University of BRISTOL

Managing Cyber Security in Industrial Control Systems using the Viable System Model

Theodoros Spyridopoulos

Supervisors: Dr. Theo Tryfonas

Dr. Anders Johansson

Support from EPSRC and IDC in Systems in gratefully acknowledged.

SC SYSTEMS CENTRE

University of BRISTOL

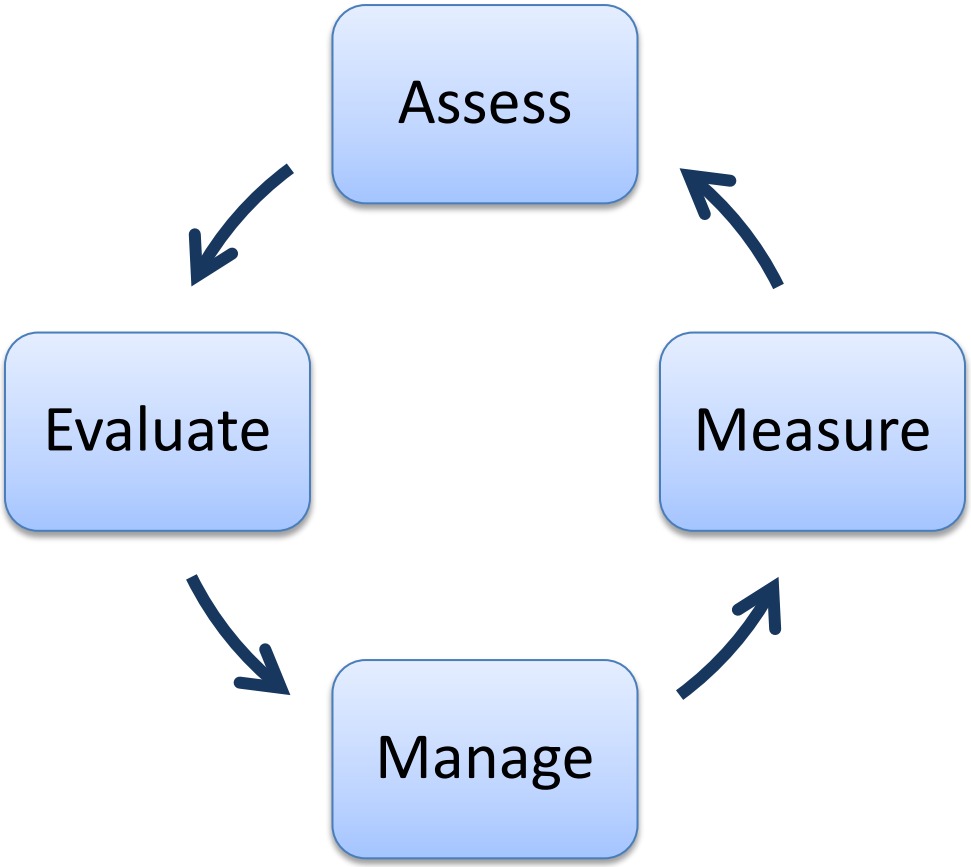
Purpose and Objectives

- Enhance traditional Risk Management methods for Critical Infrastructure and improve Cyber Security.
- ➢ Construct an ITsecurity-oriented Viable System Model for Industrial Control Systems.
- ➢ Determine in more detail the assets of the system that have to be secured.
- ➢ Explore interactions between the different parts of the organisation that affect Cyber Security.

SC SYSTEMS CENTRE

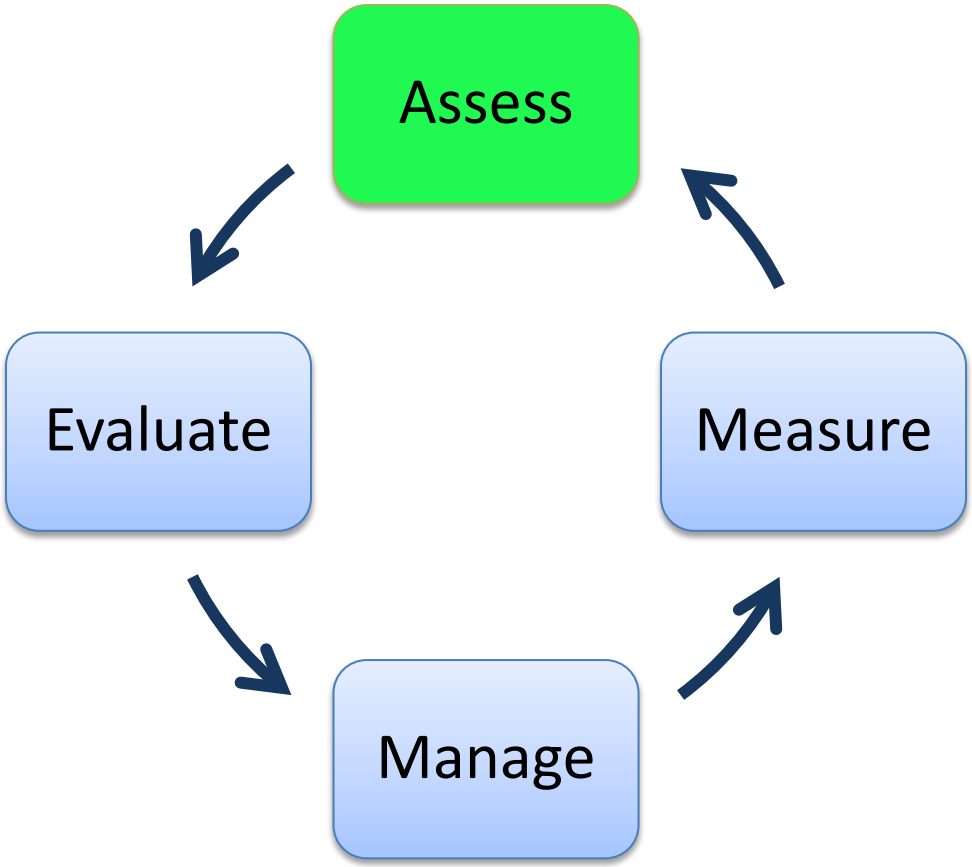
University of BRISTOL

Traditional IT Risk Management for ICSs



University of BRISTOL

Traditional IT Risk Management for ICSs

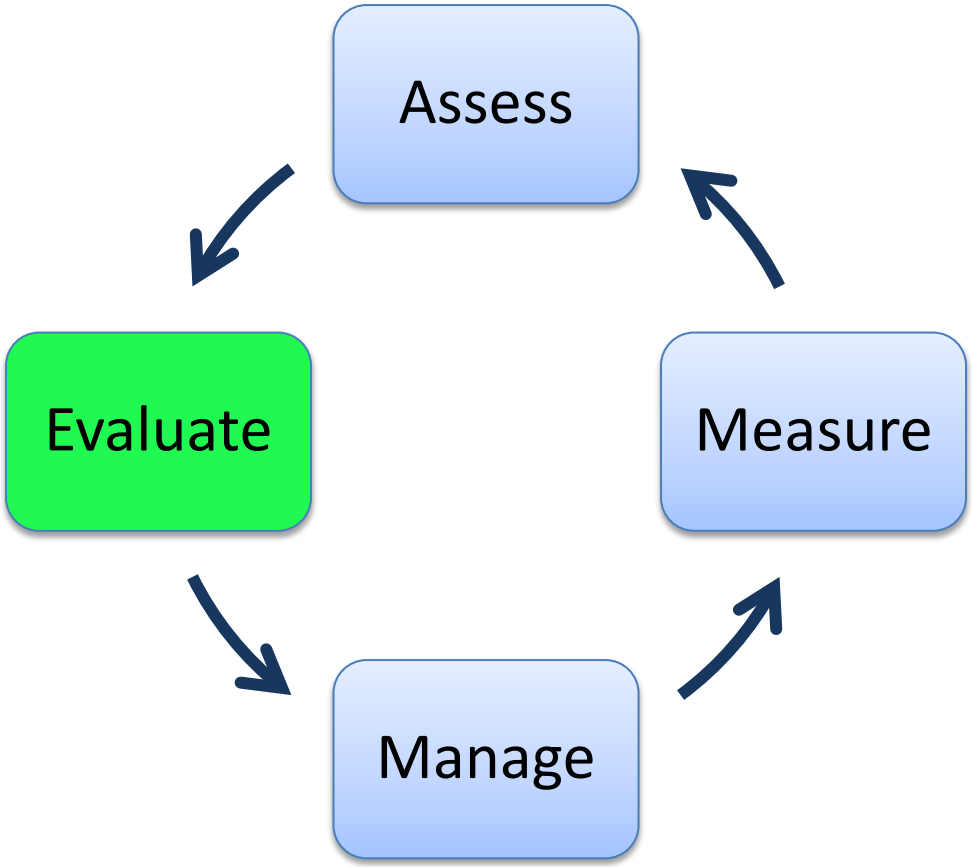


Risk Assessment (NIST [1])

- **Step 1:** System Characterisation
  - Gathering of system's information
- **Step 2:** Threat Identification
  - Source, motivation and actions
- **Step 3:** Vulnerability Identification
  - System security testing
  - Security requirements list
- **Step 4:** Control Analysis
  - Control methods and techniques
- **Step 5:** Likelihood determination
- **Step 6:** Impact Analysis

University of BRISTOL

Traditional IT Risk Management for ICSs

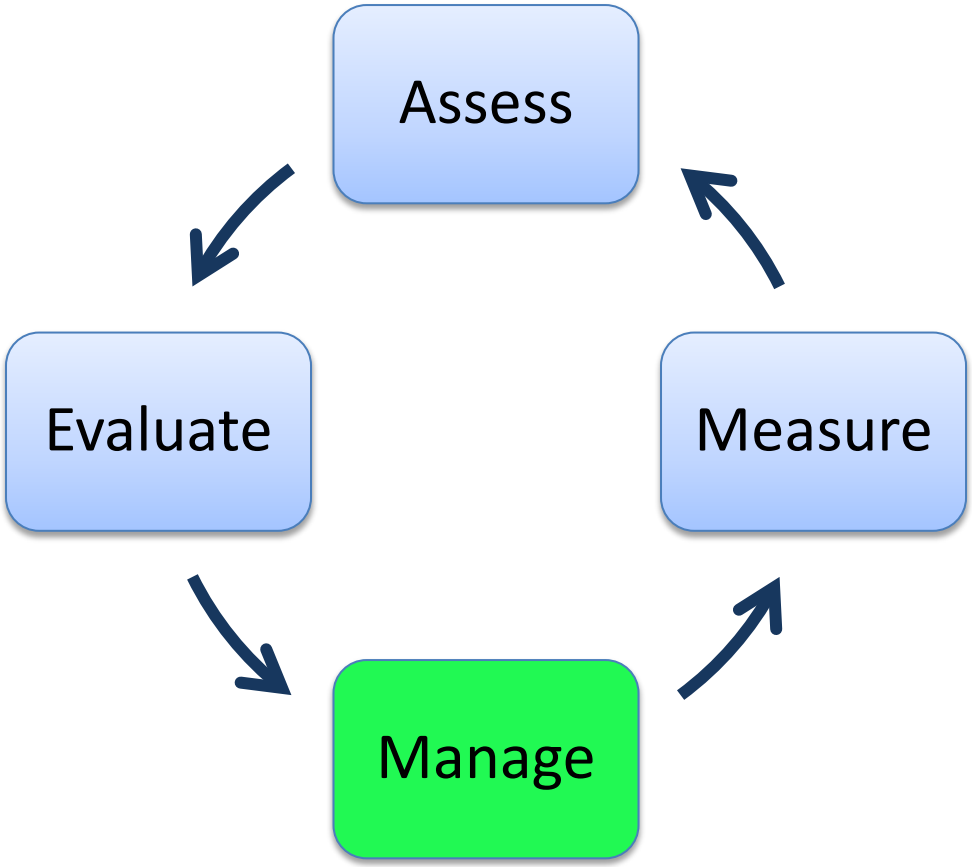


Risk Evaluation (NIST [1])

- **Step 7:** Risk Determination (Risk-level matrix)
- **Step 8:** Control Recommendations
- **Step 9:** Results Documentation

University of BRISTOL

Traditional IT Risk Management for ICSs

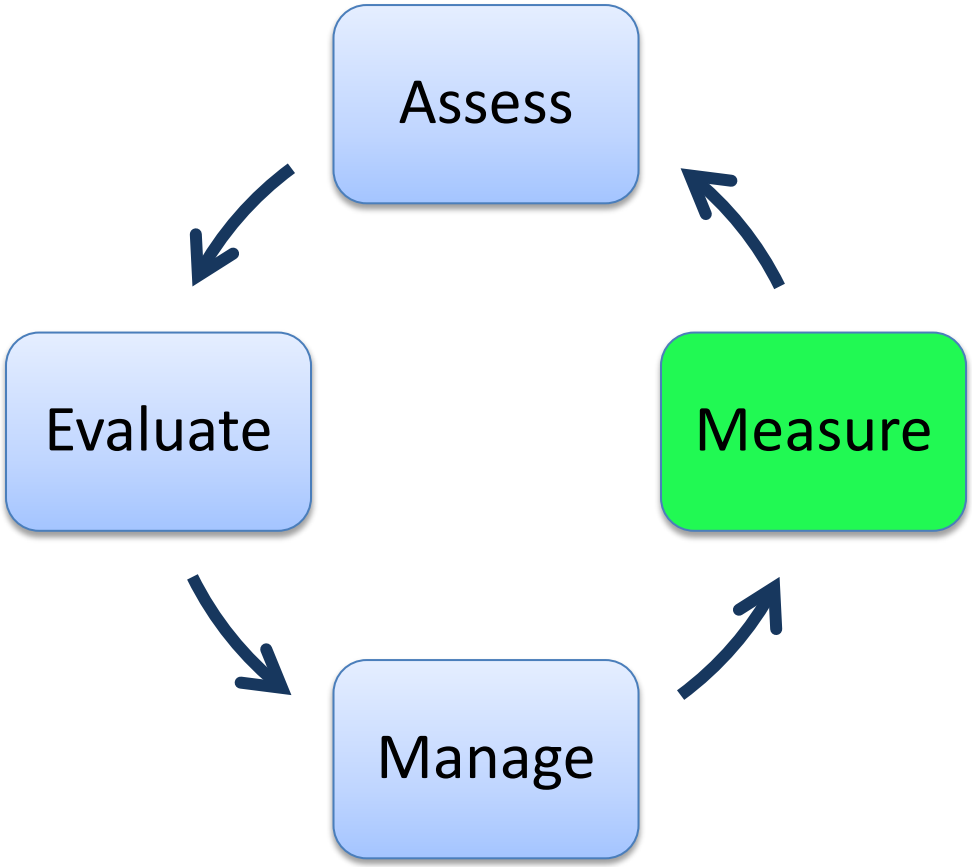


Risk Mitigation (NIST [1])

- Involves prioritizing, evaluating, and implementing the appropriate risk-reducing controls recommended from the risk assessment process.
- Cost-benefit mitigation strategies can be used in situations where the cost of eliminating the risk becomes very high.

University of BRISTOL

Traditional IT Risk Management for ICSs



Evaluation of new Risk (NIST [1])

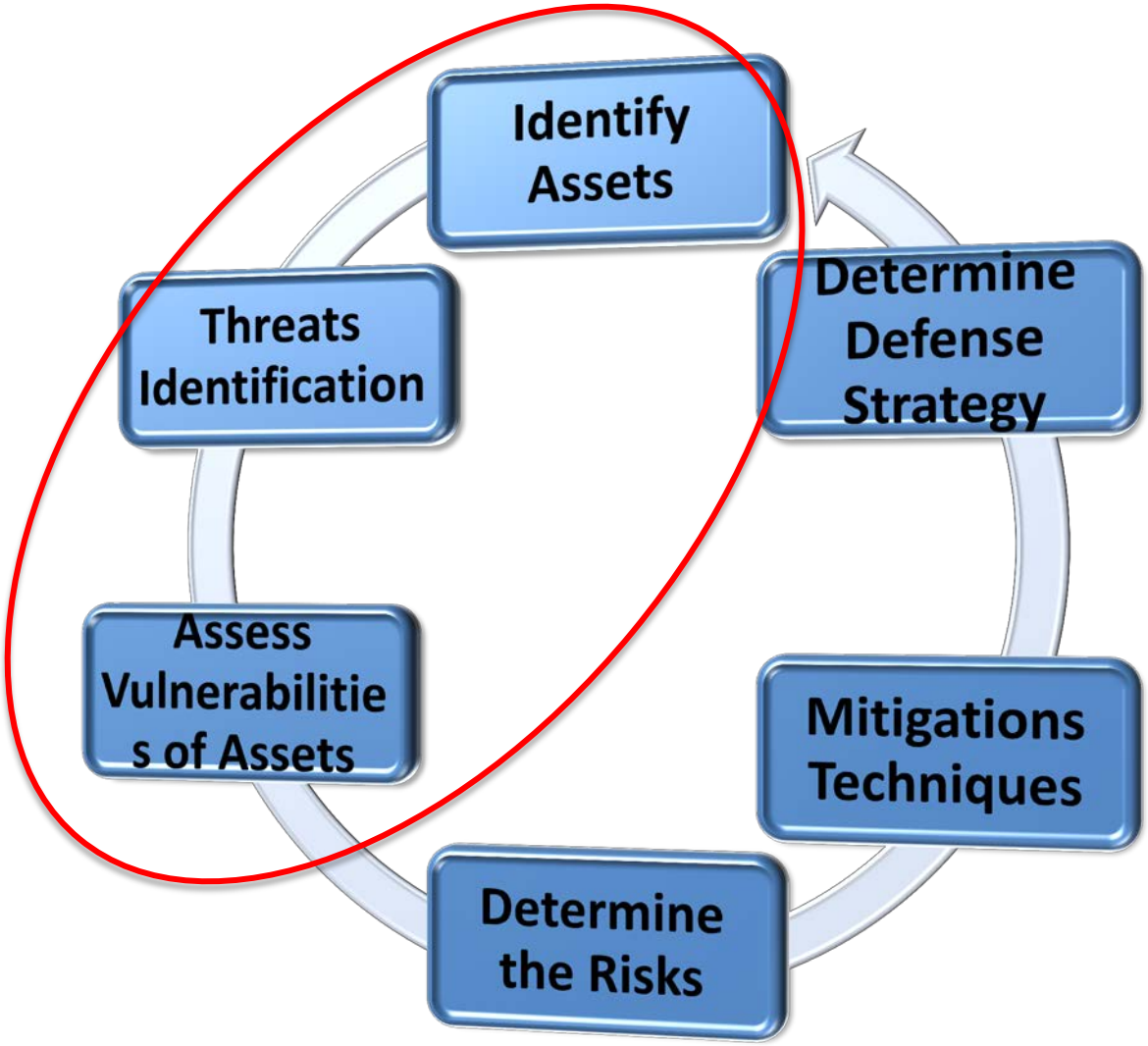
- Evaluate the new risk after mitigation strategies have been applied.
- Assessment process should be repeated at least every 3 years.

University of BRISTOL

Traditional IT Risk Assessment for ICSs

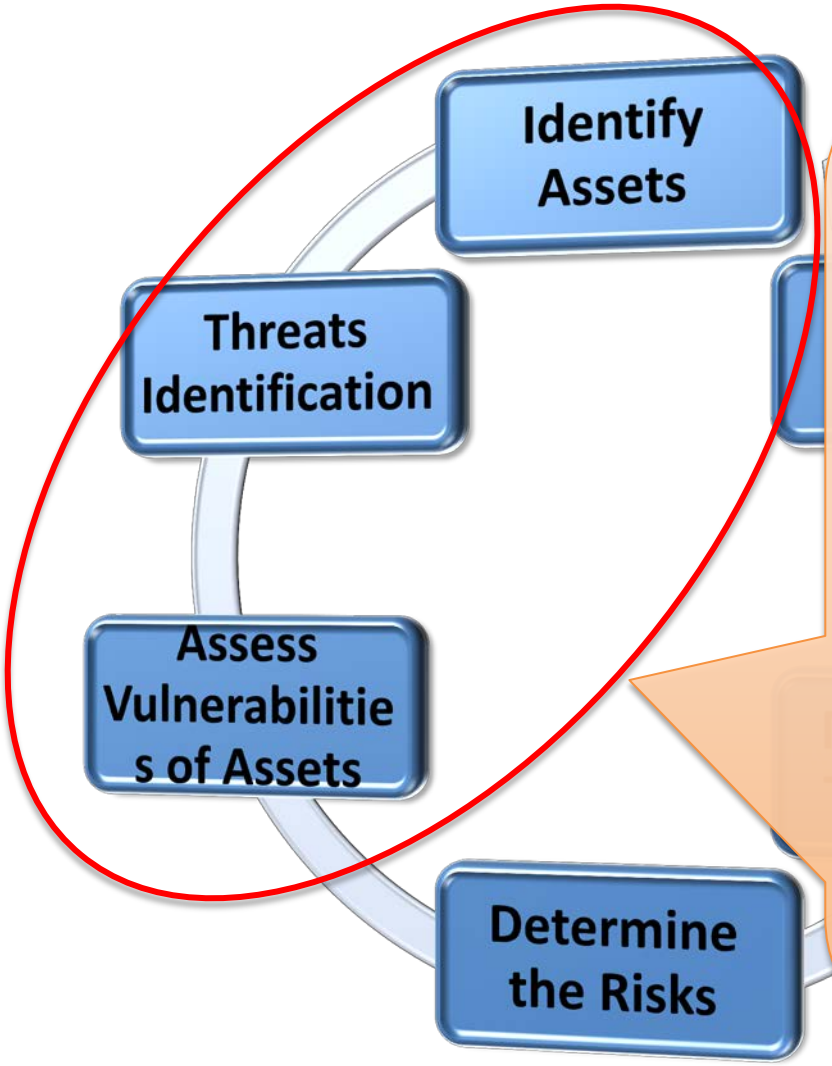
University of BRISTOL

Traditional IT Risk Assessment for ICSs



University of BRISTOL

Traditional IT Risk Assessment for ICSs



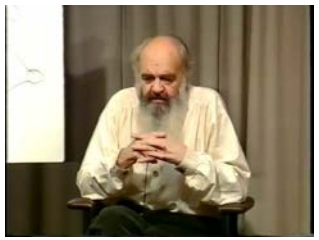
- Identification of Assets follows no formal process.
- Interactions between Assets are often neglected.
- Often the Identification step does not delve deep into the organisation's parts.
- Threats that depend on interrelationships can be neglected.

University of BRISTOL

IT Risk Assessment in ICSs using the VSM

University of BRISTOL

The Viable System Model



"We will seek the source of effective organisation in the cybernetics of natural processes - the brain itself."
Stafford Beer

He studied the human form and based an organisational model on the methods used by the central and autonomic nervous systems to manage the workings of the organs and muscles [2,3].

SYSTEM 1: All the muscles and organs. The parts that actually DO something. The basic activities of the system. **The Operation**.
SYSTEM 2: The sympathetic nervous system which **monitors** the muscles and organs and ensures that their interaction are kept stable.
SYSTEM 3: The Base Brain which **oversees** the entire complex of muscles and organs and **optimises** the internal environment.
SYSTEM 4: The Mid Brain. The connection to the outside world through the senses. **Future planning**. **Projections**. **Forecasting**.
SYSTEM 5: Higher brain functions. Formulation of **Policy decisions**. **Identity**. [4]

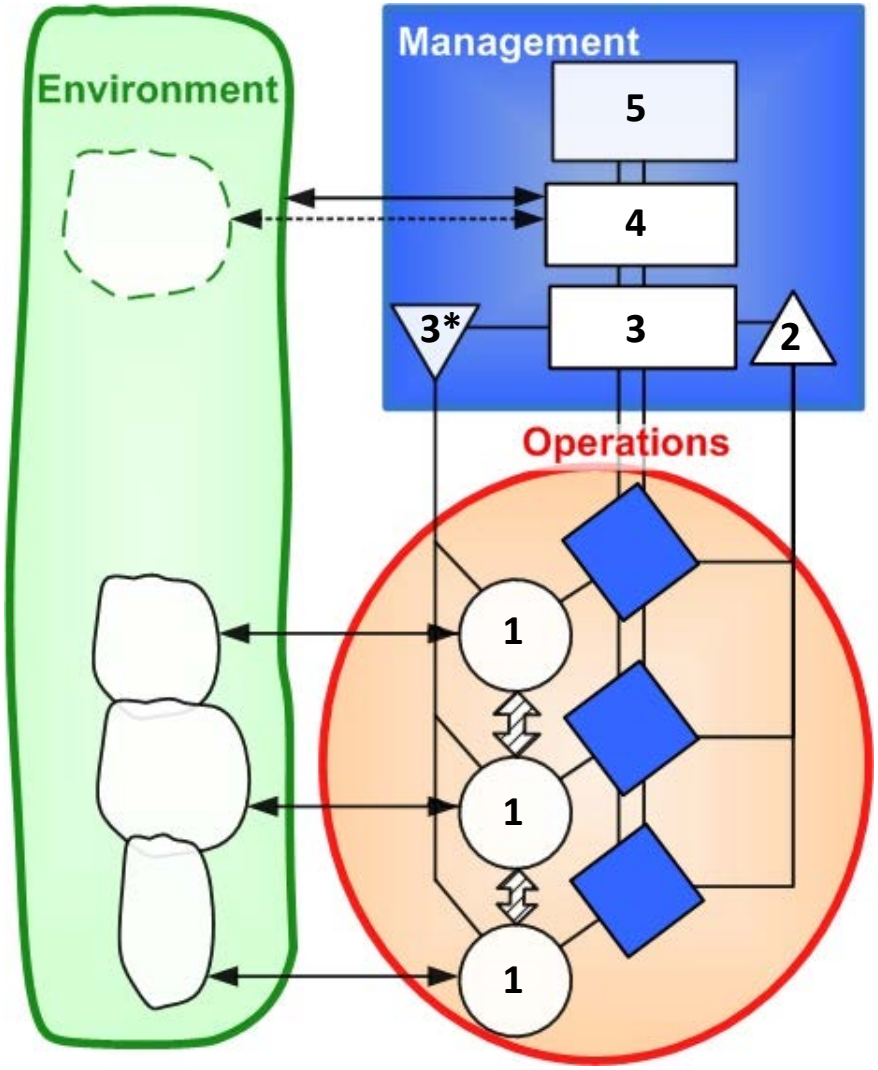
SC SYSTEMS CENTRE

University of BRISTOL

The Viable System Model

A recursive model for viable organisations.

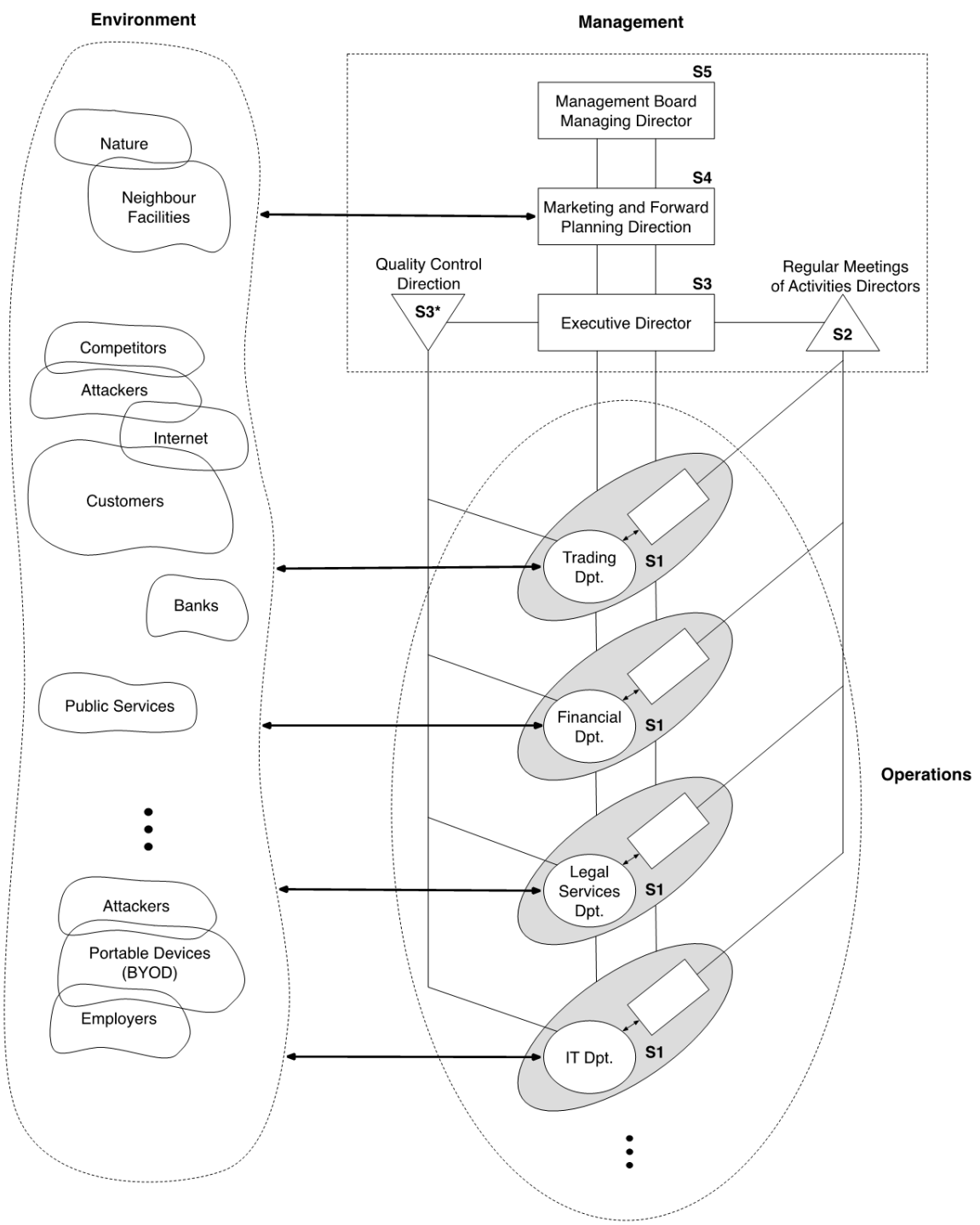
System 1: Operational units of the organisation.
System 2: Attenuation of oscillations and coordination of activities via information and communication.
System 3: Management of the collective of primary units. Provision of synergies.
System 3*: Investigation and validation of information flowing between Systems 1–3 and 1–2–3 via auditing/monitoring activities.
System 4: Management of the development of the organisation; dealing with the future and with the overall outside environment.
System 5: Balancing present and future as well as internal and external perspectives; ascertaining the identity of the organization and its role in its environment; embodiment of supreme values, norms and rules of the system. [5]



Source: http://www.closetheloop.gr/content/viable-system-model

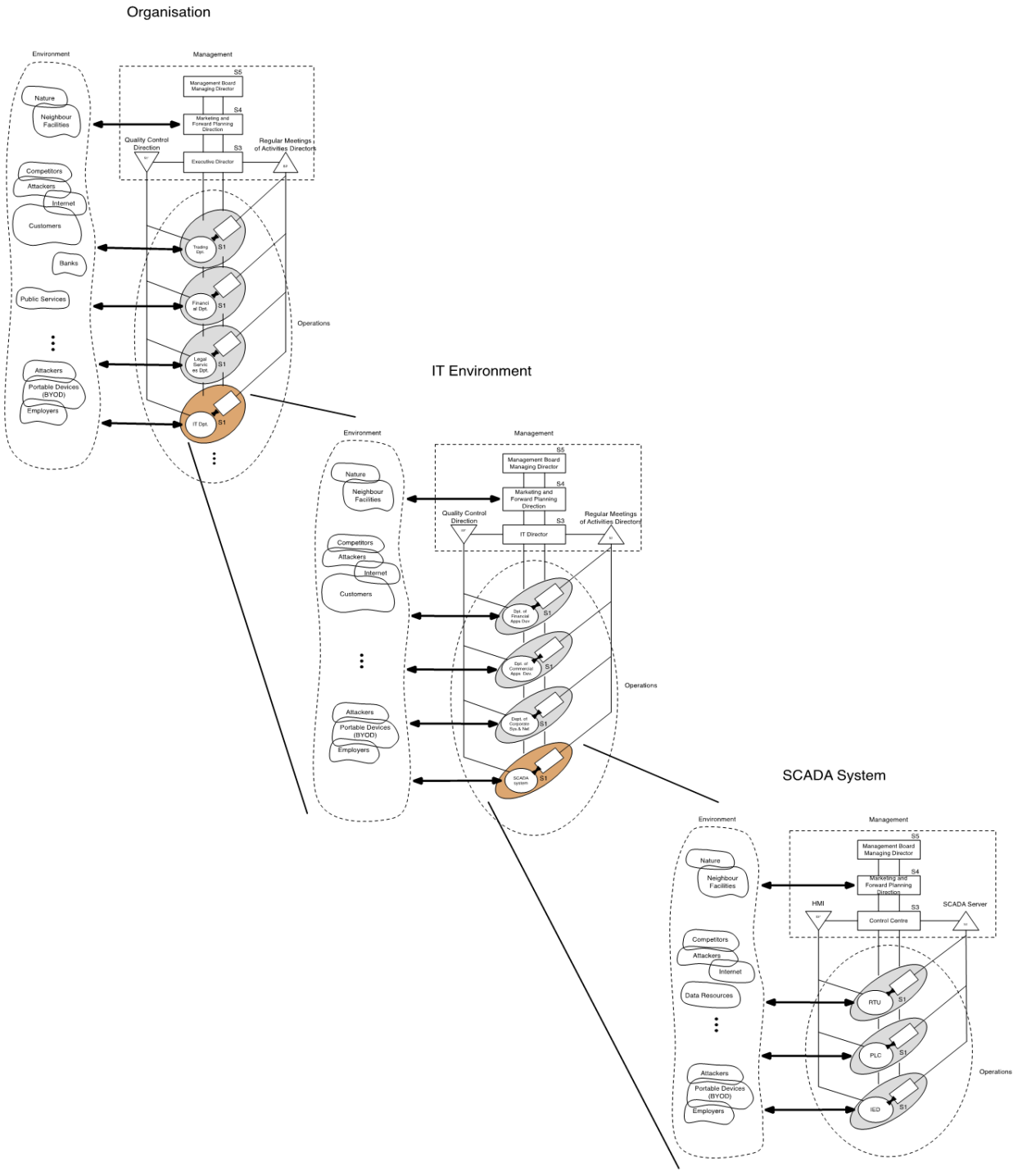
University of BRISTOL

VSM for Industrial Control Systems



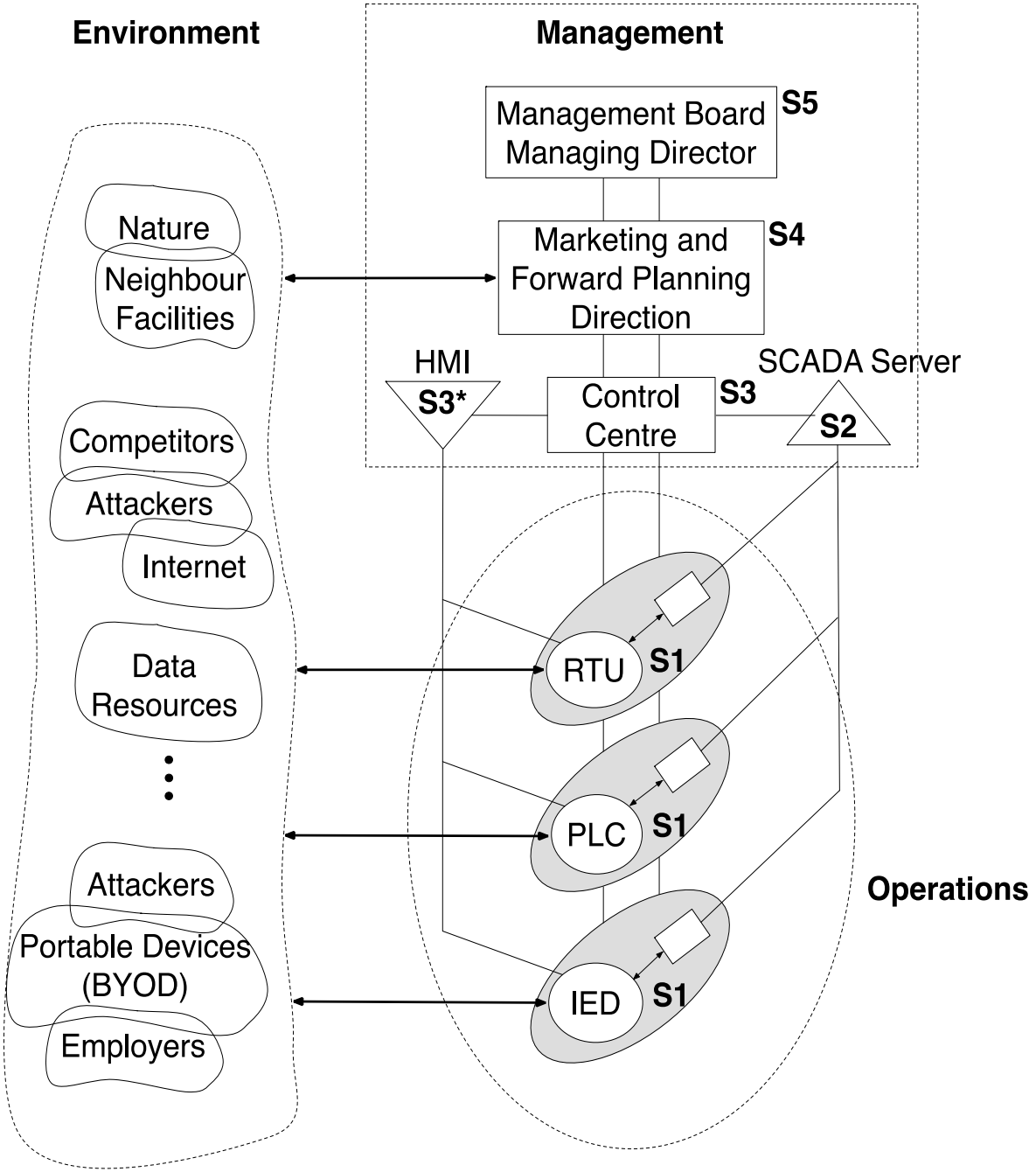
University of BRISTOL

The Recursive Nature of the VSM



University of BRISTOL

SCADA Viable System Modelling



University of BRISTOL

Security oriented VSM

Having constructed the VSM we have also identified all the systems and their interactions. => All parts of the organisation have been identified along with the way they interact with each other.

The different parts of the VSM along with the interactions between them form the new assets in the risk analysis process.

By securing all the parts and their interactions we ensure a secure system against cyber attacks. This way we also ensure viability. => **Viability = Security**

The identification of threats against viability and the assessment of the vulnerabilities of the different parts of the system can help determine the cyber security risks.

University of BRISTOL

The VSM in Risk Analysis

University of BRISTOL

Advantages of using VSM

- Risk analysis can be done by finding the gaps in the organisation based on the systems (or connections) that are missing from the VSM or are open to cyber attacks.

- The VSM can also be used as an extension to the existing risk analysis tools. It is a formal way to determine the assets (systems and connections), the vulnerabilities of the organisation and accomplish the threat assessment.

- Through its recursive functionality it can be used to examine the whole organisation in more depth and ensure that no asset or interaction is left out.

University of BRISTOL

Drawbacks

- Work is still in progress.
- Constructing the VSM is time consuming and requires special knowledge on both the VSM as a model and the various parts of the organisation.
- Need for real data to compare results of traditional risk analysis methods with the VSM model.

University of BRISTOL

Conclusions

- The Viable System Model is a model that ensures the viability of an organisation.
- It can also be used to enhance traditional risk analysis methods by providing a better way to understand the role of each part/system inside the organisation along with the way they interact with each other.
- Traditional risk analysis methods do not offer a formal way to gather information from the organisation. They are based on interviews and questionnaires which however may quite easily neglect certain parts of the organisation or important interactions that can take place and affect the security.
- Since the organisation is better understood it becomes easier to identify threats and assess vulnerabilities.

University of BRISTOL

Acknowledgements

Systems Centre Open Innovation Industry scholarship fund.

Support from EPSRC and IDC in Systems in gratefully acknowledged.

SC SYSTEMS CENTRE

University of BRISTOL

References

[1] Stoneburner, Gary, Alice Goguen, and Alexis Feringa. "Risk management guide for information technology systems." *Nist special publication* 800.30 (2002): 800-30.

[2] Beer, Stafford. *Brain of the firm: the managerial cybernetics of organization*. New York: J. Wiley, 1981.

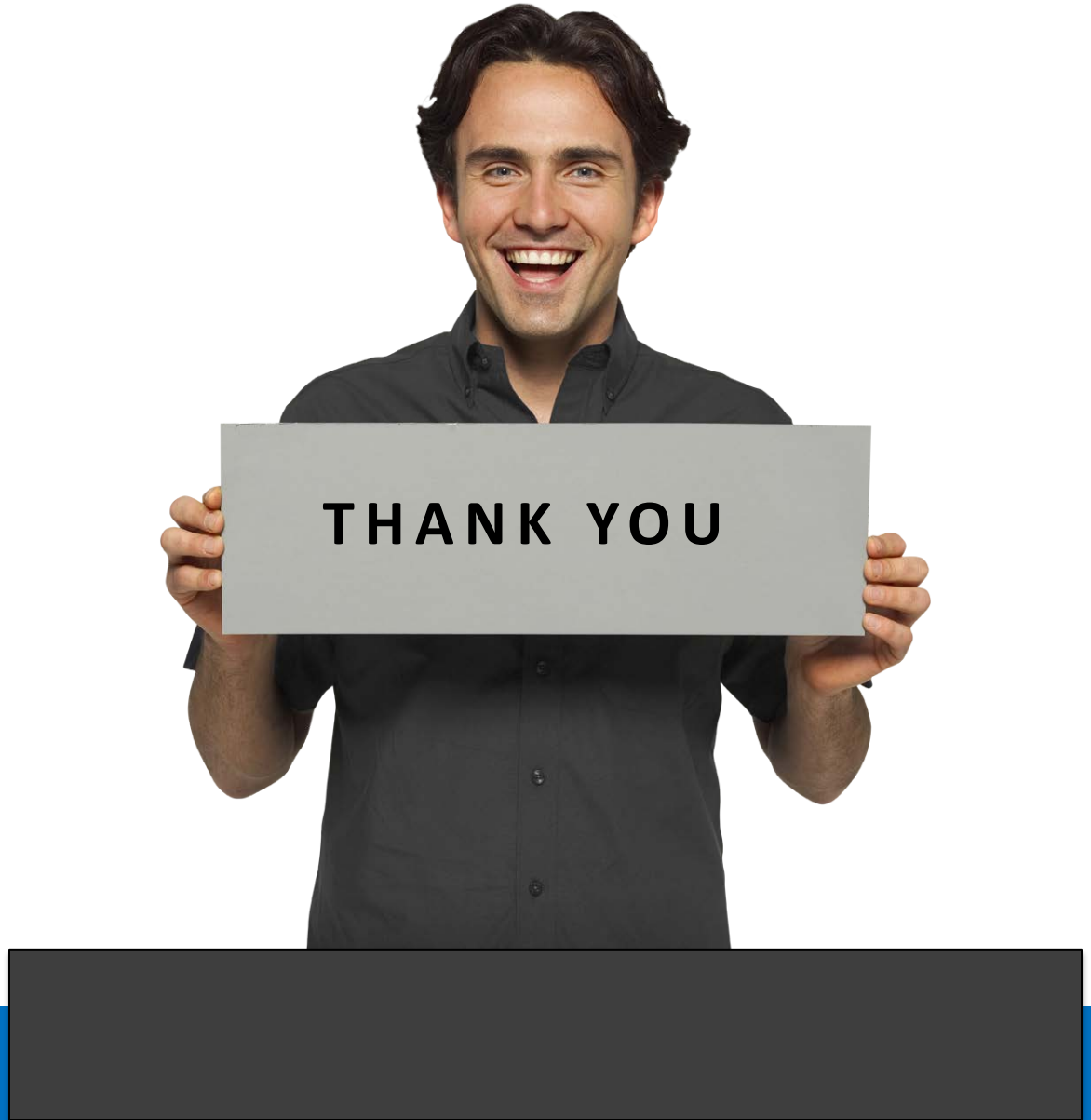
[3] Beer, Stafford. *The heart of enterprise*. Chichester: John Wiley & Sons, 1994.

[4] Walker, Jon. "The viable system model: a guide for co-operatives and federations." *Published online at< http://www. greybox. uklinux. net/vsmg_2* 2 (1991).

[5] Schwaninger, Markus, and José Pérez Ríos. "System dynamics and cybernetics: a synergetic pair." *System Dynamics Review* 24.2 (2008): 145-174.

SYSTEMS CENTRE

University of BRISTOL



SYSTEMS CENTRE

University of BRISTOL

SYSTEMS CENTRE