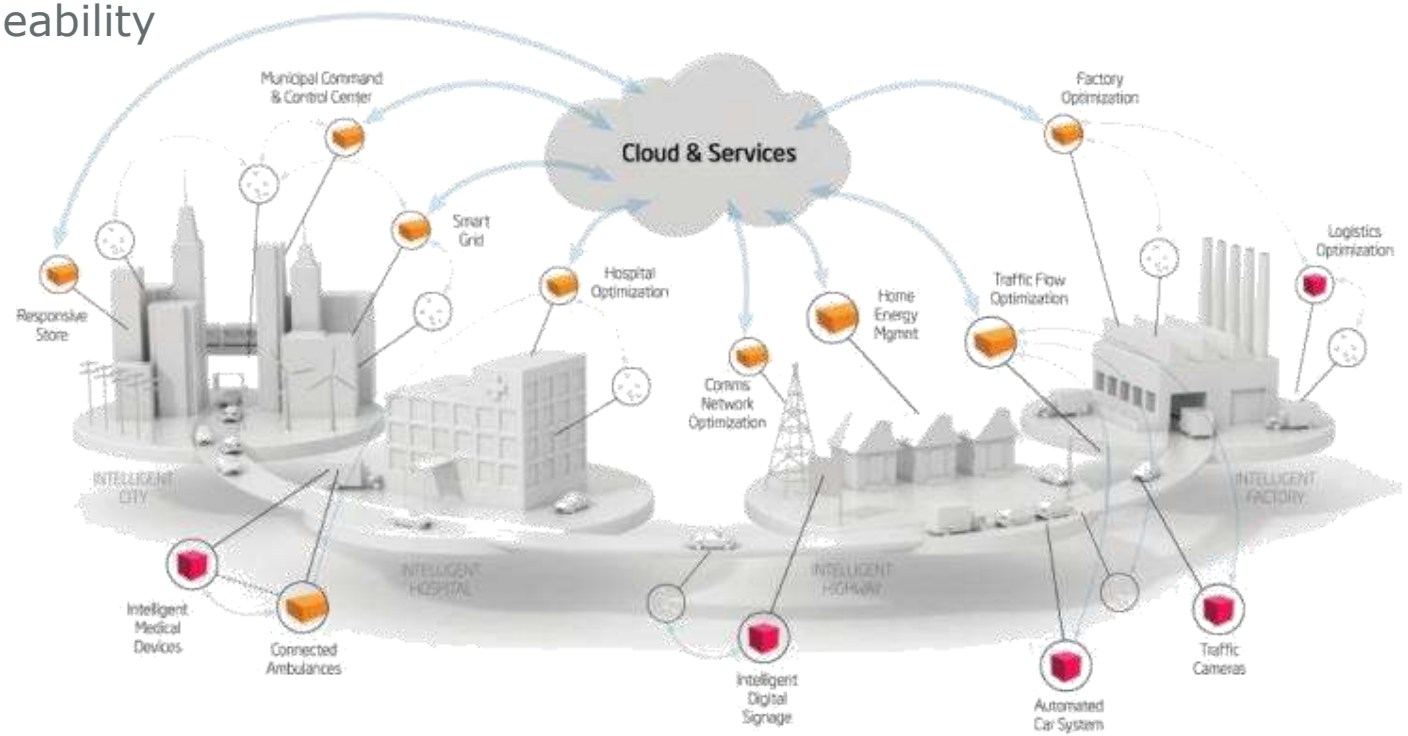
Intel Intelligent Systems Framework

Embedded Tech Trends 2013

RJ McLaren
Product Management, Military & Aerospace Products

Intel Intelligent Systems Framework

- Why Intel Intelligent Systems Framework (ISF)
  - Embedded Systems are more interconnected Internet-of-Things (IoT)
  - Fragmentation is becoming a major problem
  - ISF is a set of interoperable solutions scaling across products and applications
  - ISF ties together hardware, the OS and tools for Connectivity, Security and Manageability

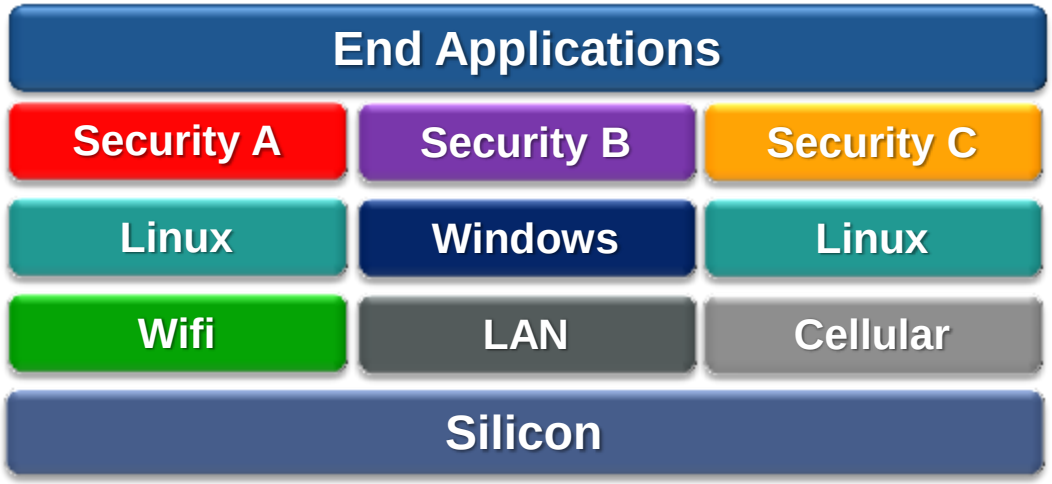


- Transformational Opportunity, what's Driving this?
  - Billions of Connected Intelligent Devices
  - User and Machine Driven Devices
  - These Devices need to share Data with each and the Cloud
  - Edge Devices need to react to streaming data in real-time
  - Data volume outpacing network and storage efficiency

What's the Problem?

Fragmentation on how to enable security, manageability, and accessibility to these intelligent devices

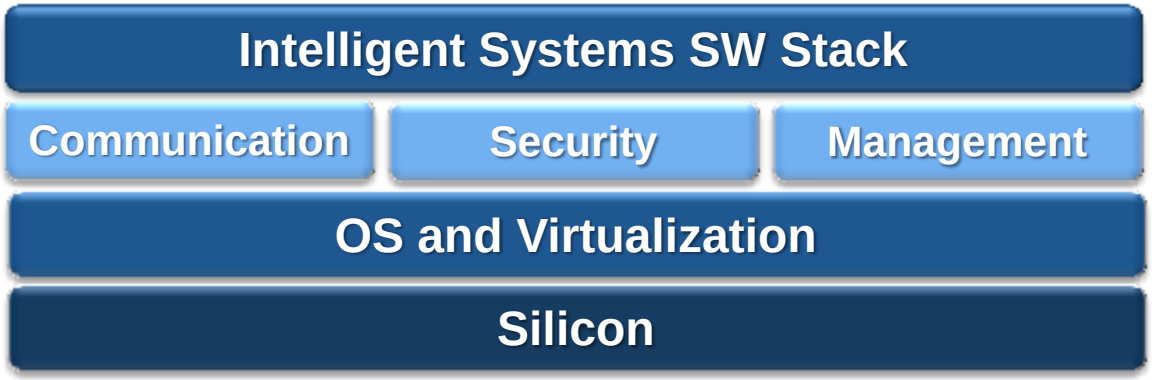
- Fragmentation drives multiple platforms
- Creates Integration issues (higher costs)
- Creates Points of Failures (higher costs)
- Reduces Time-to-Market
- Decreases User Interaction/Value



- Decrease reliability and usability of Data, etc.

What's the Solution?

- Intel Intelligent Systems Framework (ISF)
  Solutions to allow Devices to Connect, Share and Drive value from the Data
  - Connectivity (mostly IP-based communications)
  - Security
  - Manageability Features
  - Continued Performance Enhancements
- Faster-time-to-Market
  - Enables innovative services (unlocks the data)
  - Lower Development and Deployment costs

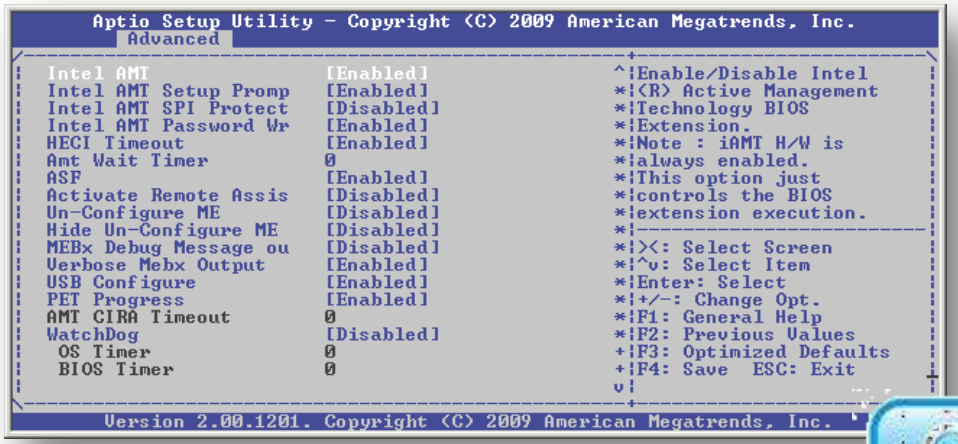


Connectivity Solutions

- Multiple Protocol (Networking technology)
  - Wired, Wireless, Local, Mobile
  - ISF Platform must support Ethernet connectivity
- Simple Integration with Intel Solutions & IA
  - Combine X-Intel Components
- Flexible Combinations
  - Easy Integration

Secured Solutions

- Platform Protection
  - BIOS & Firmware
  - Platform Hardware
  - System Reliability
- Software Protection
  - Operating System
  - Applications
  - Pre-OS
- Data Protection
  - System/App Data



Secured Solutions

- Firmware BIOS
  - FW should be based on UEFI 2.1 or greater with 2.3.1 being the ideal candidate at this time.
    - *2.3.1 includes EDK 2 support for measured boot and secure boot.*
- Trusted Platform Module (TPM)
  - Required for Intel vPro technology based platforms
  - Required for remote certification and authentication
    - *TPM 1.2*

Security Software & Middleware

- Wind River
  - Multiple offerings for secure virtualization, secure remote management, secure operating environment, VPN
- McAfee.
  - Embedded Control, lightweight SW to protect against malware and other cyber threats
  - Deep Defender provides real-time kernel monitoring to reveal and remove advanced, hidden attacks.
  - ePRO client-side component providing secure communication between McAfee ePO and managed systems.
- Intel
  - Intel Advanced Encryption Standard (AES-NI); encryption without slowing performance and manageability
  - Encrypt Faster with hardware-based high-quality random numbers using Intel Secure Key
  - Intel Anti-Theft Technology, automatically protects mobile assets against threats

Intel vPRO Technology

- Intel Virtualization Technology (VTx)
  - Protects virtual environments from malware and rootkits
- Intel Active Management Technology (AMT)
  - Remotely diagnose, isolate, and repair an infected Intelligent System regardless of operational state
- Intel Trusted Execution Technology (TXT)
  - Ability to use hardware based mechanism to verify system integrity during the boot process and system memory scrubbing

Manageable Solutions

- Reliability
  - Improved System Uptime
  - Out of band Detect/Diagnose/Repair
  - Device Management
- Efficiency
  - Remote Power Management
  - Off peak maintenance
  - Asset Management
- Hardening
  - Integration of Security & Compliance Management

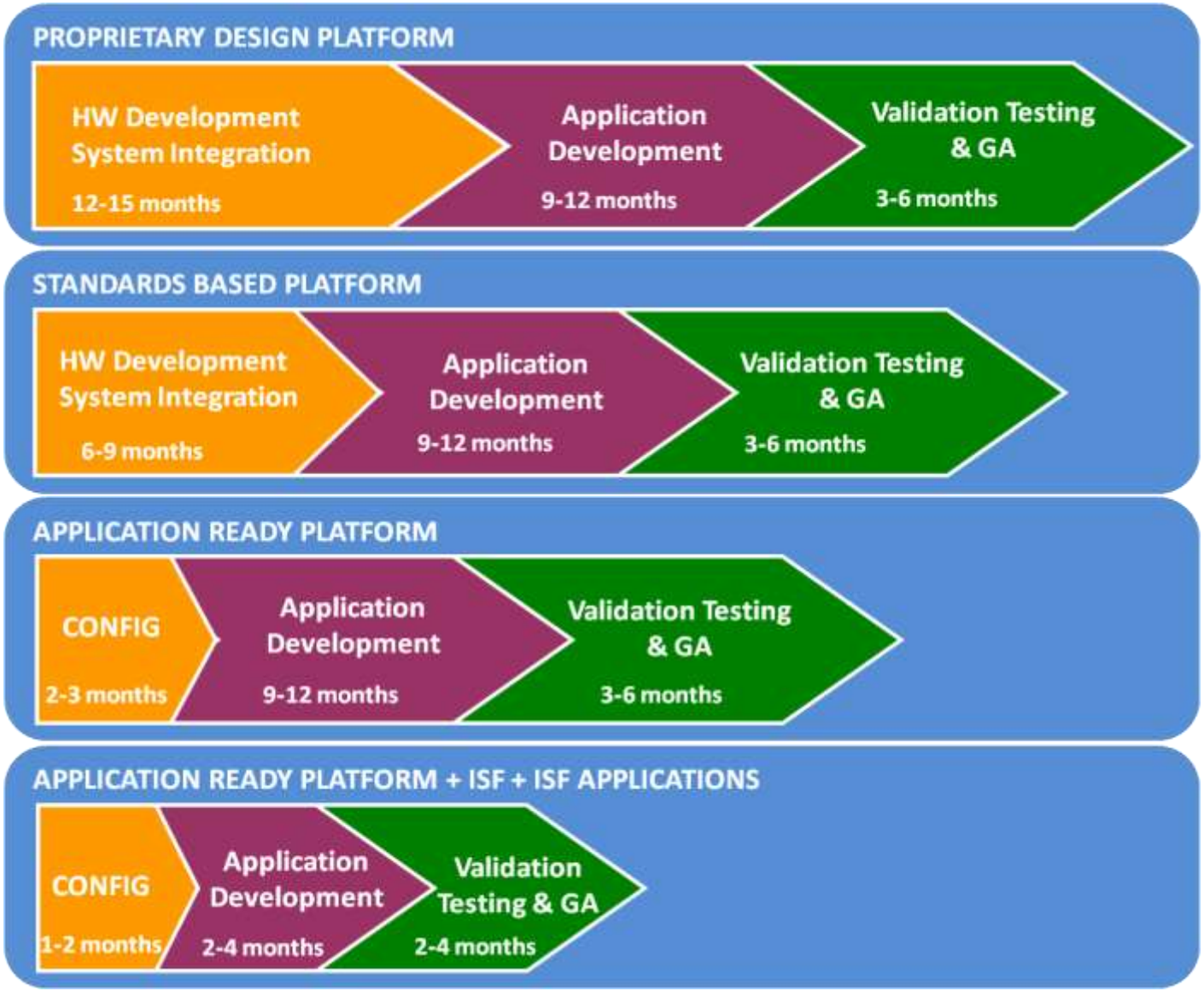
Performance Enhancements

- Intel Architecture
  Intel® Xeon®, Intel® Core™ (i5 & i7) and Intel® Atom™ processors
  - Low size, weight and power (SWaP)
  - Increase in Processing Performance
  - Increase in Power Efficiency
  - Improvements in Thermal Management
  - Increase in Graphics performance
  - Improvements in Advanced Vector Extensions (AVX) for floating-point-intensive computation

ISF Required Ingredients

Category	Required ISF Ingredients
Hardware	Intel® Processor with Intel® Trusted Execution Technology (Intel® TXT)
	Intel® Processor with Intel® Virtualization Technology (Intel® VT)
	Intel® Chipset with Intel VT, Intel TXT, Intel® Management Engine (Intel® ME)
	Trusted Platform Management (TPM) 1.2
	Intel® Ethernet/Controller Adapter
BIOS	Intel® Virtualization Technology (Intel® VT) for IA-32, Intel® 64 and Intel® Architecture (Intel® VT-x) capable BIOS
	Intel® Virtualization Technology (Intel® VT) for Directed I/O (Intel® VT-d) capable BIOS
	Intel® TXT capable BIOS
	TPM 1.2 capable BIOS
	Intel® Active Management Technology (Intel® AMT) capable BIOS
Software	Intel® ME firmware with Intel AMT
	Intel® AMT Drivers
	TPM Drivers
	Microsoft Windows 7 (64bit) Compatibility
	Microsoft Server 2008 Compatibility
	Wind River Linux Compatibility
	McAfee Embedded Control Compatibility
	McAfee ePolicy Orchestrator (McAfee ePO) Agent
	McAfee Embedded Command Compatibility

Reduce Time & Cost



Common Platforms for Intelligent Systems

kontron

Core i7 1st Generation	Core i7 2nd Generation	Core i7 3rd Generation	
x4 PCIe GETH BaseBX GETH BaseT	x4 PCIe gen2 GETH BaseBX GETH BaseT	Dual Core 14 to 25W (Configurable TDP) XMC slot x8 PCIe gen3 1/10 GETH BaseBX 1GETH BaseT	Quad Core 35W x8 PCIe gen3 1/10 GETH BaseBX 1GETH BaseT

intel Intelligent Systems Alliance Premier

COM Express* Basic

Flex ATX

Mini-ITX

3U VPX

Processor AMC

3U CompactPCI*

6U CompactPCI*

Digital Signage Application Story

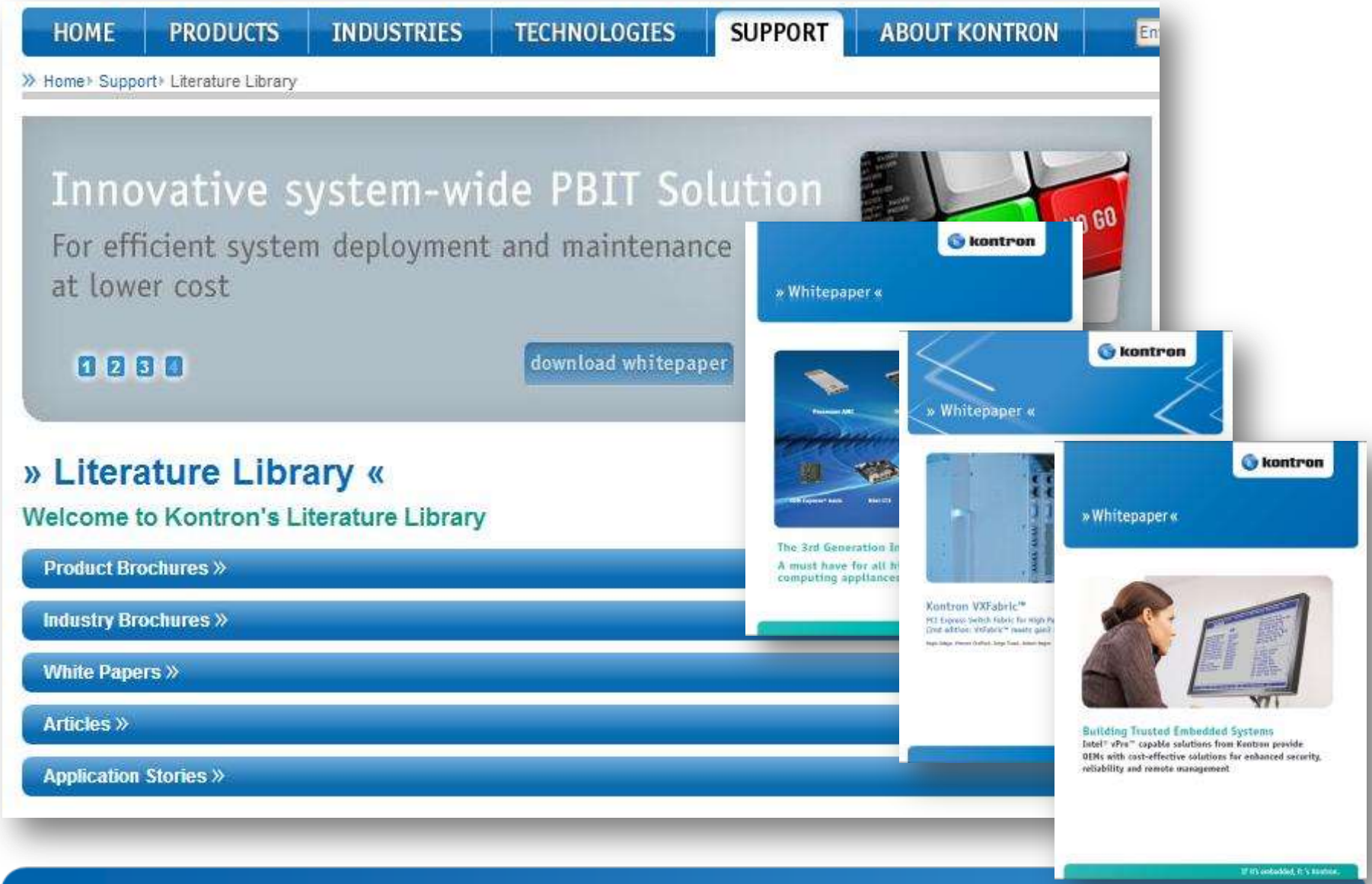
Digital Signage & OPS Standard

- Growing & Emerging market but fragmented product solutions
- IFS, DSEK (w/ ComExpress), Windows POSReady7, & Flypaper Application provide a rapid & seamless solution
- Data Analytics & Engaging Content Creation/Management provides immediate ROI
- Intel vPRO provides secure platform management
- Intel AIM Suite provides audience impression measurements

ISF Summary

- ISF provides the following
  - Consistent framework for foundational capabilities on Connectivity, Security and Manageability with ongoing performance enhancements
  - Pre-Validated Recipes provide flexibility and scalability
  - Enables vertical specialization and allows resources to focus on utilizing the data and not interoperability
- ISF Ecosystem
  - Kontron and other Alliance Members support ISF and incorporates these features onto the board level and system products solutions
  - Provides tailored solutions and compliant application software
  - Improves time-to-market and promotes reuse of proven hardware and software solutions

Reference Material



Thanks for your Attention