航空工业西安航空计算技术研究所
AVIC XI'AN AERONAUTICS COMPUTING TECHNIQUE RESEARCH INSTITUTE

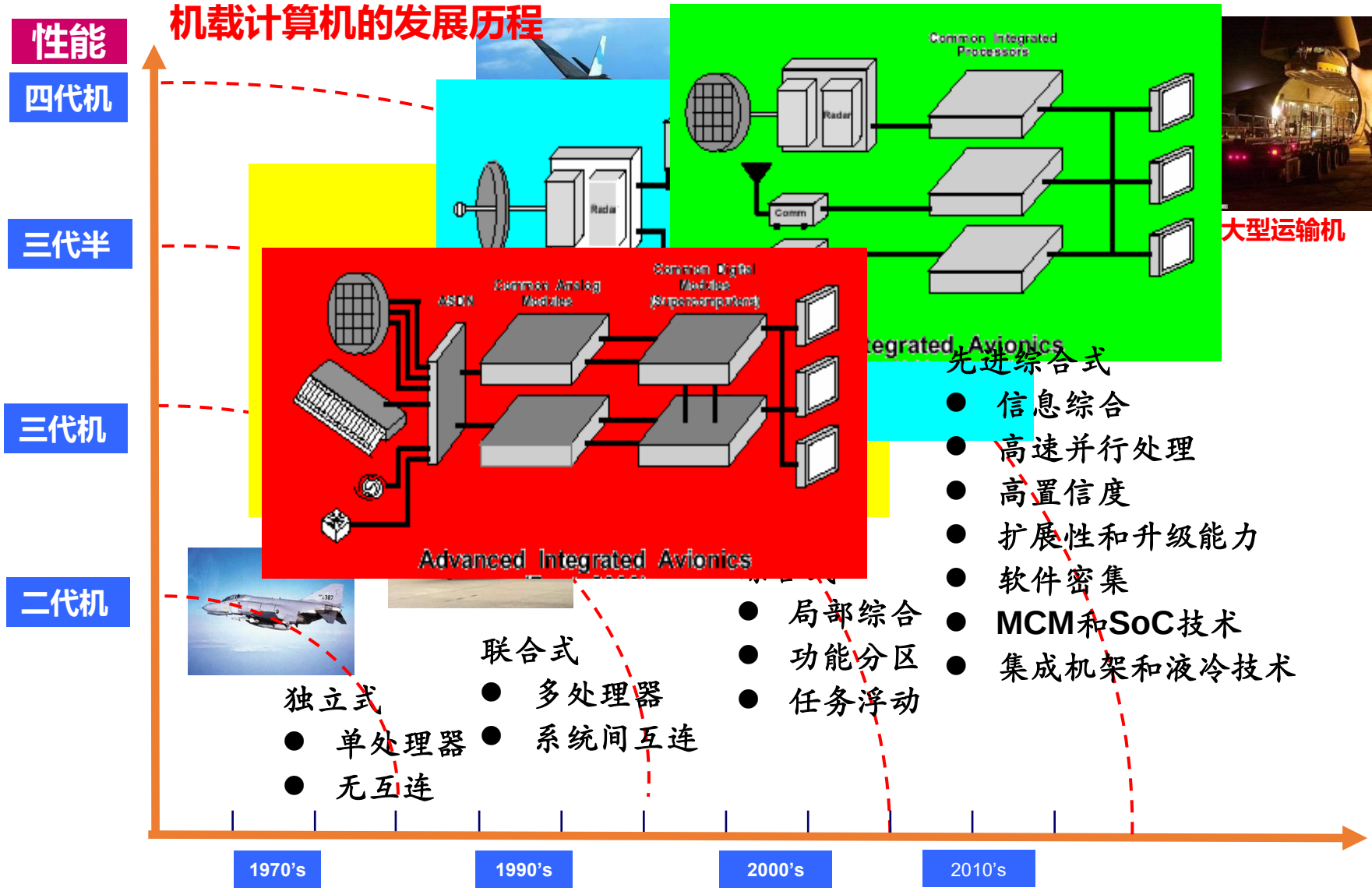
面向航空电子系统的嵌入式操作系统

崔西宁

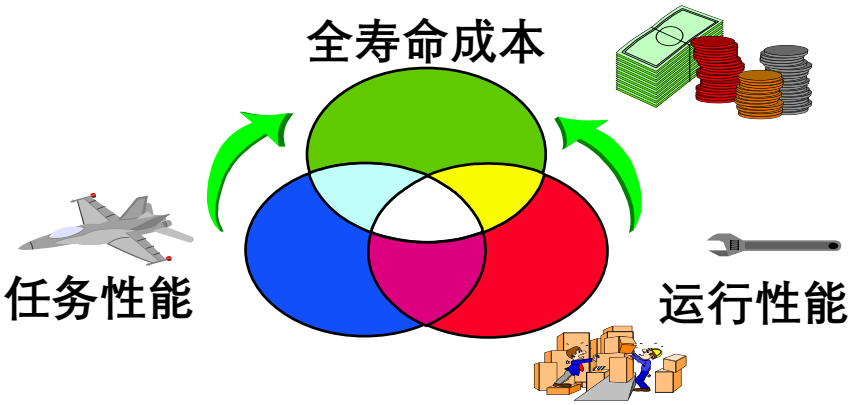
航空工业计算所

目录

航空电子系统发展历程


机载计算机的发展历程
性能
四代机
三代半
三代机
二代机
Common Integrated Processors
Radar
Comm
Integrated Avionics
Common Analog Modules
Common Digital Modules (Supercomputing)
ASDN
Advanced Integrated Avionics
大型运输机
先进综合式
信息综合
高速并行处理
高置信度
扩展性和升级能力
软件密集
MCM和SoC技术
集成机架和液冷技术
局部综合
功能分区
任务浮动
联合式
多处理器
系统间互连
独立式
单处理器
无互连
1970's
1990's
2000's
2010's

综合化是新一代飞机航电系统的趋势



任务性能

- 分布并行
- 重构能力
- 容错管理
- 故障管理
- 资源共享
- 系统综合

运行性能

- 可用性
- 可伸缩性
- 可测试性
- 可维护性
- 进程隔离性
- 安全性
- 可移植性

全寿命成本

- 开放式结构
- 系统层次结构
- 模块化结构
- 高速互联结构
- 标准信息结构
- 标准通信协议
- 标准构件

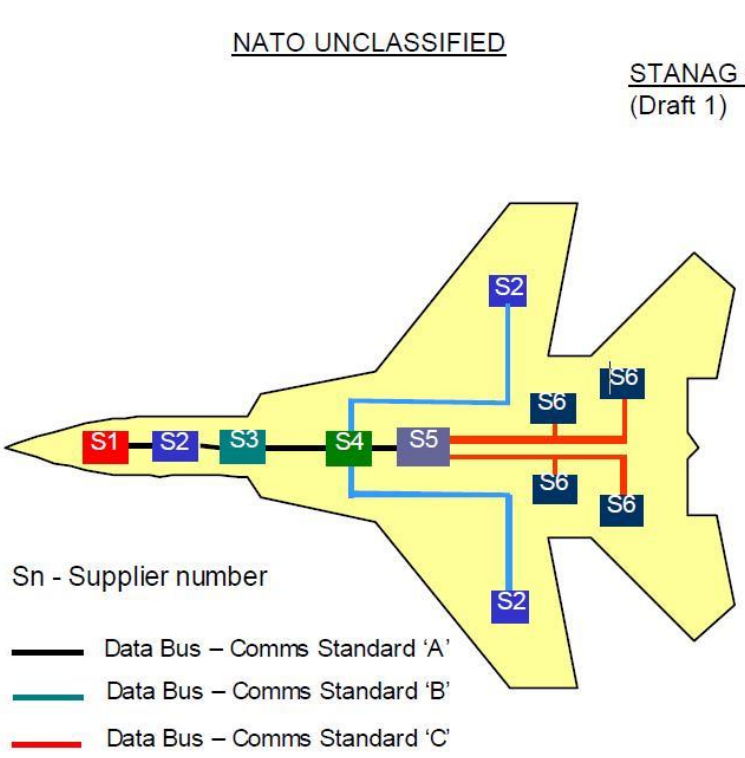
综合化是新一代飞机航电系统的趋势

- IMA的概念应用越来越广泛
  - 从军用飞机发展到民用飞机
    - F-22、F-35、歐洲战斗机—A380、B787
  - 从美国飞机发展到其它国家
    - 美国—法德英、瑞典（SAAB的DIMA）
  - 从局部综合发展到全局综合
    - ICNIS、IEWS、IVMS—全机综合
  - 从新飞机综合到老飞机的更新
    - F-16 E/F Block60 AMC

综合化是新一代飞机航电系统的趋势

✈ 综合模块化航空电子（IMA）

IMA是一组可共享、灵活、可重用、可以互操作的硬件和软件资源，当将它们集成起来时可以形成一个平台，向驻留在其上的执行飞机功能的应用提供经过设计和验证、具备预订安全型级别、满足应用性能需求的服务。



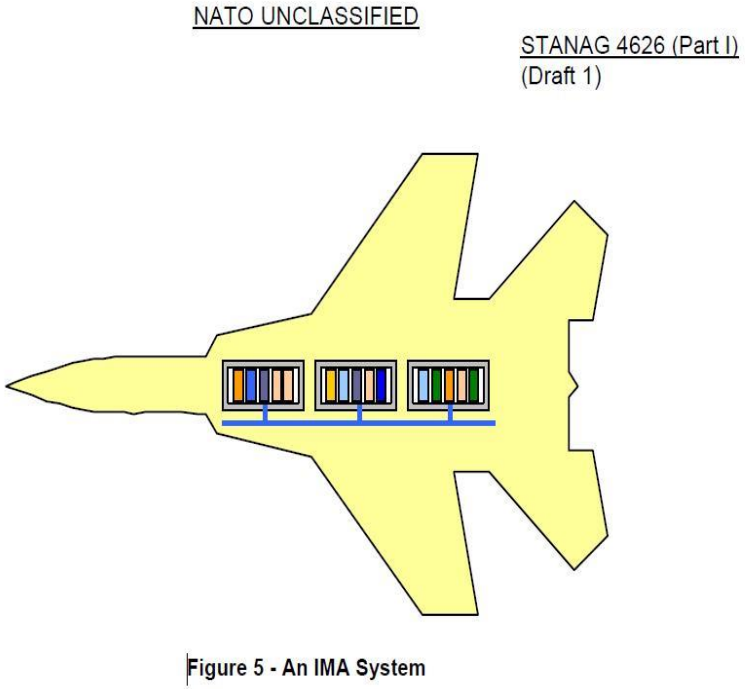


Figure 5 - An IMA System

The essence of IMA is to use a minimum set of common parts: Common Functional Modules, software and interfaces.

综合化带来的好处

- 综合化的好处来自功能综合与物理综合:
  - 功能综合提高应用的运行性能
  - 物理综合降低开发和 重复成本
    - 降低单个通用系统的设计成本
    - 降低扩充与维护的重复成本
    - 降低修复成本与高起飞率
    - 降低备份成本
    - 降低采购价格（通用部件的多厂家和高数量）

综合化对机载计算机提出的严峻挑战

- 成本大大减少：设计、采购、运行、更新
  - 可重用硬软件构件
  - 体积、重量、功耗等减少
    - 体积减少50%
    - 重量减少到接近30%
    - 电源功耗减到大约16%
    - 可靠性改进20多倍。

综合化对机载计算机提出的严峻挑战

- 一般的困难：
  - 综合系统设计复杂性增加。
  - 综合系统制造与测试更困难。
  - 综合系统更难认证。
  - 要求实时操作系统，并具有隔离保护能力。
  - 重构要求有高得多要求的检错定位能力。

综合化对机载计算机提出的严峻挑战

综合化主要特点

- 资源共享（Resource Sharing）。
  - 要求共享的资源要有高得多的处理信息的能力。
  - 要求共享资源之间要有高得多的通信能力。满足高耦合程度的要求。
  - 要求软件结构能解决规模扩大、复杂性增强（实时性、可靠性和安全性）问题。

综合化对机载计算机提出的严峻挑战

主要挑战（1）：高性能的处理单元

- 处理器能力：
  - F-22　　CIP　　400Mips
  - F-35　　ICP　　40.8Gips (提高100倍)

    每一个数据处理LRM达到百亿次运算能。支持二级维护

- 新一代：**多核多处理，LRM模块上采用多个处理器，每个处理器为多核如16核，处理能力显著提高。**
- 智能化：**智能处理，采用智能处理器实现智能处理、智能计算等**

综合化对机载计算机提出的严峻挑战

主要挑战（2）： 高性能的网络

- F-35 1-2Gb/s FC网络
- FC-AE 军机以 4Gb/s FC网络为基础
- AFDX 民机以 100Mb/s 的ARINC664 P7以太网络为基础—航电全双工交换式以太网，提高可靠性和确定性
- TTE网络，事件触发以太网，1Gb/s的同步以太网，达到高确定性
- TSN网络，时间敏感网络，1Gb/s、10Gb/s的同步以太网，适合多种业务传输的网络。

综合化对机载计算机提出的严峻挑战

主要挑战（3）：　高性能的软件

- 软件规模越来越大
- 软件设计越来越复杂

综合化对机载计算机提出的严峻挑战

F-22的软件配置

全飞机	各系统	子系统
总数 1.7MSLOC （百万源代码行）	航空电子 87% (1.5MSLOC)	RADAR 11.5%
		CNI 28.6%
		EW 14.9%
		IRS 16.0%
		MISSION 13.4%
		C&D 8.8%
		SMS 2.0%
		核心处理 6.3%
	VMS 5.3%	
	U&S 7.7%	

综合化对机载计算机提出的严峻挑战

F-35的软件配置

- 全F-35软件有15MSLOC：
  - 机载有 6 MSLOC
    - 任务系统 4.5 MSLOC
    - 飞行器管理 1.5 MSLOC
  - 地面开发(模拟器)有 6 MSLOC
  - 辅助性的有 3 MSLOC

综合化对机载计算机提出的严峻挑战

软件复杂性增强

- 实时性：确保满足多个周期任务、非周期任务和零散任务的实时要求
- 可靠性：故障对多种应用的影响扩大、模式更为复杂。采用分布式容错方法检测、滤波、诊断、屏蔽、降级、重构、恢复、预测的工作。
- 安全性：多个独立的关键性和安全级别不同的应用任务共享同一计算资源。确保故障不能蔓延.

综合化对机载计算机提出的严峻挑战

综合化对系统结构的挑战

- 综合式（局部综合）系统 ：

  综合使用资源，大大节省成本，提高资源的利用率，但是相对而言应用之间交往过多，很难防止故障传播、抵御信息攻击。

- IMA结构目标是实时可靠安全地资源共享

  共享即资源在应用之间分配，处理器、存储器、通道及设备等可以持久分享或分时占用

目录

ARINC653简介

ARINC653规范

ARINC653规范--“avionics application software standard interface”。

最早于1997年提出，目前已发展到ARINC653多个版本。

ARINC653规范已形成国军标：GJB5357-2005。

ARINC653简介

□计算机技术的飞速发展是ARINC653的技术推动

- 由于计算机技术和微电子技术的进步，到90年代末期CPU芯片的速度较之80年代有了几个数量级的增加，相应存储器的速度也有了大幅度的提高。一个小小的CPU已经可以承担原先大型机才能完成的任务。

□综合化航空电子系统的发展是ARINC653的需求牵引

- 为了降低航空电子系统的成本，以及重量、体积、功耗和提高可靠性，要求实现计算资源的高度共享。高度共享最基本的要求是在一个CPU上运行多个任务。

ARINC653简介

需求牵引和技术推动相结合之后出现的新问题

- 共享资源的任务间不能互相影响
- 在三代“联合式”航空电子系统中，各任务占有自己独立的计算资源，相互之间采用物理隔离防止了相互之间的影响。
- 在第四代“综合化”航空电子系统中，计算资源高度共享，如何消除共享计算资源的各任务之间的不利影响，即一个任务的错误不能影响其它正常任务的运行。

ARINC653简介

□问题的解决方法－ARINC653分区概念的提出

- 在ARINC653中提出的“分区”概念，是解决共享计算资源的各任务之间的相互影响的有效方法，也是ARINC653提出的初衷。

□ARINC653带来的好处－降低了不同重要性级别软件的测试和验证代价

- 如果没有分区的概念，共享计算资源的任务，必须按所有任务中最高的重要性级别进行测试和验证；
- 采用了分区概念后，各任务相互之间是“隔离”的，因此可依据各分区中任务的不同重要性级别进行相应的测试验证。

ARINC653的主要特征

- 为解决实时系统共享计算资源各任务之间的保护问题，引进了分区的概念：时间分区、空间分区。
- 利用CPU状态解决实时系统共享计算资源的各任务对操作系统的保护。

ARINC653规范的主要特征

- 保证实时系统的确定性
  - 实时系统区别于其它系统的特点之一是实时系统不仅要求计算结果的正确性，而且要求正确结果产生时间的精确性。这就是实时系统的时间确定性。
  - 在ARINC653规范中，操作系统的任务调度分为两级，即分区调度和进程调度。

ARINC653规范的主要特征

□故障处理机制－健康监控

- 为了提高系统的可靠性和维护性，实现故障后系统仍然能够正常工作和推迟维护（deferred maintenance）的目标,容错技术将在航空电子系统中广泛应用，成为系统必不可少的一部分。为此，在ARINC653规范中引进了故障处理机制－健康监控（health monitoring）服务机制。
- 健康监控是操作系统的一项功能，它负责监控和报告应用软件、操作系统软件和硬件的故障，帮助故障的隔离和防止故障的传播。

ARINC653简介

□ ARINC653标准

- 分区管理（Partition Management）
- 进程管理（Process Management）
- 时间管理（Time Management）
- 存储器管理（Memory Management）
- 通讯（Communications）
  - 分区内通讯
  - 分区外通讯
- 健康监控（Health Monitoring）

目录

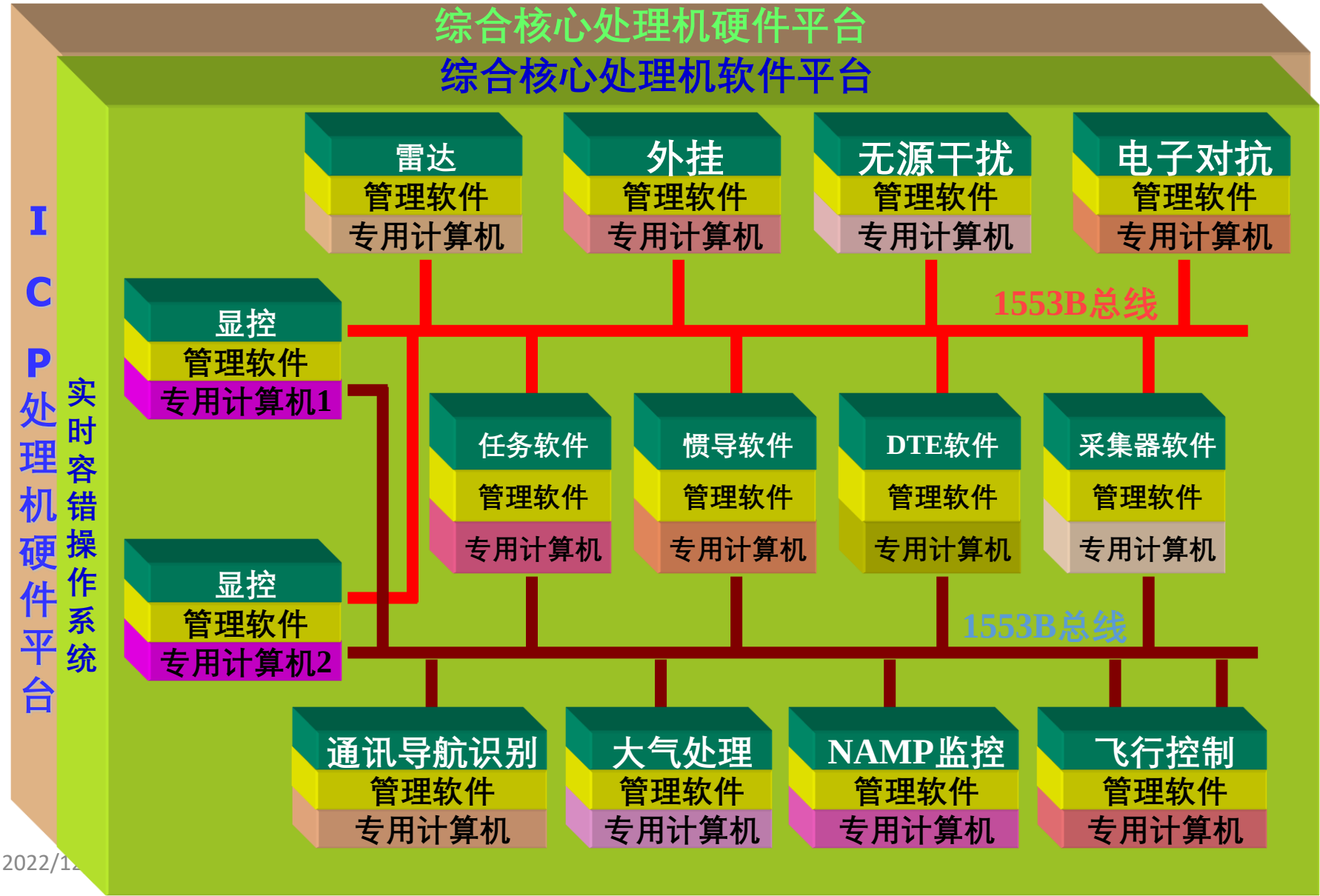
综合化对机载操作系统的需求

- 满足ARINC653接口标准的高安全实时操作系统成为综合化航电系统的必然需求。

- 也是综合化航电任务抽象管理的基本支持

综合化对机载操作系统的需求

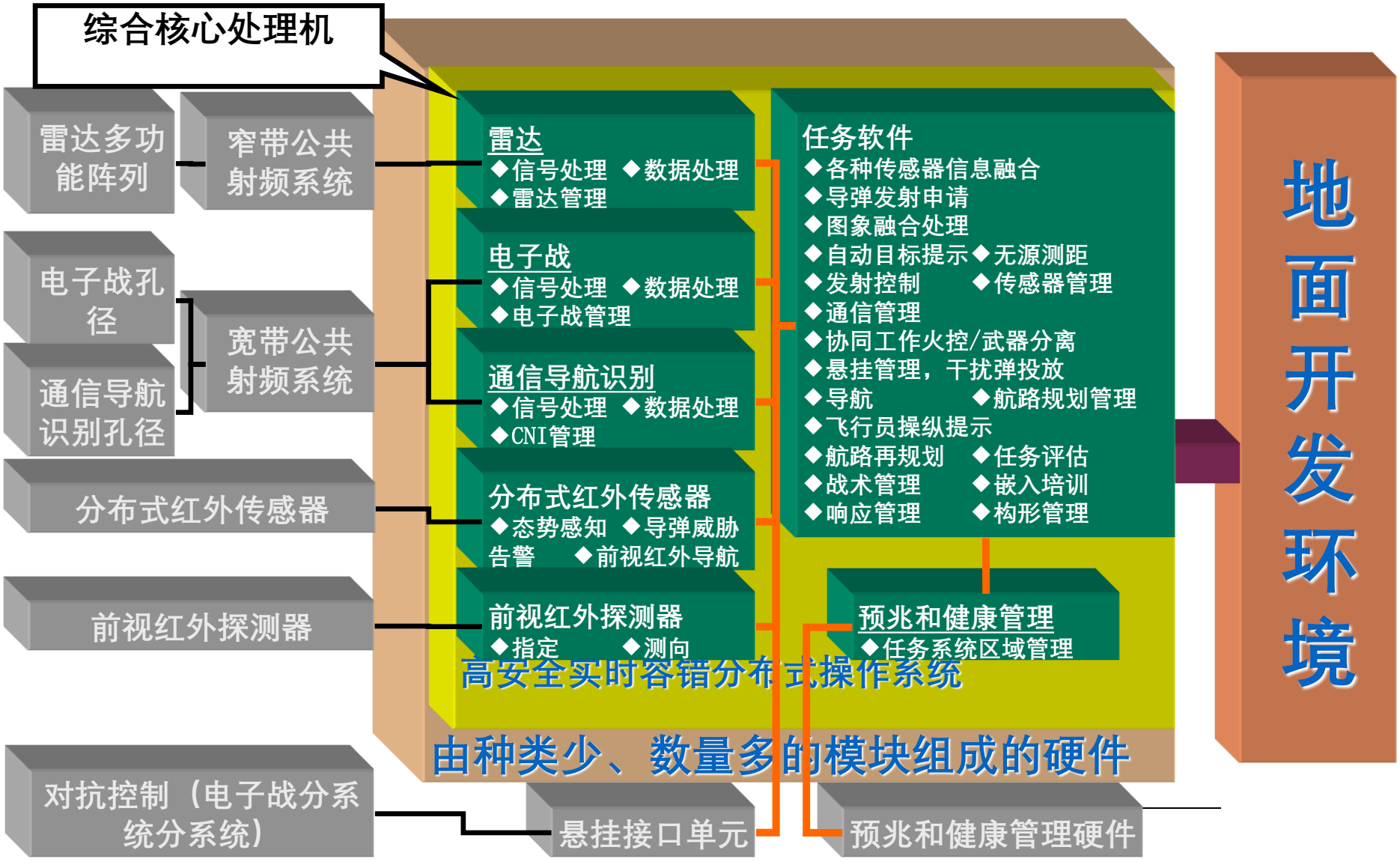
- 独立的子系统
- 独立的计算机
- 独立的控制和显示



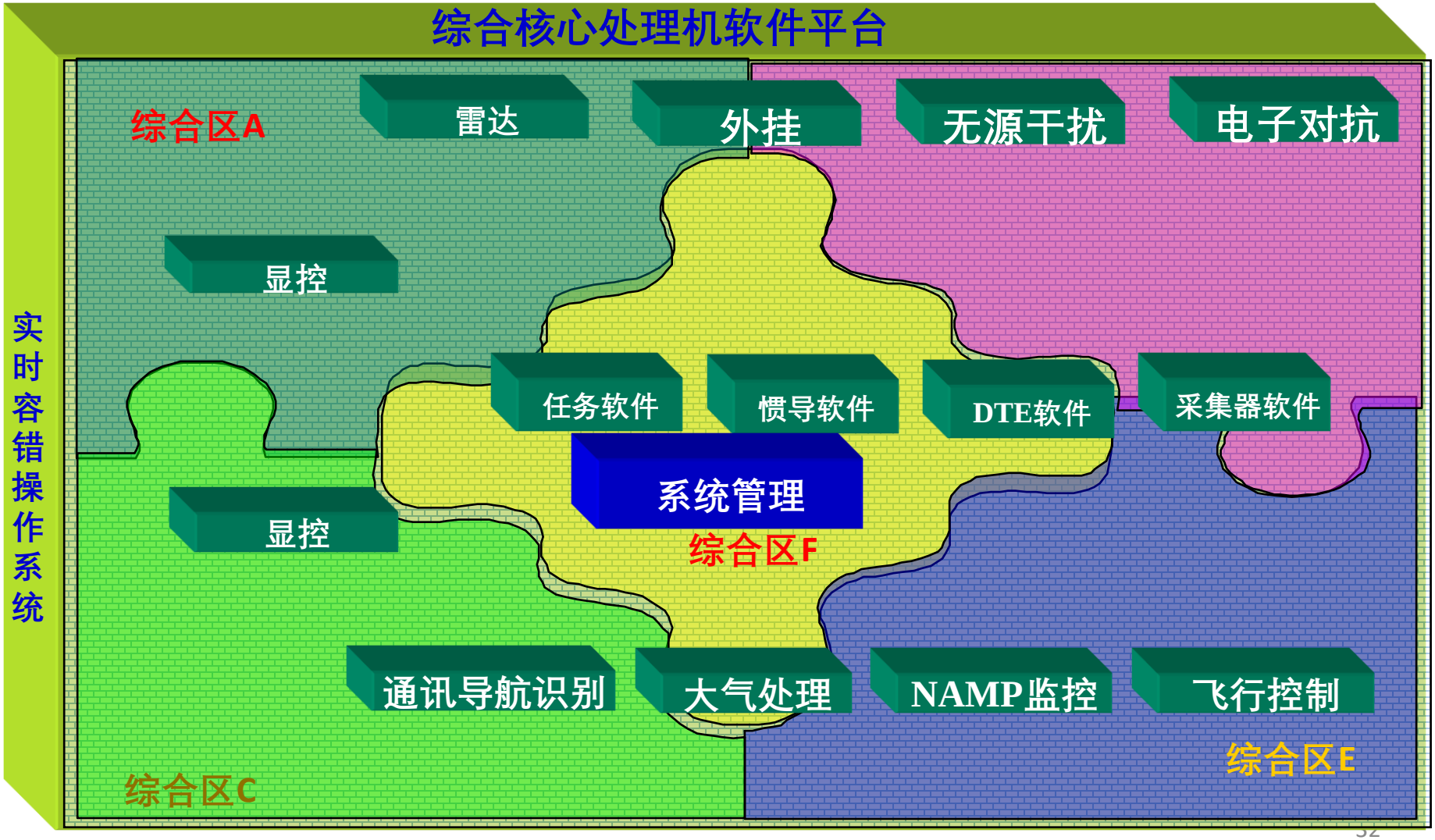
综合化对机载操作系统的需求

综合化概念----计算机应用软件综合

综合化对机载操作系统的需求



综合化对机载操作系统的需求



目录

天脉嵌入式实时操作系统

天——天空，驰骋疆场

脉——脉络，机体运行的通道

- 核心基础软件自主保障
- 完全自主知识产权
- 高安全/高可靠/强实时
- 机载“Windows”

满足装备需求的操作系统产品

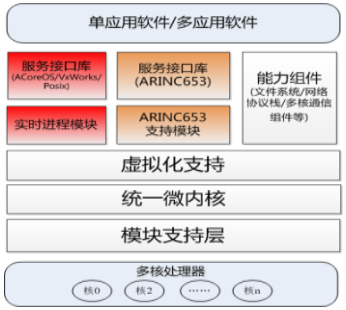
天脉1

●**场景**：通用机载电子设备对实时任务需求
●**特征**：多任务调度、中断/异常机制、支持单核。
●**状态**：已定型

天脉2

●**场景**：综合化航空电子对于多应用间安全隔离需求
●**特征**：时/空隔离、多级故障管理、支持单核。
●**状态**：已定型

天脉3



●**场景**：航空装备对高性能多核信息处理平台的需求
●**特征**：多核支持、安全加强、64位设计。
●**状态**：已技术验证与选用

天脉系列产品构成

桌面开发工具

机载工具套件
- 批量部署
- 监视&分析
- 外场维护
- ...

集成开发环境
- 编译工具链
- 调试工具链
- 虚拟仿真平台
- 目标机管理
- IMA综合工具

嵌入式系统

能力扩展组件

文件系统	网络协议栈	向量运算	OpenGL图形库	嵌入式数据库
Vx兼容接口库	POSIX接口库	系统管理	IO服务组件	通信中间件

操作系统

天脉1操作系统 (实时多任务)

天脉2操作系统 (安全分区)

天脉3操作系统 (多核处理)

Windows

麒麟 (Linux)

PowerPC (国微) (58所)

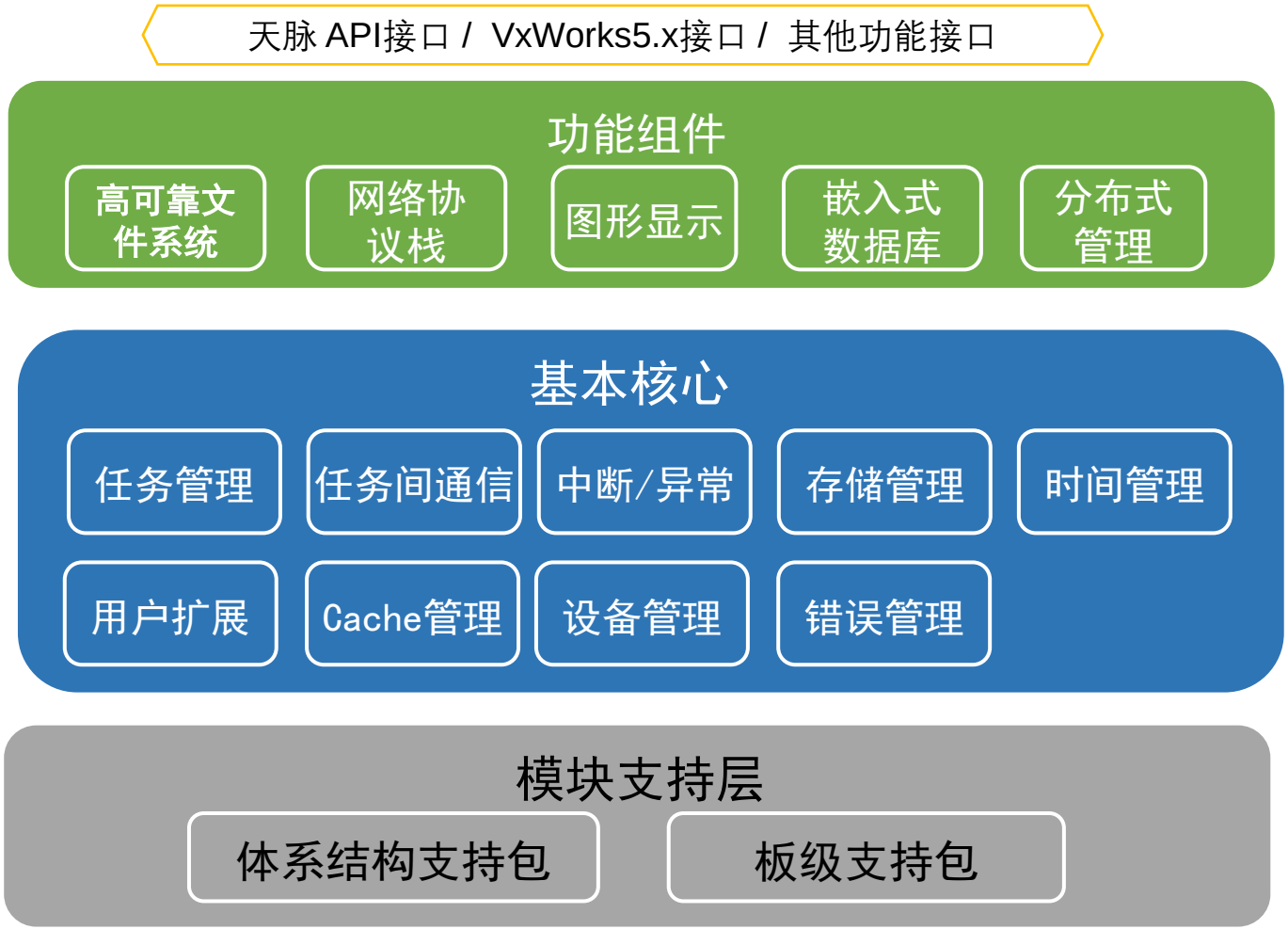
ARM (飞腾) (复旦微) (海思)

intel inside (国微)

MIPS (龙芯) (华睿)

天脉1操作系统—实时多任务

分层架构：提高重用性、可移植性



- **支持机载常用组件**
  - TCP/IP
  - 数据库
  - 高可靠文件系统
  - OpenGL
- **支持处理器系列**
  - PowerPC全系
  - X86
  - ARM（飞腾）
  - MIPS（龙芯）

天脉1能力与VxWorks5.x相当，接口兼容

天脉1—机载特性设计

实时性确定性
- 时间粒度可配，默认1ms
- 周期任务支持
- 中断嵌套支持

可靠安全
- 存储空间保护
- 只读数据保护
- 函数接口调用限制

多组件集成
- 高可靠文件系统
- 图形支持：OpenGL、QT
- 嵌入式数据库

平台适应性
- 多系列处理器平台
- 支持多种国产处理器
- 参数可配置，组件可剪裁

周期任务接口：无需应用设计周期机制，简单方便

空间保护：空指针检测、地址越界检测

安全信号量：防止任务优先级翻转，提高系统安全

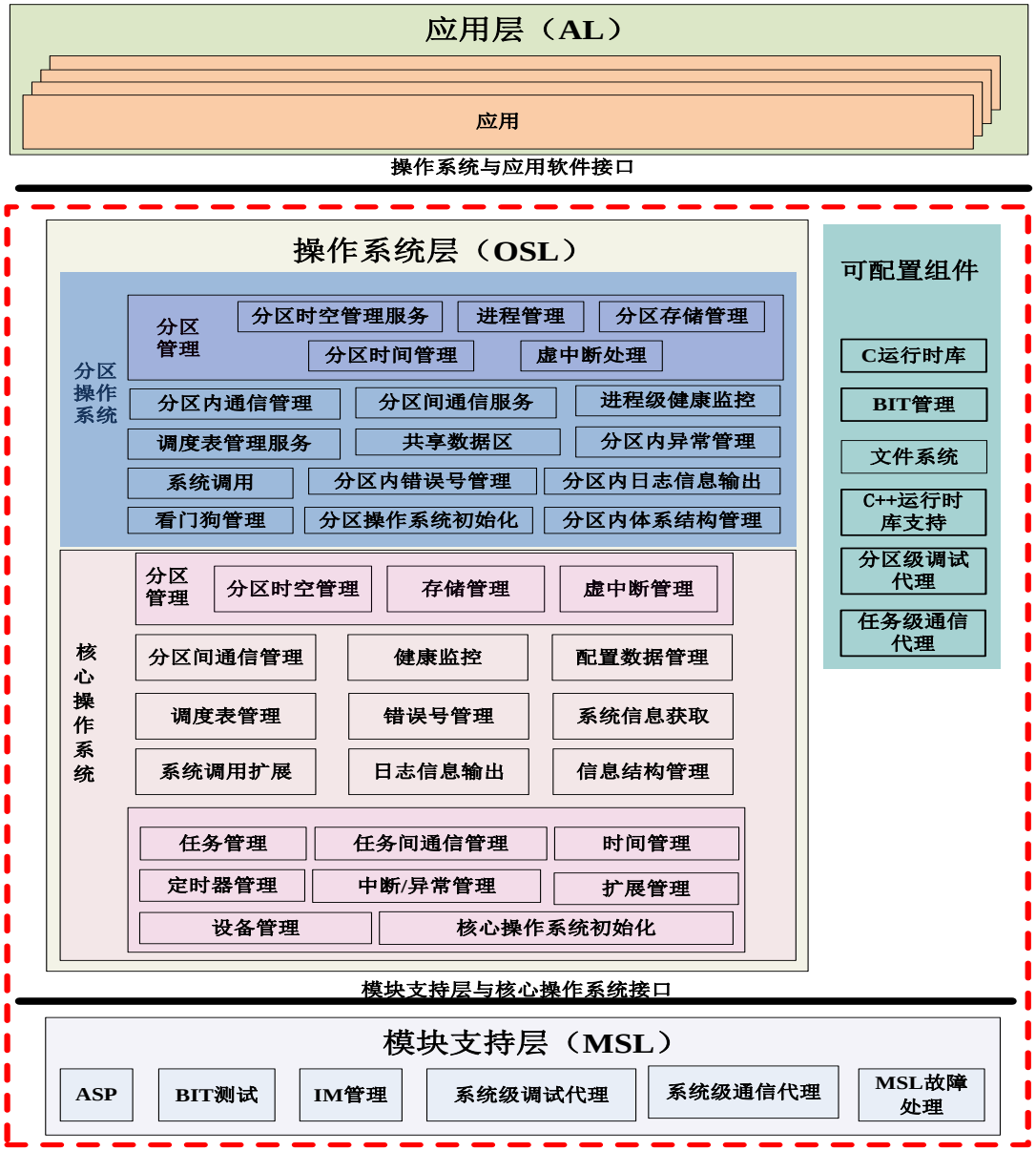
VxWorks兼容包：提高移植效率

可剪裁配置：各类组件可选配置，代码规模小

处理器支持：支持PPC、ARM、MIPS、X86四系列数十种处理器；

国产硬件：飞腾、龙芯、锐华、国微等国产处理器支持

天脉2—安全分区



◆时间/空间隔离技术：解决多应用共享资源带来的冲突；

◆健康监控机制：解决大规模复杂软件故障处理问题

◆标准APEX服务：实现应用分区的平台无关，快速迁移和验证

◆确定性配置：提高机载应用的安全性、可靠性

天脉2—机载特性设计

综合化
- 符合ARINC653规范
- 采用XML静态配置资源
- 分区模块化，独立开发/升级

安全性
- 分区技术，防止故障故障
- 时空分区，资源隔离
- 静态配置的健康监控

确定性
- 空间、时间静态配置
- 通信通道、频率静态配置
- 运行模式禁止资源分配

平台适应性
- 多系列处理平台
- 多种国产处理器
- 参数可配置，组件可剪裁

ARINC653：符合国际标准，可与国外OS相互移植

时间分区：时间片与优先级两级调度，保证时间安全

空间分区：空间静态配置，存储保护保证空间安全

健康监控：故障模式、动作、策略静态确定，更安全可靠

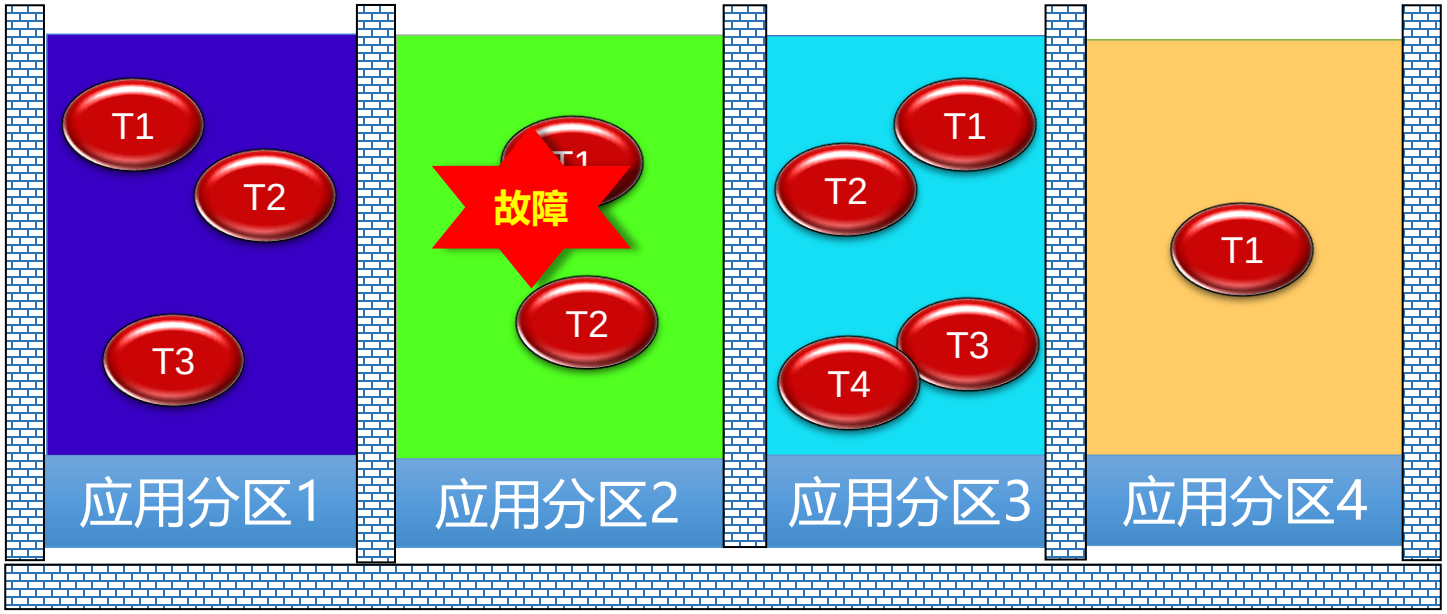
分区间通信：标准通信机制，提高确定性、可移植性

XML规则文件：静态资源配置、合理性编译前检查

硬件平台：支持PPC、ARM、X86数十种处理器，以及多种国产处理器

天脉2—时空隔离

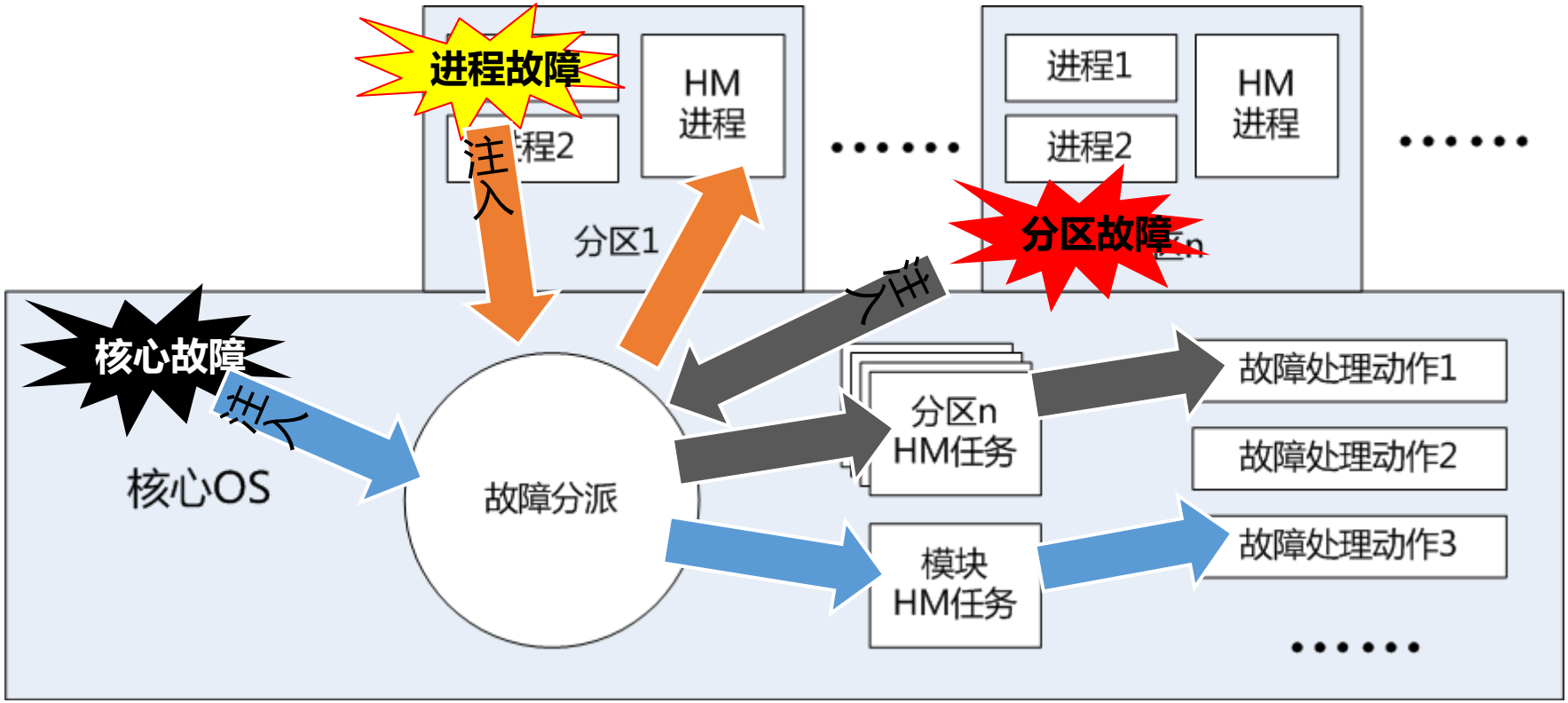
高效的安全隔离能力：应用运行时间进行确定性配置，实现CPU资源的划分与共享；借助硬件存储管理功能，实现空间资源的划分与保护，有效解决多系统对共享资源的分配与利用。



分区	P1	P4	P2	P3	P4	P1	P4	P2	P3	P4	P1
时间窗口偏移	0.000	0.020	0.030	0.040	0.070	0.100	0.120	0.130	0.140	0.170	0.180
时间窗口	0.020	0.010	0.010	0.030	0.010	0.020	0.010	0.010	0.030	0.010	0.020

天脉2—健康监控

完备的故障处理能力：定义三级故障模式，实现了各级故障的诊断、上报、派发、处理的流程，处理动作可以进行预先配置，有效解决多系统并存情况下、大规模复杂软件故障难于处理的问题。



天脉3操作系统—多核处理

What's a multicore processor?

- Multicore processor is characterized by N (N ≥ 2) processing cores + a set of shared resources (Memories, PCIe, Ethernet, Cache, Registers, etc.)

■ 飞机能力提升->机载信息处理平台具备更高处理效能；

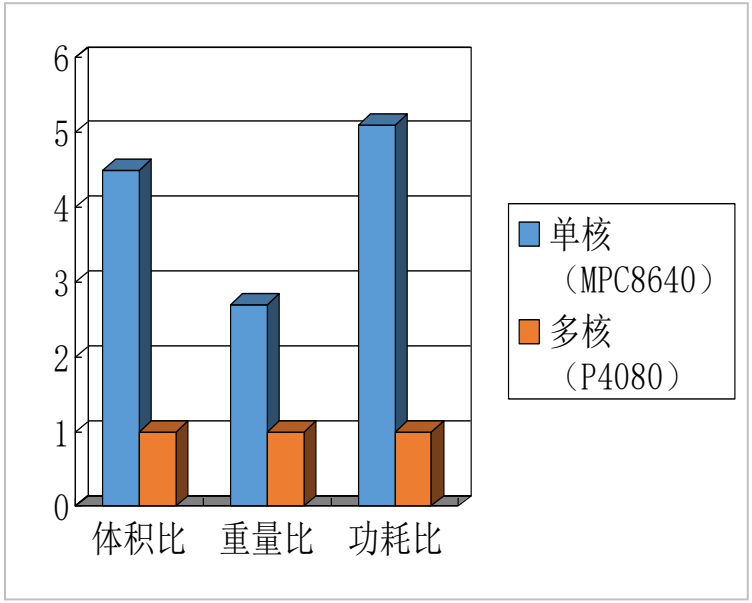
- **综合范围扩大；**
- **SWaP不断追求**

■ 有效途径：多核处理器+多核操作系统，操作系统是关键。

■ 采用多核典型机载计算机

- **综合核心处理计算机（如：ICP）**
- **雷达、电子战、光电等计算机**

（如：高并发、多流水的算法）。



相同性能下SWaP的比较

天脉3—产品能力

天脉3

◆**非分区模式**

◆支持任务调度、任务间通信、中断/异常、时钟/定时器等

◆支持实时进程（RTP），具备任务间隔离，以及时间表调度能力；

◆支持POSIX接口、国外OS兼容接口。

◆支持SMP调度以及任务绑定核；

◆支持PowerPC、ARM、MIPS架构，以及DSP；

◆**与VxWorks7.0相当。**

◆**分区模式**

◆支持分区管理、健康监控、分区间通信、分区进程管理、进程同步/通信；

◆支持分区绑定处理核调度（BMP），符合ARINC653 P1-3、P2-1；

◆支持分区内进程SMP调度，符合ARINC653 P1-4、P2-3；

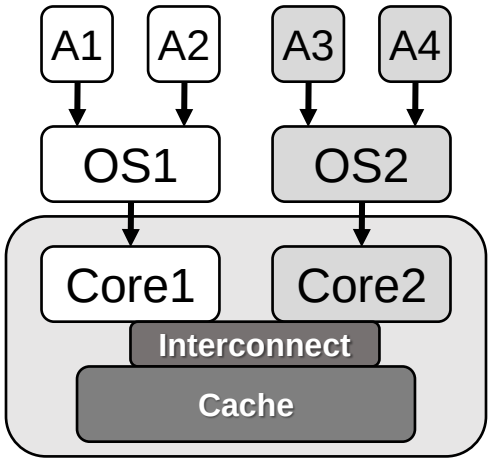
◆支持PowePC、ARM、MIPS架构；

◆**与VxWorks 653 3.x相当。**

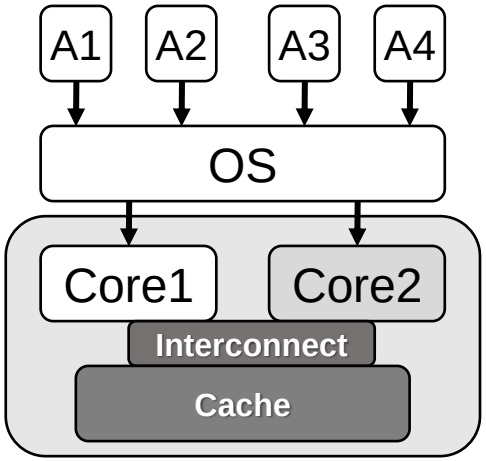
天脉3—多核运行模式

■ 主流的多核模式与架构 （AMP/SMP/BMP）

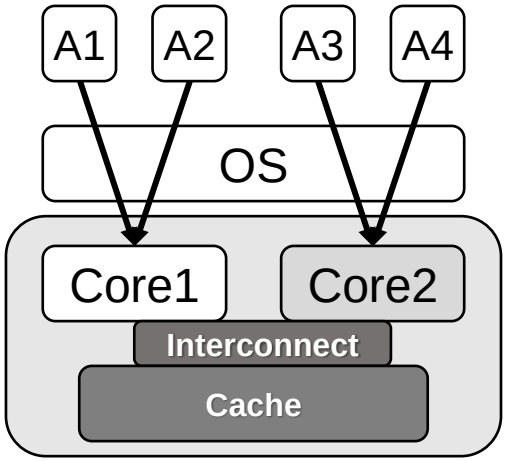
多核系统模式	说明
非对称多处理 AMP（Asmmectric Multiprocessing）	每个CPU内核运行一个独立的OS实例
对称多处理 SMP（Symmetric Multiprocessing）	一个OS实例同时管理所有CPU内核，应用并不绑定到某个处理核
绑定多处理 BMP（Bound Multiprocessing）	一个OS实例同时管理所有CPU内核，每个应用被绑定到指定的处理核



AMP



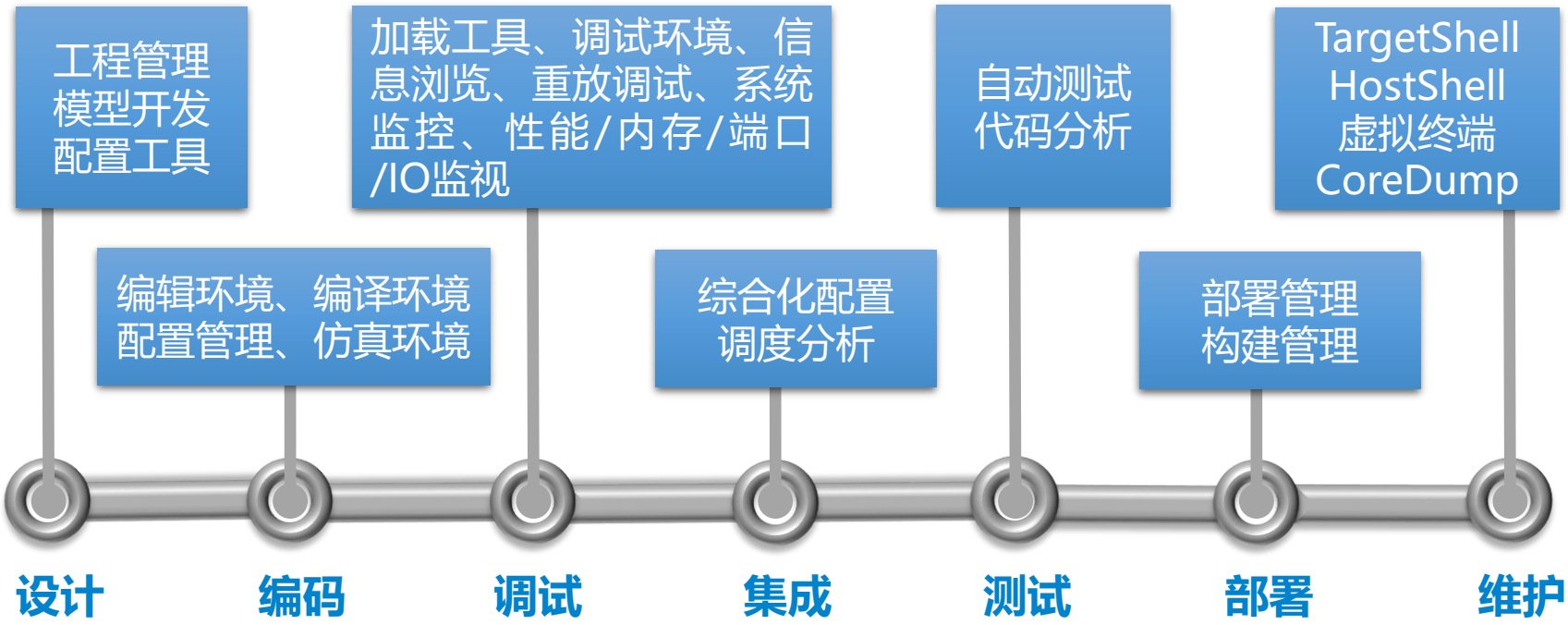
SMP



BMP

ACoreIDE—天脉集成开发环境

开发环境由**最初人工协同**到支持全生命周期**工具集合。**



ACoreIDE的应用软件全生命周期支持工具集
(30余个子工具)

天脉—处理器支持情况

天脉操作系统支持的CPU涵盖了PowerPC全系、ARM主流、x86、MIPS等多种架构的处理器，能够满足型号项目的常见需求。

类型	型号（红色为国产处理器）	操作系统
PowerPC	440、HKSP6101、HKSP7101、860系列	天脉1
	603e系列，603R、82XX(JSC8245/8247/8260/8270/ 8280等)	天脉1/天脉2
	604系列，75X（SM750/SM755等）、74XX（7447A/7448等）	天脉1/天脉2
	E300系列，5121E、83XX（8315E/8349E/8315/8377/8379等）	天脉1/天脉2
	E500系列，85XX（8548/8555/8560等）、P10XX（P1010/P1020/1021/1024等）、P20XX（P2020/2010/JSP2020等）	天脉1/天脉2/天脉3
	E600系列，86XX（8640/8640D/8641/8641D等）	天脉1/天脉2
	E5500系列，P50XX（P5020/5040等），T10XX（T1020/1040等）	天脉1/天脉2/天脉3
	E6500系列，T2080/T2081等	天脉3
ARM	V4系列、V5系列，ARM920T、ARM926E、LPC3250	天脉1
	v7A系列，TI66AK2H14/i.MX6Q(Cortex-A8/Cortex-A9/Cortex-A15)、Zynq7045、FMQL45T900、HKSA1502	天脉1/天脉2/天脉3
	v8A系列，飞腾FT1500A/飞腾2000AHK、Hi3559A	天脉1/天脉2/天脉3
X86	Atom/Core i7/GX-210(i386/486/pentium系列/Core系列/GX系列)	天脉1/天脉2
MIPS	龙芯系列，LS2H、LS2K1000、LS3A	天脉1/天脉3
	华睿系列，华睿2号	天脉1/天脉3

能力扩展组件

组件类型	组件名称	自有/集成	操作系统
网络协议栈	TCP/IP v4	自研	天脉1/天脉2
	TCP/IP v6	集成	天脉3
	FC、AFDX、1394机载网络协议栈	自研	天脉1/天脉2
文件系统	FAT文件系统	自研	天脉1/天脉2/天脉3
	网络文件系统	自研	天脉1/天脉2
	高可靠文件系统Reliance	集成	天脉1/天脉2/天脉3
向量运算	VSI/Pro向量库	集成	天脉1/天脉2/天脉3
系统中间件	通用系统管理GSM	自研	天脉1/天脉2
	数据分发服务DDS	集成	天脉1/天脉2
	嵌入式数据库eXtremeDB	集成	天脉1/天脉2
	通信中间件	自研	天脉1/天脉2
图形驱动	OpenGL	集成	天脉1/天脉2
	WindML/miniGUI	集成	天脉1
	QT、VAPS XT	集成	天脉1
外部接口	VxWorks兼容接口库	自研	天脉1/天脉3
	POSIX接口库	自研	天脉1/天脉3
硬件外设	M9/M96/E8860/APU/JM5400等显卡	集成	天脉1/天脉2
	USB协议栈（键盘、鼠标、存储）	集成	天脉1
	SATA、Flash等存储	自研	天脉1/天脉2/天脉3

覆盖机载常用能力组件，支撑平台级解决方案。

生态建设

已建成满足航空装备应用需求的软件基本生态

目录

较为广泛的用户群体

已有用户**70余家单位**，分布航空工业、中国电科、中国商飞、中国中车、航天科技、航天科工、中国兵器及高校等。

航天科技

航天科工

中国兵器

谢谢