Link-failure assessment in redundant ICS networks supported by the Interconnected-asset Ontology (IO)

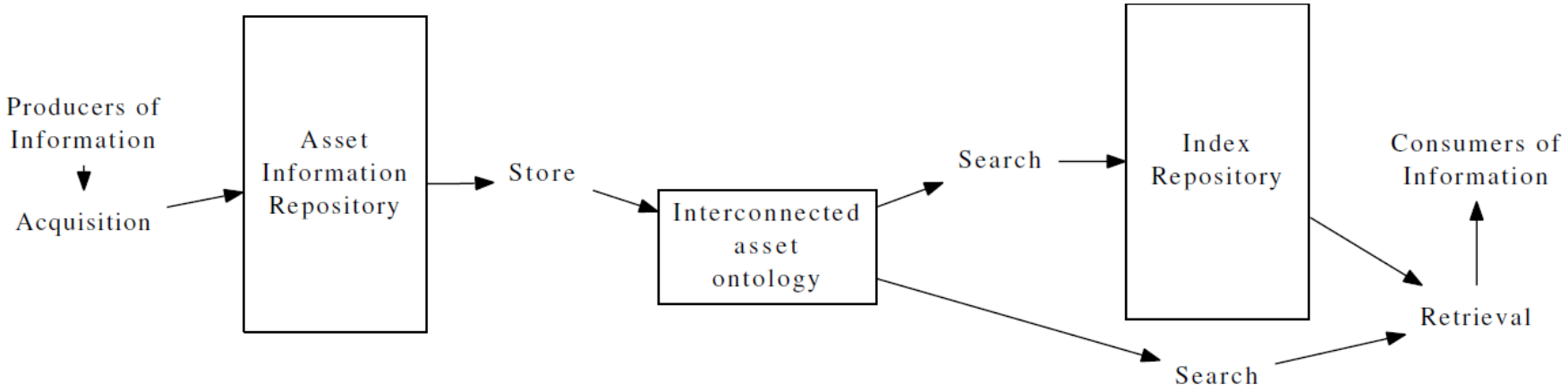
henk.birkholz@sit.fraunhofer.de

CASED

Fraunhofer SIT

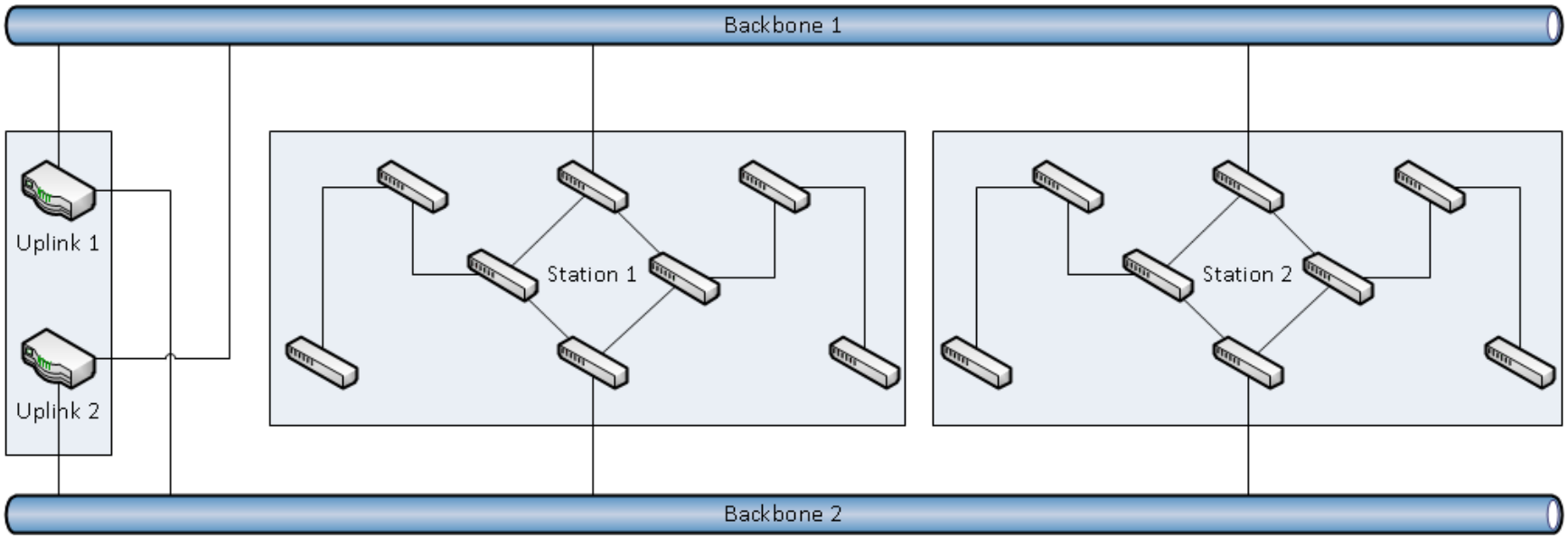
IO processes

- The Interconnected-asset Ontology (IO) is the tool used to **acquire** information about a network directly from its components or indirectly from management tools (producer of information), to **aggregate and associate** it, and to **provide** it to automatic post-processes (consumer of information)
- The acquisition process takes into account the continuous change of infrastructure and is designed to update the IO in intervals



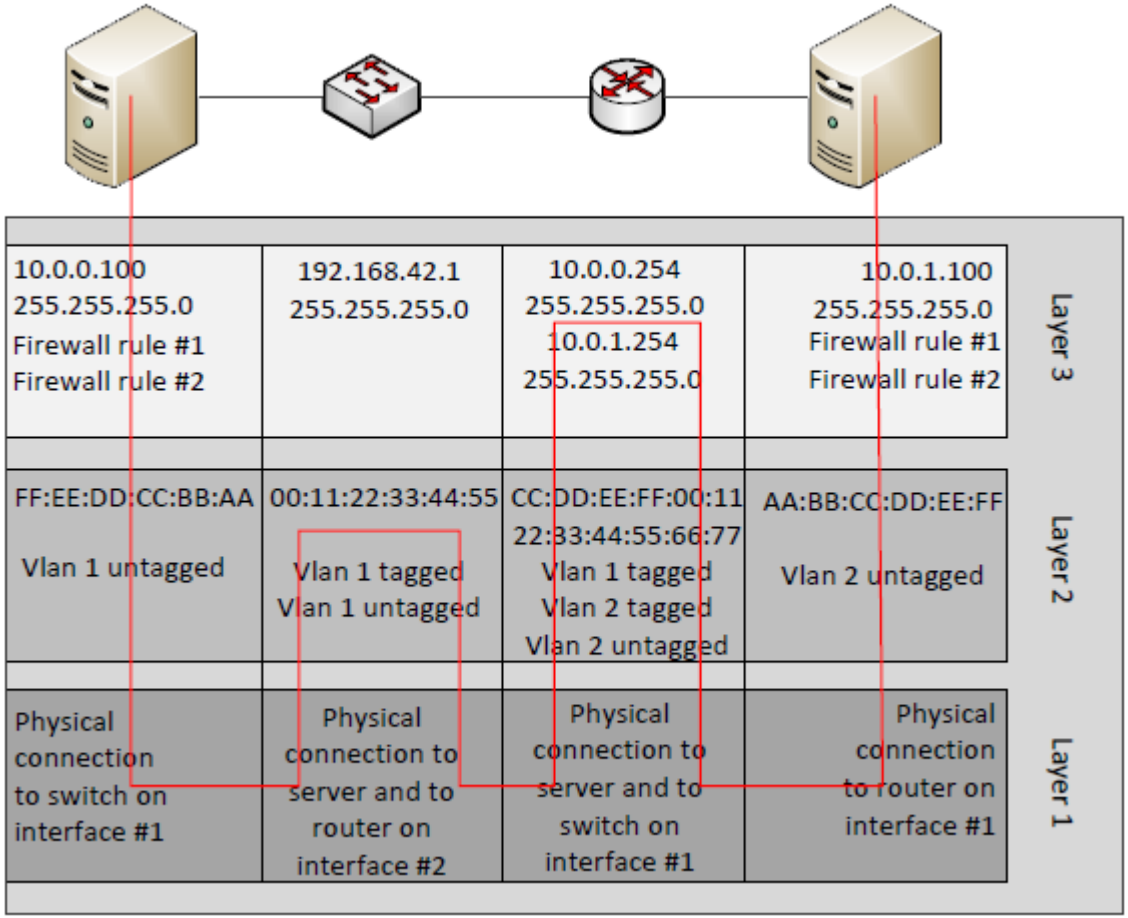
Topologies composed of endpoints

- The IO-framework aggregates endpoint **configuration** and **state** attributes in a semantic **property graph** with **description logic** (Ontology in OWL format)
- "The **network**" is an **implicit information** derived from the constitution of configuration and state of every involved endpoint

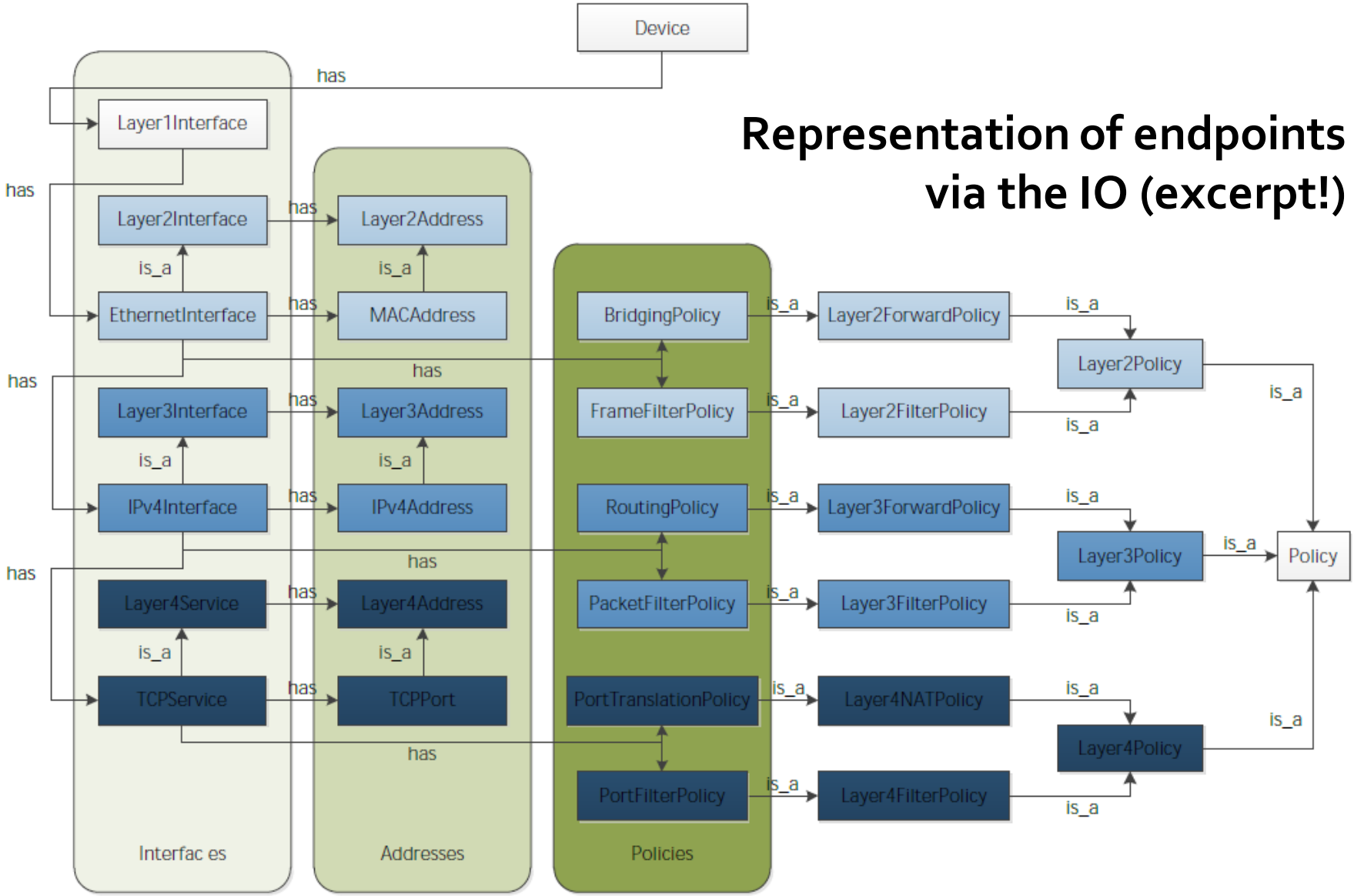


Example: network paths traversing endpoints

- Network paths can be inferred out of the sum of all endpoints composing the topology
- E.g.: inference of layer 2 **broadcast domains**
- E.g.: **redundant paths** between endpoints -> basis **for link-failure assessment** -> basis for **service availability**



Representation of endpoints via the IO (excerpt!)



Redundancy assessment

- Proof-of-Concept is based on a single ICS Ethernet broadcast domain composed by **192 endpoints** with **2730 ports,** providing **208 active links**. RSTP and link over-provisioning are used to increase resilience
- Proof-of-concept: **All possible paths** between all pairs (or a pair) of endpoints (nodes) are acquired via a modified breadth first search
- From this result set**, KPI** regarding **resilience** can be derived. KPI are generated for nodes**,** links and resulting paths.
- KPI illustrated by a given pair of nodes:
  - Number of paths per pair of nodes (4/2/1)
  - Number of redundant links on paths (12/3/0)
  - Cumulative path length (24/5/3)
  - Non-redundant links per pair of nodes (0/1/3)
- Absolute number of line of codes required to implement proof-of-concept: 681
- The approach can be applied to virtually every network related domain/layer including service availability assessment