HÖGSKOLAN I SKÖVDE

EUROPEAN UNION
Internal Security Fund ISF

Enterprise Modeling for Critical Infrastructure Operators

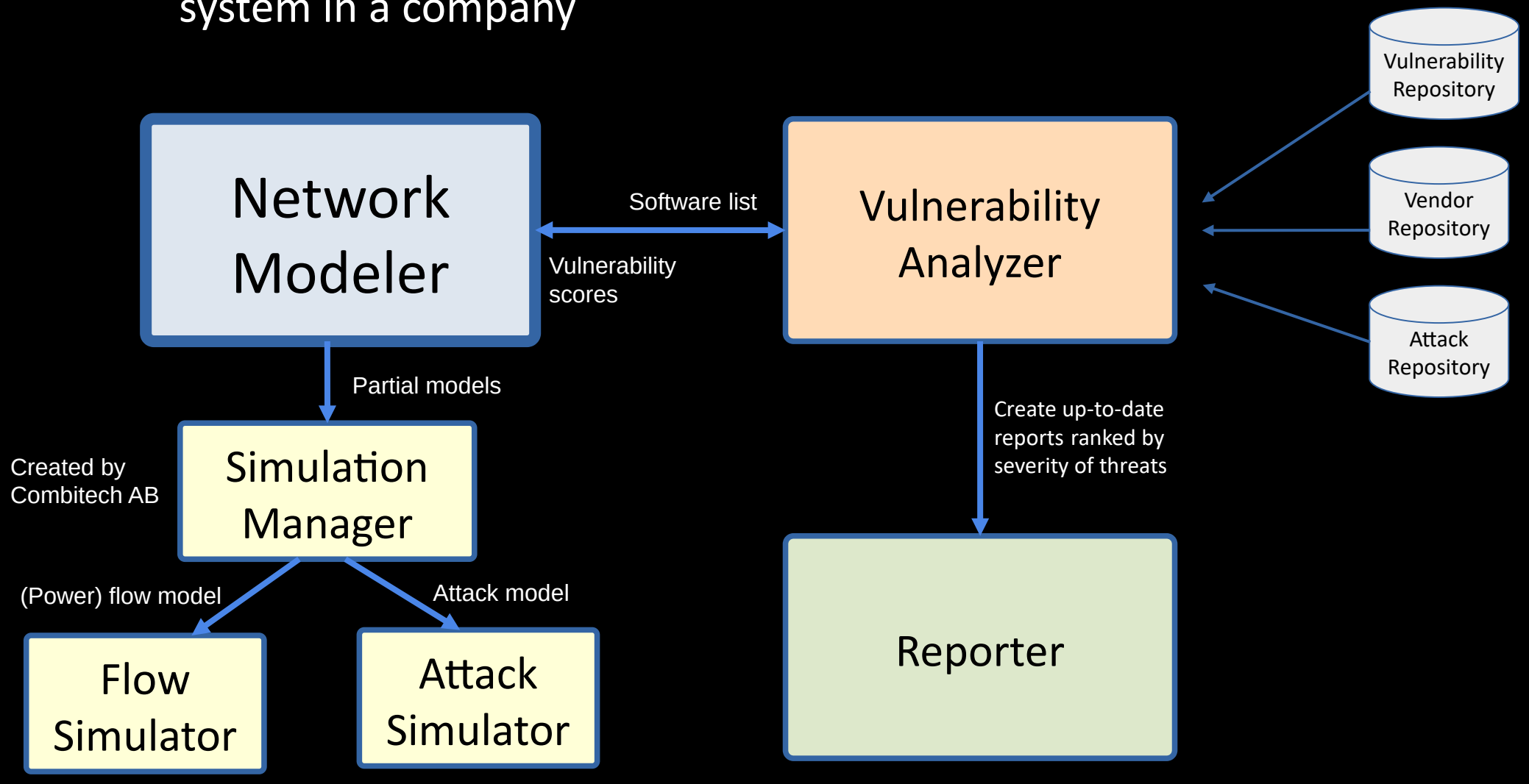
Manfred Jeusfeld *
PICS Seminar Skövde, 2023-04-13
conceptbase.cc/mjf

- ELVIRA architecture
- Taxonomy (ontology) of components
- Creating conceptual models of the power grid
- Computing and visualizing criticality and vulnerability

* with contributions from all ELVIRA project members! See also his.se/elvira

ELVIRA* Architecture

Create a comprehensive "network model" of the IT system in a company



* ELVIRA is now a product of Norgald AB

Ontologies vs. Knowledge Bases vs Databases

- Ontology: emphasize class definitions; consistency checks of the ontology

- Knowledge Bases: Emphasize rules (not just SWRL but also Datalog or production rules). Note that the property 'transitive' cannot be captured in pure first-order logic (OWL is a subset of first-order logic)

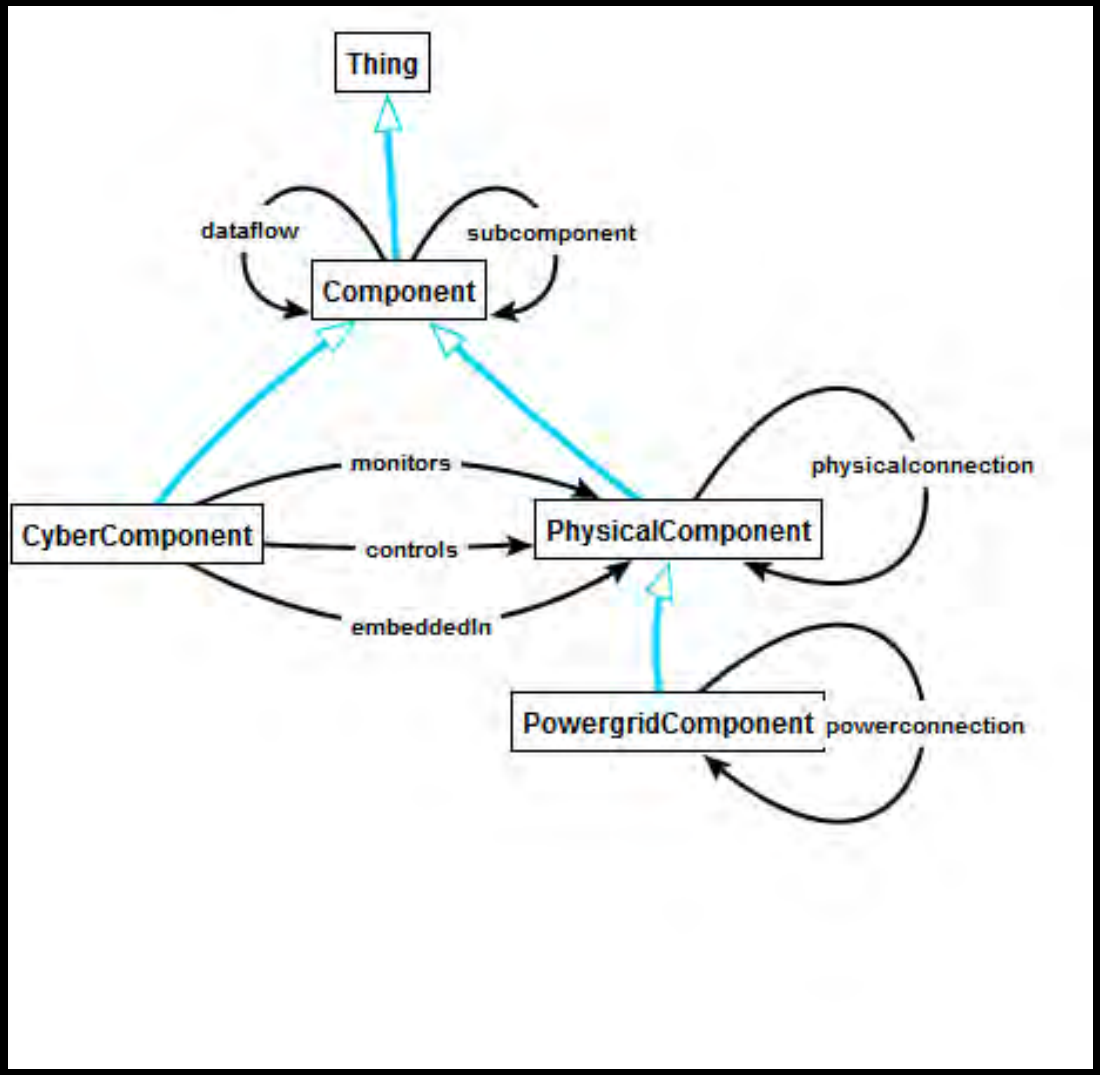
- Databases emphasize the definition of instances (= one possible interpretation of the database schema, A-Box).
  DB schema syntactically corresponds to a T-Box but ontologies are not concerned with data representation issues such as normalization. Further, a DB Schema can violate ontological principles such that some classes are not disjoint.

We eventually decided to use the open-source **ConceptBase** system (conceptbase.cc) because it allows to represent meta classes, classes, and instances in a uniform way. It also has a sophisticated query language to analyze large (graphical) models.

Taxonomy (Ontology) of Components

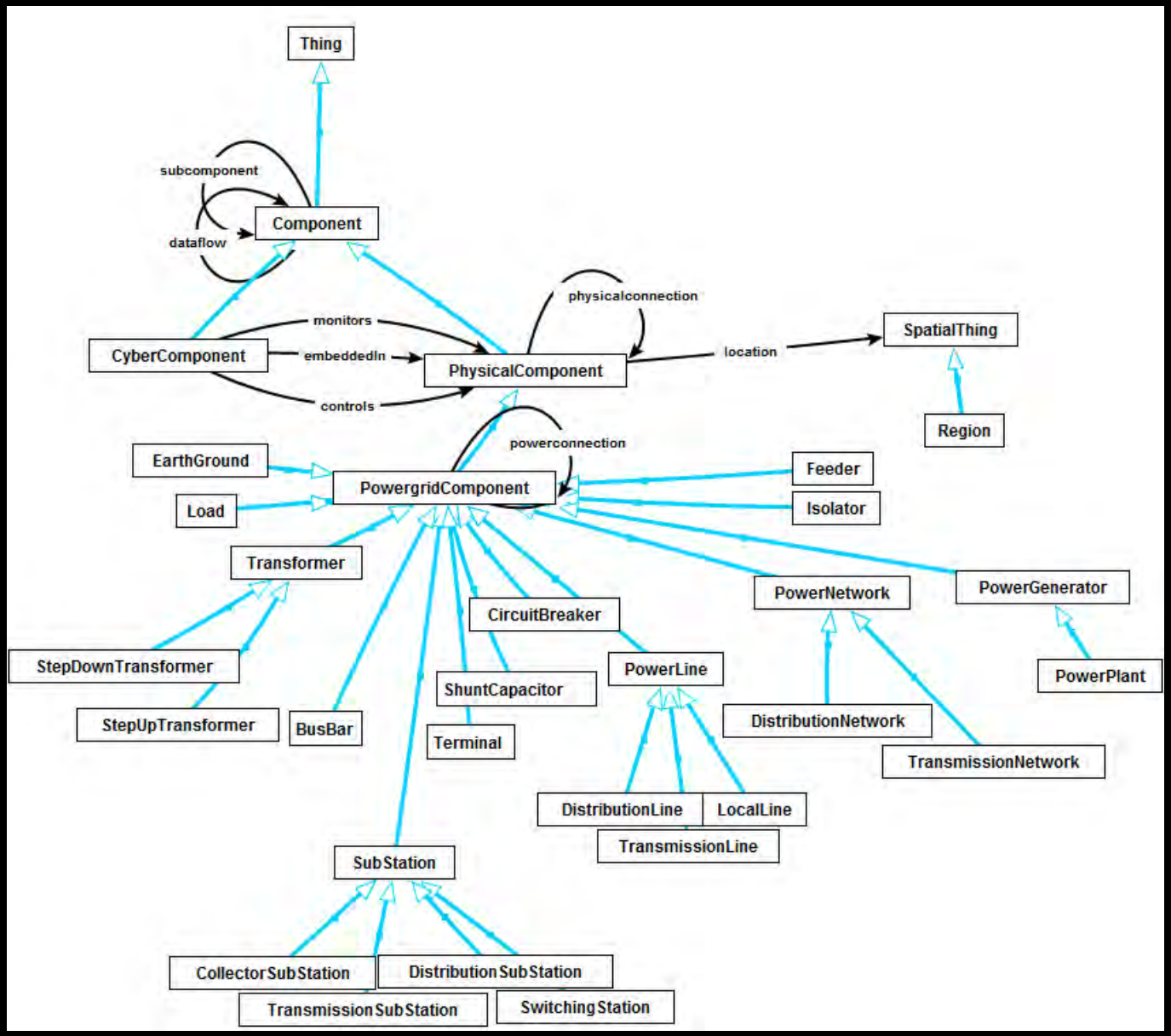
- represent both power components and IT (“cyber”) components
- create a taxonomy of these components but also of their possible relations (power connections, data flows, ...)
- the ontology is augmented by rules to analyze an example power grid model
- use a single central server to maintain the ontology

Taxonomy of Components: Top View



Only top-level shown here.
Blue links denote subclasses.
Black links denote associations.

Powergrid Components

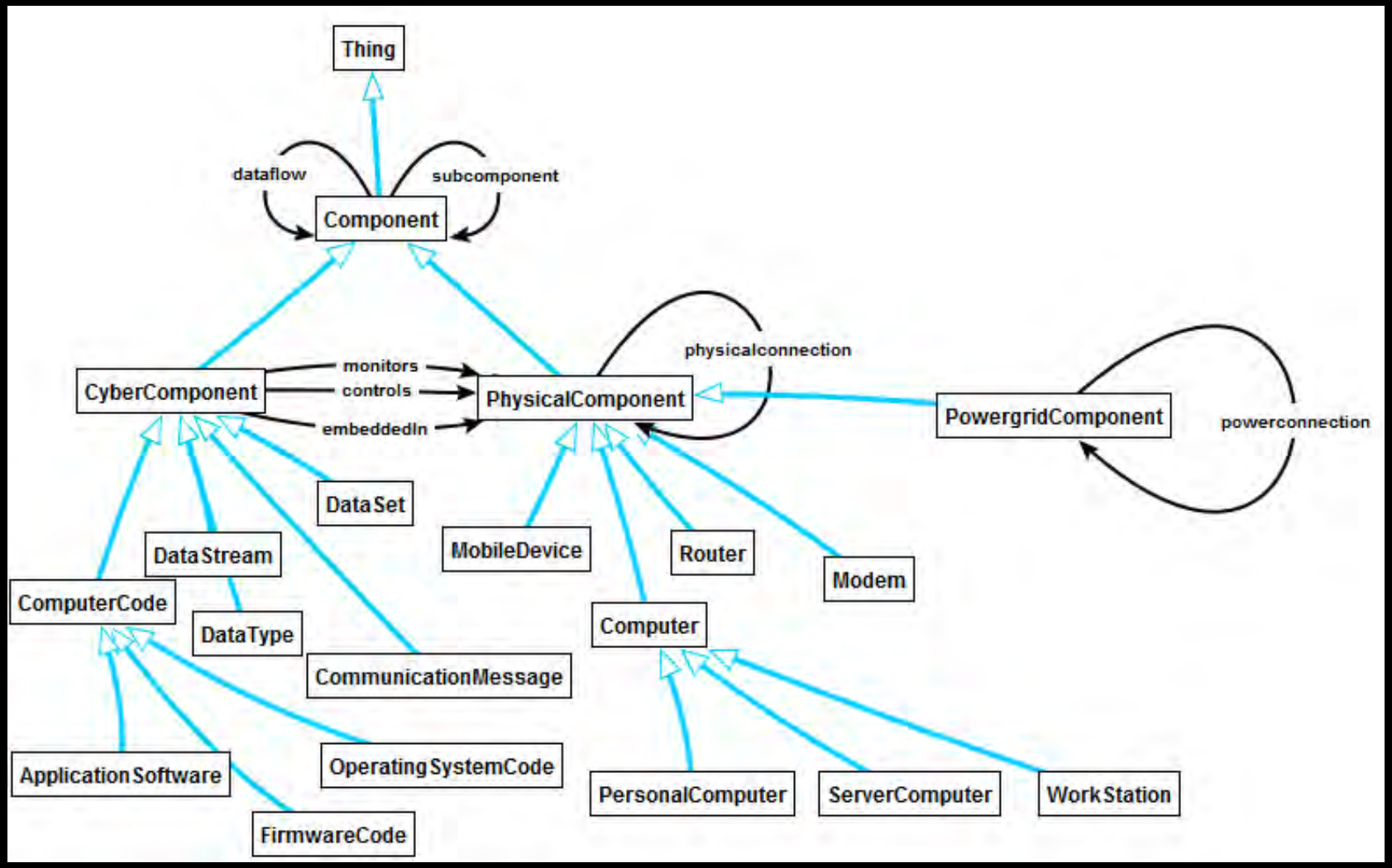


This taxonomy also is the schema for describing example powergrids (e.g. Nordic32)

Rules for the Power Grid

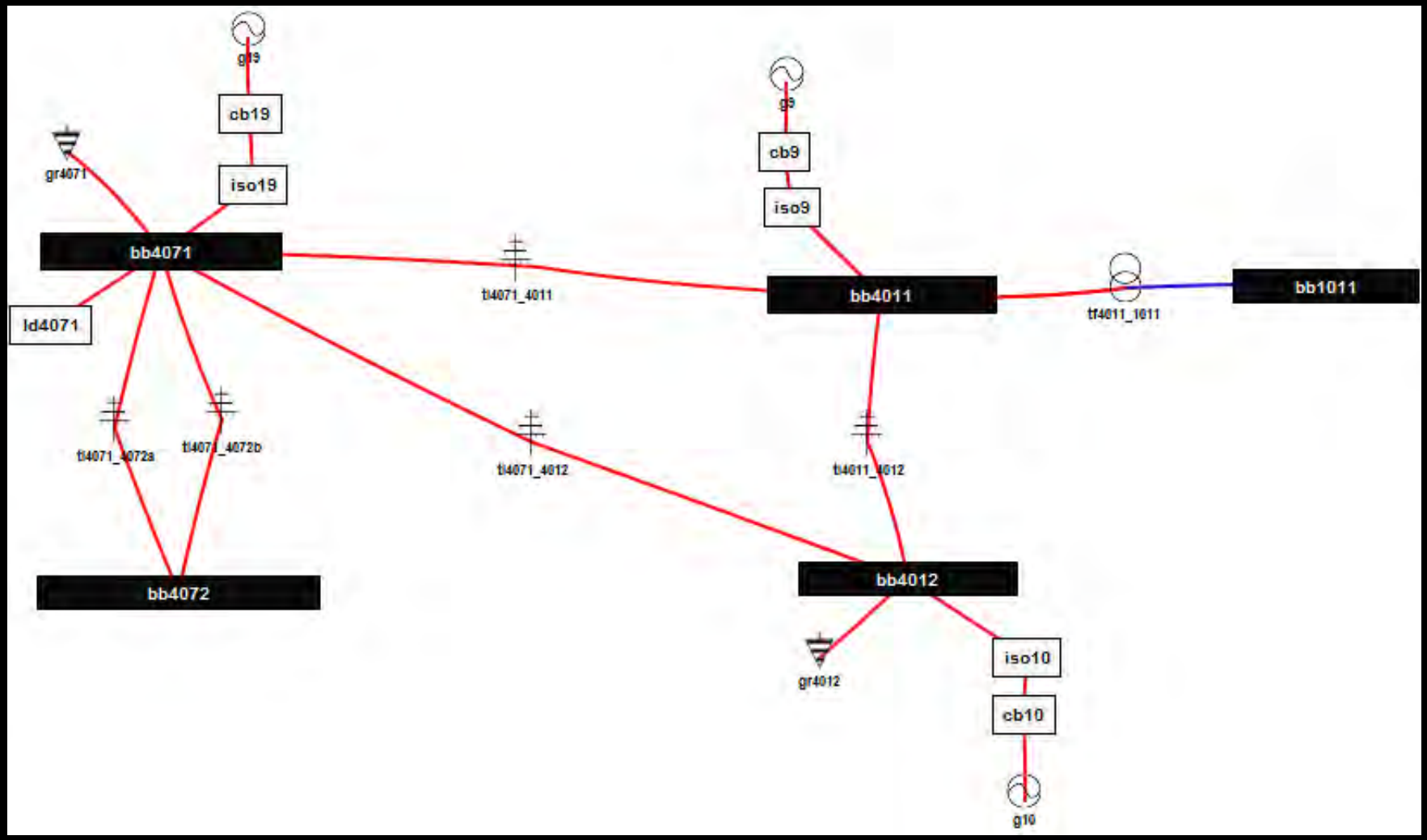
```
PowergridComponent in Class isA PhysicalComponent with
  attribute
    powerconnection : PowergridComponent;
    nominalvoltage : String;
    nominalfrequency : String
  rule
    voltrule : $ forall p1,p2/PowergridComponent v/String
                ((p1 powerconnection p2)  or (p2 powerconnection p1)) and (p1 nominalvoltage v)  and
                  not (p1 in Transformer) and not (p2 in Transformer) ==> (p2 nominalvoltage v) $
end

Transformer in Class isA PowergridComponent with
  attribute
    lowervoltage : String;
    uppervoltage : String
  rule
    voltrule1 : $ forall t/Transformer pc1,pc2/PowergridComponent v1,v2/String
                          (pc1 nominalvoltage v1) and (pc2 nominalvoltage v2) and (v1 < v2)
                      ==> (t lowervoltage v1) $;
    voltrule2 : $ forall t/Transformer pc1,pc2/PowergridComponent v1,v2/String
                          (pc1 nominalvoltage v1) and (pc2 nominalvoltage v2) and (v1 < v2)
                      ==> (t uppervoltage v2) $
end
```

Cyber Components



Cyber components are embedded in physical components. Some are used to monitor and to control them. Taxonomy is extensible at any time.

Nordic32 Power Grid as instance of the taxonomy



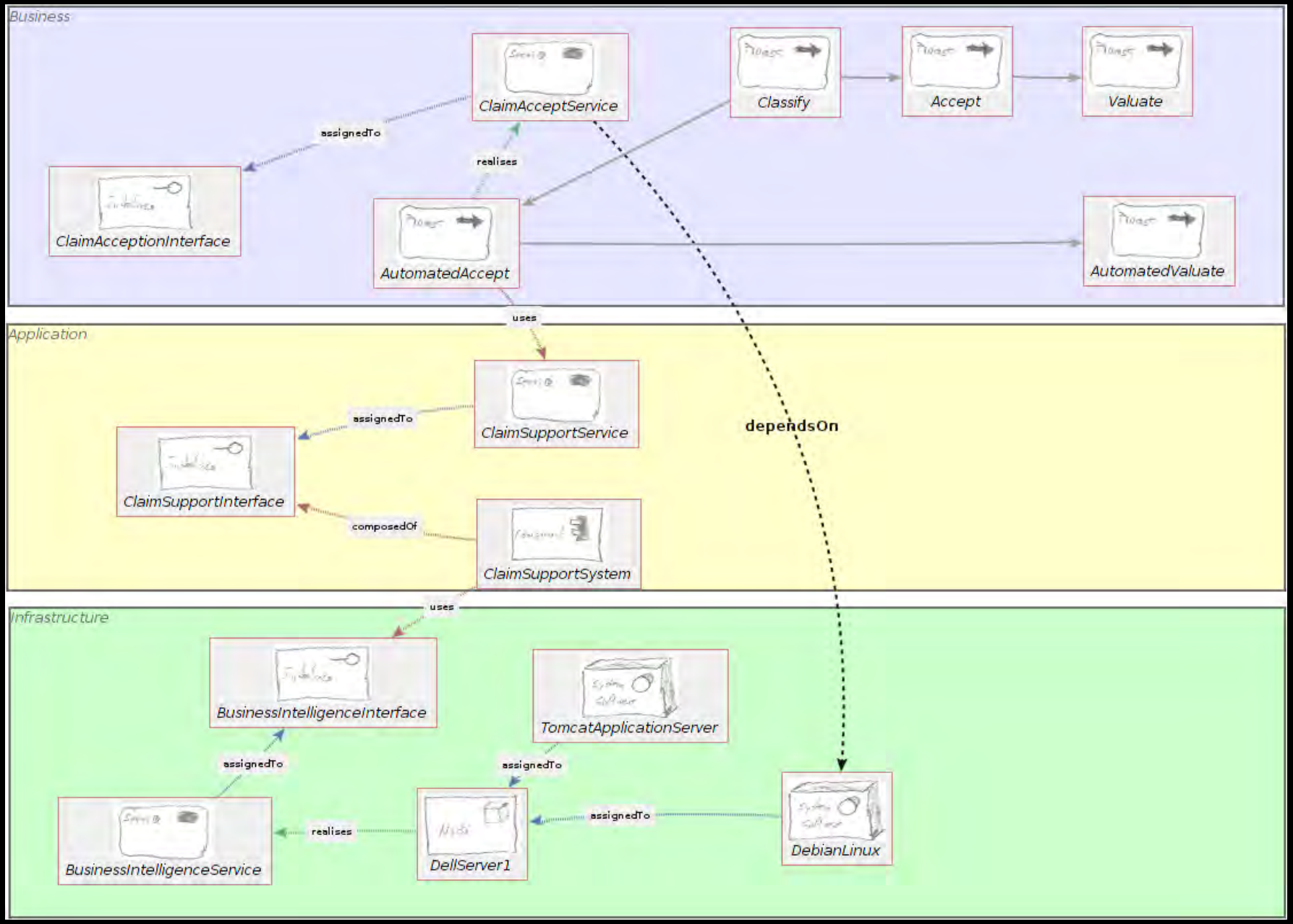
Black rectangles symbolize ‘bus bars’: massive copper components to link power components.
Power genarators: g19, g9, g10
Transformer: tf4011_1011
Power lines

Relation of W7 to Enterprise Architectures (Zachman Framework)

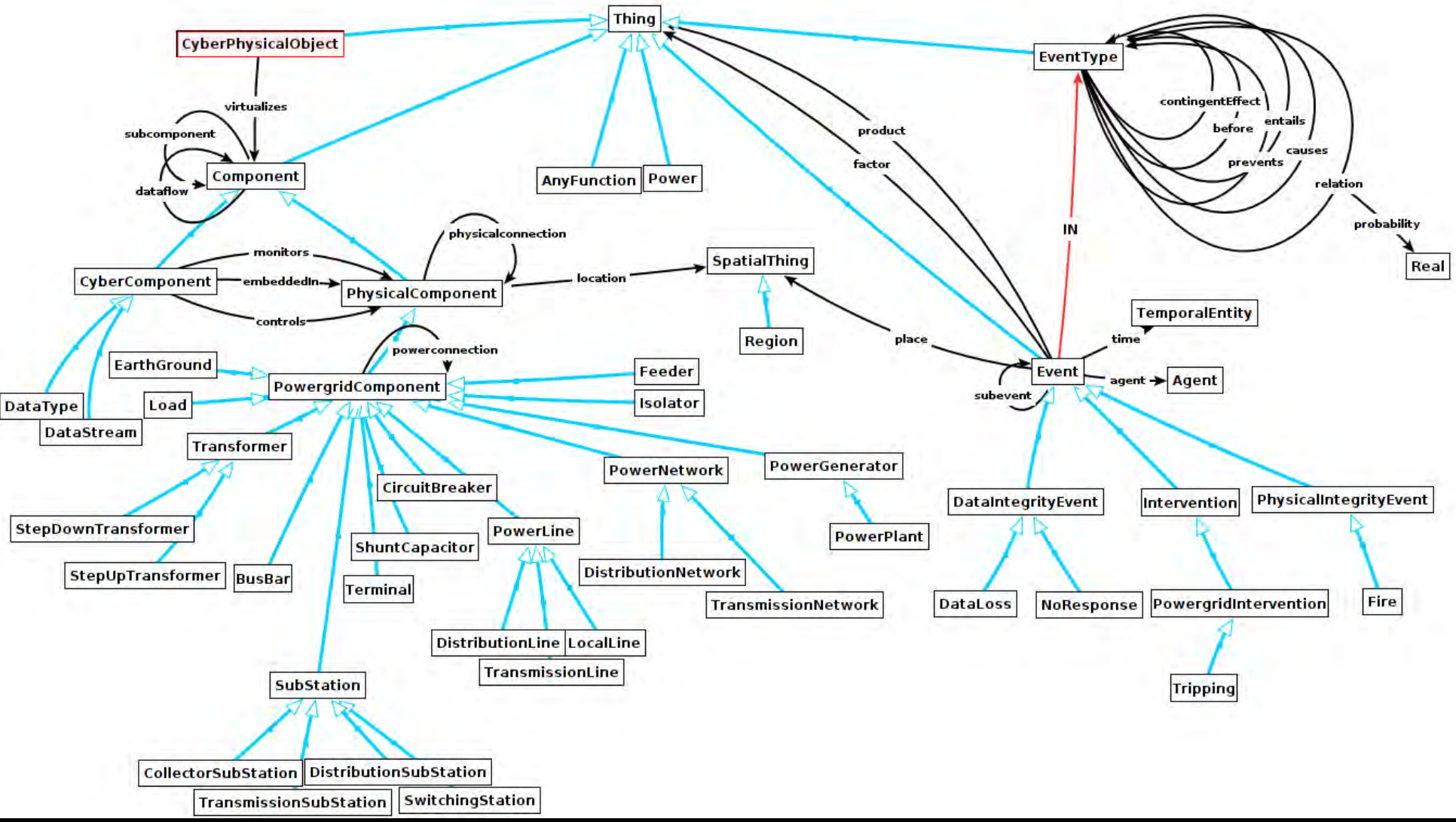
abstractions / perspectives	DATA *What*	FUNCTION *How*	NETWORK *Where*	PEOPLE *Who*	TIME *When*	MOTIVATION *Why*
SCOPE *Planner* contextual	List of Things - *Important to the Business*	List of Processes - *the Business Performs*	List of Locations - *in which the Business Operates*	List of Organizations - *Important to the Business*	List of Events - *Significant to the Business*	List of Business Goals and Strategies
ENTERPRISE MODEL *Owner* conceptual	e.g., Semantic Model	e.g., Business Process Model	e.g., Logistics Network	e.g., Work Flow Model	e.g., Master Schedule	e.g., Business Plan
SYSTEM MODEL *Designer* logical	e.g., Logical Data Model	e.g., Application Architecture	e.g., Distributed System Architecture	e.g., Human Interface Architecture	e.g., Processing Structure	e.g., Business Rule Model
TECHNOLOGY CONSTRAINED MODEL *Builder* physical	e.g., Physical Data Model	e.g., System Design	e.g., Technical Architecture	e.g., Presentation Architecture	e.g., Control Structure	e.g., Rule Design
DETAILED REPRESEN-TATIONS *Subcontractor* out-of-context	e.g. Data Definition	e.g. Program	e.g. Network Architecture	e.g. Security Architecture	e.g. Timing Definition	e.g. Rule Specification
FUNCTIONING ENTERPRISE	DATA Implementation	FUNCTION Implementation	NETWORK Implementation	ORGANIZATION Implementation	SCHEDULE Implementation	STRATEGY Implementation

Large overlap with W7, only 'which' dimension missing (is implicit in the technology model)

ArchiMate: a simple Enterprise Architecture framework



Full ELVIRA Ontology



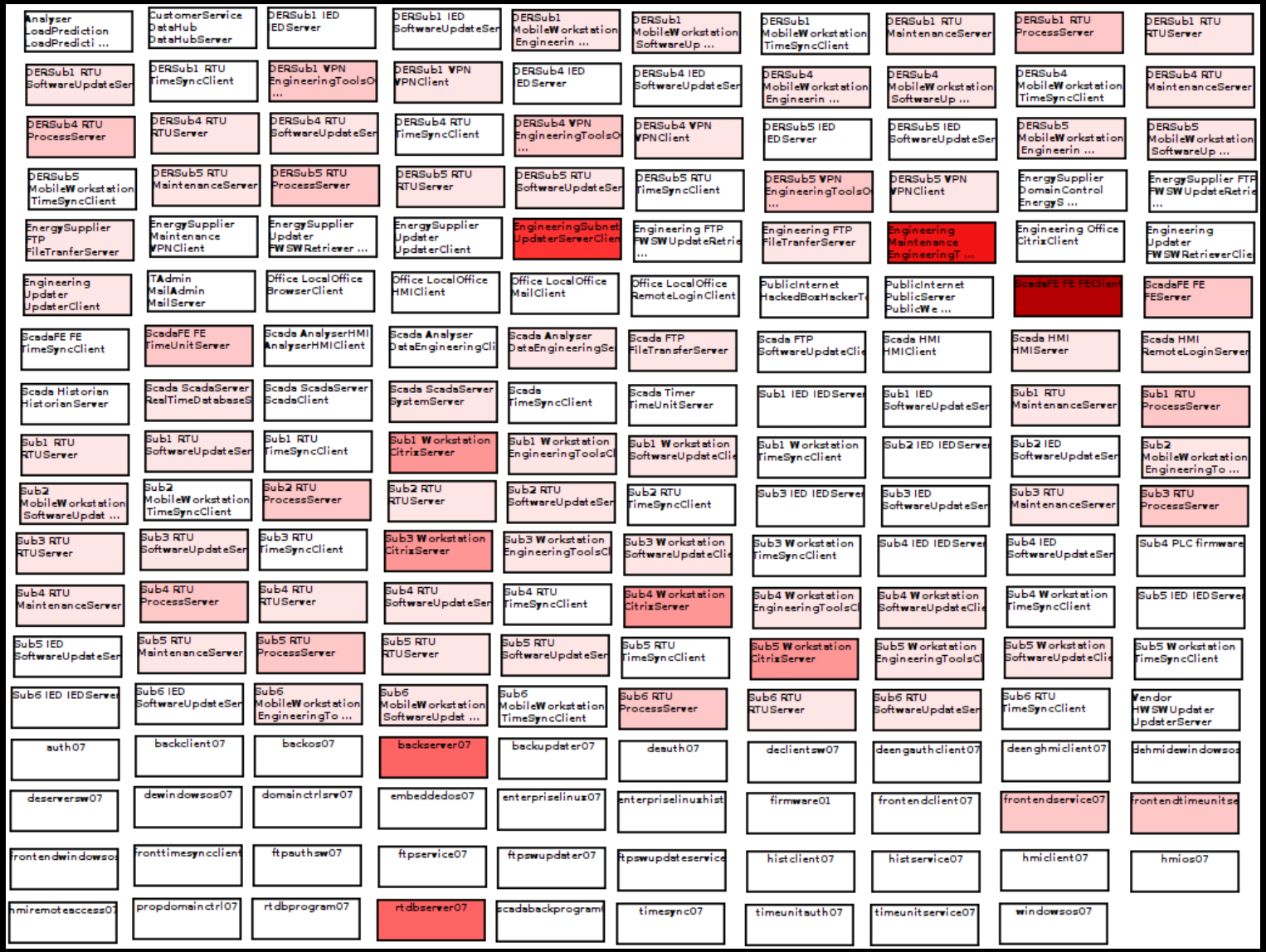
Computing Criticality and Vulnerability Scores of Components

- A set of rules describes when a component c2 directly depends on a component c1 (for example, if c1 send control messages to c2)
- Form the transitive closure of ‘dependsOn’, i.e. if (c3 depends on c2) and (c2 dependsOn c1), then (c3 dependsOn c1)
- Criticality of a component c can then be expressed as the number of compenents That depend on c

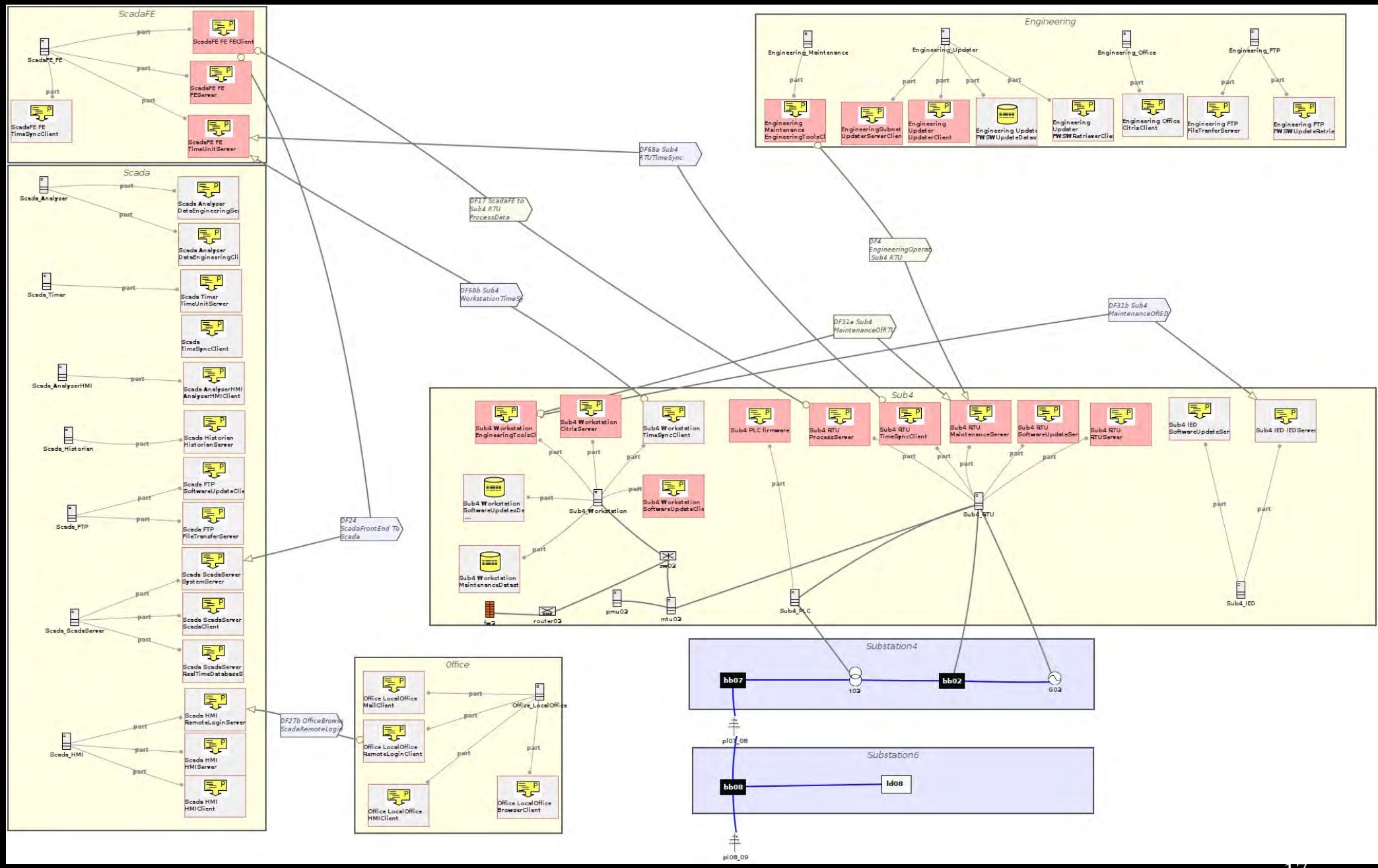
This simple metric can then be combined with other metrics, such as the vulnerability score of a software component according to data from CVE/NVD/CVSS to identify critical components that are also vulnerable

Score(c) = Criticality(c) * Vulnerability(c)

Heatmap of critical (software) components



Critical components highlighted in the network model



Future work

- Need to add the business layer to the enterprise model to cover critical processes such as trading,billing, finance, which are needed for the primary process (here energy supply)

- Measure likely disruption of business functions by linking software assets to the business processes

Journal paper

Y. Jiang, M.A. Jeusfeld, J. Ding, E. Sandahl: Model-Based Cybersecurity Analysis - Extending Enterprise Modeling to Critical Infrastructure Cybersecurity. Appears in Business & Information Systems Engineering (BISE), 2023, postprint available upon request. BISE is an AIS-affiliated journal published by Springer.

Commercial tool

- Norgald AB (norgald.com) commercializes the ELVIRA toolset

Questions?

Contact: manfred.jeusfeld@his.se