.DE
Markt&Technik
DESIGN & ELEKTRONIK
KNOW-HOW FÜR ENTWICKLER

Trade fair organizer
NürnbergMesse GmbH
Tel +49 (0) 911.86 06-49 12
visitorservice@nuernbergmesse.de

Congress organizer
WEKA FACHMEDIEN GmbH
Tel +49 (0) 89 2 55 56-13 49
info@embedded-world.eu
Keep your FPGA System Integration on Target and Above Water

Wild40 OpenVPX EcoSystem for 6U and 3U

12TB in One 6U VPX Slot
6GB/s Bandwidth

Hot-Swappable Exclusive to Wild40 EcoSystem

Annapolis Micro Systems, Inc.
410-841-2514
Module and System-Level Solutions from X-ES

**Intel® and Freescale™ Single Board Computers**
- **XPedite7570**: 4th Gen Intel® Core™ i7-based 3U VPX SBC with XMC/PMC
- **XCalibur1840**: Freescale QorIQ T4240-based 6U VPX SBC with dual XMC/PMC
- **XPedite2400**: Xilinx Virtex-7 FPGA-based XMC with high-throughput DAC

**High-Performance FPGA and I/O Modules**
- **XPedite2400**: Xilinx Virtex-7 FPGA-based XMC with high-throughput DAC

**Secure Ethernet Switches and IP Routers**
- **XPedite5205**: Secure Gigabit Ethernet router XMC utilizing Cisco® IOS®
- **XChange3018**: 3U VPX 10 Gigabit Ethernet managed switch and router

**High-Capacity Power Supplies**
- **XPm2220**: 3U VPX 300W power supply with EMI filtering for MIL-STD-704 & 1275

**Rugged, SWaP-Optimized, COTS-Based Systems**
- **XPand4200**: Sub-½ ATR, 6x 3U VPX slot system with removable SSDs
- **XPand6200**: SFF 2x 3U VPX system with removable SSD and integrated power supply
- **XPand6000**: SFF Intel® Core™ i7 or Freescale QorIQ-based system with XMC/PMC

---

X-ES
Extreme Engineering Solutions
608.833.1155  www.xes-inc.com

USA Designed, manufactured, and supported in the USA