SMIF

Information Federation with Semantic Models

Using threat and risk examples

Cory Casanave

(cory-c at modeldriven dot com)

OMG®

OBJECT MANAGEMENT GROUP

magicdraw®

Model Driven Solutions

Where Business Meets Technology

Question?

How can we have different people

- In different organizations
- With different vocabularies
- And different perspectives
- For different purposes
- Using different schema

Our proposition is semantics – understanding what something means independent of how it is expressed

Share and federate information about the same things?

Copyright (c) 2012-2023 Model Driven Solutions, Inc.

Semantic Modeling

Capability – Information Federation, Synthesis & Analytics

- Ingest and interpret information and processes from multiple divergent sources
  - Situational awareness
  - Federated analytics "Connecting the dots"
  - Joint missions and desperate industries
  - Risk reduction

Capability – Information Sharing & Brokerage

- Translate information between diverse sources and consumers
- Configurable gateways for diverse schema and protocols
- Systems integration

Capability – Design for Interoperability

- Instead of designing "from scratch", use semantic models as the foundation for new systems. This reduces cost and errors while building in interoperability. Leverages MDA model execution & Code/Schema Generation. Can forward engineer to semantic web.

Copyright (c) 2012-2023 Model Driven Solutions, Inc.

Analogy: Role of the interpreter

Copyright (c) 2012-2023 Model Driven Solutions, Inc.

What we expect of interpreters

Retention of meaning across languages, communities and cultures

Communicate what is said without judging, coloring or filtering it

Common concepts

Interpreters leverage substantial preparation; learning syntax, grammar, vocabulary and cultural idioms.

Interpreters can only communicate what they understand and what can be understood in the languages they deal with – the common concepts

They then communicate ***what other people said*** based on how those concepts are expressed in different languages – they also communicate the provenance

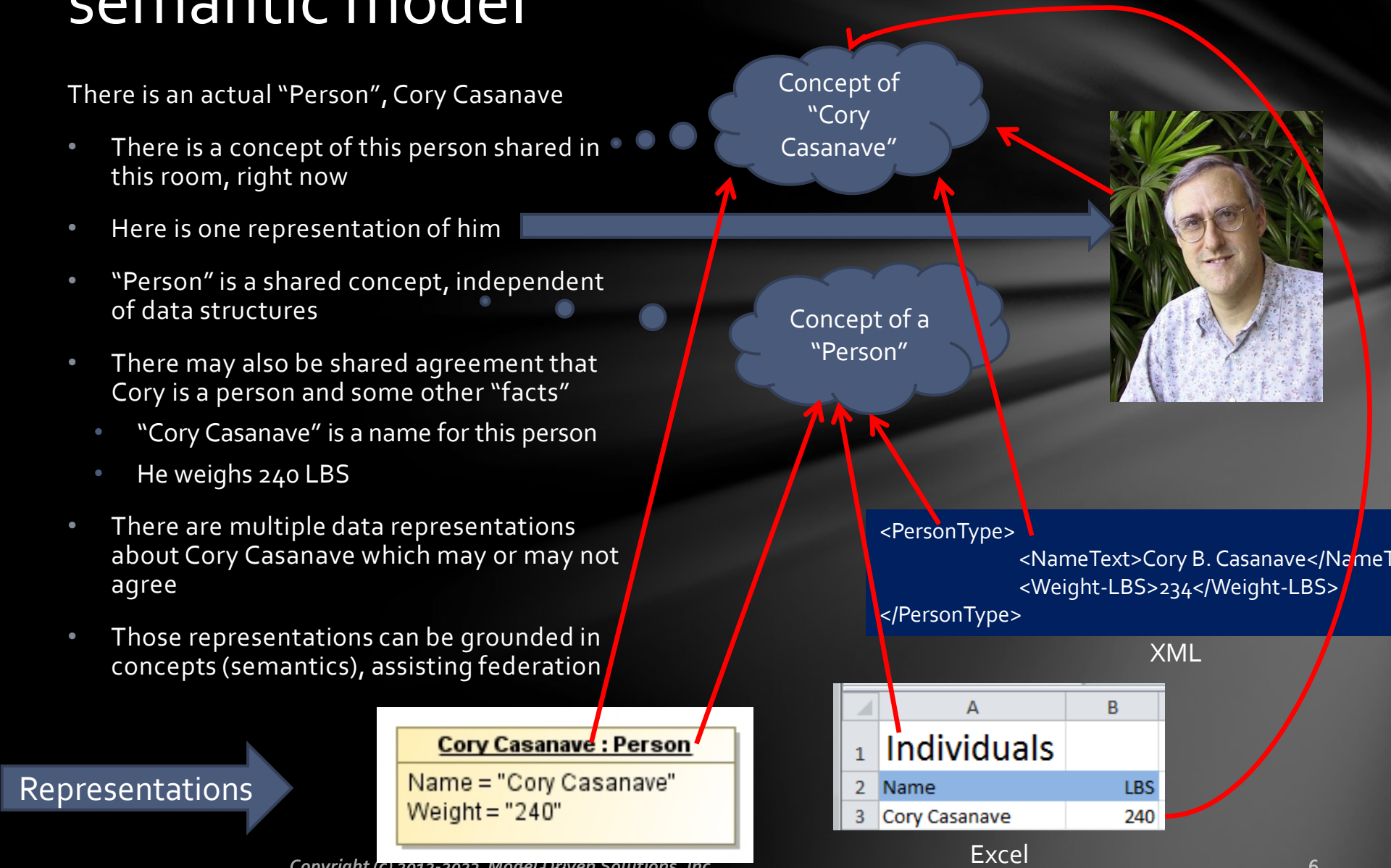
Interpreters are preforming *semantic mediation*

Copyright (c) 2012-2023 Model Driven Solutions, Inc.

Example of "Pivoting" through a semantic model

There is an actual "Person", Cory Casanave

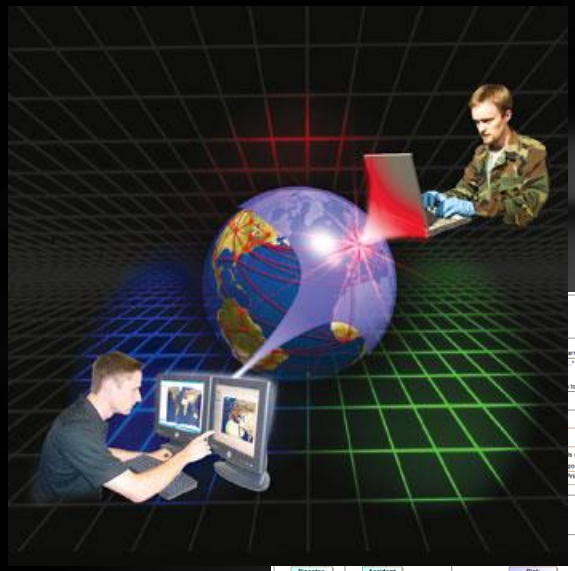
- There is a concept of this person shared in this room, right now
- Here is one representation of him
- "Person" is a shared concept, independent of data structures
- There may also be shared agreement that Cory is a person and some other "facts"
  - "Cory Casanave" is a name for this person
  - He weighs 240 LBS
- There are multiple data representations about Cory Casanave which may or may not agree
- Those representations can be grounded in concepts (semantics), assisting federation

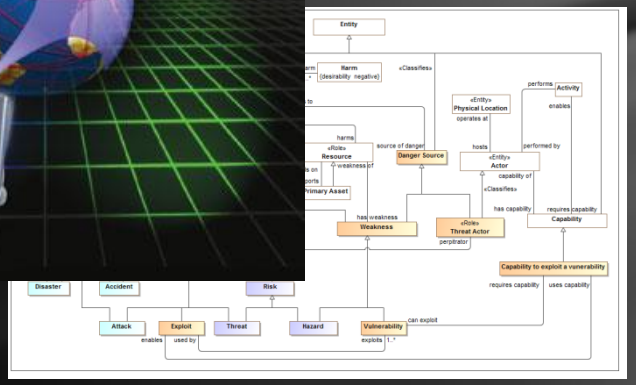


Copyright (c) 2012-2023 Model Driven Solutions, Inc.

Threat information example

STIX
Cyber Information





NIEM
(Justice and public safety)

Federated conceptual reference model

Copyright (c) 2012-2023 Model Driven Solutions, Inc.

Example: What is a threat actor?

Threat Actor

Data About

Data element, not a threat actor.

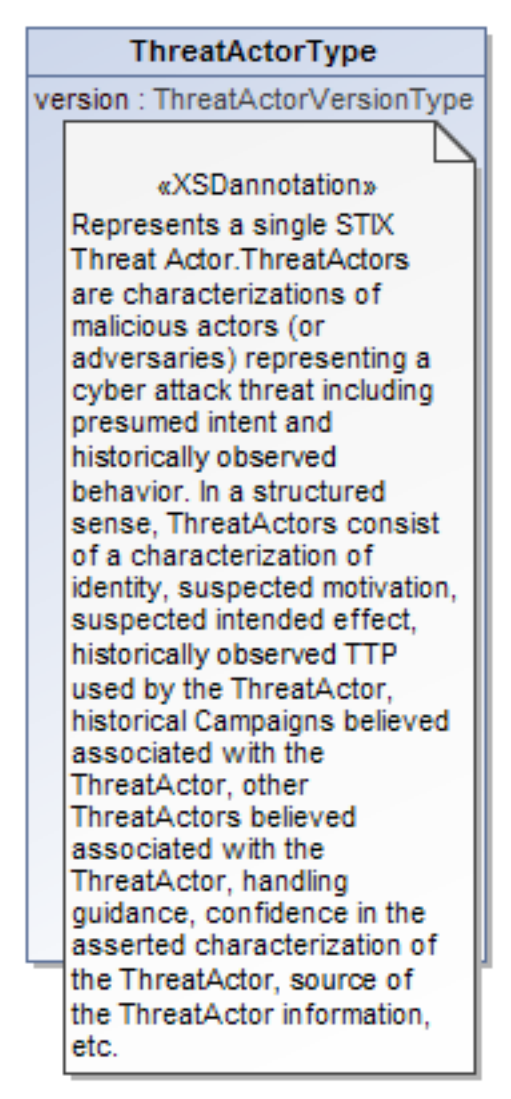
Dictionary

A threat actor, also called a malicious actor, is an entity that is partially or wholly responsible for an incident that impacts – or has the potential to impact -- an organization's security.

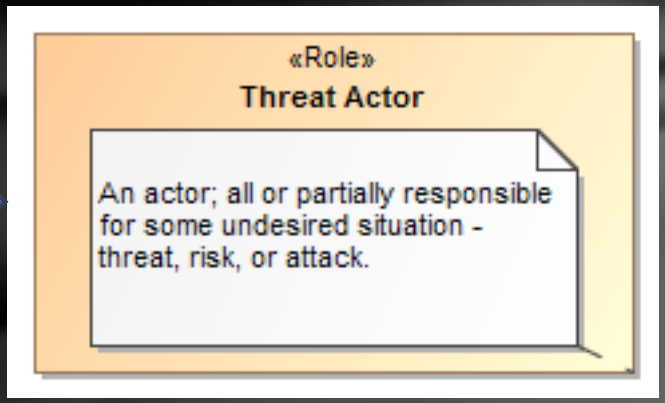
```
<xs:complexType name="ThreatActorBaseType">
    <xs:annotation>
        <xs:documentation>This type represents the STIX Threat Act
        feature by the STIX Threat Actor type itself. Users of thi
        do so using the xsi:type extension feature. The STIX-defi
        http://stix.mitre.org/ThreatActor-1 namespace. This type
        http://stix.mitre.org/XMLSchema/threat_actor/1.1.1/threat_
        <xs:documentation>Alternatively, uses that require simply
        elsewhere can do so without specifying an xsi:type.</xs:do
    </xs:annotation>
    <xs:attribute name="id" type="xs:QName">
```

Copyright (c) 2012-2023 Mod

Data represents concepts



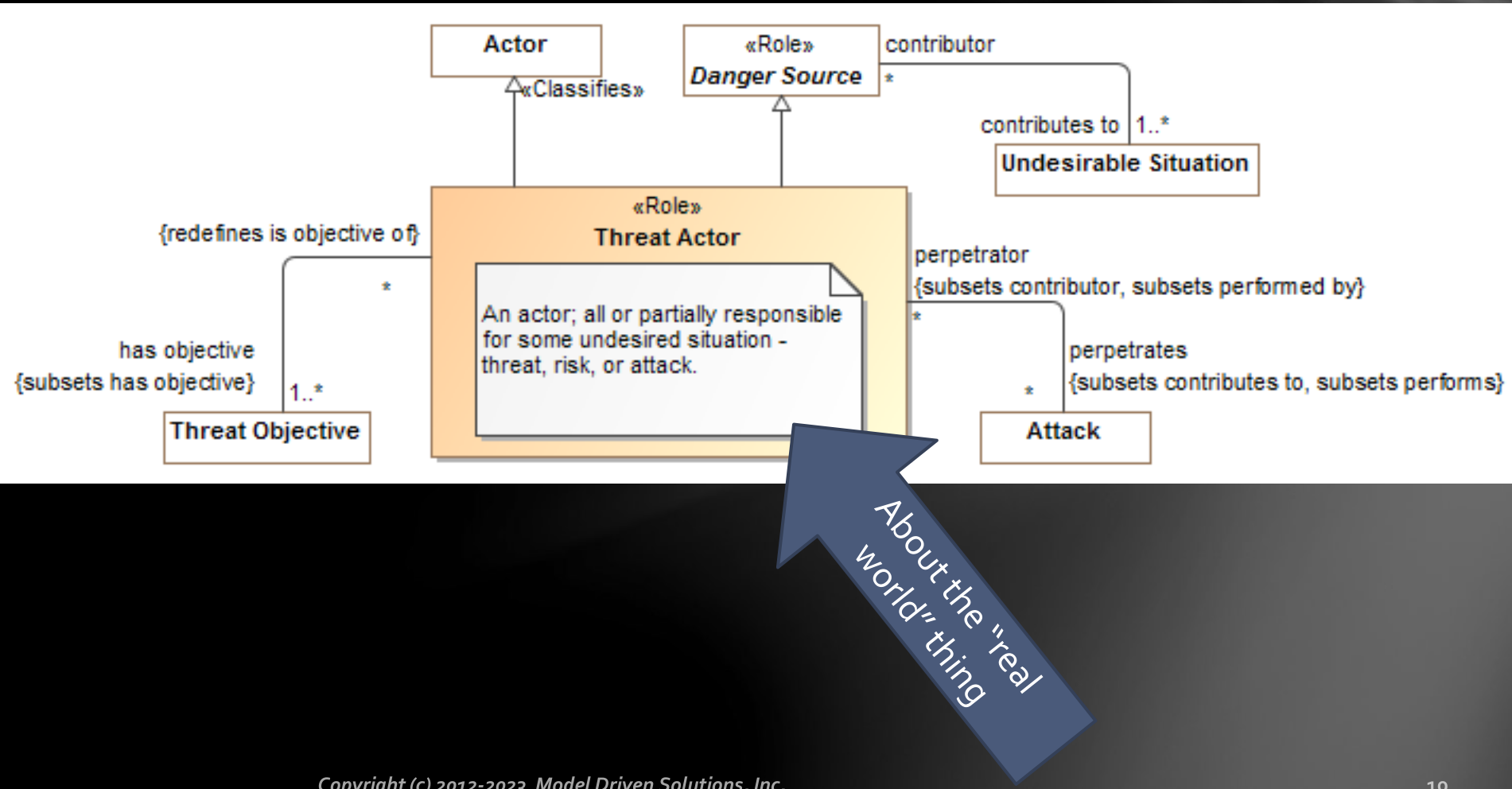
Represents



We want to "reference" the semantic reference model) from the solution architecture (data, process and services perspectives).

Copyright (c) 2012-2023 Model Driven Solutions, Inc.

What is a threat actor? Semantic Model



Copyright (c) 2012-2023 Model Driven Solutions, Inc.

Semantic models Vs System Design Models

Most models that have been creating are design models

- They represent the design of particular systems
- They constrain the model to the needs of that design
- The model concepts represent the solution

BUT

Design models are hugely valuable.

- They facilitate critical team level thinking
- They can validate the design as consistent
- They can validate the deign meets requirement
- Models can be simulated
- Models can be used to generate solutions (from code to hardware)

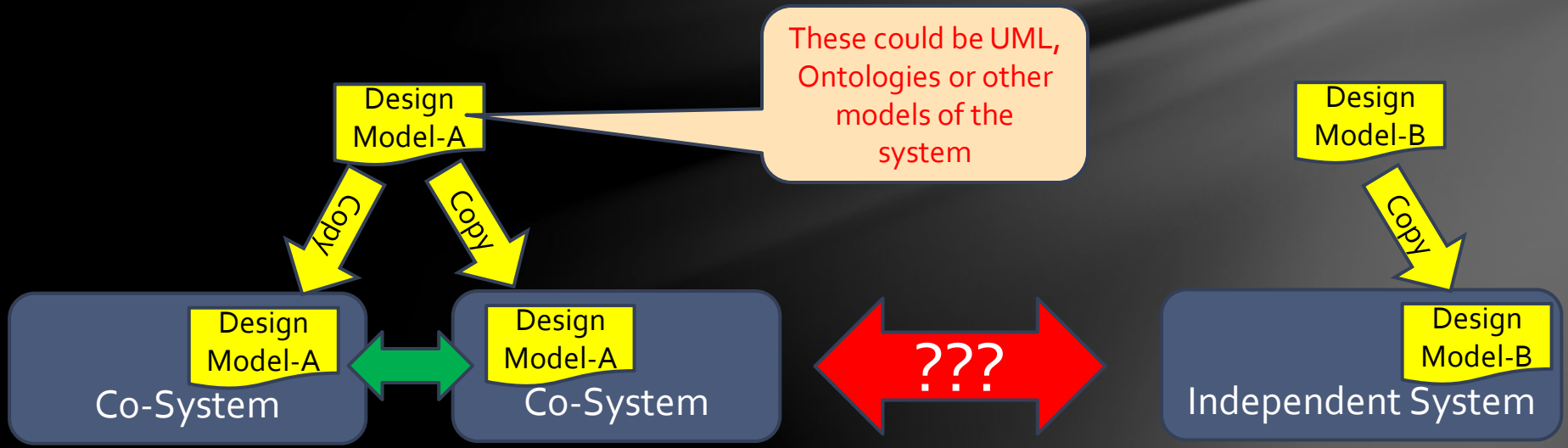
Copyright (c) 2012-2023 Model Driven Solutions, Inc.

Design Models

Design models are (of course) about a specific design – application or system

They fall down when you try and use them to federate designs, integrate systems, share data

Independently designed systems can't be integrated with design models unless every system shares the same design (Designed may be standard interfaces)



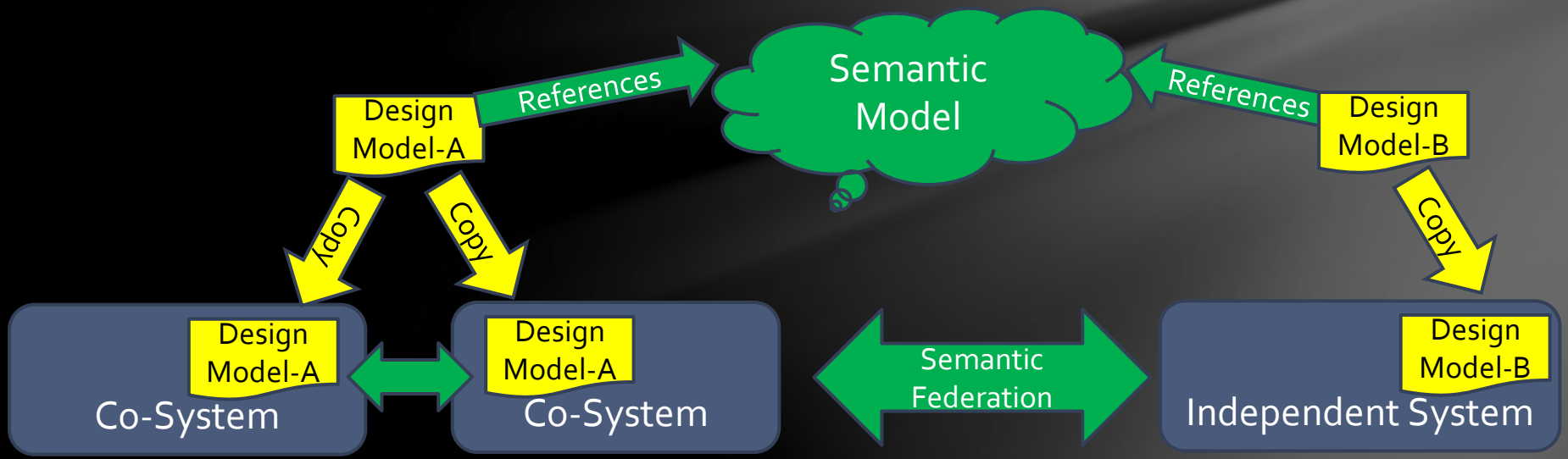
Copyright (c) 2012-2023 Model Driven Solutions, Inc.

Conceptual Reference Models

A reference model provides a library of concepts that "ground" the semantics of the designs

The design model elements represent data about the reference concepts by referencing them

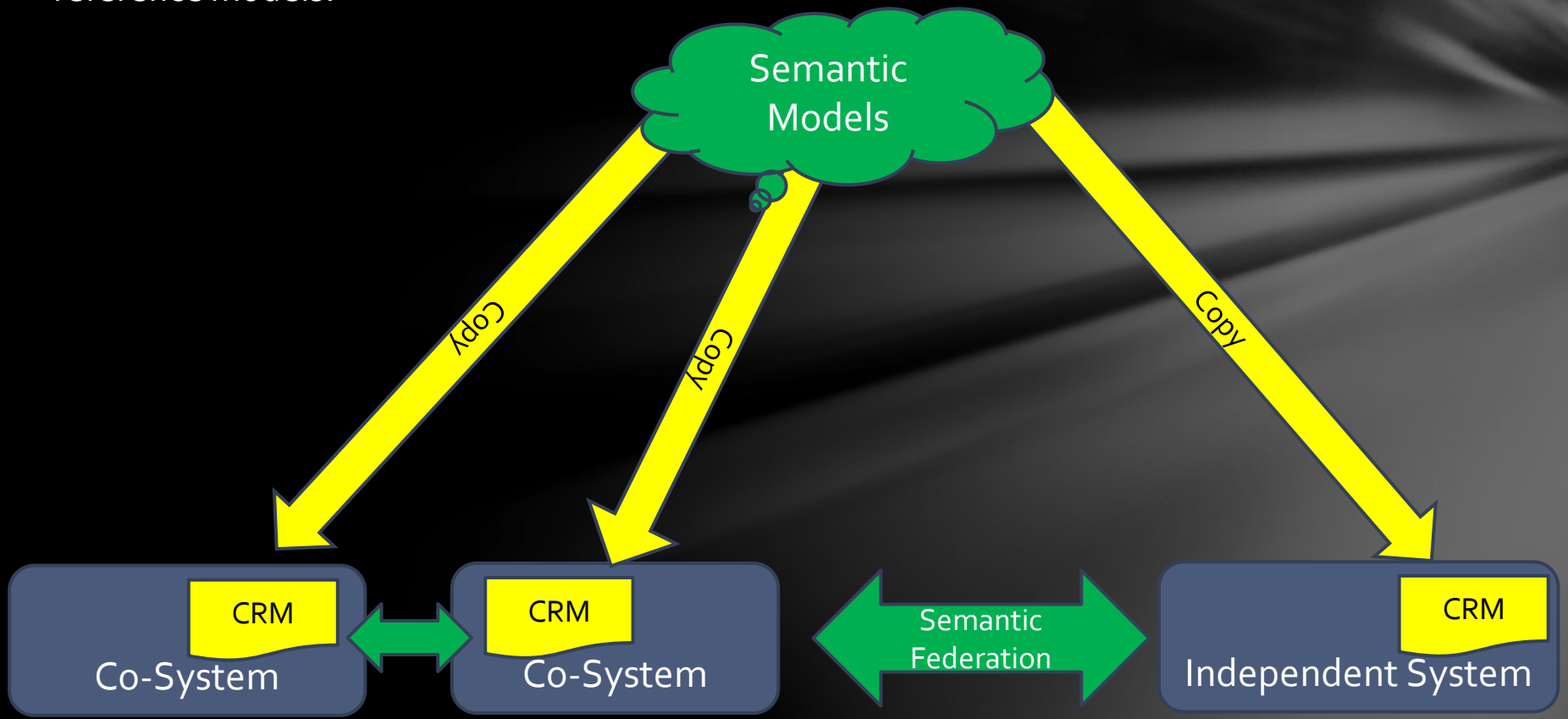
They are not directly coupled with the design – only use what is needed.



Copyright (c) 2012-2023 Model Driven Solutions, Inc.

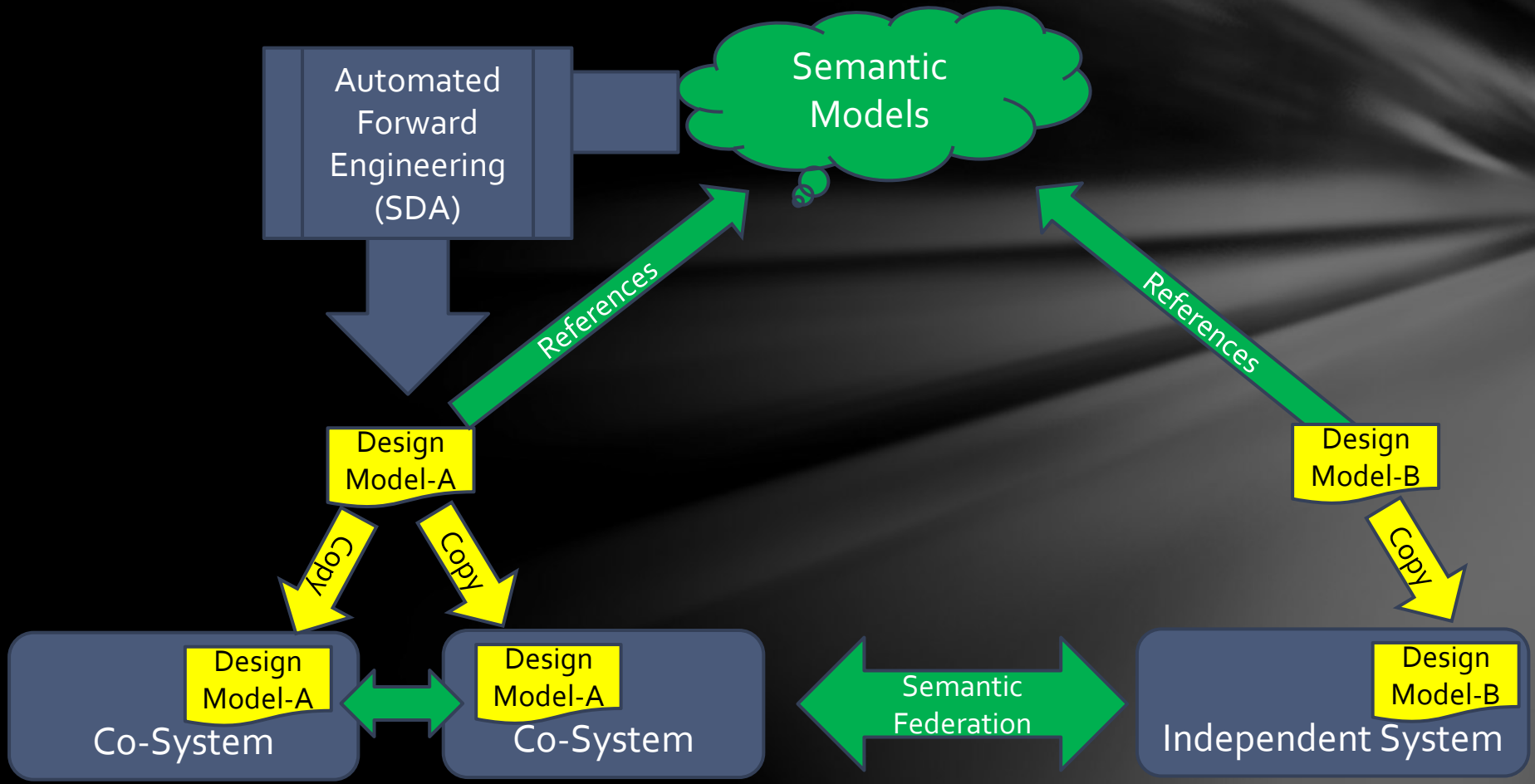
Anti-pattern

Don't couple implementations directly to reference models.



Copyright (c) 2012-2023 Model Driven Solutions, Inc.

This works well

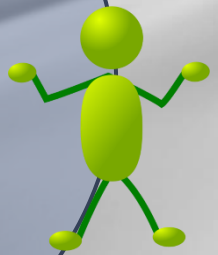


Copyright (c) 2012-2023 Model Driven Solutions, Inc.

Forming a federation space

Integration Space

Semantic
Models



Information Sharing
Systems Integration
Federated Analytics