Making Ideas a Reality

Aonix

# Safety Critical and COTS Solutions

# Aonix Customers

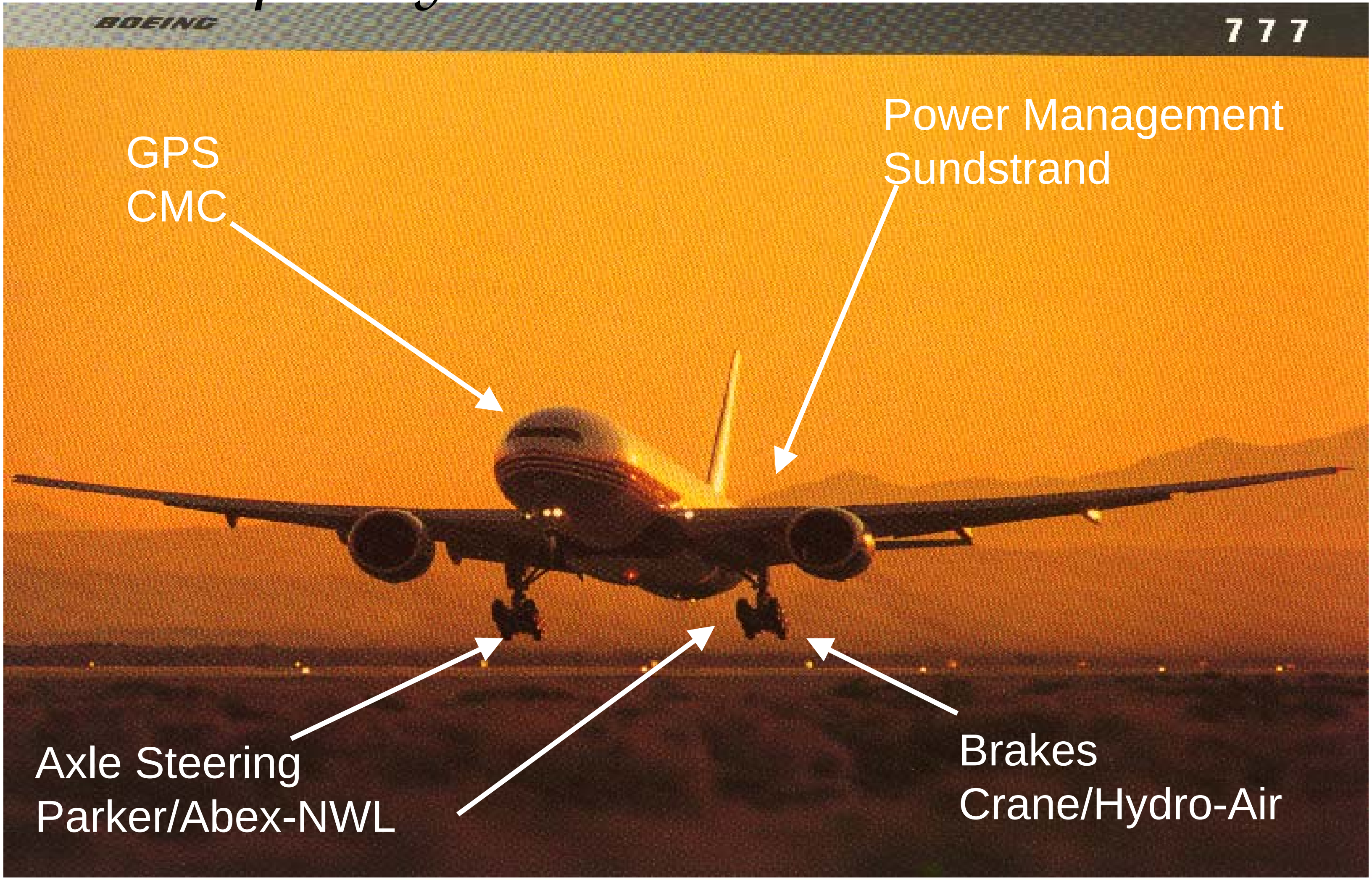
Aonix Experience

# Sample Safety Critical Applications

- Boeing 777
- Boeing 737
- Westinghouse Electric - Nuclear Shutdown
- Lockheed Martin - C130J and C27
- Westinghouse Brake and Signals
  - London Underground - Jubilee Line extension
    - Biggest Project In Europe
  - Automatic Brakes and Signaling

# *Boeing 777*

## *Sample Systems*



GPS
CMC

Power Management
Sundstrand

Axle Steering
Parker/Abex-NWL

Brakes
Crane/Hydro-Air

# Hercules - C130J

Aonix SC Products used for:

Flight Management Unit

Ground Collision Avoidance System

Back-up FMU

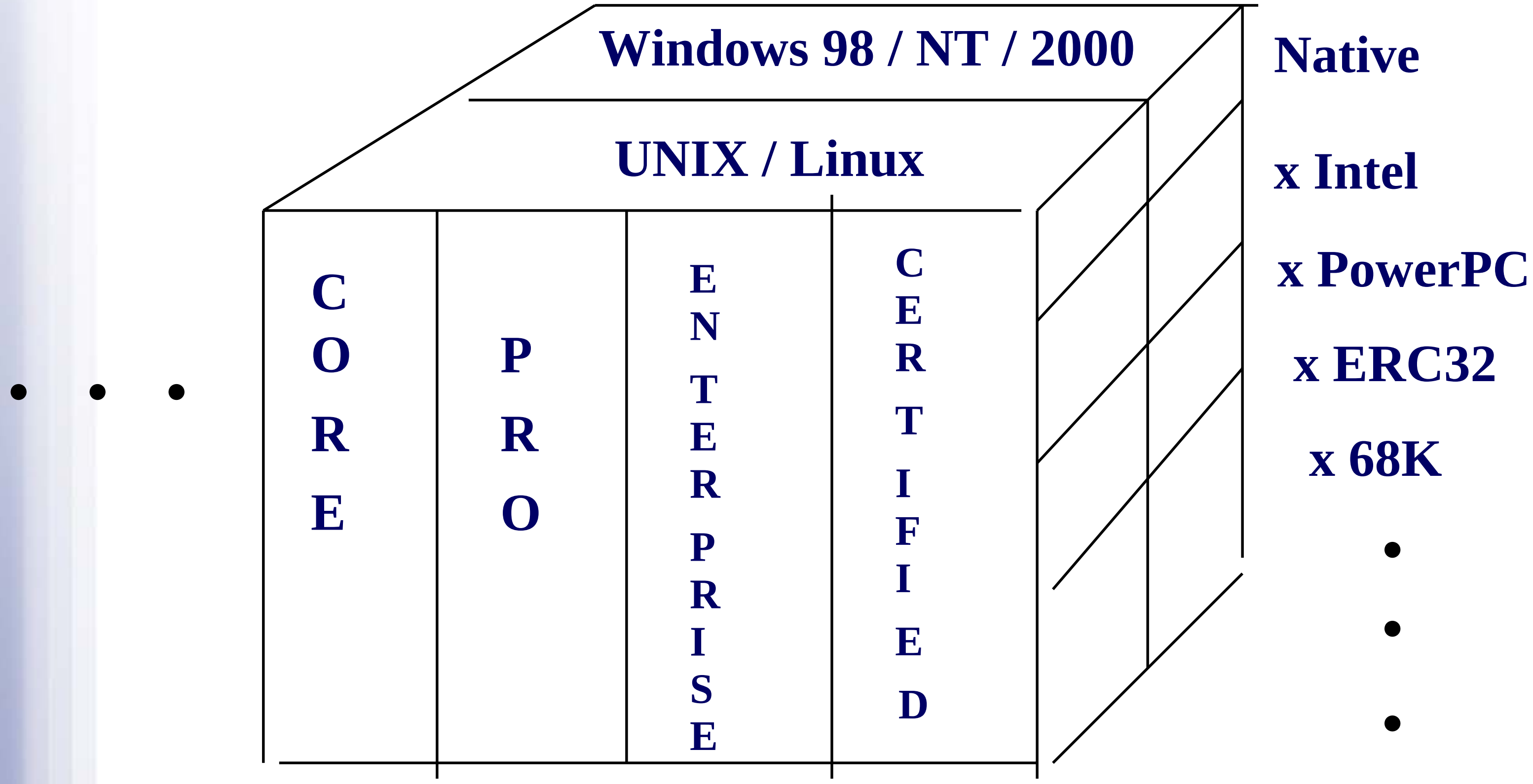
# ObjectAda Raven

# Safety Critical Software Development Environments

# Offerings

- Complete Development Environments
- Group Coordination Tool Support
- High Integrity Application Support
  - Safety Critical
  - Mission Critical
- Life Cycle Tool Support
  - UML or SE
  - Large Scale Controlled Code Generation
- COTS Certification Packages
  - Certified to DO-178B Level A

# Product Line Organization



Windows 98 / NT / 2000

UNIX / Linux

CORE

PRO

ENTERPRISE

CERTIFIED

Native

x Intel

x PowerPC

x ERC32

x 68K

# Required Safety Critical CM - SCCI Support

List Files

Comment

Get Latest

Check In

Add to CM

Show History

CM Properties

Keep Checked Out

Select / UnSelect All

Check Out

Undo Check Out

Remove from CM

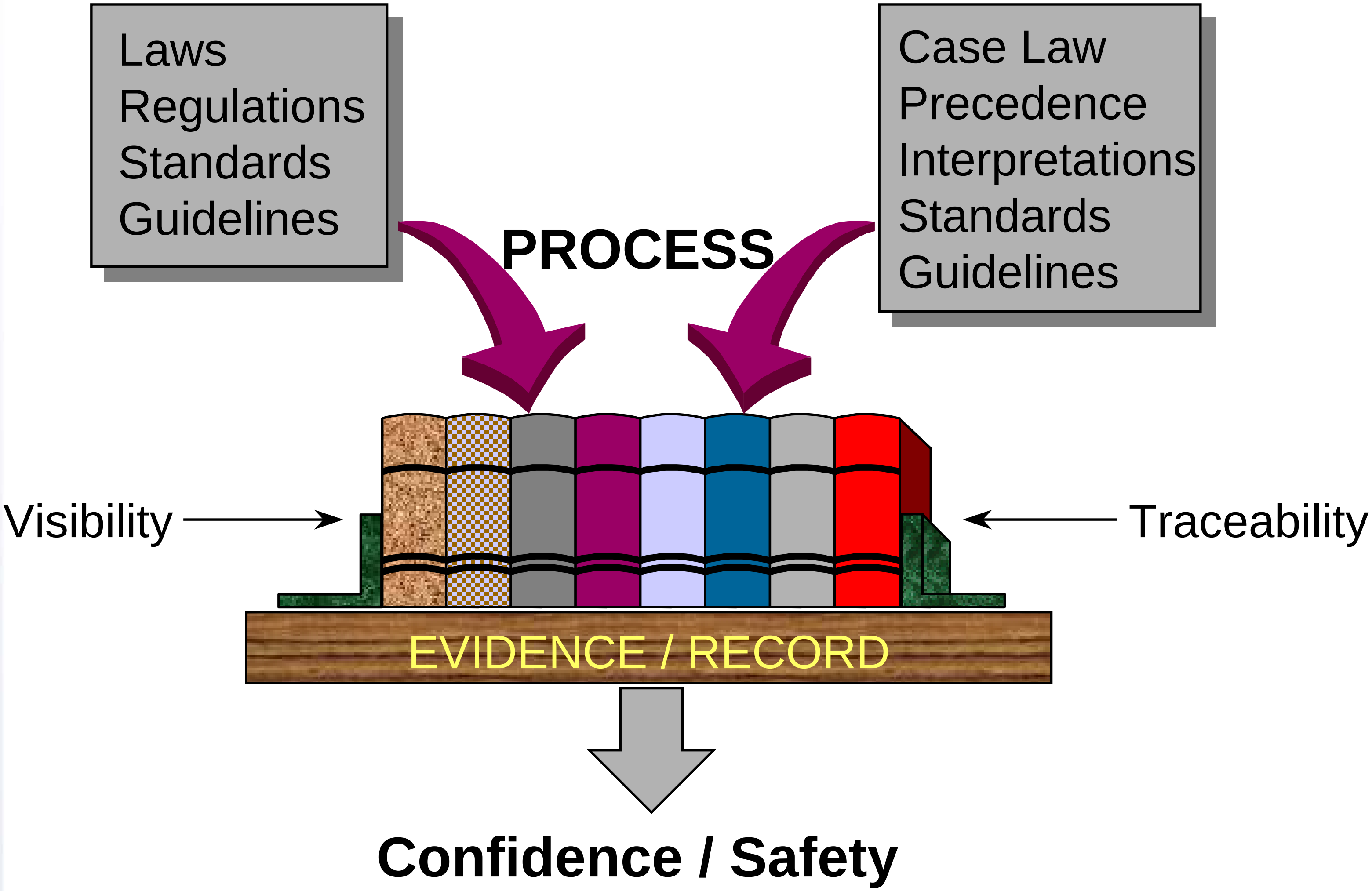
Show Differences

Invoke External CM

# ObjectAda Raven

# Certified/Certifiable Compiler/RTS

# ( Legal ) Safety Systems



Laws
Regulations
Standards
Guidelines

Case Law
Precedence
Interpretations
Standards
Guidelines

**PROCESS**

Visibility

Traceability

EVIDENCE / RECORD

**Confidence / Safety**

# RTS / Kernel Certification

- DO-178B Level A

**Traceability Purpose**

- Full Requirements through Test Results Mapping
- 100% Source Level Coverage
- 100% Machine Level Coverage
- Full MCDC Coverage

**MCDC Purpose**

- An RTS/Kernel Can be Certified but,
  - Termed Certifiable
  - An RTS/Kernel is Nothing Unto Itself

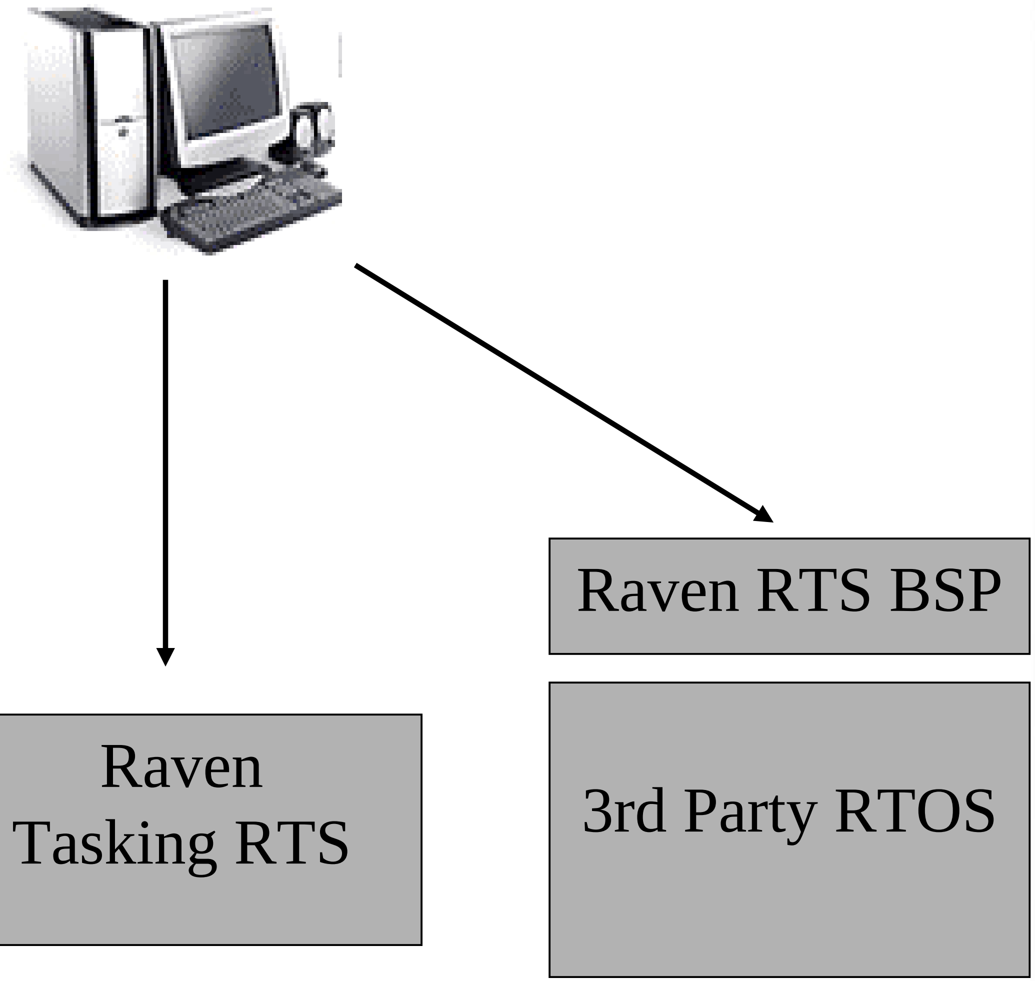
# Certified Kernels

- Ada83 - C-SMART Sequential Kernels
  - Intel
  - 68k
  - eMIPS
  - ERC32
- Ada95 - Raven Multi-Tasking Kernels
  - PowerPC
  - Intel
  - ERC32

# Safety Critical
# Real-time Approach

- Aonix technology for safety-critical applications
- **Raven Environments**
  - Conforms to Ravenscar Profile
  - Flags Ravenscar Profile Violations at Compile Time
  - Level A Certification Package Available
  - VectorCast for Test Harness and Source Level Coverage
  - AdaCover machine level coverage analysis
  - New support for bounded tasking model
  - New support for segregated loads

# Raven Board Level Configurations



Sequential RTS

Raven Tasking RTS

Raven RTS BSP

3rd Party RTOS

# Raven Board Level Configurations

- Sequential RTS/Kernel
  - Small and Fast
  - No Tasking Support
- Full Raven RTS/Kernel
  - Larger But Just As Fast
  - Full Tasking and Interrupt Support
  - Optional Non-Certifiable Feature Use
- Layered on Top of an RTOS
  - More General Capabilities from RTOS
  - Larger Collection of Drivers
  - Larger Foot Print
  - Likely a Bit Slower

# Raven Packages

- Designed For Project Size
  - Packages for Small or Large Programs
  - Higher Level Packages add Group Coordination Between Developers
- Designed For Criticality of Application
  - Packages for General up to Safety Critical Applications
  - Higher Level Packages add Greater Test and Safety Capabilities

# Raven Packages

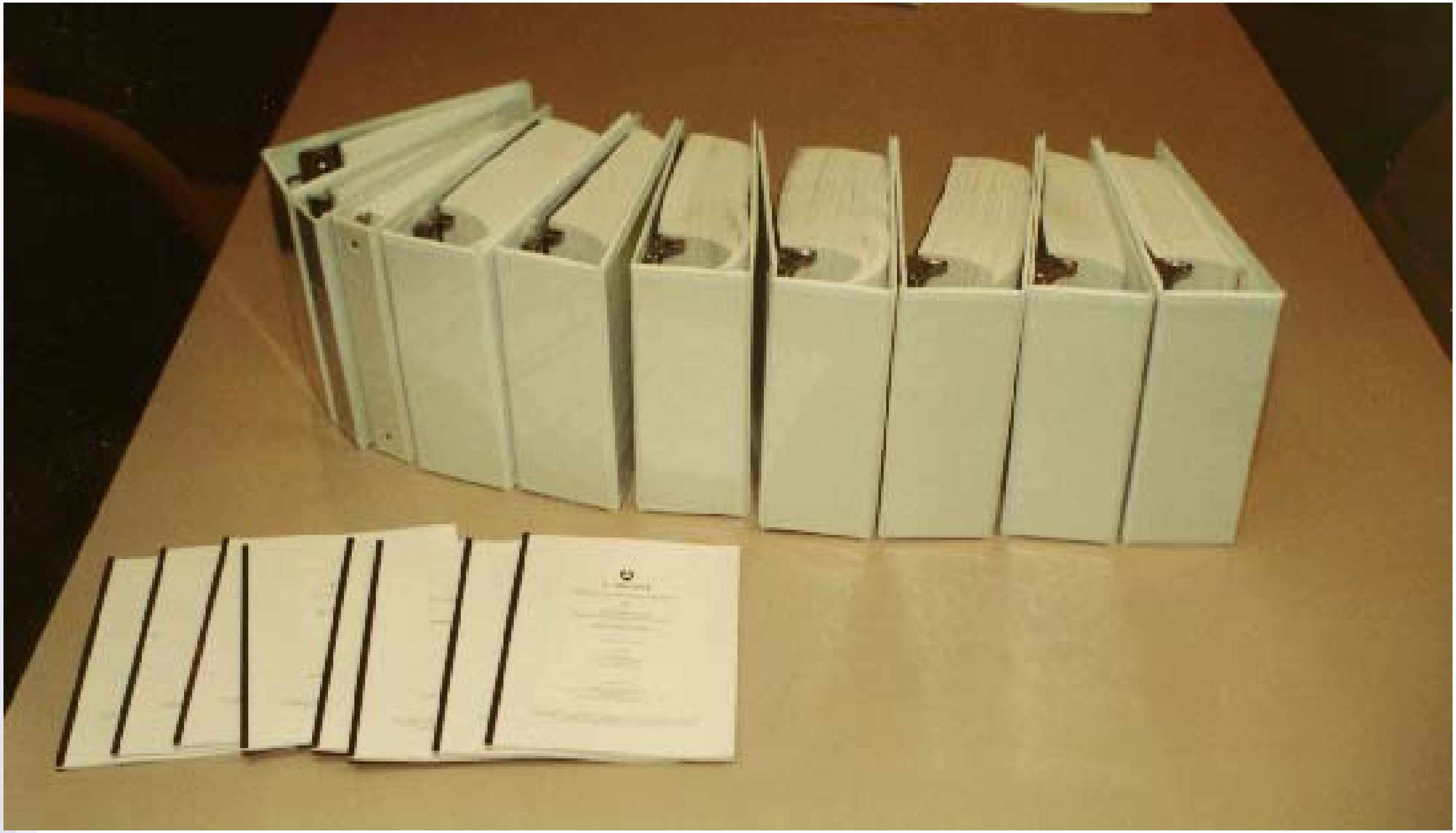
- Core Pack
  - For Small Groups Needing a Basic Development Environment
- Project Pack
  - Multiple Developer Source Navigation Tools
  - Advanced Language Sensitive Editor for Larger Group Source Consistency and Style Guideline Conformance Checking
- Test Pack
  - For Projects Needing a Higher Level of Quality for Mission or Safety Critical Development
- Safety Critical Pack
  - For Groups Needing to Test to Safety Critical Standards
- Design Pack
  - For Projects Needing a Life Cycle Solution to Accompany the Development Environment

# Certification Pack

- Complete Certification Evidence
  - For Applicable RTS/Kernel
- Available for:

- Ada83 C-SMART
  - Intel, 68k, eMIPS, and ERC32
- Ada95 Raven
  - Intel, PowerPC, and ERC32

# One Set of Certification Evidence Delivery 170 lb



# Now: One CD-ROM Captures All SDF's

# More... Aonix Customers

More Aonix Experience

# Safety Critical Customers

**Aircraft/Avionics –**

□ • Global Positioning System (**GPS**) (Sextant Avionique)

□ • Flight control data concentrator: **AIRBUS A330-A340** (Sextant Avionique)

□ • Braking and steering control unit: AIRBUS A330-A340 (Thomson CSF/DOI and Messier Bugatti)

□ • Air Traffic Control (ATC): Ground-based instrument landing system (Navia, formerly Normarc)

□ • Air Traffic Control (ATC): Germany, England, France and Belgium (EUROCONTROL)

□ • Flight Management System (**FMS**): (EUROCONTROL)

□ • Gauge control system: FALCON (Dassault/Intertechnique) France, Germany

□ • Mission computer and data concentrator: TIGER and NH-90 (Eurocopter

□ • (ATC): Denmark, Belgium, New Zealand, South Africa, Kenya, Pakistan, and Greece (Thomson CSF/SDC)

□ • Air Traffic Control simulators: Switzerland, Ireland (Thomson CSF/SDC)

□ • Air Traffic Control System (ATC): (FAA)

□ • Radar system: Civil avionics (Wilcox Electric)

□ • Engine control system: (Chandler Evans)

□ • Flight Management: **Lockheed C130J** (Lockheed Martin)

□ • Ground Collision Avoidance: Lockheed C130J (Aerosystems International)

□ • Displays: Lockheed C130J (Lockheed Sanders)

□ • Global Positioning System: **Boeing 777** (CMC)

□ • Axle Steering System: Boeing 777 (Parker/Abex-NWL)

□ • Power Management System: Boeing 777 (Sundstrand)

□ • Brakes: Boeing 777 (Crane/Hydro-Air) Nuclear and Electricity

# Safety Critical Customers

**Nuclear/Power -**

- □ • Power plant control: (Sema Group)
- □ • Power generating system simulation: (Thomson CSF/DSI)
- □ • Nuclear reactor project: (Nuclear Electric)
- □ • Power plant power transmission system: (ABB Relays AG)
- □ • Nuclear reactor control simulation: (CEA Cadarache)
- □ • **Nuclear Shutdown System**: Nuclear power station in Czech Republic (Westinghouse Electric)

**Trains and Railways –**

- □ • Subway network control systems: Paris, Calcutta, and Cairo (GEC ALSTHOM)
- □ • Railway and signal control system: TGV for north lines and the **Channel**
- □ • Brake system for the TGV: the TVM 430 project (CSEE Transports)
- □ • Brake and signals system: **London Underground**, Jubilee Line extension (Westinghouse)
- □ • Railway and signal control system: TGV Mediterranee
- □ • Railway Signaling System in China: KCRC project (Alstom)

**Space –**

- □ • **Satellite positioning system**: (Alcatel SEL)
- □ • Launching platform: Ariane V project (Aerospatiale with the CNES and Matra Marconi Space)
- □ • Satellite imaging system: SPOT project (CNES)
- □ • Columbus part of International Space Station: (ERNO Raumfahrttechnik)
- □ • Data management systems and network control system: **International Space Station** (NASA)
- □ • Inertial Reference System: QUASAR 3000 project (Thalès Avionics) for ArianeV
- □ • Data management system: APM (Atmospheric Pressure Module) for International Space Station

# Some New Safety Critical Customers

- Pratt and Whitney
  - » PW6000 Commercial Jet Engine
  - » New JSF F-35:  F135-PW-100 Jet Engines
- Honeywell Canada (formerly Allied Signal)
  - » ECS 2000, Environmental Control System
  - » for the 777 LR/ER planes
- Honeywell Florida
  - » Multiple Military Avionics (certifiable)
  - » Positioned for Military AND Commercial Avionics
- BF Goodrich
  - » HUMS
- MAO Bechtel
  - » PPDSU, Nuclear Submarine Display
- Litton => F-22 (certifiable)

# Summary

- Flexible, well-planned product architecture
- Lightweight implementation technology

UML MDA for Raven next ?

- Aonix...
- Vast Experience in Safety Critical Systems
- Supplier of Certifiable RTS and Needed Support Tools
  - Leading Safety Critical Supplier for Ada83
  - Leading Safety Critical Supplier Today for Ada95
- Off-The-Shelf Certification Packages

- Partnerships with Leading Safety Critical Experts

# OMG UML MDA Solution for Raven

**This may be of interest,**

**based on Tullio Vardanega's presentation…**

# OMG UML MDA Solution for Raven

- Ravenscar Profile:
  - Presentation by: Tullio Vardanega
- Ravenscar Frameworks or Task Patterns

- Implemented by Aonix using UML and MDA
  - Defined a MDA Ravenscar Profile

# UML, MDA, and Profiles

- Use UML Notation for Expressing Design
- MDA **Profile** Defines Meanings to Notation
  - Classes, State Machines, etc.
- Profile Defines **Transformation** (Code Generation)
- A Ravenscar MDA Profile:
  - Use StereoTypes to define Raven Classes (Patterns)
  - Use TaggedValues for Class specific data
  - Use associations for Class relationships
  - Support both Class and State diagrams
    - State Diagram for Application Logic

# MDA Raven Profile StereoTypes

- Primary design patterns found within Raven systems:
  - Main
  - Repetitive
  - Cyclic (or Periodic)
  - Sporadic (Sporadic Suspension)
  - Sporadic Data
  - ResourceControl
  - Synchronization
  - Suspension
  - Interrupt
- General purpose Raven Stereotypes
  - General PO
  - EventHandler

# MDA Raven Profile Refinement

Class TaggedValues

- Priority
- StackSize
  - For all Raven Task Classes
- Period
  - For Periodic or Cyclic Raven Tasks
- SharedData
  - For all Protected Object Classes
- IntId
  - For InterruptHandler Protected Objects Classes
  - Or Optionally Any Protected Object

Checks for and Marks Illegal Values

- Priority > Priority’Last, missing Period, SharedData, IntId, ...

# Sample Transformation Template

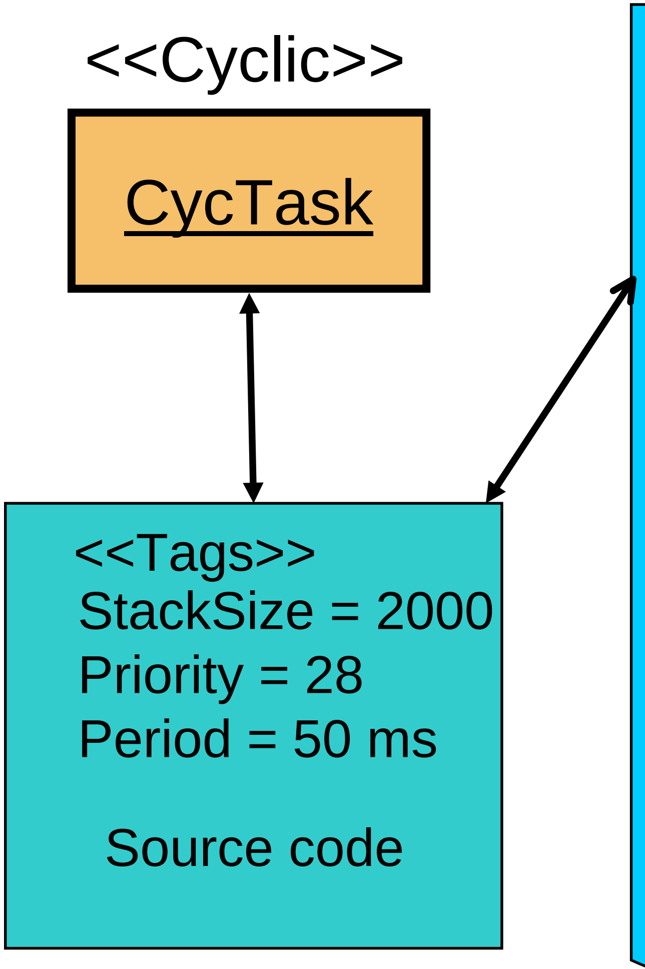
- Generate a Repetitive Raven Task

```
/******************************************************************/
 /* Generate a Repetitive Raven Task                                  */
 /*********************************************************************/
 template RepetitiveTaskSpec(MClass)

 --*** <<Repetitive>> StereoType Raven Task
 with System; -- for Priority value.
 package [MClass.name]_Pkg is

   task [MClass.name] is
 [Priority([MClass])]
 [StackSize([MClass])]
   end [MClass.name];

 end [MClass.name]_Pkg;
 end template
```

# MDA Raven Transformation Examples

- Task Stereotypes
  - Repetitive (no trigger, background activity)
  - Cyclic or Periodic (time-triggered)
  - Sporadic (event-triggered)
    - Suspension object (no data)
    - Protected object (with data)
- Synchronization Stereotypes
  - Shared resources
  - Protected entries
  - Suspension objects
  - Interrupts

# Cyclic Task Stereotype with attributes



<<Cyclic>>

CycTask

<<Tags>>
StackSize = 2000
Priority = 28
Period = 50 ms

Source code

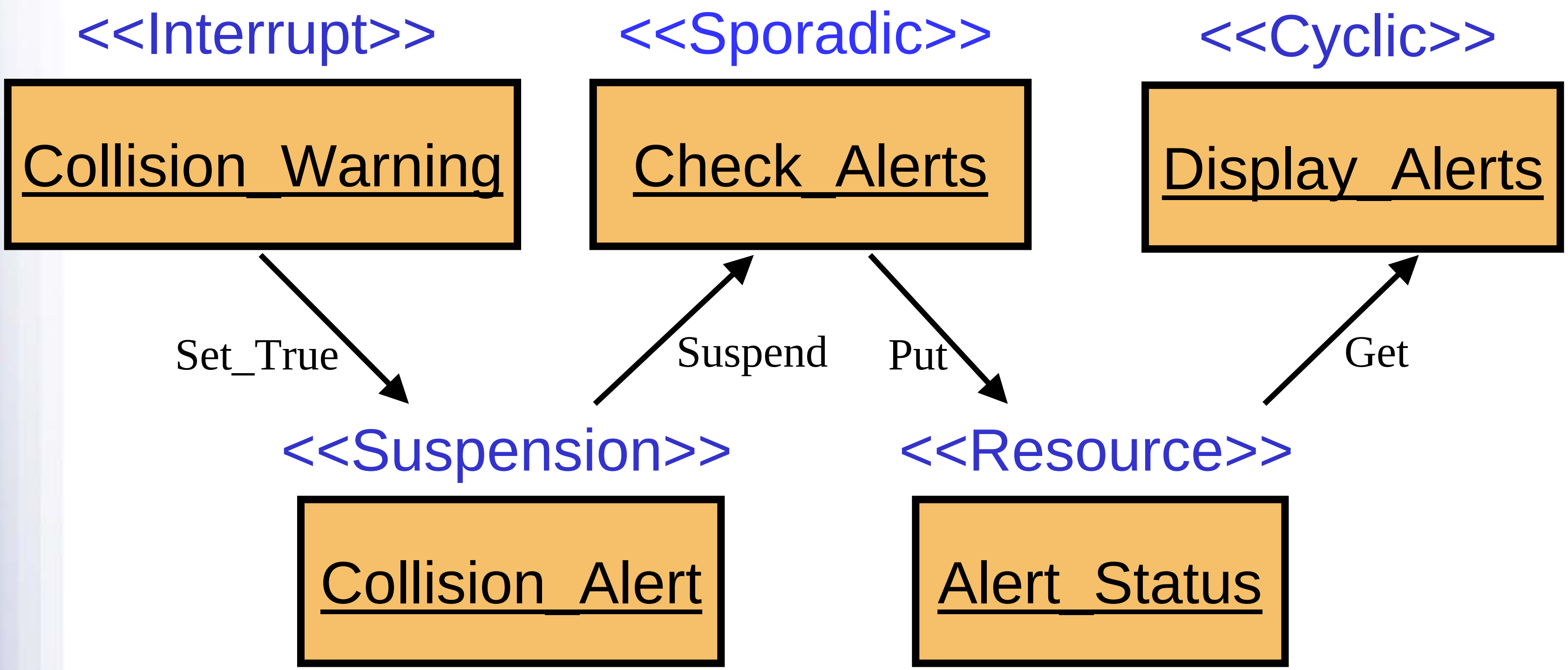
**Generated Code (part)**

```
task CycTask is
   pragma Priority (28);
   pragma Storage_Size (2000);
end CycTask;

task body CycTask is
  Next_Time : Time;
  Period : Time_Span := Milliseconds(50);
begin
   Next_Time := Clock;
   loop
      delay until Next_Time;
      --  body
      Next_Time := Next_Time + Period;
   end loop;
end CycTask;
```

# MDA Raven Profile Rules

- Raven Task to Task associations are defined to be illegal, since Raven tasks can not define entries and Task rendezvous are not supported.
  - Communications is achieved via Protected Objects (Resource Control, Synchronization, and Event Handlers) and Suspension Objects
- All Sporadic Tasks must be associated with a Suspension Class Object
- All SporadicData Tasks must be associated with a Synchronization Class Object

# MDA Raven Class/Task Interaction Diagram



# State Machine Transformations

- Each UML Design Class May Have a State Machine
- MDA Raven Transformations Generate Body Logic
  - This can be a large amount of the final application logic
  - Not discussed in detail here

# OMG UML MDA Solution for Raven

- Provides Defined UML Design Objects for Ravenscar
- Generates Complete Design Patterns
- Enforces Ravenscar Class/Task Interactions
- Generates Application Logic as Well

- This is a whole separate presentation
- Presented briefly here as an implementation example of Tullio Vardanega's concepts put into practice

- Designed a couple of years ago by:
  - myself, Brian Dobbings and George Romanski

# And Now Back To Our Regularly Scheduled Program...

# Summary

- Flexible, well-planned product architecture
- Lightweight implementation technology

- Aonix...
- Vast Experience in Safety Critical Systems
- Supplier of Certifiable RTS and Needed Support Tools
  - Leading Safety Critical Supplier for Ada83
  - Leading Safety Critical Supplier Today for Ada95
- Off-The-Shelf Certification Packages

- Partnerships with Leading Safety Critical Experts