Fraunhofer FKIE

RHEINMETALL DEFENCE

Selex ES
A Finmeccanica Company

THALES

VRC
Vetronics Research Centre

Functional View
Network & Computer View
Operating System & Middleware View
Computer Program View

LAVOSAR

EUROPEAN DEFENCE AGENCY

EDA Workshop #2 (“Industry Workshop”) 25/06/13
Computing and Communication Environment

Olivier SCHMIDT – THALES Communications & Security

Thales Communications & Security

Introduction (1/2)

Analysis of Computing & Communication Environments

- Identify current mission equipment technologies
- Propose a list of technologies candidates for a future open vehicle architecture standard

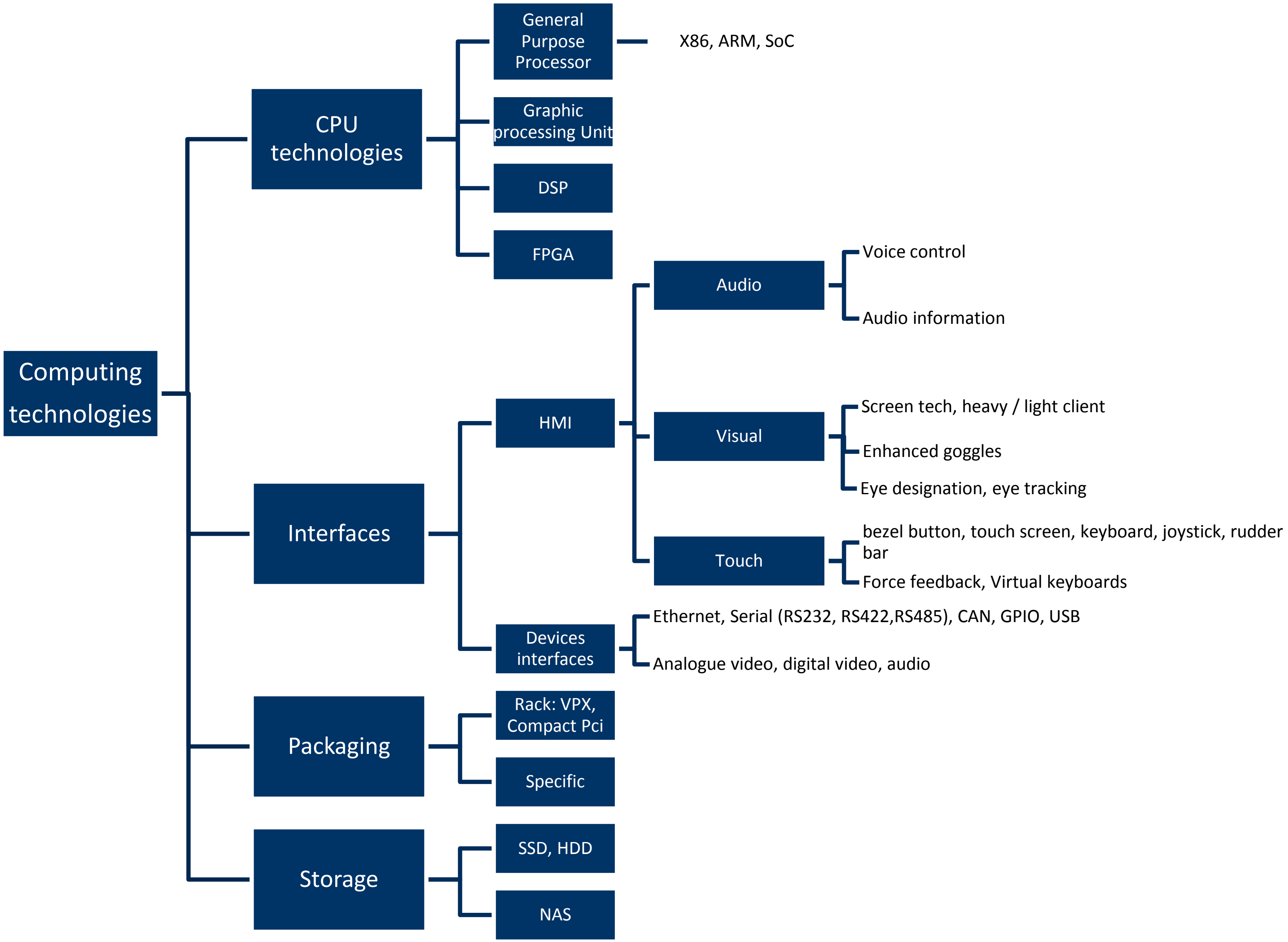
Outputs

- Document on Candidate technologies of present and future computing and communications environment for standardization with identified advantages and disadvantages
- Document for assessment of technologies against key LAVOSAR criteria

Agenda : Computing and Communication Environment

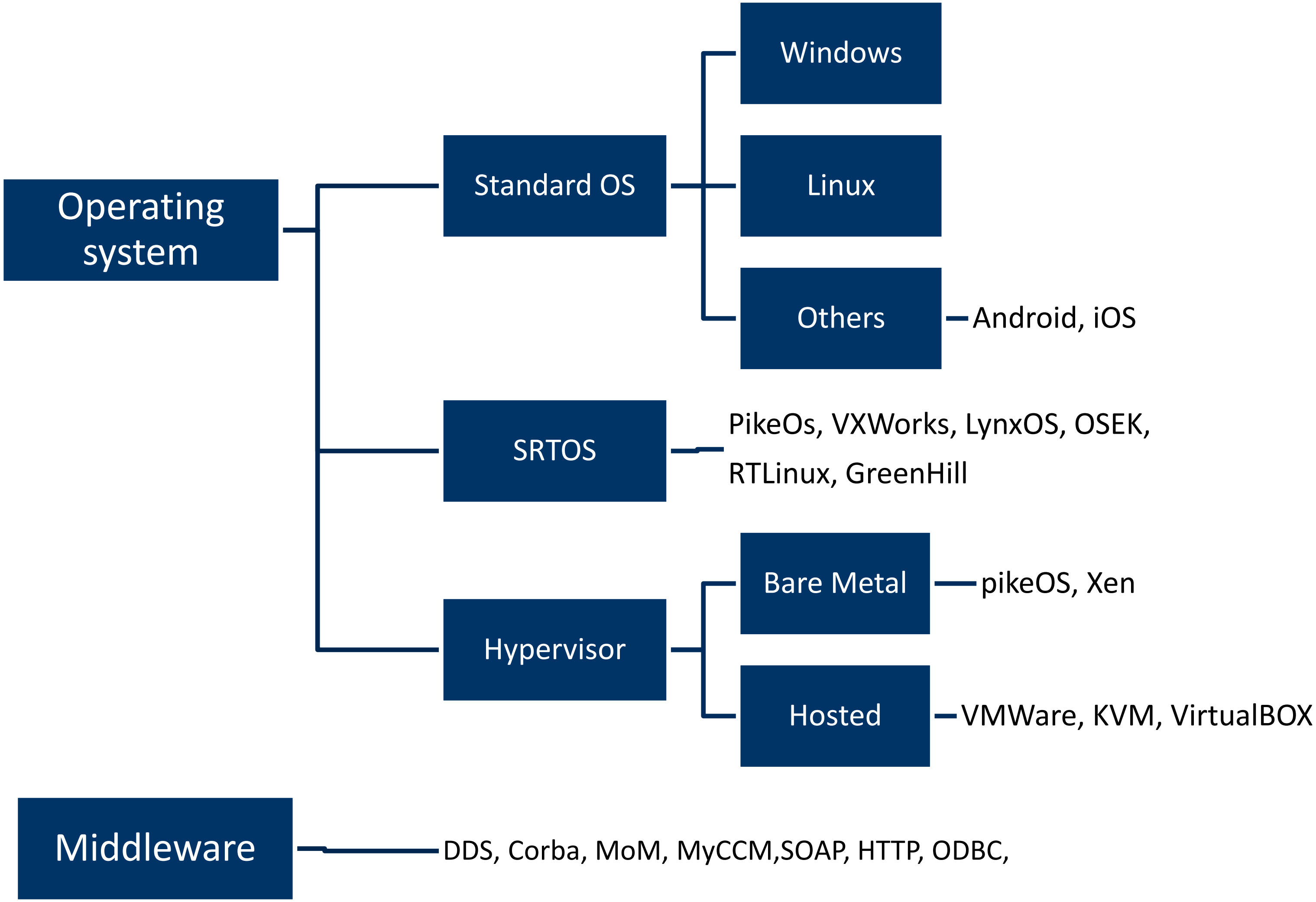
- **Introduction**
- **Technological trees**
- **Technological state of the art**
  - Computing technologies
  - Operating Systems
  - Middleware
  - Communications
  - Network Infrastructure
  - Security & Safety aspects
  - Further Technologies Aspects according Normative Framework

Technological tree (1/3)



- Computing technologies
  - CPU technologies
    - General Purpose Processor
      - X86, ARM, SoC
    - Graphic processing Unit
    - DSP
    - FPGA
  - Interfaces
    - HMI
      - Audio
        - Voice control
        - Audio information
      - Visual
        - Screen tech, heavy / light client
        - Enhanced goggles
        - Eye designation, eye tracking
      - Touch
        - bezel button, touch screen, keyboard, joystick, rudder bar
        - Force feedback, Virtual keyboards
    - Devices interfaces
      - Ethernet, Serial (RS232, RS422,RS485), CAN, GPIO, USB
      - Analogue video, digital video, audio
  - Packaging
    - Rack: VPX, Compact Pci
    - Specific
  - Storage
    - SSD, HDD
    - NAS

Technological tree (2/3)



Operating system

Standard OS

Windows

Linux

Others

Android, iOS

SRTOS

PikeOs, VXWorks, LynxOS, OSEK, RTLinux, GreenHill

Hypervisor

Bare Metal

pikeOS, Xen

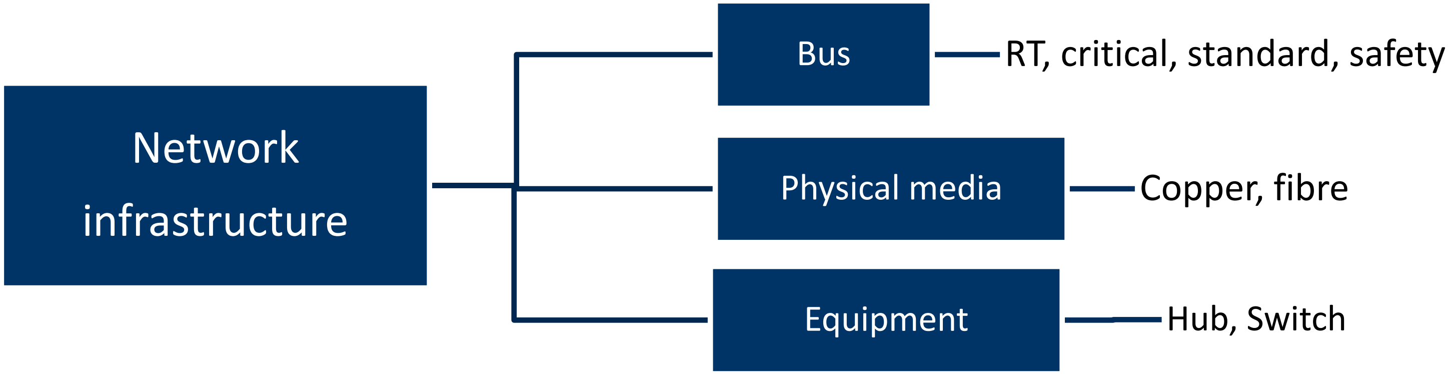
Hosted

VMWare, KVM, VirtualBOX

Middleware

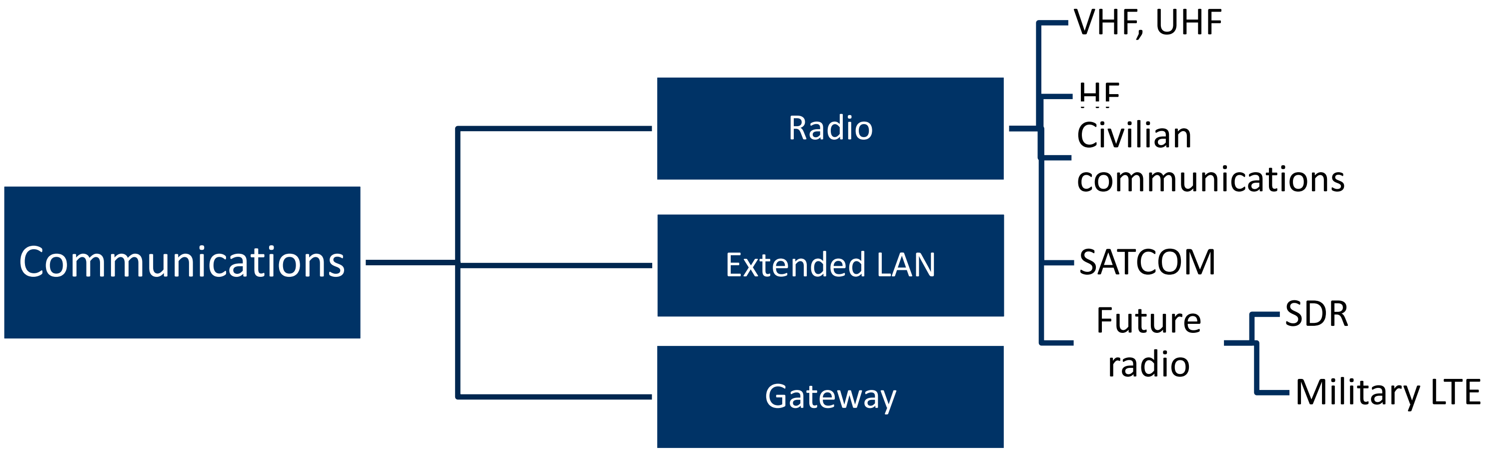
DDS, Corba, MoM, MyCCM,SOAP, HTTP, ODBC,

Technological tree (3/3)



Network infrastructure

- Bus — RT, critical, standard, safety
- Physical media — Copper, fibre
- Equipment — Hub, Switch



Communications

- Radio
  - VHF, UHF
  - HF
  - Civilian communications
  - SATCOM
  - Future radio
    - SDR
    - Military LTE
- Extended LAN
- Gateway

Computing technologies – Ruggedized Computer Architecture

Selection or Design of modules & Daughter Boards based on industrial standards

PICMG, VITA, PC/104, …

Conforming to

MIL-STD-1275

Equiped Chassis conforming to

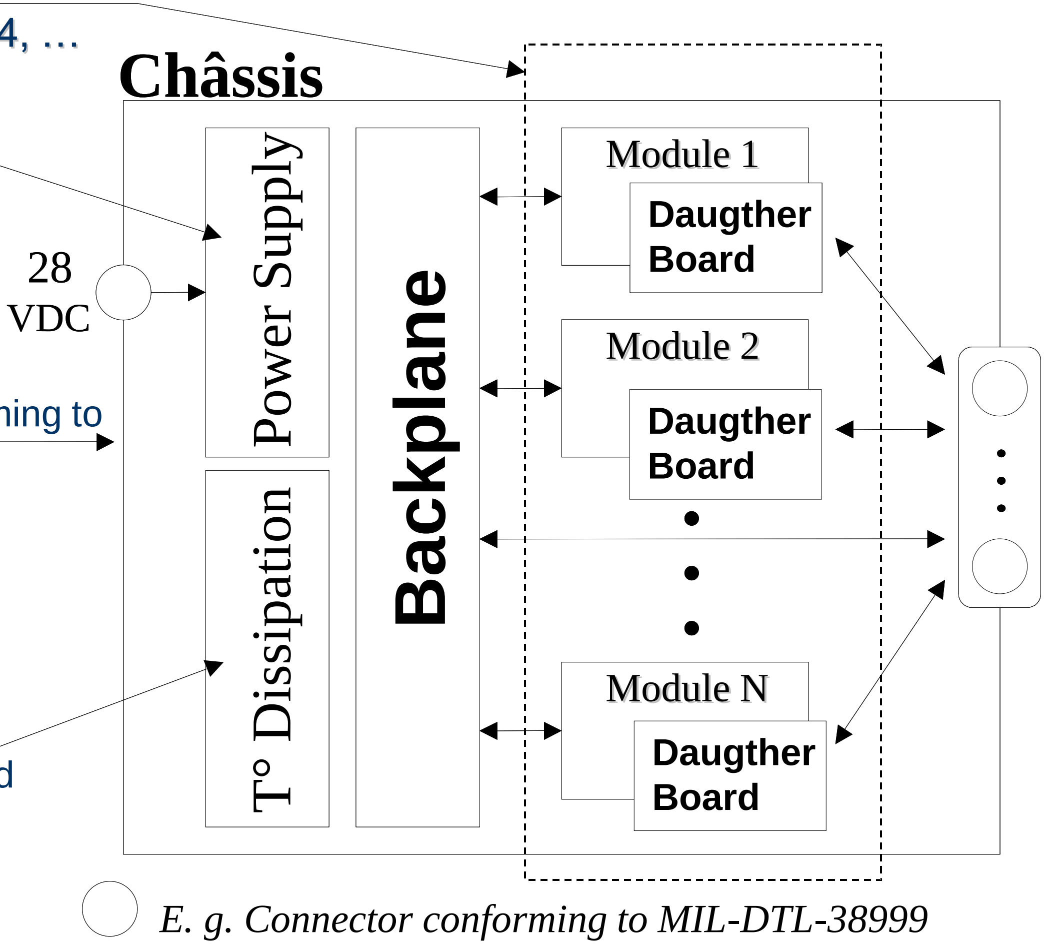
MIL-STD-810F

(T°, vibrations/shoks)

MIL-STD-461E

(EMI / EMC)

Conduction/Convection Cooled



Châssis

28 VDC

Power Supply

T° Dissipation

Backplane

Module 1

Daugther Board

Module 2

Daugther Board

Module N

Daugther Board

E. g. Connector conforming to MIL-DTL-38999

Technology Theme : Computing – processing Units

Technology	+	-	Comments
GP CPU	- Versatile technology - Multicore - Security ext. - Virtualization ext.	- Not allways Power Efficient	x86, Atom, ARM based, PowerPC,
Network Processors	- Network Optimized		- QorIQ
GPU	- Massively //	- High Power	- Graphics
FPGA	-CPU IP Cores -Low Power Consumption	- High Dev Cost	
DSP	- Signal Processing		

CPU HW Extension for Virtualization & Security

INTEL

- Core I3, I5, I7
- Atom (some members)

FREESCALE

- Familly e500v2 e500mc, e5500 e6500
- QorIQ P3/P4/P5 series QorIQ T Series

ARM

- Cortes Ax Familly (Trustzone).

Computing Technologies – Packaging

- **Standardization organisations**
  - PC/104 Consortium
    - PC/104-Plus
    - PCI-104
    - PCI/104-Express
    - EBX
    - EPIC
    - EPIC Express
  - PICMG Consortium
    - COM Express
    - AdvancedTCA
    - MicroTCA
    - CompactPCI
    - CompactPCI Express
  - VITA (VME International Trade Association)
    - VITA-74 : NanoATR SFF Computer
    - VITA-46 : VPX Computers (3U)
    - VITA-41 : VXS Computer (6U)
    - VITA-42 : XMC Daughter board
  - IEEE
    - PCI Mezzanine Card. IEEE 1386.1

Computing Technologies – Computer On Module

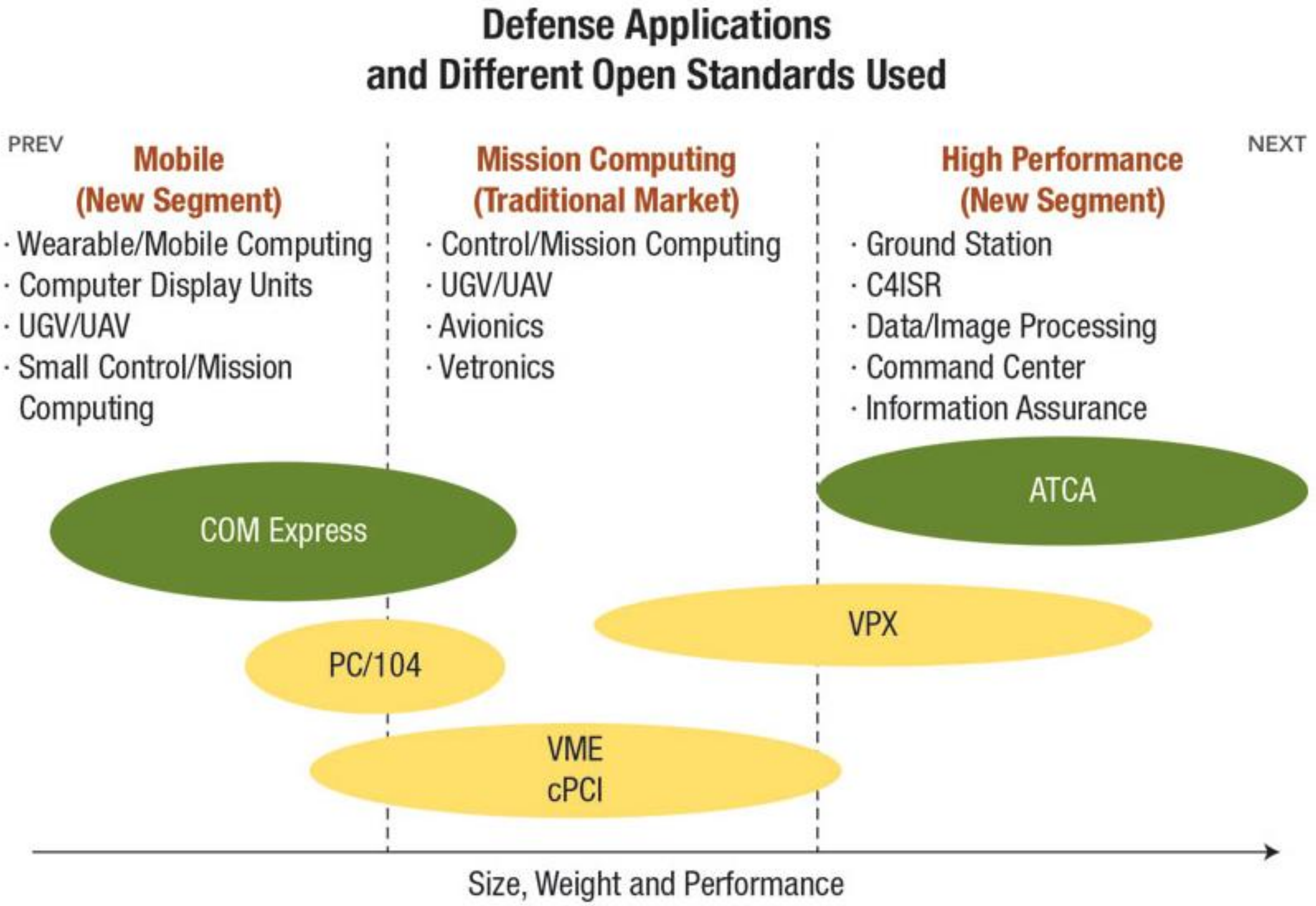
- **Design strategy is based on**
  - COTS Computer on modules (Daugther boards), e.g. COMExpress
  - All I/O interfaces are handled by the carrier board which custom designed to fit each dedicated applications.

- **E. g. COMExpress**
  - CPU on module
  - I/O on carrier Boards
  - Standardized CPU Module/ Carrier interface
  - 4 different Form factors (Mini: 55 x 84 mm, Compact: 95 x 95 mm, Basic: 95 x 125 mm, Extended: 110 x 155 mm).
  - 6 differents Carrier board interface Type

Computing Technologies – Packaging

- **uTCA (based on AMC modules)**
  - Not well suited for reggudized environments (ongoing work)
  - Less adapted to support & distribute I/Os
- **3U Compact PCI Express**
  - Low number of I/Os on backplane
  - Compromised standard following introduction of VITA 46/VPX 3U
- **PC/104**
  - Too small formfactor to support high end applications
  - Exists in PCI express version but low market offers
  - Lots of choice in PCI and/or ISA bus standards
- **VITA 46 / VPX 3U**
  - Dedicated for hardened applications (designed w/ VITA 48 / REDI hardening standard).
  - Compatibility with 3U cPCI standard
    - 3U Eurocard FF , PMC/XMC daughter board, Conduction Cooled (VITA 30.1)

Computing Technologies – Packaging



Defense Applications
and Different Open Standards Used

PREV

NEXT

Mobile (New Segment)
- Wearable/Mobile Computing
- Computer Display Units
- UGV/UAV
- Small Control/Mission Computing

Mission Computing (Traditional Market)
- Control/Mission Computing
- UGV/UAV
- Avionics
- Vetronics

High Performance (New Segment)
- Ground Station
- C4ISR
- Data/Image Processing
- Command Center
- Information Assurance

Technology Theme : Computing – Storage

Technology	+	-	Comments
USB Key		-Fragile Interface -Security	Needs IDS
Micro-SD Card		- Fragile Interface -Security	Needs IDS
Rugged DataKey	- Tactical use	- I2C/SPI memory	- Used on US IP encryptor
SATA Flash	- No Moving parts	- Limited number of writes	Cyphered Options
NAS Network Access Server	-Ethernet - High Capability	- Another Dedicated Network Equipment	Can secure exchanges at the expense of performance

Technology Theme : Operating Systems

Operating Systems

- Generic Purpose OS : MS Windows, Linux
- Hard Real Time OS : LynxOS, QNX, VxWORKS, Integrity, PikeOS

Virtualization Technology

- HyperVisors

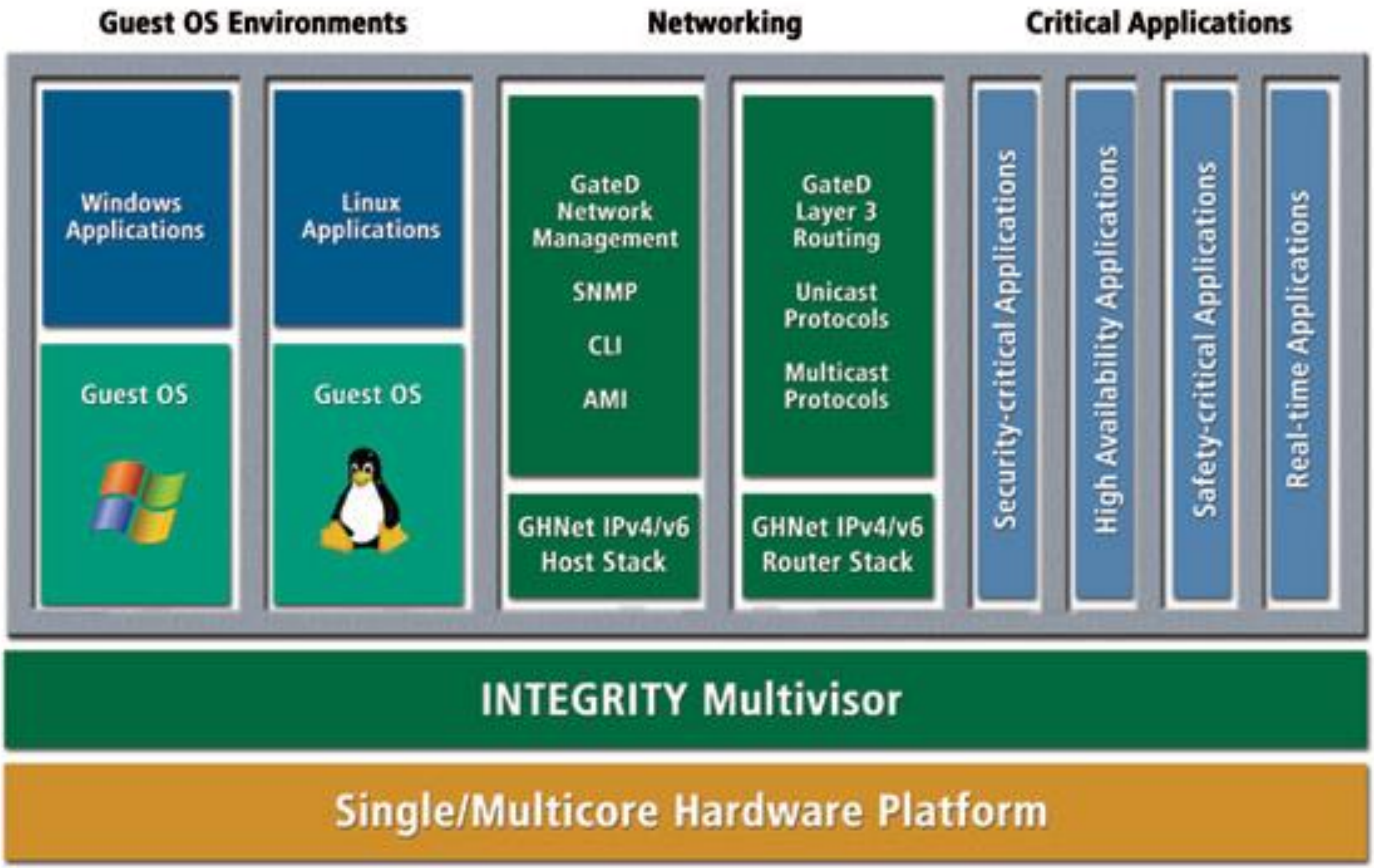
Application to Virtualization

- Secure Partitioning of Operating Systems for Multi Level Security (MLS) & Safety

Secure Operating systems

- PolyXene, SINA, NetTop, SELinux, Thin Client

Technology Theme : E.g. Hypervisor + Operating Systems

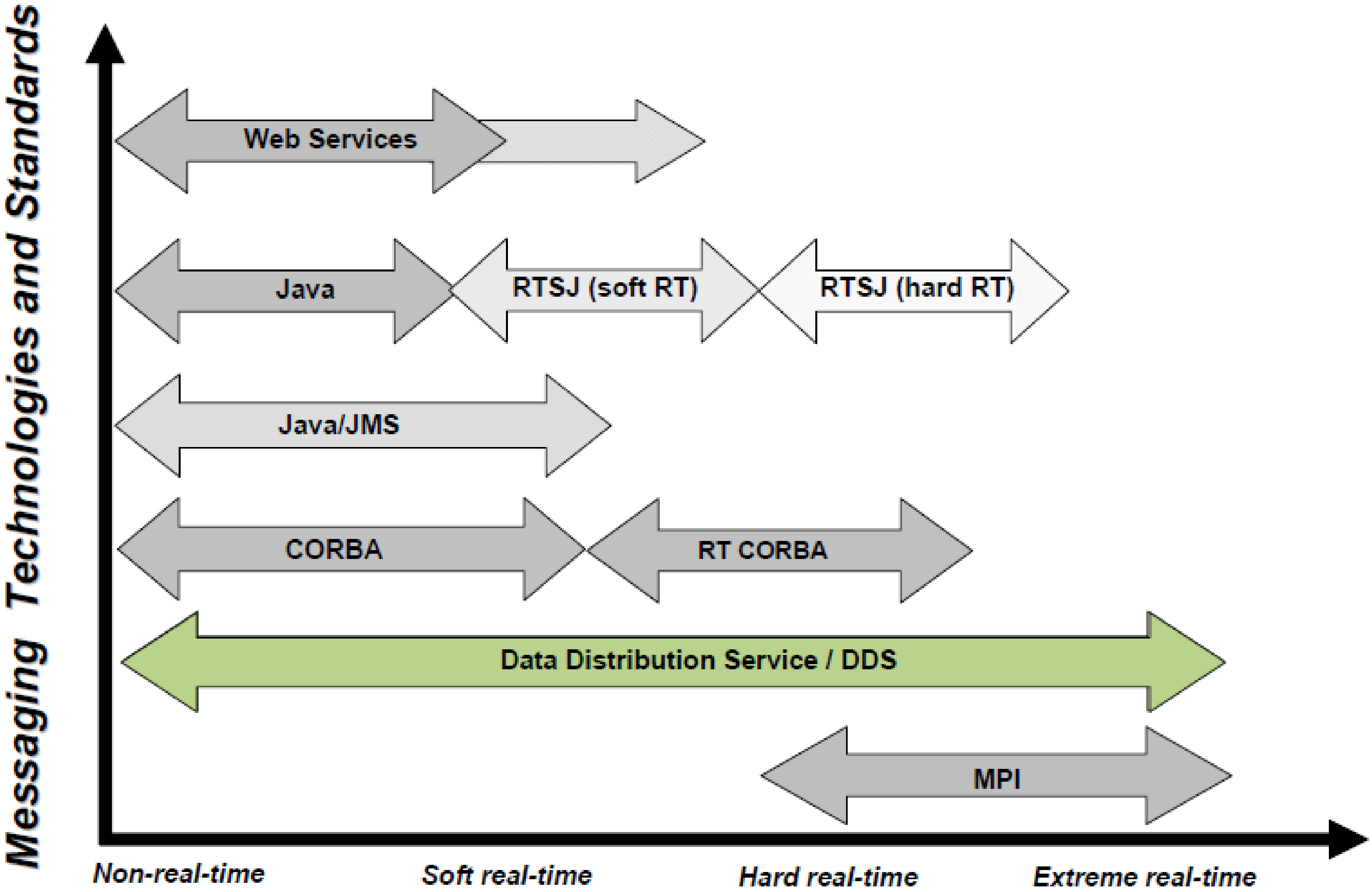


Middelware SW (1/3)

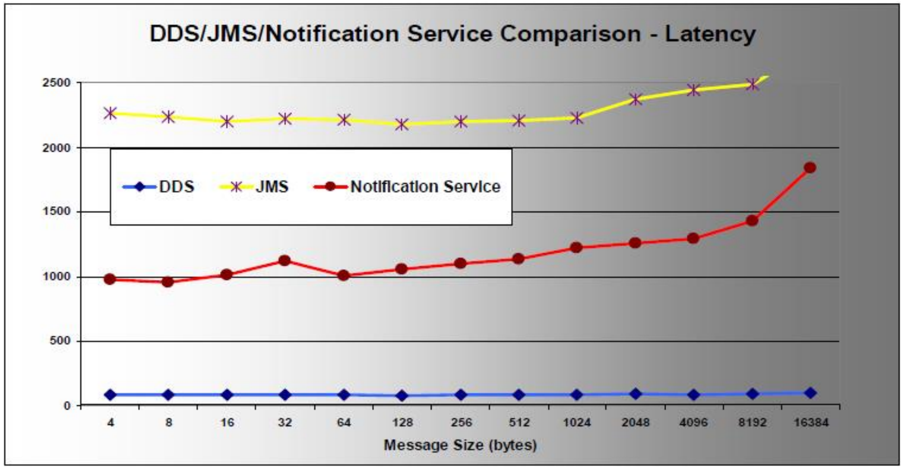
- **Middleware Terminology**
  - Middleware : API and service layer above operating system and below “application” code that abstracts common interaction patterns
  - Network Middleware : Most popular class of middleware, Middleware used for developing distributed applications
  - Distributed Applications : Those requiring interaction/communication between multiple computers

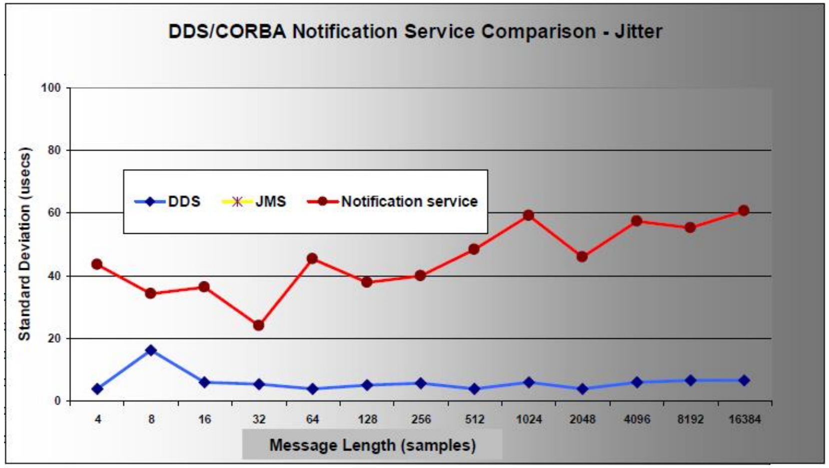
- **Middleware types**
  - Communications middleware
  - User interactions middleware
  - Components assembly middleware

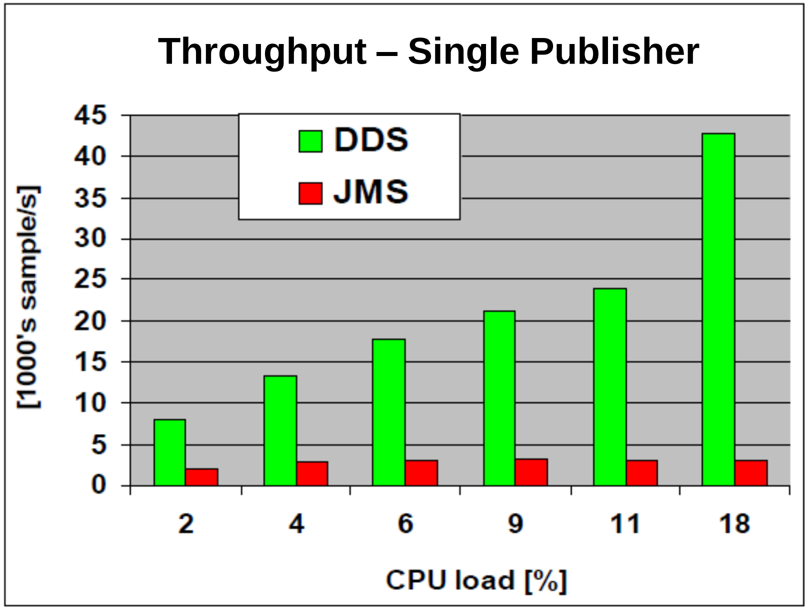
Middleware : Data-Distribution and Real-Time (2/3)



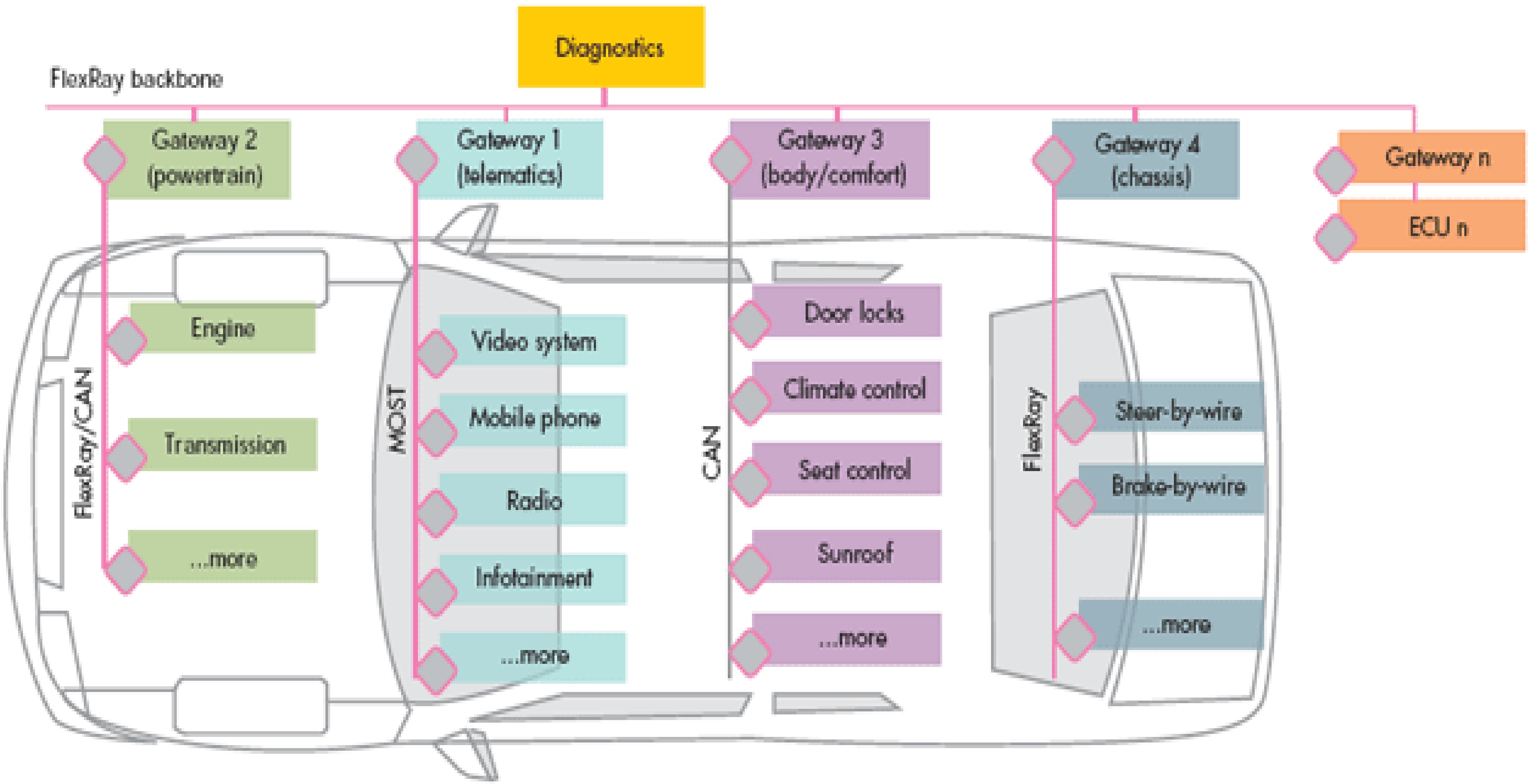
Middleware : DDS vs Other Technologies (3/3)



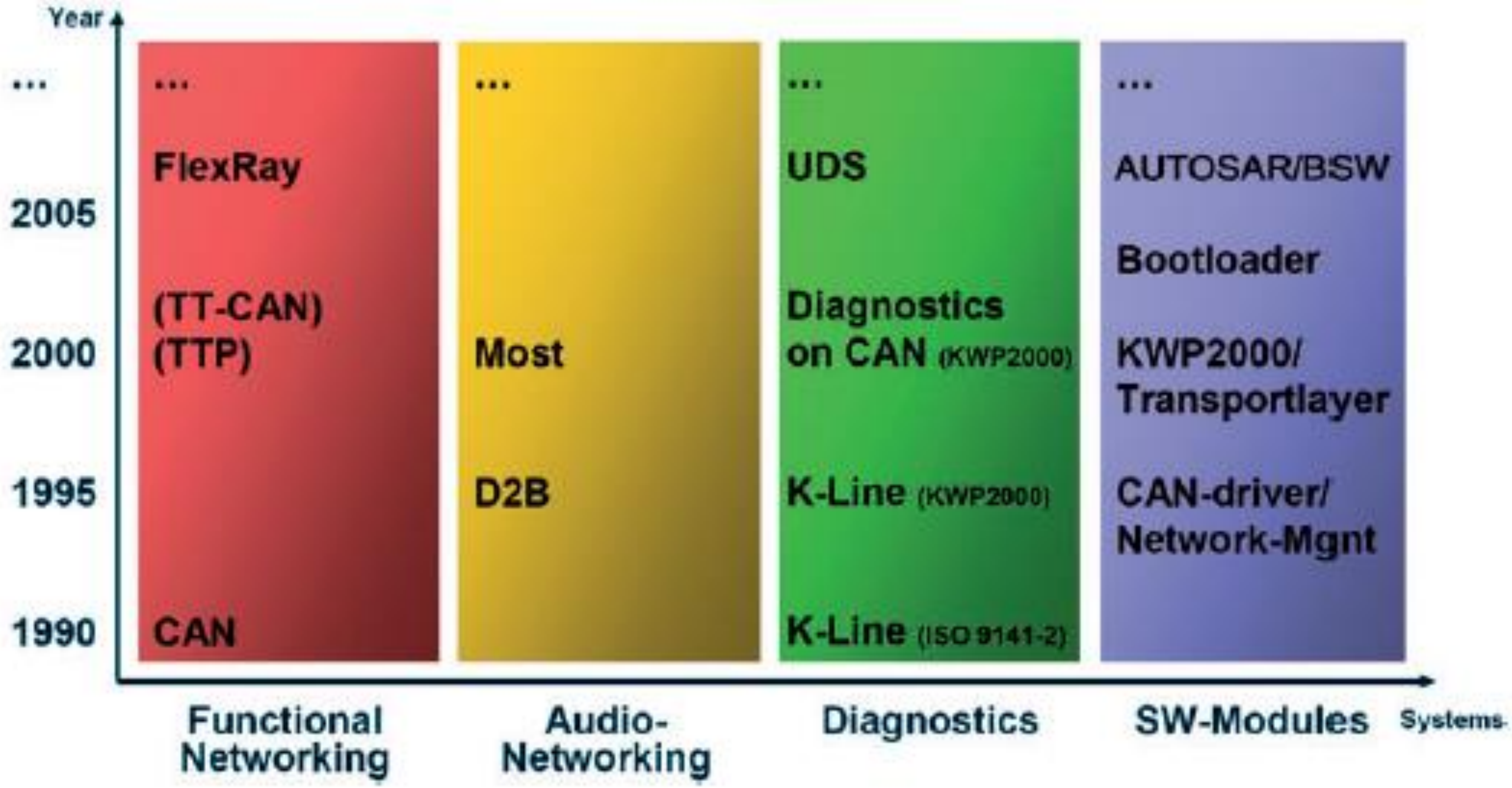




Vetronics Backbone – Automotive status



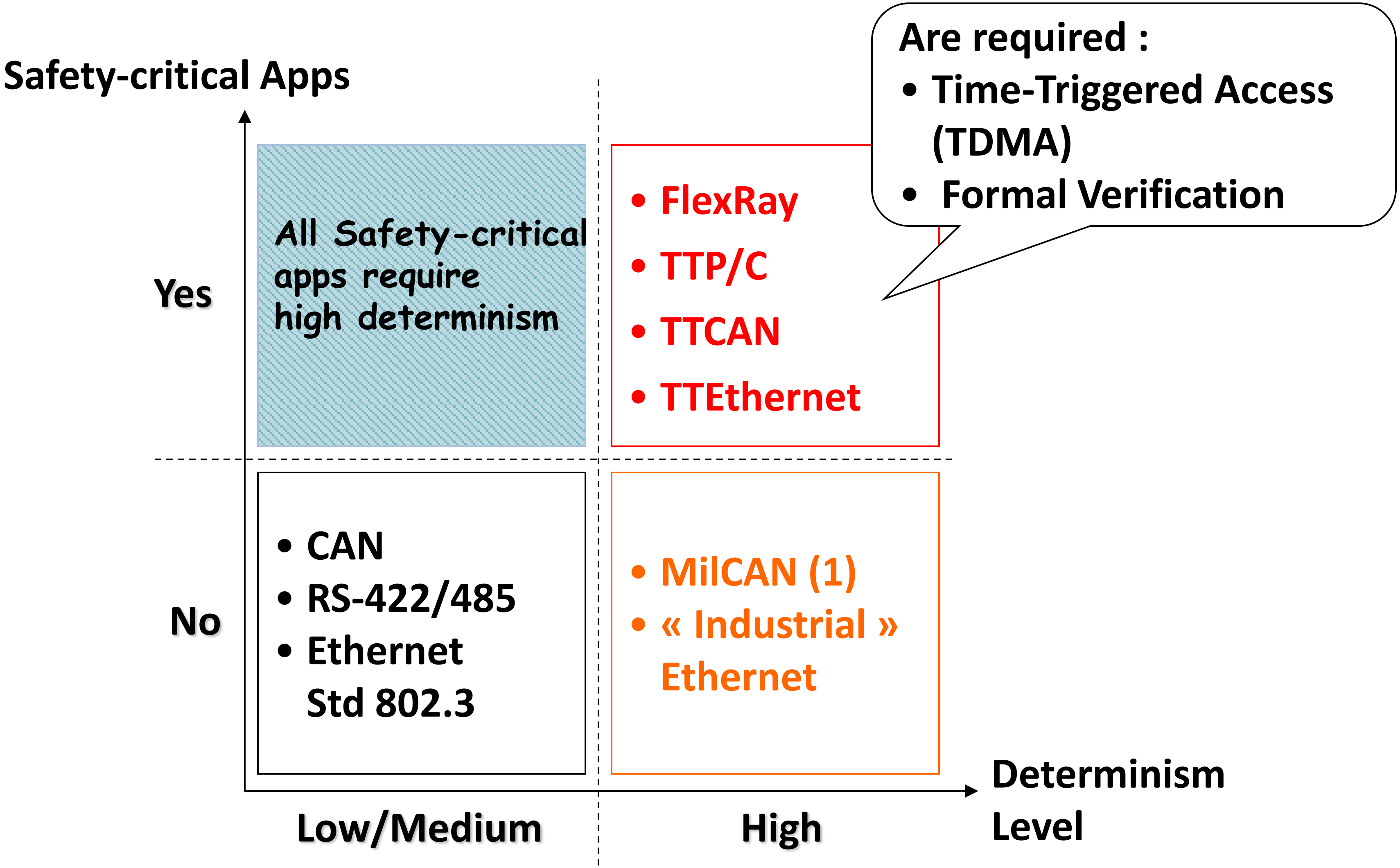
Vetronics backbone – Bus Historical Evolution



Year	Functional Networking	Audio-Networking	Diagnostics	SW-Modules
...	...	...	...	...
	FlexRay		UDS	AUTOSAR/BSW
2005				
				Bootloader
2000	(TT-CAN) (TTP)	Most	Diagnostics on CAN (KWP2000)	KWP2000/ Transportlayer
1995		D2B	K-Line (KWP2000)	CAN-driver/ Network-Mgnt
1990	CAN		K-Line (ISO 9141-2)	

Systems

Available technologies for handling Safety-Critical Apps



Safety-critical Apps

Yes

All Safety-critical apps require high determinism

- FlexRay
- TTP/C
- TTCAN
- TTEthernet

Are required :

- Time-Triggered Access (TDMA)
- Formal Verification

No

- CAN
- RS-422/485
- Ethernet Std 802.3

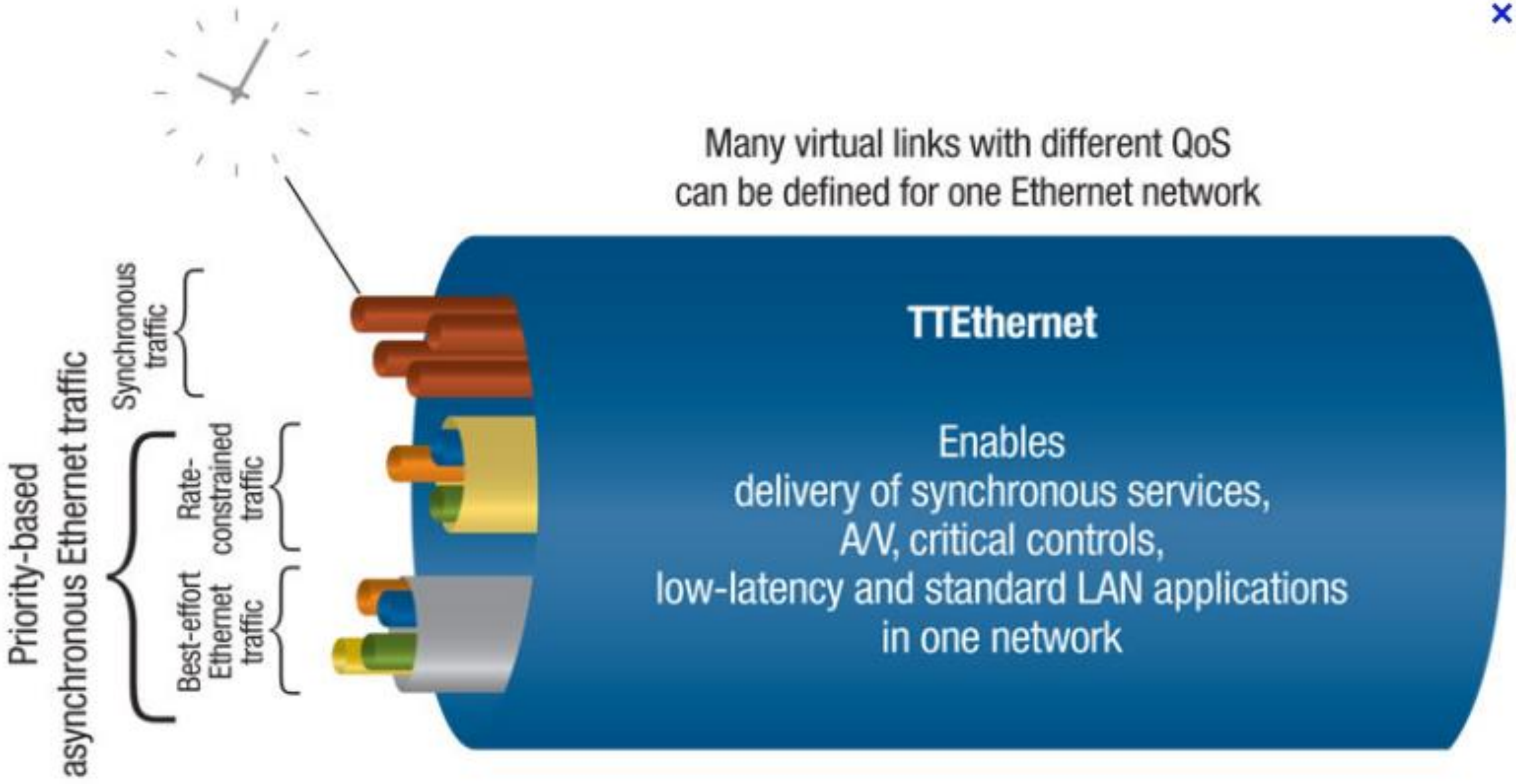
- MilCAN (1)
- « Industrial » Ethernet

Low/Medium

High

Determinism Level

Example of Industrial Ethernet : TTEthernet


Many virtual links with different QoS can be defined for one Ethernet network
TTEthernet
Enables delivery of synchronous services, A/V, critical controls, low-latency and standard LAN applications in one network
Synchronous traffic
Rate-constrained traffic
Best-effort Ethernet traffic
Priority-based asynchronous Ethernet traffic

- **Backbone technology Used within last generation airplanes (A380, B787…)**

Vetronics Backbone technology

- **Market acceptance of Flexray limited**
- **TTCAN limited Bandwidth**

Solutions

- **TTEthernet is fast but still expensive (Avionics) and only a few source**
- **Point 2 Point Usual Ethernet with switching technology**
- **2 // Technologies**
  - Ethernet
  - Flexray or TTCAN ?

Video Interface standards

Digital Video Compression standards

- IP H264 Compression standard
- MPEG 4 - H264 Hw encoder within 2nd gen Intel Core i3/i5/i7
- MPEG 5 – new w/ low latency
- JPEG2000 Video
- …. Latency shall be kept lower than 100 ms (you use the video to drive, fire…)

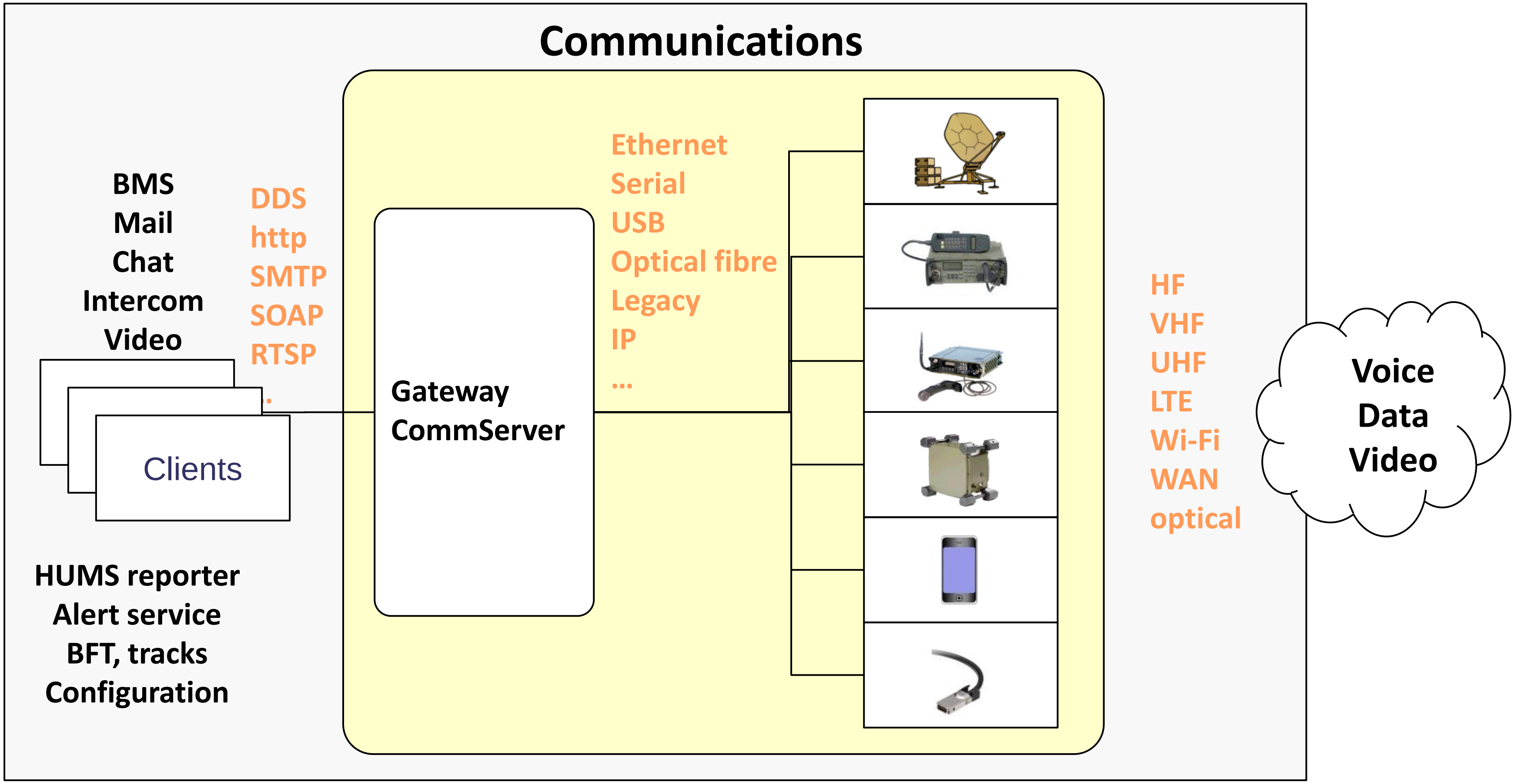
Digital Video Uncompressed interfaces

- HDMI (limited to about 10 meters
- DVI
- HD-SDI (Coaxial - up to 300m@270Mbps)
- Camera Link

Video Transmission Standards (over Ethernet)

- GigEVision
- Defstan 00-82 (VIVOE)
- STANAG 4678 (PLEVID)
- STANAG 4609 (Motion Imagery) – Meta Data STD

Gateway: interface to communication means



Communications

BMS
Mail
Chat
Intercom
Video

DDS
http
SMTP
SOAP
RTSP
..

Clients

HUMS reporter
Alert service
BFT, tracks
Configuration

Gateway
CommServer

Ethernet
Serial
USB
Optical fibre
Legacy
IP
…

HF
VHF
UHF
LTE
Wi-Fi
WAN
optical

Voice
Data
Video

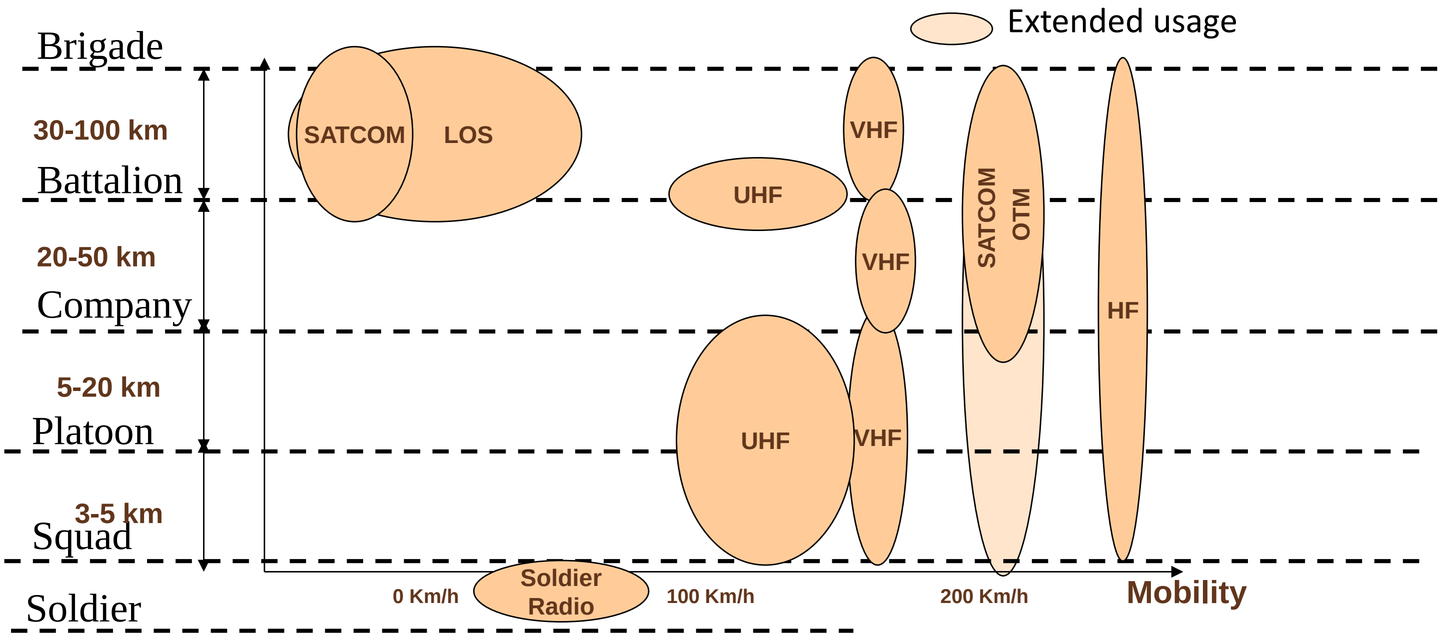
Gateway

- **Find the external routes**
- **Adapt VMS information and distribution to bearer services**

To transport information in an heterogeneous world !

Radio Technologies and what they are good for

Transmission	VHF	UHF	SATCOM OTM	HF	Soldier Radio
Jamming Support	High	Medium	High	High	Low
Useful Bandwidth	1-20 kb/s	256 kb/s - 1 Mb/s	20-100 kb/s	3 kb/s	100 kb/s - 1 Mb/s
Radio Range	20-30 km	4-8 km.	> 100 km	> 100 km	< 1 km
Propagation	NLOS	NLOS	LOS	BLOS	NLOS
Channel Access Time	~1-5s	~0.1-0.5s	~0.5s	> 5-10s	< 10 ms
Packet Loss Ratio	<< 1%	1-5%	<< 1%	<< 1%	1-5%
Mobility	< 300 km/h	< 200 km/h	< 500 km/h	300 km/h	



Radio Communications challenges

….. Video on VHF

Broad CNR: 90 kbps

Target: 115 kbps

Canalization: 75 kHz

Safety Standards : Overview

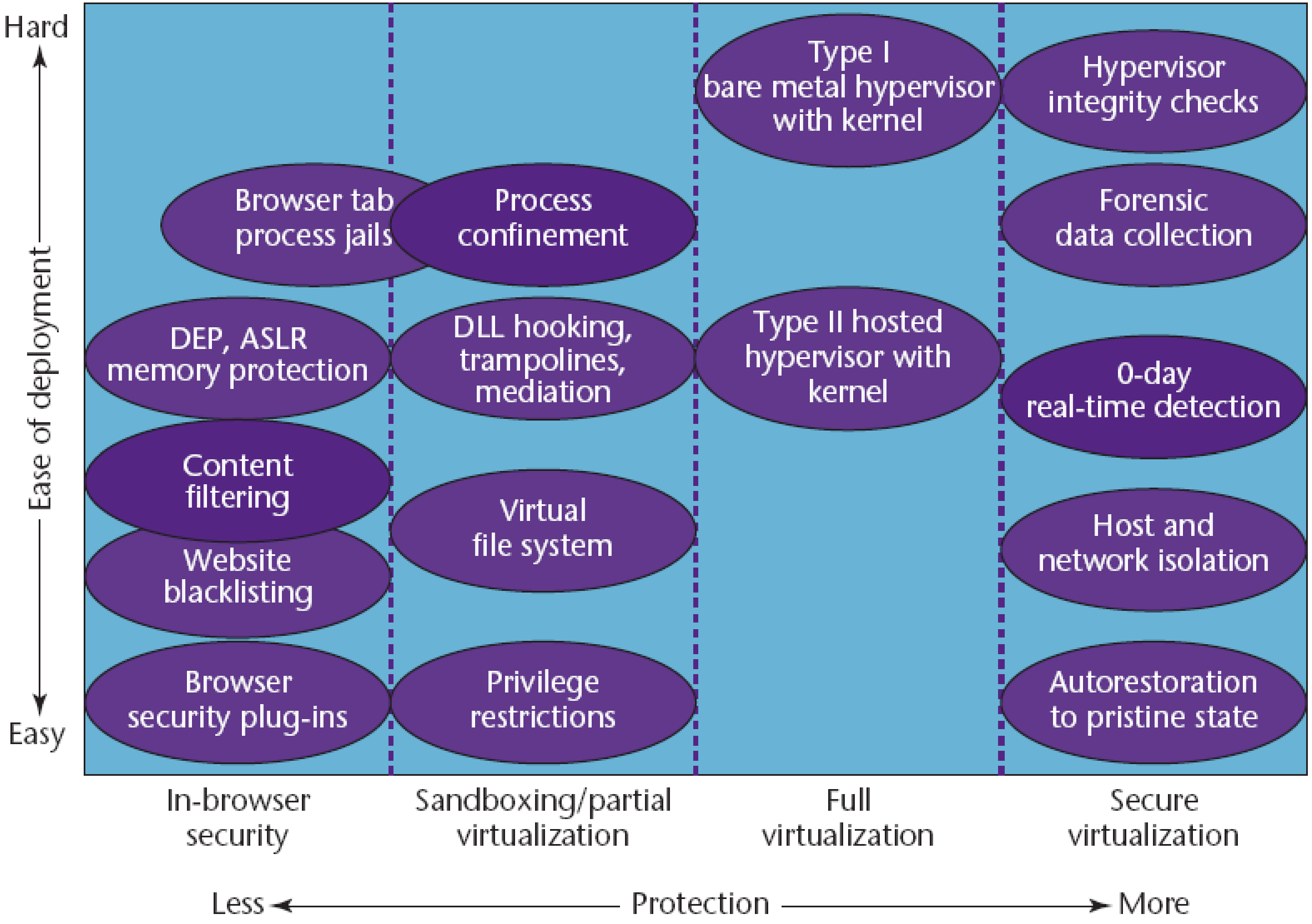
IEC 61508 : Functional safety standard applicable to all kinds of industry

- **ISO 26262 : Road Vehicle – Functional Security**
  - ASIL A-D grades (Automotive Safety Integrity Levels)
  - Certification required typicaly for : Steering, Braking and Chassis Control, Transmission,Powertrain,HEV/EV Battery Management,Advanced Driver Assistance Systems (ADAS),Body
- **IEC 62279 : Rail software**
- **IEC 61511 : Process industries (chemical…)**
- **IEC61513 : Nuclear power plants**
- **IEC 62061 : Machinery**

MIL-STD-882 C – System safety program requirements ...

DO-178B - Safety of software used in airborne systems

Technology Theme : Security technologies


Hard
Easy
Ease of deployment
Type I bare metal hypervisor with kernel
Hypervisor integrity checks
Browser tab process jails
Process confinement
Forensic data collection
DEP, ASLR memory protection
DLL hooking, trampolines, mediation
Type II hosted hypervisor with kernel
0-day real-time detection
Content filtering
Website blacklisting
Virtual file system
Host and network isolation
Browser security plug-ins
Privilege restrictions
Autorestoration to pristine state
In-browser security
Sandboxing/partial virtualization
Full virtualization
Secure virtualization
Less
Protection
More

Source : "Sandboxing and Virtualization Modern Tools for Combating Malware"

Technology Theme : Security Aspects

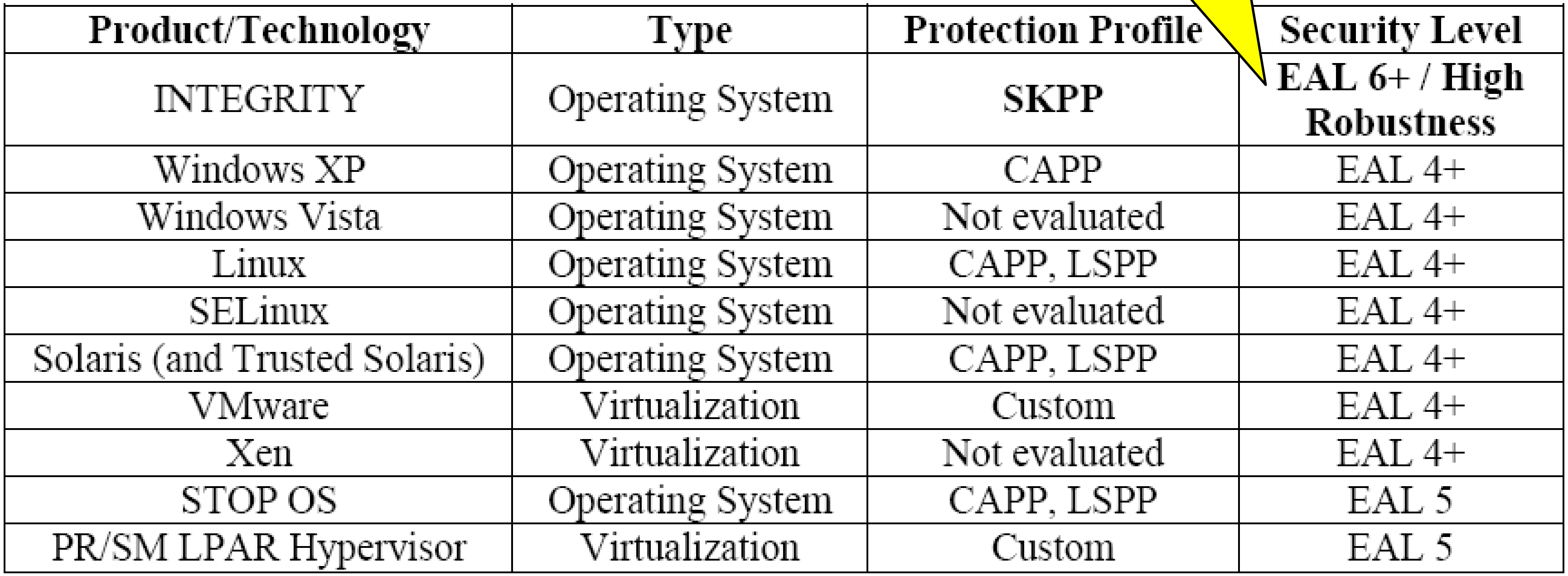
Technology	+	-	Comments
ISO 15408 (CC v2.3)			Standard Protection Profiles
FIPS-140			Cryptography
SDIP 27 (TEMPEST)			
SDIP 29			Sensible equipment design
AC/322-D/0047-REV1			Requested Failure resistance
AC/322(SC/4-AHWG/14)WP(2004)0004-REV4			

Technology Theme : Security equipments

- **IP Encryptors**
  - Enables to « tunnel » sensible information in lower level Networks
  - But cryptographic « Wall » can not be crossed
- **IP Data Diode**
  - Enable information to go from Low level Restricted to Classified
  - Garanty that no Data will flow out
  - Drawback : Once in… Information can not go Out
- **Gateways**
  - Will enable information to go out to lower security level under very controlled conditions
  - For dedicated applications (Mail, …).
- **MultiLevel Data Terminal**
  - New Class of Equipement that will enable to manipulate data of Different levels on the same terminal
- **KVM**
  - Brings Secure Switching of Video/keyboard.Mouse

Technology Theme : Security technologies for OS

+LynxSecure + PikeOS



Product/Technology	Type	Protection Profile	Security Level
INTEGRITY	Operating System	**SKPP**	**EAL 6+ / High Robustness**
Windows XP	Operating System	CAPP	EAL 4+
Windows Vista	Operating System	Not evaluated	EAL 4+
Linux	Operating System	CAPP, LSPP	EAL 4+
SELinux	Operating System	Not evaluated	EAL 4+
Solaris (and Trusted Solaris)	Operating System	CAPP, LSPP	EAL 4+
VMware	Virtualization	Custom	EAL 4+
Xen	Virtualization	Not evaluated	EAL 4+
STOP OS	Operating System	CAPP, LSPP	EAL 5
PR/SM LPAR Hypervisor	Virtualization	Custom	EAL 5

Table 2 – Operating System Products and their Security Levels

Questions ?