Introduction to Modelling Languages

Antonio F. Gómez Skarmeta
University of Murcia (Spain)

DESEREC

Dependability and Security by Enhanced Reconfigurability

Modelling Alternatives for Dependability

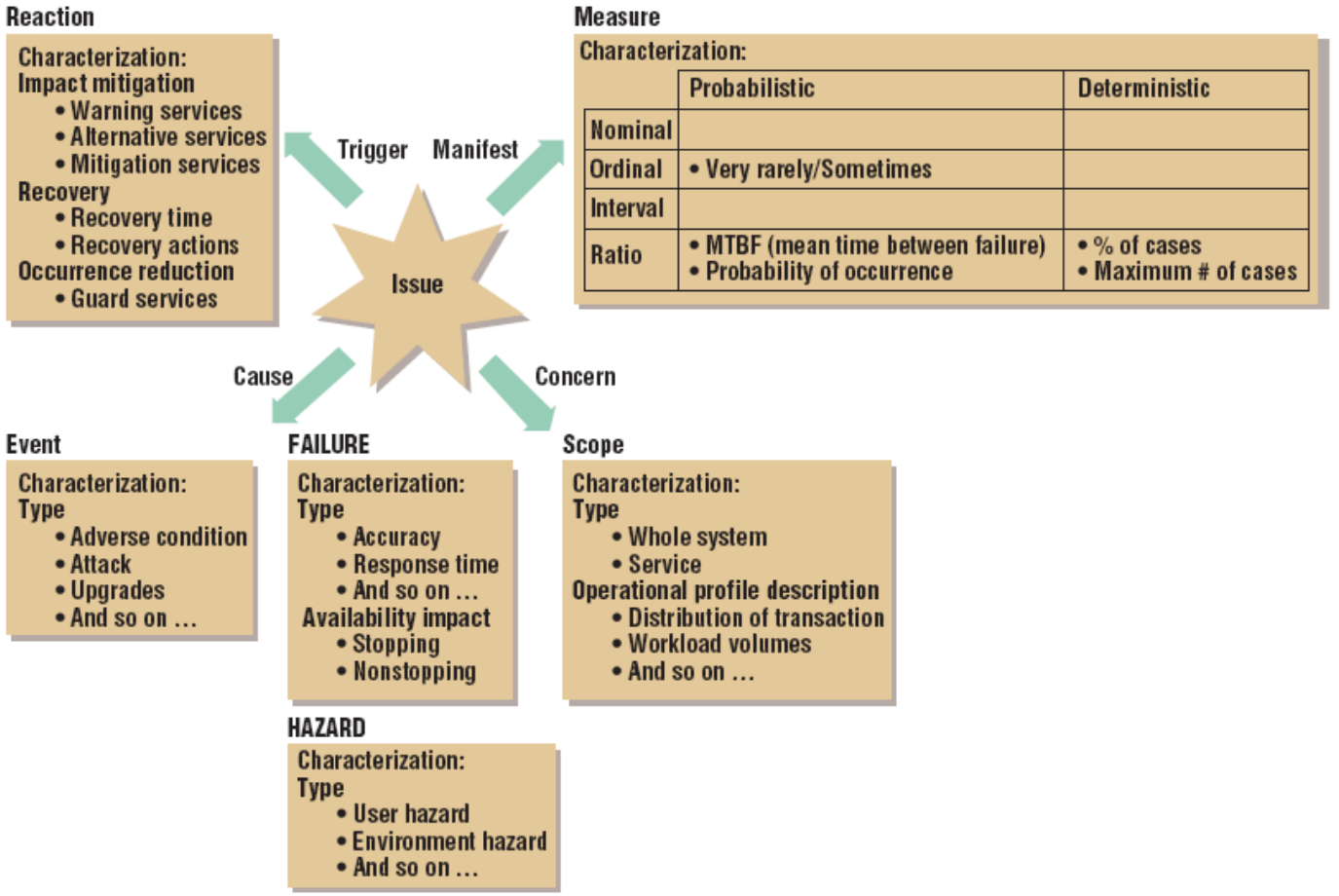
State of the art on modelling languages

- Unified Model of Dependability (UMD)
- Unified Modelling Language (UML)
- Situation-Aware Contract Specification Language (SA-CSL)
- Ponder
- Domain Modelling Language (DML)
- Summary
- Others proposals

Unified Model of Dependability (UMD)

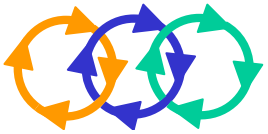
- UMD aims to establish a common language for discussing a variety of dependability attributes, and to make them measurable
- Take into account different aspects of a dependability attribute:
  - Affected system functionalities
  - Manifestation of a specific failure (hazard) or class of failures (hazards)
  - External events (adverse conditions, attacks, etc.)
  - Expected system reaction
- Designed for working “bottom-up” (from failures to dependability attributes) instead of “top-down” (from attributes to failures)
- Offers a structured framework for eliciting and organizing dependability needs
  - Include definitions which stakeholders may use, alter and extend
    - Categorization of the *issues* (the term used in UMD for “problem”) which divides them into “failures” and “hazards”
    - Classifying events
    - Issue scopes and measurements
    - System reactions

UMD structure



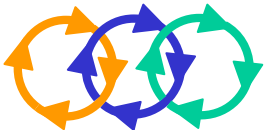
Unified Modelling Language (UML)

- Standard language for specifying, visualizing, constructing and documenting all the artefacts of a software system
- Some works have extend UML in order to offer security and dependability requirements
  - Security: UMLSec
  - Dependability: DMP (Dependability Mechanisms Profile)
- Close related to CIM (UML & CIM)



UMLSec

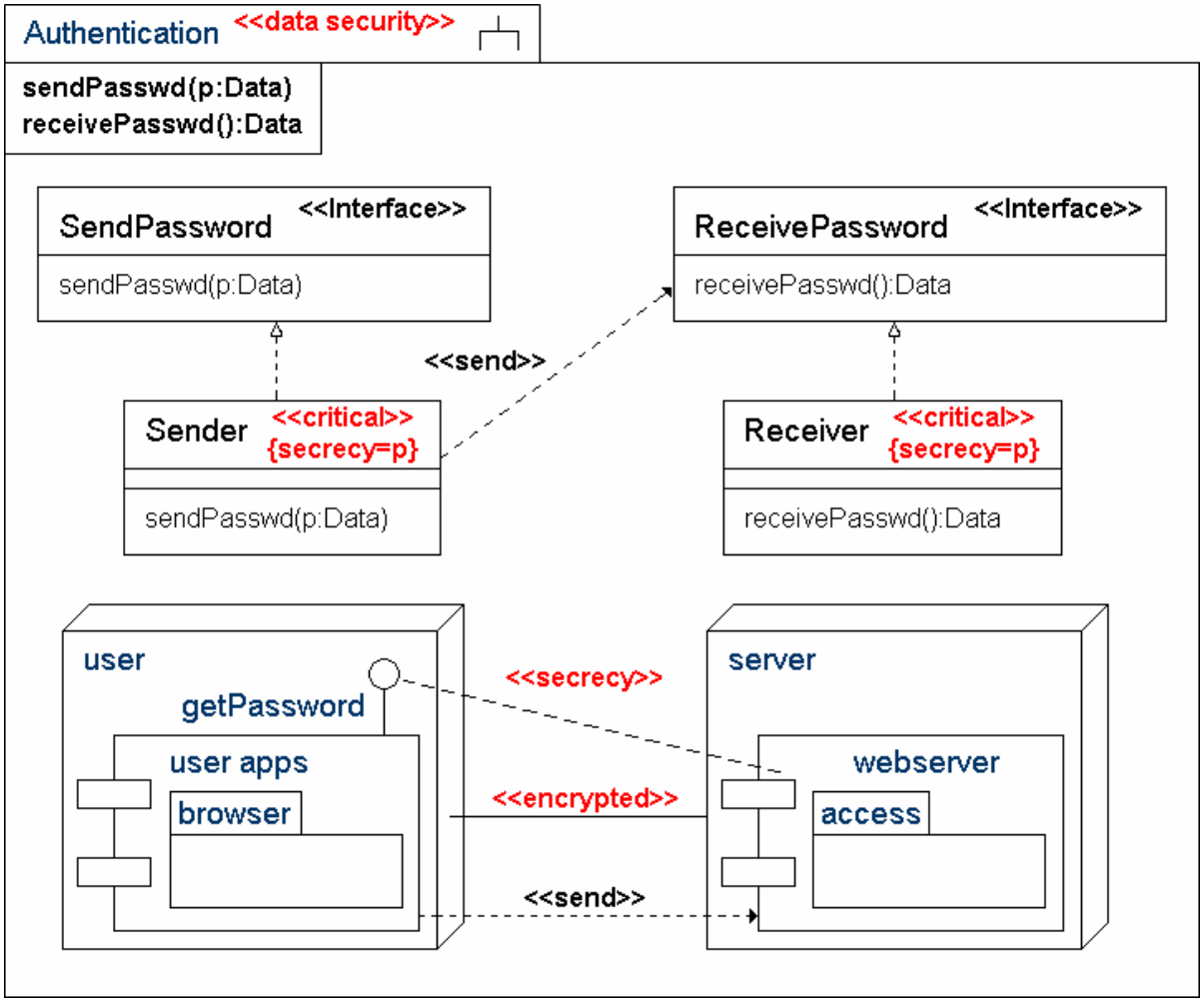
- UML extension for secure systems deployment thinking in developers which are not security experts
- Main goals:
  - Evaluate UML specification for vulnerabilities in design
  - Encapsulate security engineering patterns
  - Consider design from the early design phases
- Provides basic security requirements to represent:
  - Confidentiality, integrity
  - Secure information flow, access control
  - Auditing, protocol analysis
- Adds security relevant information to model three kinds of elements:
  - Security assumptions on the physical level of the systems: «Internet»
  - Security requirements on the logical structure of the system: «secrecy», «critical»
  - Security policies systems are supposed to obey: «fair exchange», «secure links», «data security» and «no flow-down»



UMLSec – Stereotypes

Stereotype	Base class	Tags	Constraints	Description
Internet	Link			Internet connection
Encrypted	Link			Encrypted connection
LAN	Link			LAN connection
Secure link	Subsystem		Dependency security matches by links	Enforces secure communication links
Secrecy	Dependency			Assumes secrecy
Secure dependency	Subsystem		«call» «send» respect data security	Structural interaction data security
Critical	Object	Secret		Critical object
Data security	Subsystem		Provides secrecy	Basic datasec requirements

UMLSec – Example



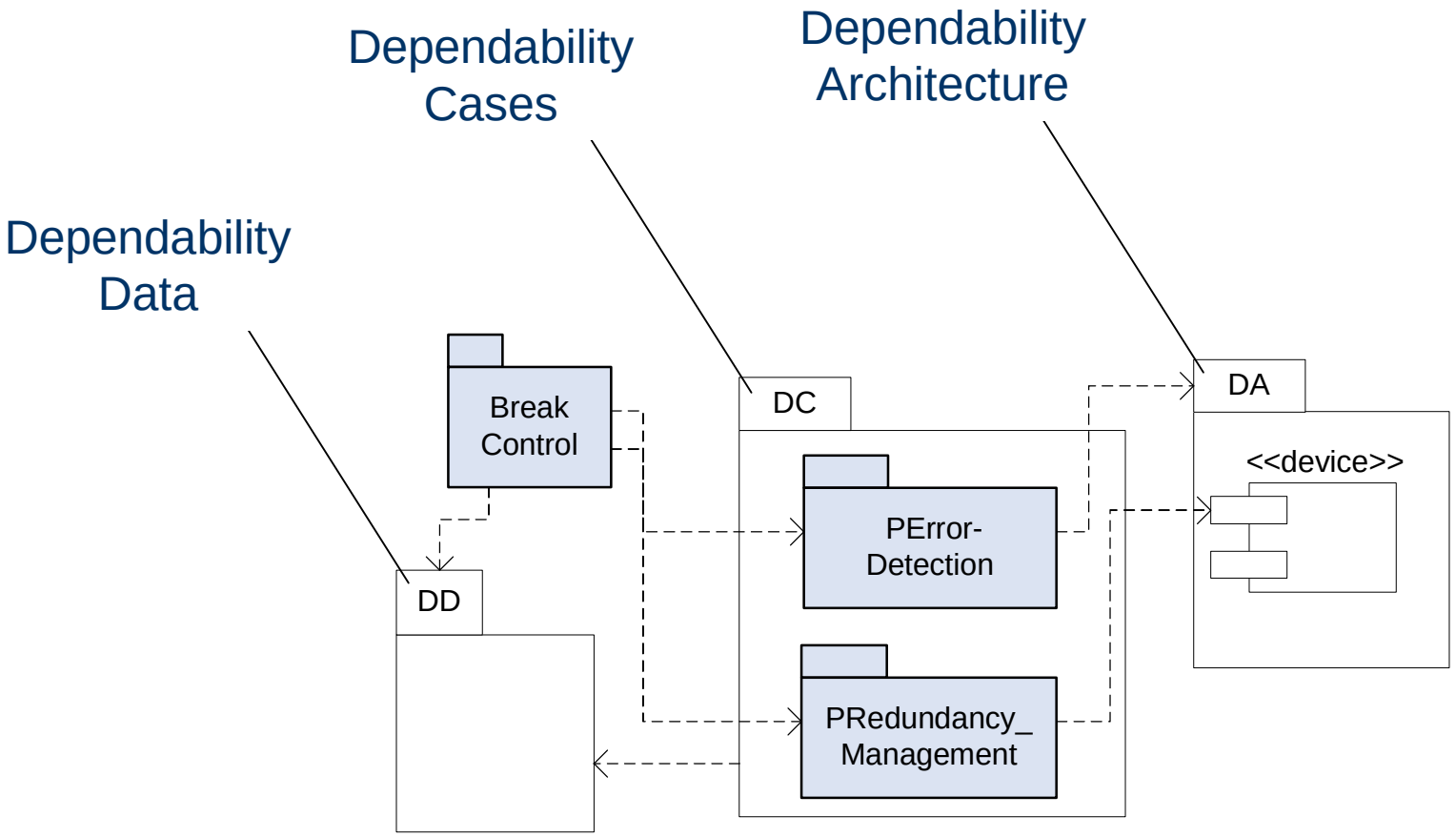
Dependability Mechanisms Profile (DMP)

- Defines a language for defining, visualizing, analysing and documenting dependability mechanisms
- Includes:
  - Dependability Architecture: defines the main dependability components
    - Error detection units
    - Error detection mechanism
    - Redundancy management strategies, etc.

    Each component is defined by a set of ports and interfaces
  - Dependability Cases: defines mechanisms and their action on the system
    - Classifier acting as a group of components providing a dependability feature
  - Dependability Data: contains structured classes and diagrams to define data
    - Fault patterns, fault statistics, repair time distributions, etc.

DMP – Example

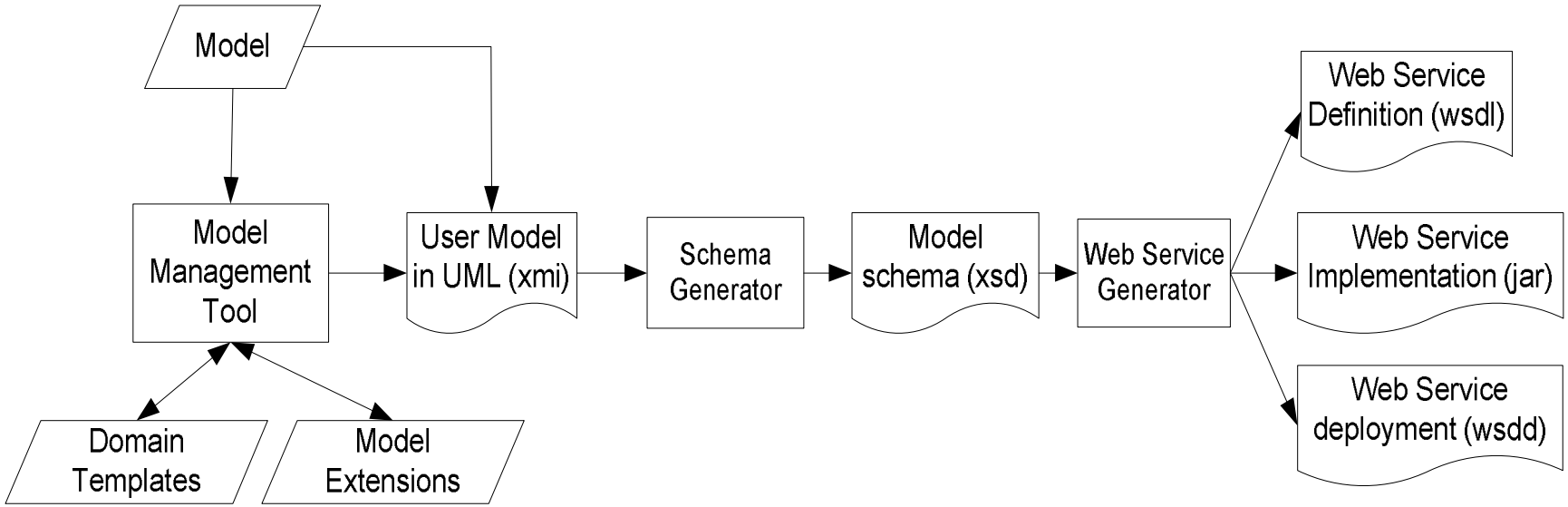
- Break Control model that may contain sub-models composed by stereotypes representing error detection, channel switching, etc.



UML & CIM

- An innovative research line
- Both standards can be put together in order to allow CIM metamodel be defined using UML
  - DMTF uses the metamodel abstraction concept to describe the syntax and structure of CIM
  - The metamodel of CIM has been described using the Management Object Format (MOF)
  - UML could provide a better representation of the CIM model for non expert users
- UML Profiles provide a mechanism to extend UML metamodel
  - CIM metamodel could be defined as a UML profile
  - This approach has been chosen by the DMFT to map CIM into UML

UML & CIM – Proposed framework

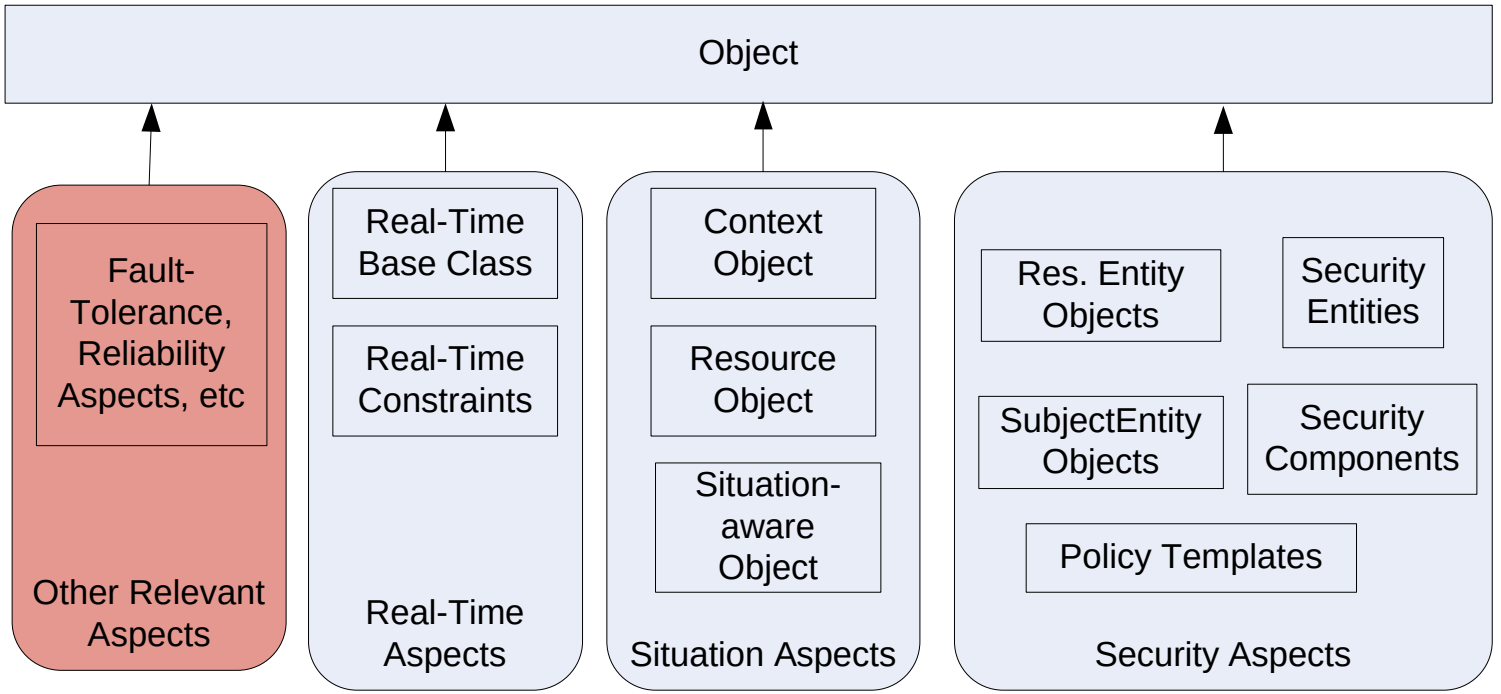


Situation-Aware Contract Specification Language (SA-CSL)

- Thinking in ubiquitous computing, applications use different situation changes to trigger different application actions
  - *Situation*: set of pass context attributes and/or actions of devices relevant to determine device actions
  - *Context*: instantaneous and relevant condition of the environment or device
- SA-CSL extends the Situation-Aware Interface Definition Language (SA-IDL) to support real-time and security services
- Associates the situation that affects the application or device and the associated actions to be taken to respond to the situation
- It could be extended to include QoS properties, fault tolerance, scalability, etc.

Situation-Aware Contract Specification Language (SA-CSL)

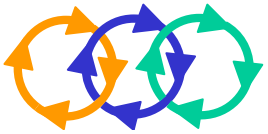
- Object hierarchy in SA-CSL



Ponder

- Declarative and object-oriented language developed for specifying management and security policies
- Support obligation policies:
  - Event triggered condition-action rules
  - For policy-based management of distributed communication systems
- Can also be used for defining security management policies

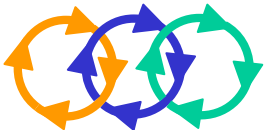
- Primitive policies:
  - Authorization
  - Obligation
  - Information filtering
  - Refrain
  - Delegation



- There are three types of composed policies:
  - Roles: provide a semantic grouping of policies with a common subject
  - Relationships: groups the policies defining the rights and duties of roles towards each other
  - Management structures: defines configurations in terms of instances of roles, relationships and nested management structures relating to organizational units

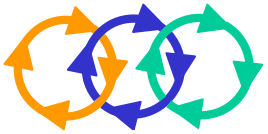
- Example:

```
Type auth+ auth-policy1 (subject <admin> a, target <database> db) {
    action modify-access-permissions if belongs (a, db.ACL) {
        result = enable;
    }
}
```



Domain Modelling Language (DML)

- Defines a public-domain standard for attribute databases
- Can be used for model configuration and verification
- Supports extensibility, inheritance and substitution of attributes
- Data structure:
  - DML expression is just a blank-separated sequence of named attributes
  - Values may be either basic types (integers, strings, etc.) or another DML expression enclosed in square brackets
  - This allows modelling data hierarchies, as collections of attributes
  - Referenced via XPath-like locator expressions
- DML has also validation capabilities, through the usage of *schemas*
  - DML schema is a DML expression which defines how another expression should be built
  - It includes which attributes must be present and which are the allowable values for them



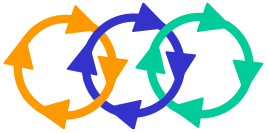
Domain Modelling Language (DML)

```
ipConf [
    ipAddress 2001:600:3::5
    ipAddress 2001:610:1::3
    gateway 2001:600:3::1
]
```

Sample DML expression

```
restartService [
    execute stop_service.sh
    execute clean_logs.sh
    execute start_service.sh
]
```

Modelling a command sequence

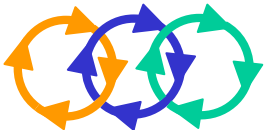


Summarize

Model	Expressiveness	Required skills	Comments
UMLSec	Security requirements	UML	-
DMP	Dependability architecture, cases, data and requirements	UML	Not widely extended and not much related work
OCL	Constraints on UML	UML	Operates on an existing UML model
SA-CSL	Real time event handling	-	Limited applicability due to immaturity
Ponder	Event-triggered management and security policies	-	Evolved to XML
DML	Hierarchical “attribute/value” data collections	-	Immature, and not very powerful

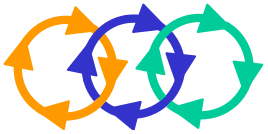
More proposals

- UML-Q: A UML Profile for QoS Management Information
  - QoS Management
- SPNP: Stochastic Petri Net Package
  - Input language is CSPL (C-based SPN language)
- ULTRASAN
  - Models specified using a variant of SPNs known as stochastic activity networks (SANs)
- PRIDE
  - Integrated software development environment for dependable systems based on UML
- MEADEP (MEAsure DEPendability)
  - Failure data based dependability analysis and modelling tool



More proposals

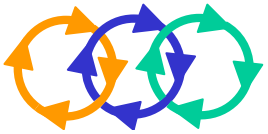
- ADEPT
  - Single modelling language and mathematical foundation to create a unified design environment
- VIATRA (VIsual Automated model TRAnsformations)
  - Tailored for UML-based system verification
- DEEM (DEpendability Evaluation of Multiple-phased systems)
  - Dependability modelling and evaluation tool specifically tailored for the time-dependent analysis of MPS



Common Information Model (CIM)

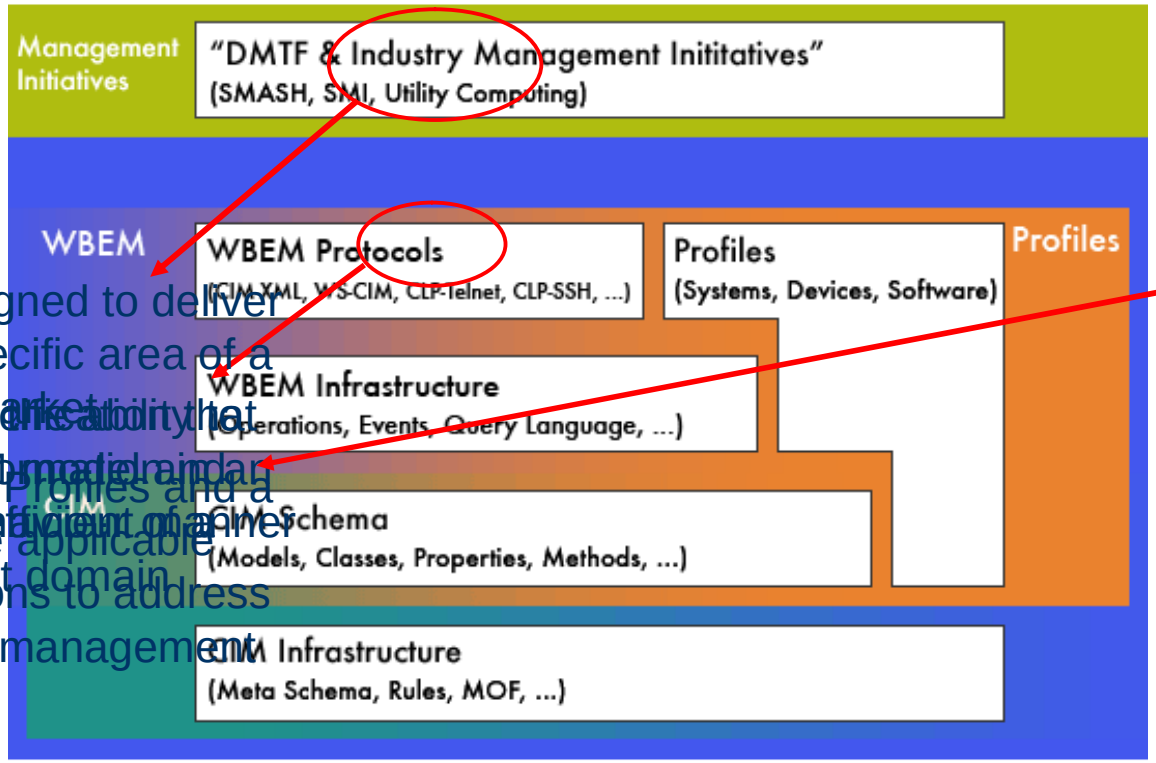
DMTF CIM is a conceptual information model for describing computing and business entities in enterprise and Internet environments

- CIM enables the management of real world managed objects
- It is a hierarchical, object-oriented paradigm with relationship capabilities
  - Object-oriented modelling is used to model hardware and software elements
- An object-oriented model can be described using a diagramming convention such as UML
- Object-oriented information model (**NOT language**)
- The standard language used to define elements of CIM in a text format is Managed Object Format (MOF)



Technology Diagram

- DMTF technologies are designed as building blocks
  - In conjunction, they enable solving real world problems for distributed enterprise management



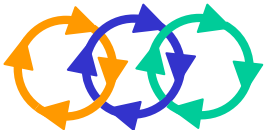
An Initiative is designed to deliver a solution for a specific area of a WBEM vertical market that defines CIM information and WBEM specifications to address a specific area of management

It includes a set of Profiles and a reference to the applicable management domain

Common Information Model (CIM)

- Main advantages:
  - Independence from platform, programming language and compiler
  - Independence from information model
  - Extensibility
  - Easy integration of new management capabilities
  - Security and Internet accessibility
  - Development and resources

- Taking the CIM policy model as a basis, IETF defined the:
  - Policy Core Information (PCIM)
  - Policy Core Information Model Extensions (PCIMe)



Common Information Model (CIM)

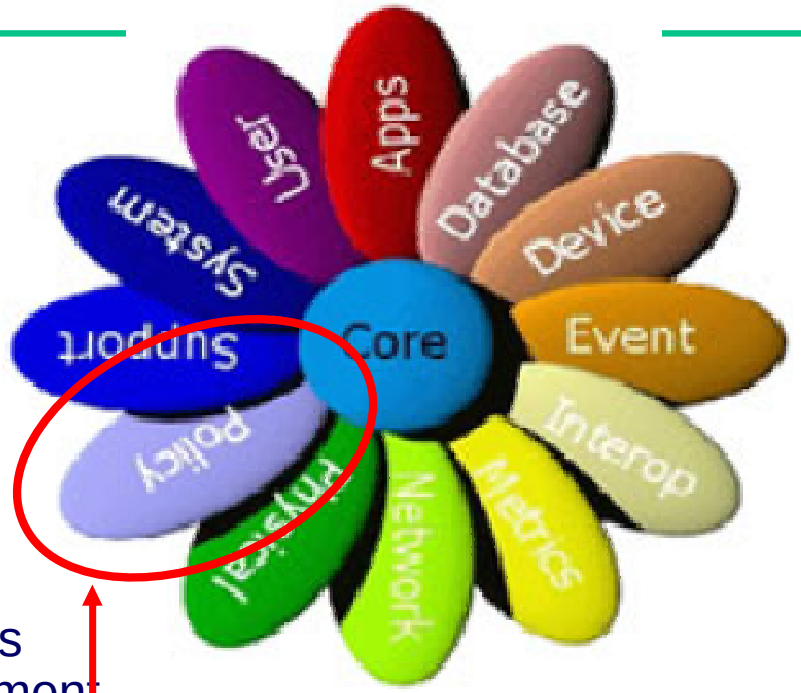
- CIM can be divided in four main groups:
  - Modelling language and syntax
  - Management schema
    - Core model
    - Common model
    - Extension schemas
  - Protocol to encapsulate syntax and schema (XML/HTTP)
  - Compliance document, but no test suites

Modelling language and syntax

- Meta schema is formal definition of the model
  - Terms are defined to express model, usage, and semantics
- UML is used to define the structure of the meta schema
  - Basic object-oriented concepts of:
    - Classes
    - Properties
    - Methods
    - Associations
    - ...
- Managed Object Format (MOF) is the language used to describe management information
  - Can be encoded in Unicode or UTF-8

Common Information Model (CIM)

Management Schema



CIM Schema

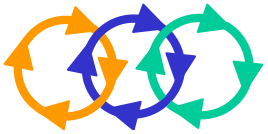
- Core model
  - An information model that captures notions that are applicable to all areas of management
- Common model
  - Captures notions that are common to particular management areas:
    - Systems, applications, networks, devices and policies
  - Independent of a particular technology or implementation
  - Provides a set of base classes for extension into the area of technology-specific schemas (i.e. extension schemas)
- Extension schemas
  - Represent technology-specific extensions of the common model
  - These schemas are specific to environments

CIM Policy Model

- Provides a framework for specifying configuration and operational information in a scalable way using rules
- CIM policy model consider policies as rules in the form:

> ***if*** *condition(s)* ***then*** *action(s)*

- Specify which action(s) must be taken when certain condition(s) are satisfied
  - The "**condition**" part of the rule can be a simple or combined expression specified in either conjunctive or disjunctive normal form
  - The "**action**" part of the rule can be a set of actions that must be executed when the conditions are evaluated to true



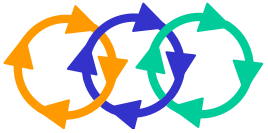
Comparative Analysis

Most of the current policy languages

- Precision (no ambiguity)
- Consistency
- Easy of specification (different levels of detail)
- Intuitiveness

Just CIM, PCIM and PCIMe

- Standard
- Generic (i.e. not tied to one particular service and/or application)
- Compatibility with the capabilities supported by the network device, service or application



Introduction to Modelling Languages

Antonio F. Gómez Skarmeta
University of Murcia (Spain)

Thank you!

DESEREC

Dependability and Security by Enhanced Reconfigurability