



# The Italian National Cybersecurity Framework as the base for a dynamic approach to the evaluation of Cyber Risks in SMEs

*Stefano Armenia<sup>1</sup>, Marco Angelini<sup>2</sup>, Fabio Nonino<sup>2</sup>, Giulia Palombi<sup>2</sup>, Mario F. Schlitzer<sup>2</sup>*

<sup>1</sup> *Department of Research, Link Campus University of Rome, Rome, Italy*

<sup>2</sup> *Department of Computer, Control and Management Engineering, Sapienza University of Rome, Rome, Italy*

# Issues in Cyber Risk evaluation

- The growing amount of cyberspace threats highlights the need to define security policies in a context where information on the potential threats can be incomplete or require great efforts to be managed in relation to the dimension of the organization.
- Furthermore, looking at the cyberspace from only one point of view makes it difficult to deal with every threat, as in fact potential vulnerabilities are hidden everywhere: hardware, software, organizational procedures, contracts and regulations.
- The need to evaluate cybersecurity risks and hence plan for effective investments by means of appropriate tools has been already largely recognized (*Khan and Sepúlveda Estay, 2015; Steen and Aven, 2011*)
- Several studies focused on the **management of cyber risk** (*Collier et al., 2013; Jensen, 2015; Katsumata et al., 2010; Nazareth and Choi, 2015; Rohmeyer, 2017; Ganin et al., 2017; Carayannis et al., 2019*) ...
- ...and on the **allocation of protection budget** related to cyber risk (*Bojanc and Jerman-Blazinc, 2008; Katsumata et al., 2010; Steen and Aven, 2011; Chen et al., 2011; Paté-Cornell et al., 2018*).

# Latest developments

- The Cybersecurity Framework, published by the US National Institute of Standards and Technology (NIST), offers an important guidance and provides guidelines, best practices and standards for research and applications in cyber security risk management
- Nevertheless, the existing approaches lack the capacity to integrate across multiple domains of cyber systems (Ganin *et al.*, 2017) and to include uncertainty and the dynamics of cyberattacks” (Paté-Cornell *et al.*, 2018).
- Recent contributions to this strain of literature includes the study by Nazareth and Choi (2015) that, using a **system dynamics model**, evaluated alternative security management strategies through an investment and security cost lens, providing managerial guidance for security decision such as the fact that investing in security detection tools has a higher payoff than does deterrence investment



# Goal of this study

- To the best of our knowledge, a practical dynamic and easy to use model able to identify and estimate the cyber risk related to a specific SME does not exist yet.
- Therefore, the aim of this study is to propose a system dynamics-based (as well as based on the Italian Cybersecurity Framework and NIST Cybersecurity Framework) **tool for the evaluation of cyber risk and for the planning of effective investments in SMEs** aimed at risk mitigation
- It is important for SMEs to be able to manage their current cybersecurity policies, especially with reference to related investments but also to internal changes to their organizational model
- It is also important for insurance companies and/or brokers to have a tool capable of supporting them in their **economic evaluation of the residual risk** that SMEs ask to externalize.
- It is crucial for this tool to be dynamic, able of addressing organizational complexity, and to be used at regular intervals in order to assess cyber risks and related changing contexts over time.

# Proposed approach

- With this research, we propose a new approach and a tool for improving cyber risk assessment as well as for decision-making on proper investments for improving the risk profile of a SME
- This work stems from the concepts and economic models that were proposed for the first time in:
  - *Baldoni R., Montanari L., Querzoni L., Armenia S. et al. (2016) **The 2016 Italian Cybersecurity Report: Essential controls for cybersecurity in SMEs***
  - *Armenia S., Ferreira Franco E., Nonino F., Spagnoli E., Medaglia C. M. (2019). **Towards the Definition of a Dynamic and Systemic Assessment for Cybersecurity Risks***

# Source 1: 2016 Cybersecurity Report

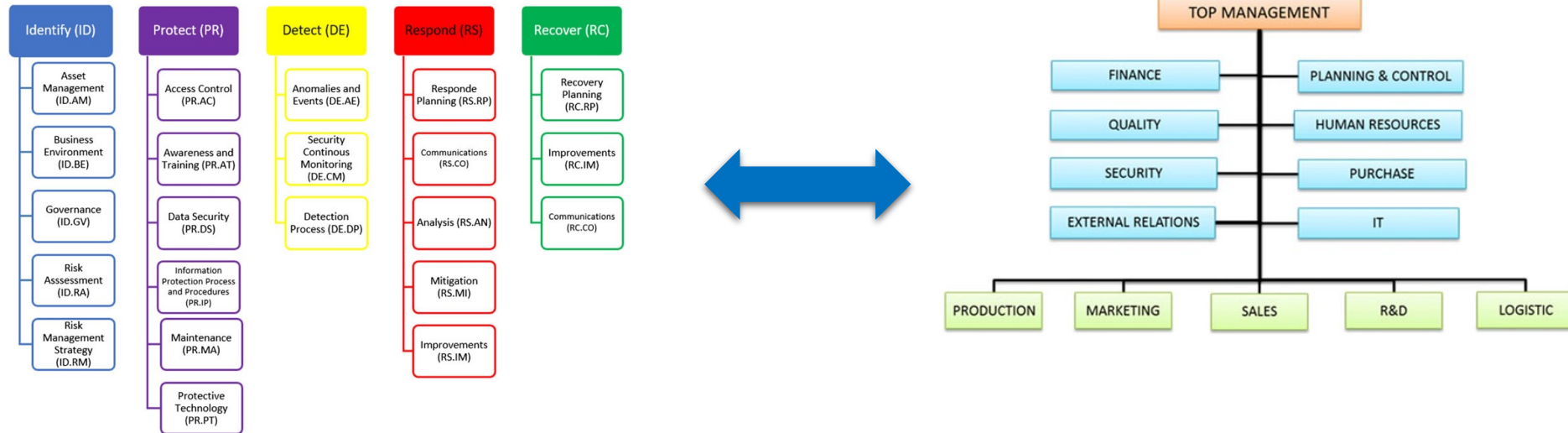
CONTROLLO	STIMA DI COSTO PER AZIENDA TIPO 1	STIMA DI COSTO PER AZIENDA TIPO 2	COSTO MEDIO AZIENDA TIPO 1	COSTO MEDIO AZIENDA TIPO 2
1 - Esiste ed è mantenuto aggiornato un inventario dei sistemi, dispositivi, software, servizi e applicazioni informatiche in uso all'interno del perimetro aziendale.				
2 - I servizi web (social network, cloud computing, posta elettronica, spazio web, ecc...) offerti da terze parti a cui si è registrati sono quelli strettamente necessari.	700 €	1.500 €	Basso	Basso
3 - Sono individuate le informazioni, i dati e i sistemi critici per l'azienda affinché siano adeguatamente protetti.				
4 - È stato nominato un referente che sia responsabile per il coordinamento delle attività di gestione e di protezione delle informazioni e dei sistemi informatici.	300 €	300 €	Basso	Basso
5 - Sono identificate e rispettate le leggi e/o i regolamenti con rilevanza in tema di Cybersecurity che risultino applicabili per l'azienda.	1.000 €	5.000 €	Medio	Alto
6 - Tutti i dispositivi che lo consentono sono dotati di software di protezione (antivirus, antimalware, ecc...) regolarmente aggiornato.	650 €	1.000 €	Basso	Basso
7 - Le password sono diverse per ogni account, della complessità adeguata e viene valutato l'utilizzo dei sistemi di autenticazione più sicuri offerti dal provider del servizio (es. autenticazione a due fattori).	500 €	600 €	Basso	Basso
8 - Il personale autorizzato all'accesso, remoto o locale, ai servizi informatici dispone di utenze personali non condivise con altri; l'accesso è opportunamente protetto; i vecchi account non più utilizzati sono disattivati	0 €	0 €	Basso	Basso
9 - Ogni utente può accedere solo alle informazioni e ai sistemi di cui necessita e/o di sua competenza.	0 €	0 €	Basso	Basso
10 - Il personale è adeguatamente sensibilizzato e formato sui rischi di cybersecurity e sulle pratiche da adottare per l'impiego degli strumenti aziendali (es. riconoscere allegati e-mail, utilizzare solo software autorizzato, ...). I vertici aziendali hanno cura di predisporre per tutto il personale aziendale la formazione necessaria a fornire le nozioni basilari di sicurezza	2.500 €	7.500 €	ALTO	ALTO

CONTROLLO	STIMA DI COSTO PER AZIENDA TIPO 1	STIMA DI COSTO PER AZIENDA TIPO 2	COSTO MEDIO AZIENDA TIPO 1	COSTO MEDIO AZIENDA TIPO 2
11 - La configurazione iniziale di tutti i sistemi e dispositivi è svolta da personale esperto, responsabile per la configurazione sicura degli stessi. Le credenziali di accesso di default sono sempre sostituite.	250 €	250 €	Basso	Basso
12 - Sono eseguiti periodicamente backup delle informazioni e dei dati critici per l'azienda (identificati al controllo 3). I backup sono verificati periodicamente e sono conservati in modo sicuro	600 €	2.100 €	Basso	Basso
13 - Le reti ed i sistemi sono protetti da accessi non autorizzati attraverso strumenti specifici (es: Firewall e altri dispositivi/software anti-intrusione)	2.150 €	4.100 €	Alto	Medio
14 - In caso di incidente (es. sia rilevato un attacco o un malware) vengono informati i responsabili della sicurezza e i sistemi vengono messi in sicurezza da personale esperto.	1.850 €	2.100 €	Medio	Basso
15 - Tutti i software in uso (inclusi firmware) sono aggiornati all'ultima versione consigliata dal produttore. I dispositivi o i software obsoleti e non più aggiornabili sono dismessi.	0 €	0 €	Basso	Basso

Stima costi annui: 7.800 € 19.800 €  
 Stima costi iniziali: 2.700 € 4.650 €

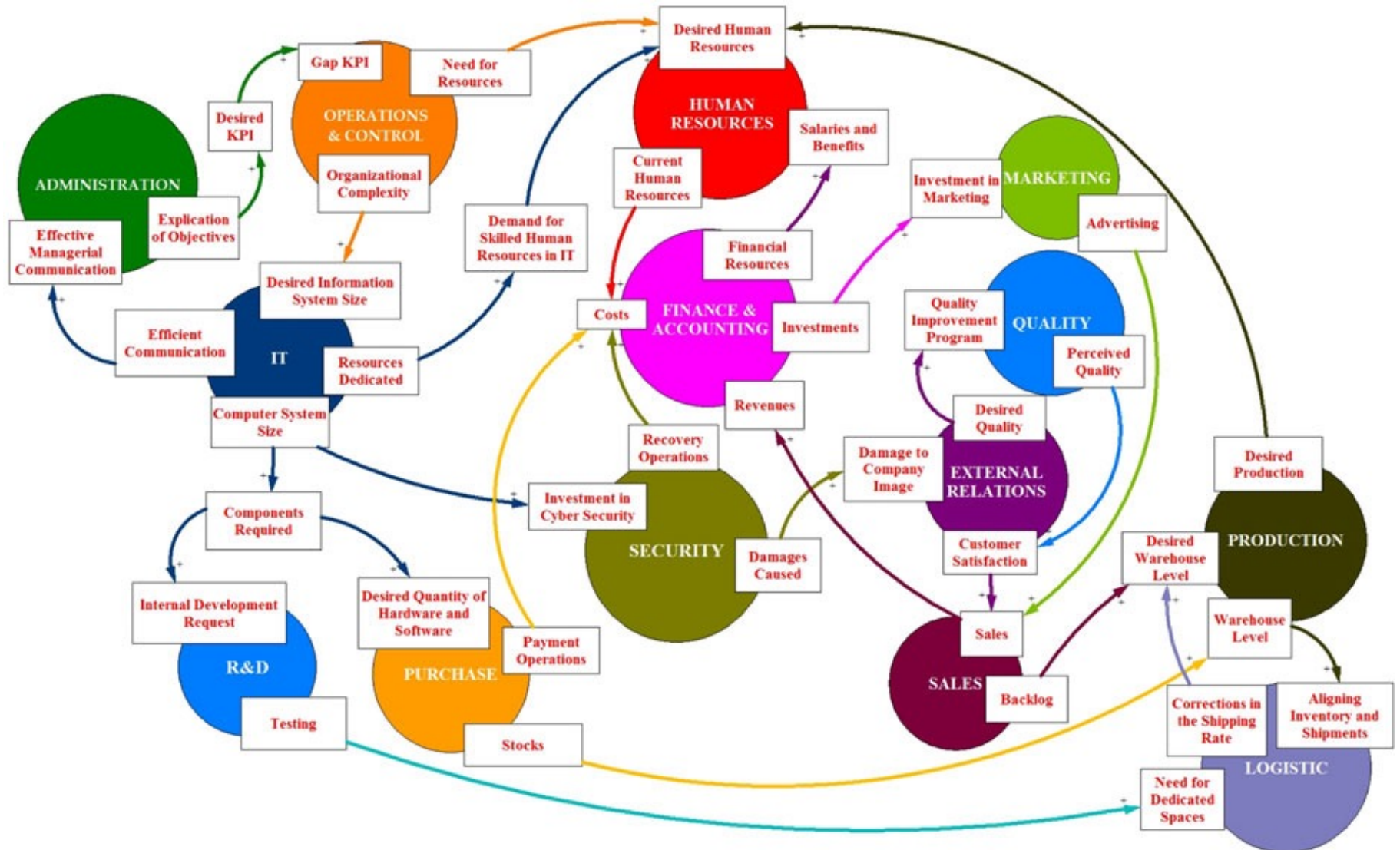
Two different company types (different activity sector, different parameters, etc.)

# Source 2: Systems Research and Behavioural Science



- Organizational perspective of the firm seen under a systemic approach (System Dynamics and Systems Thinking CLDs)
- Framework categories mapped on the organizational model
- Systemic relationships among categories defined (Categories CLD)

# Bubble diagram (overall org. CLD)



# What is System Dynamics (I)

System dynamics is a computer-aided approach to policy analysis and design.

*It applies to dynamic problems arising in complex social, managerial, economic, or ecological systems — literally any dynamic systems characterized by interdependence, mutual interaction, information feedback, and circular causality.*

The system dynamics approach involves:

- Defining problems dynamically, in terms of graphs over time.

- Striving for an endogenous, behavioral view of the significant dynamics of a system, a focus inward on the characteristics of a system that themselves generate or exacerbate the perceived problem.

- Thinking of all concepts in the real system as continuous quantities interconnected in loops of information feedback and circular causality.

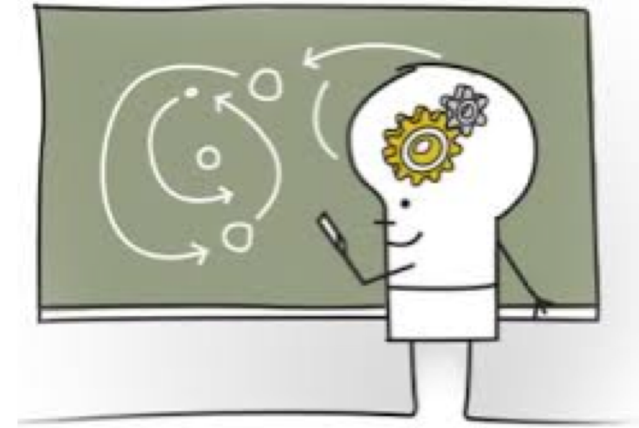
- Identifying independent stocks or accumulations (levels) in the system and their inflows and outflows (rates).

- Identify also structural delays, non-linear relationships, human behaviour (delayed perception of phenomena)

- Formulating a behavioral model capable of reproducing, by itself, the dynamic problem of concern. The model is usually a computer simulation model expressed in nonlinear equations, but is occasionally left unquantified as a diagram capturing the stock-and-flow/causal feedback structure of the system.

- Deriving understandings and applicable policy insights from the resulting model.

- Implementing changes resulting from model-based understandings and insights.





# What is System Dynamics (II)

Conceptually, the **feedback concept** is at the heart of the system dynamics approach.

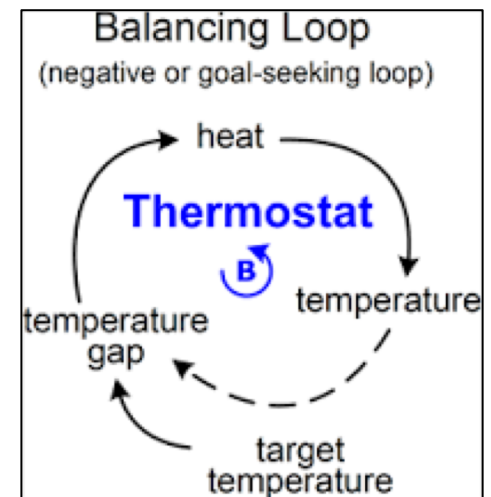
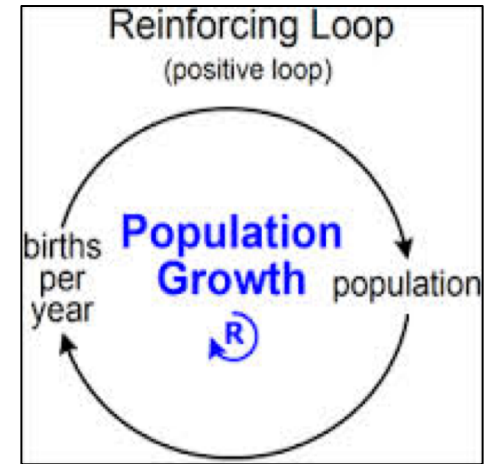
Diagrams of loops of information **feedback** and **circular causality** are tools for conceptualizing the structure of a complex system and for communicating model-based insights.

A feedback loop exists when information resulting from some action travels through a system and eventually returns in some form to its point of origin, potentially influencing future action.

If the tendency in the loop is to reinforce the initial action, the loop is called a **positive or reinforcing feedback loop**; if the tendency is to oppose the initial action, the loop is called a **negative or balancing feedback loop**.

- - Reinforcing loops are sources of growth or accelerating collapse, they are disequilibrating and destabilizing.
- - Balancing loops can be variously characterized as goal-seeking, equilibrating, or stabilizing processes.

Combined, reinforcing and balancing circular causal feedback processes can generate all manner of dynamic patterns called “Archetypes”.



For more info visit: <http://www.systemdynamics.org/what-is-s/>






# How to build CLDs

Information that might be deduced from System Dynamics methodology is based on the creation of a Causal Loop Diagram (CLD), in which causal feedback loops can be identified.

These loops are the result of a combination of causal links between variables. Links can be of two types:

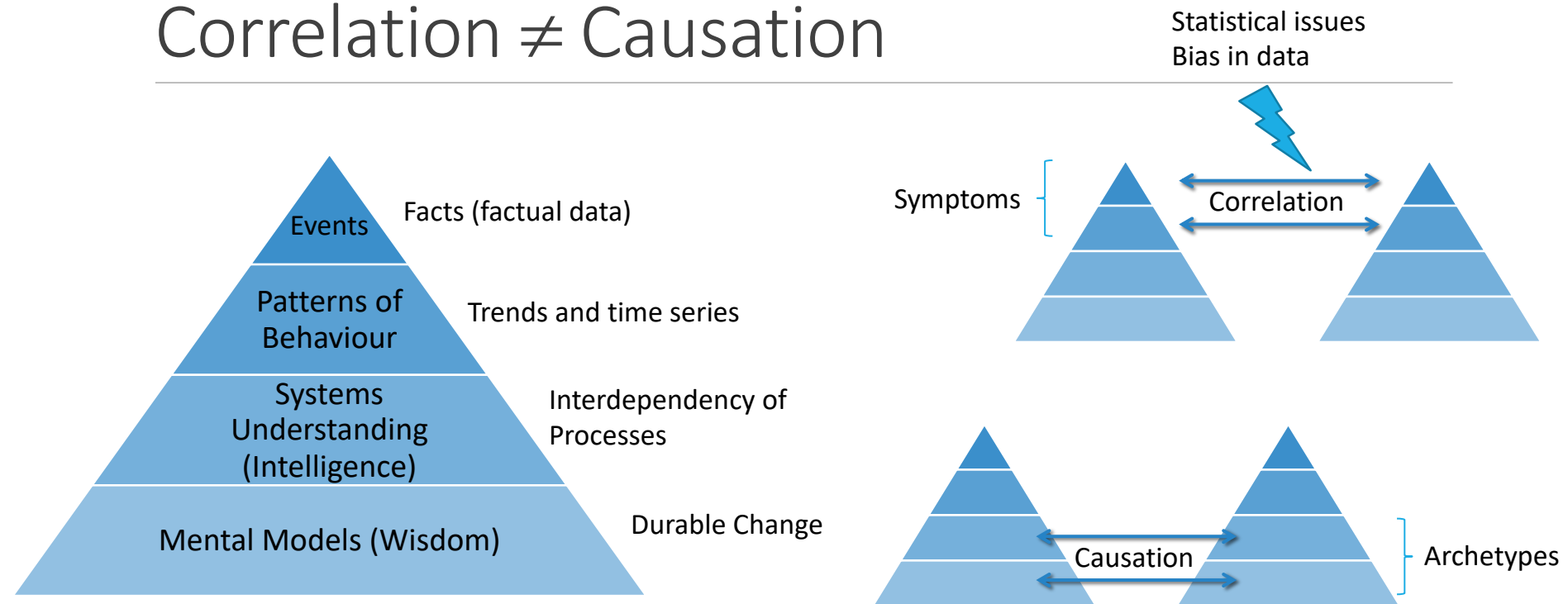
positive (S or +): when the independent variable (arrow tail) changes, then the dependent variable (arrow head) changes in the Same direction;

negative (O or -): when the independent variable (arrow tail) changes, then the dependent variable (arrow head) changes in the Opposite direction.

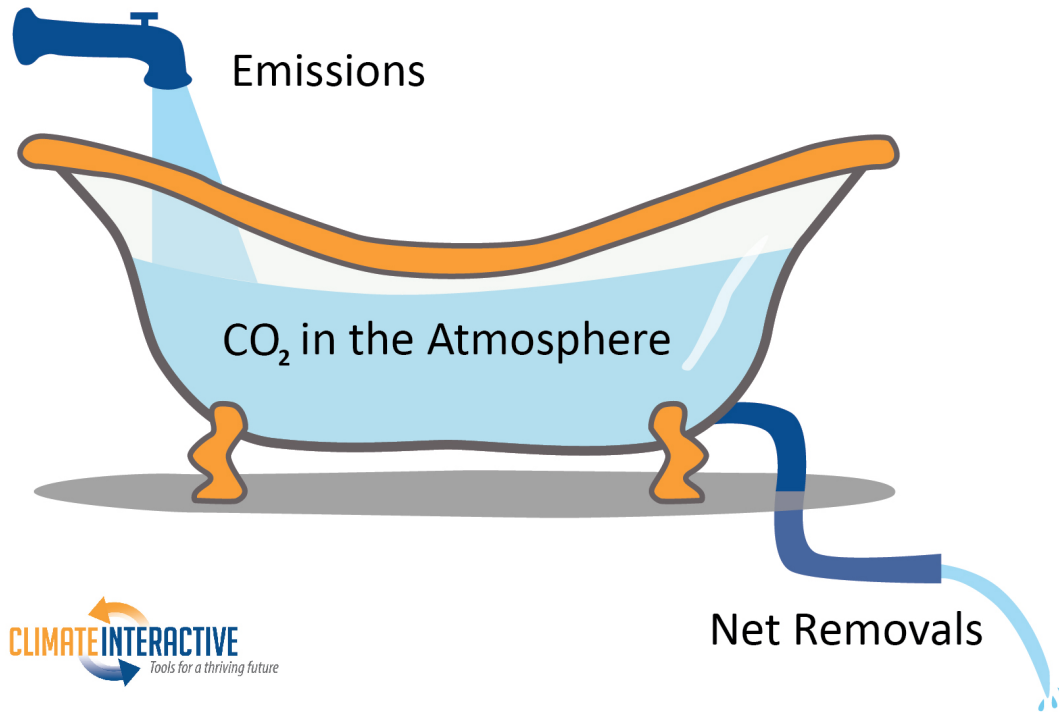
	Read as W causes Z with +ve link polarity or mathematically as $(\partial Z / \partial W > 0)$ . If the cause increases, the effect increases above what it would otherwise have been.
	Read as A causes B with -ve link polarity or mathematically as $(\partial B / \partial A < 0)$ . If the cause increases, the effect decreases below what it would otherwise have been.
	Read as X causes Y with +ve link polarity but only after some delay.
	Label to indicate a balancing feedback loop.
	Label to indicate a reinforcing feedback loop.

# SD vs Stochastic-econometric approaches

## Correlation $\neq$ Causation

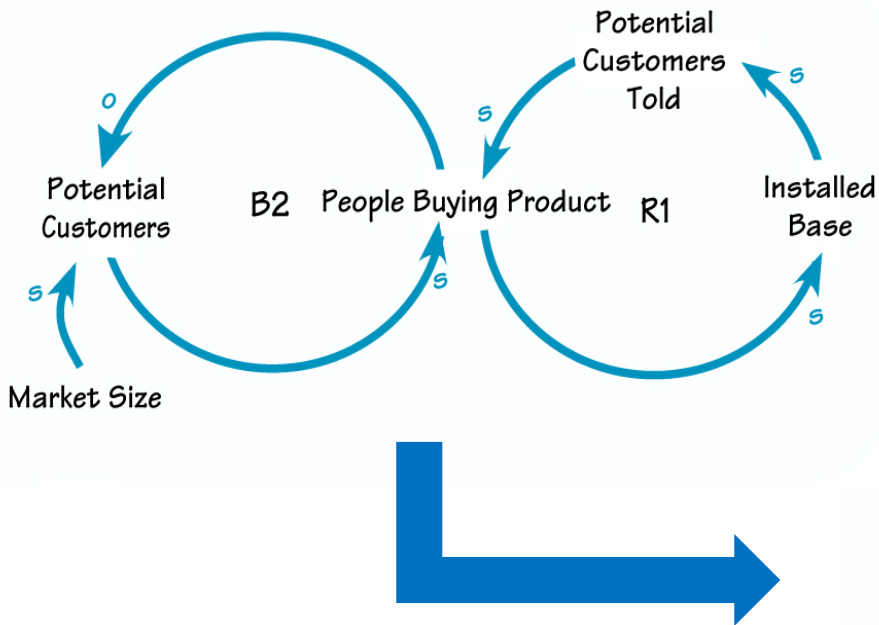


# Dynamics of Stocks and Flows

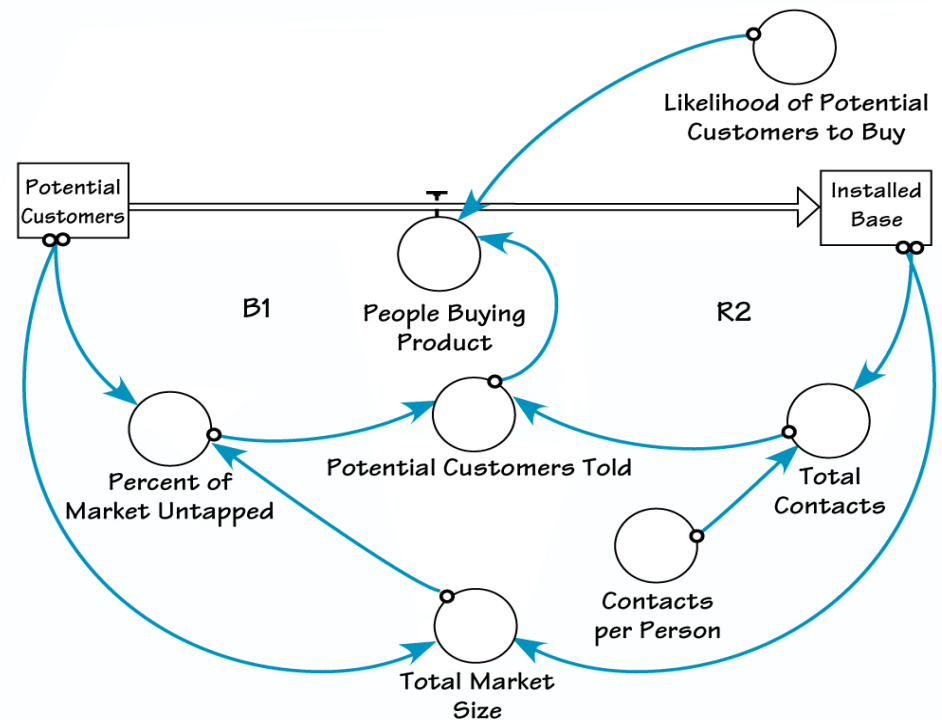


# Typical Modeling Approach

## Causal Loop Diagram

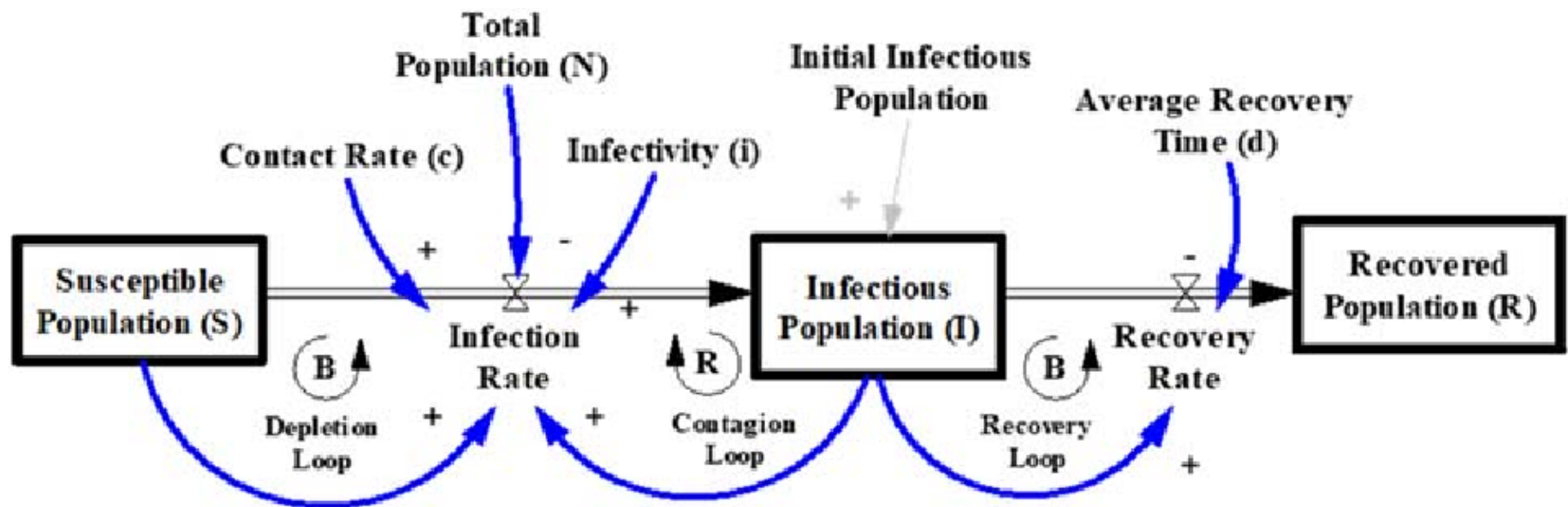


SD can easily integrate also soft / social variables/aspects that normally are neglected into such models (cybersecurity is also heavily affected by social counterintuitive behaviour)



## Stock & Flow Diagram

# Examples: spread of infectious diseases / marketing !!!





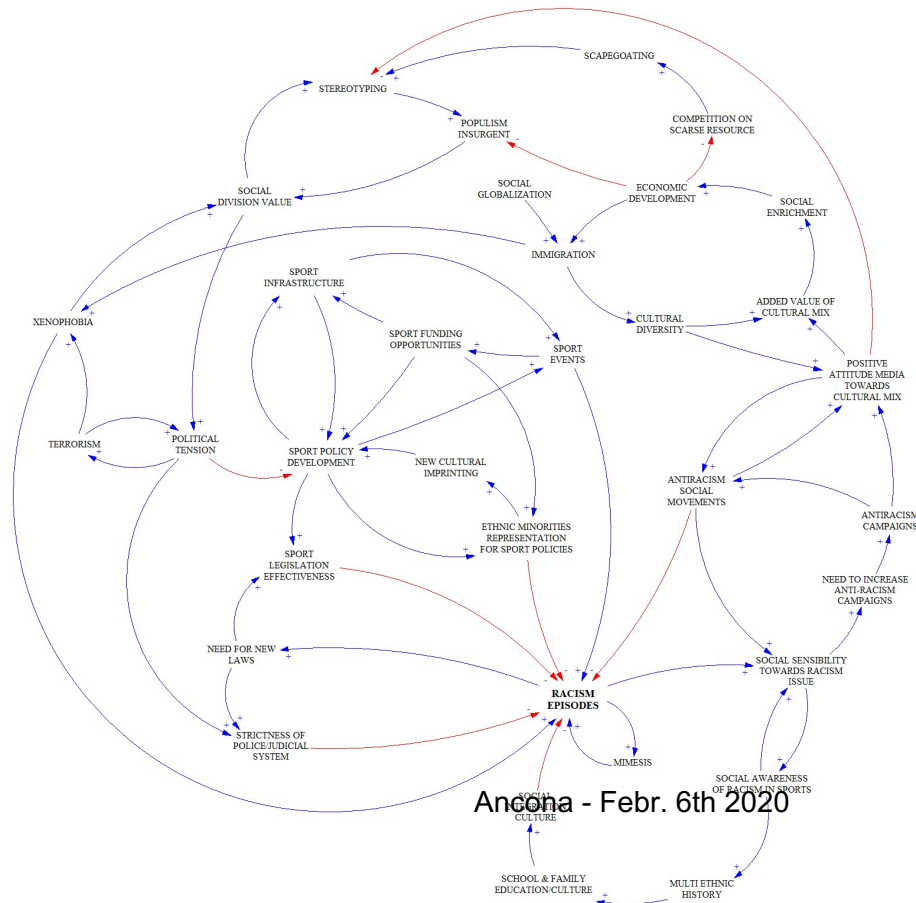
# Examples: social issues



## **BRISWA** the BALL ROLLS IN the SAME WAY for ALL



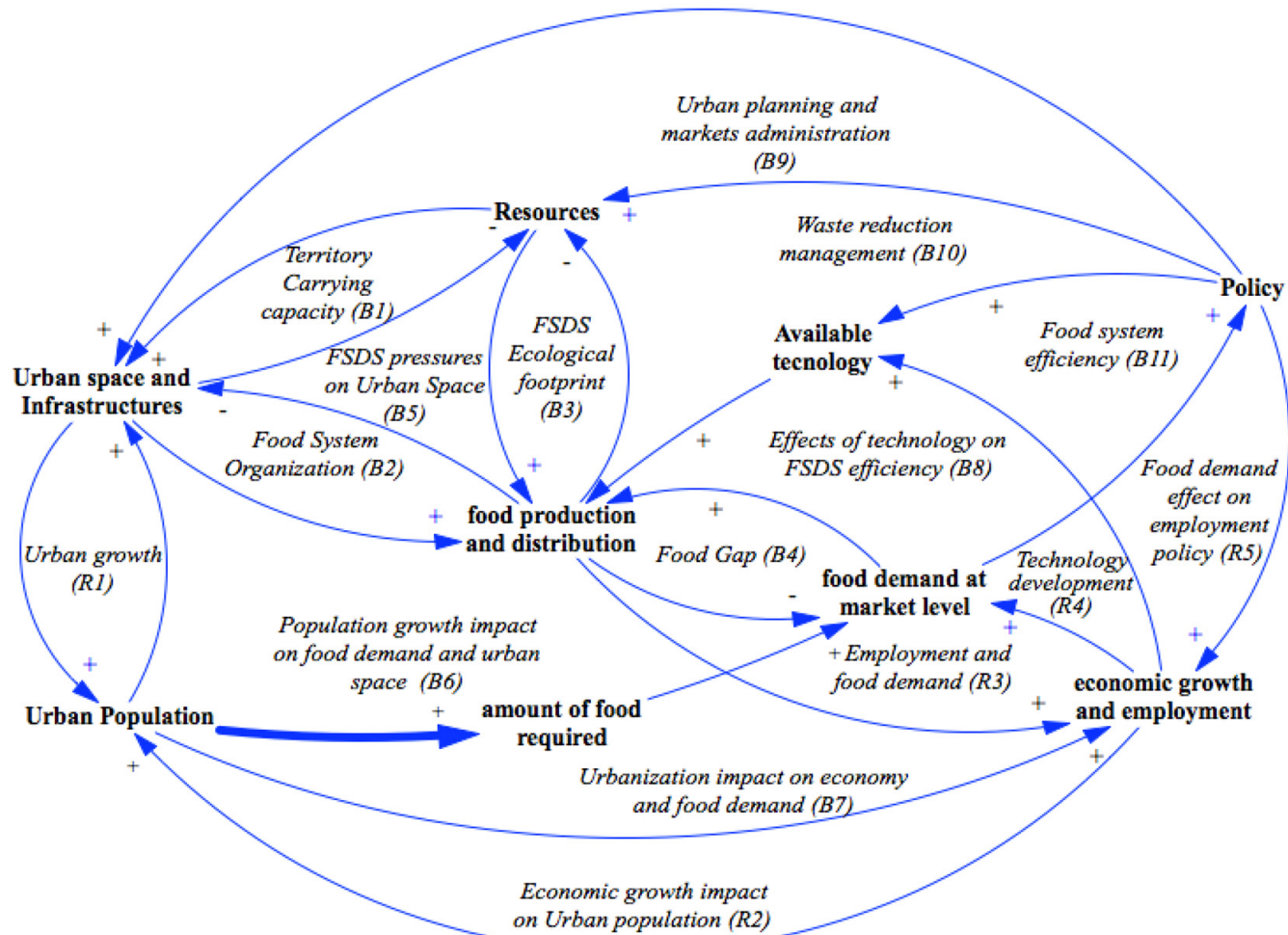
Co-funded by the  
Erasmus+ Programme  
of the European Union



## Examples: sustainability



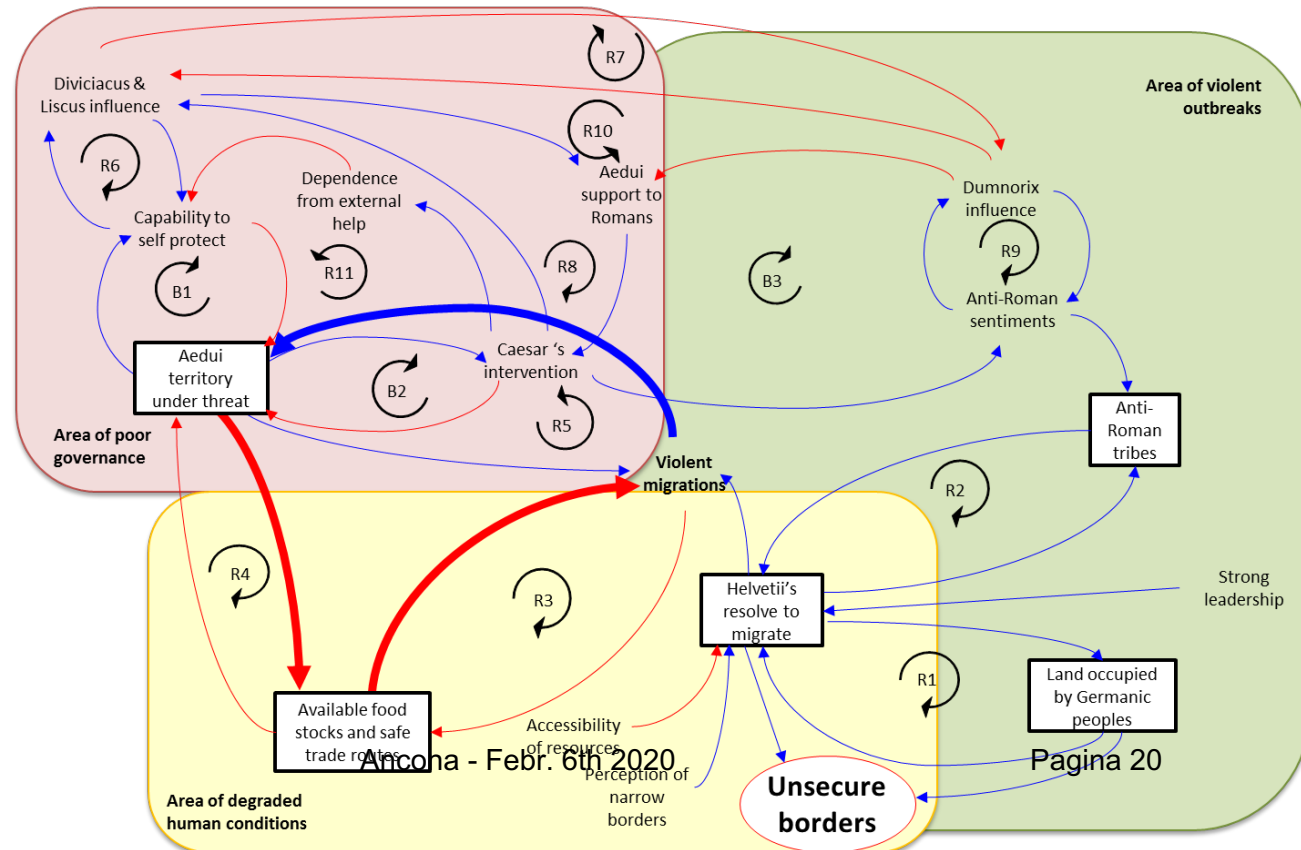
# Examples: Food Systems



# Examples: international crises



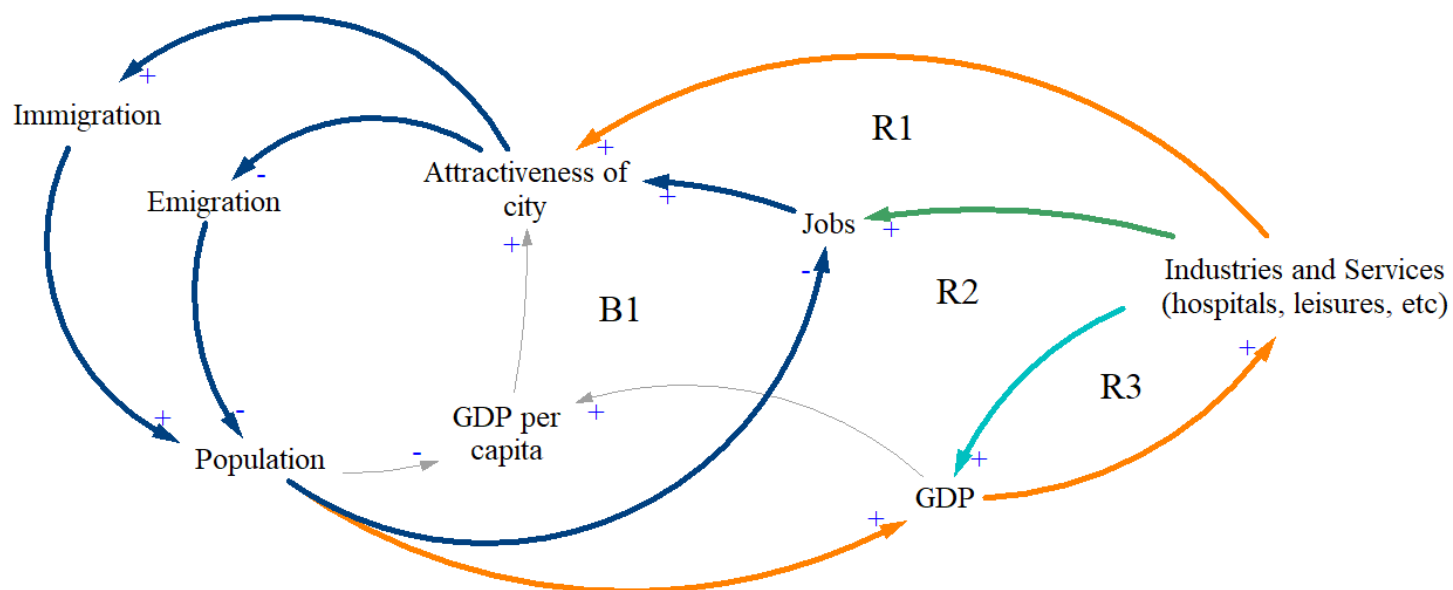
## Julius Caesar – De Bello Gallico



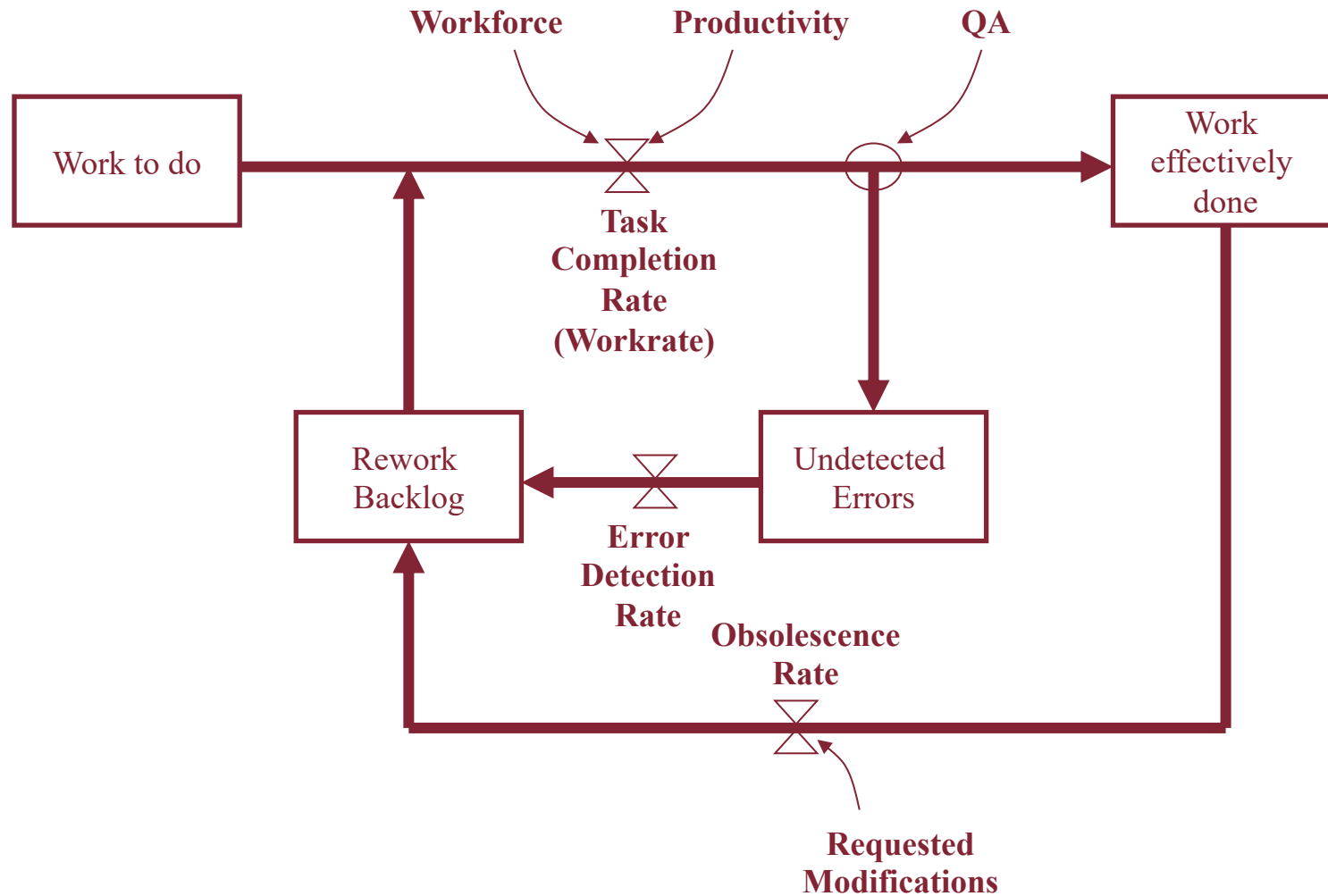
# Examples: urban sustainability



Co-funded by the  
Erasmus+ Programme  
of the European Union



# Examples: Work / Rework Cycle in Projects (I)





# Examples: Work / Rework Cycle in Projects (II)

*Average Exp. Level, Quality*

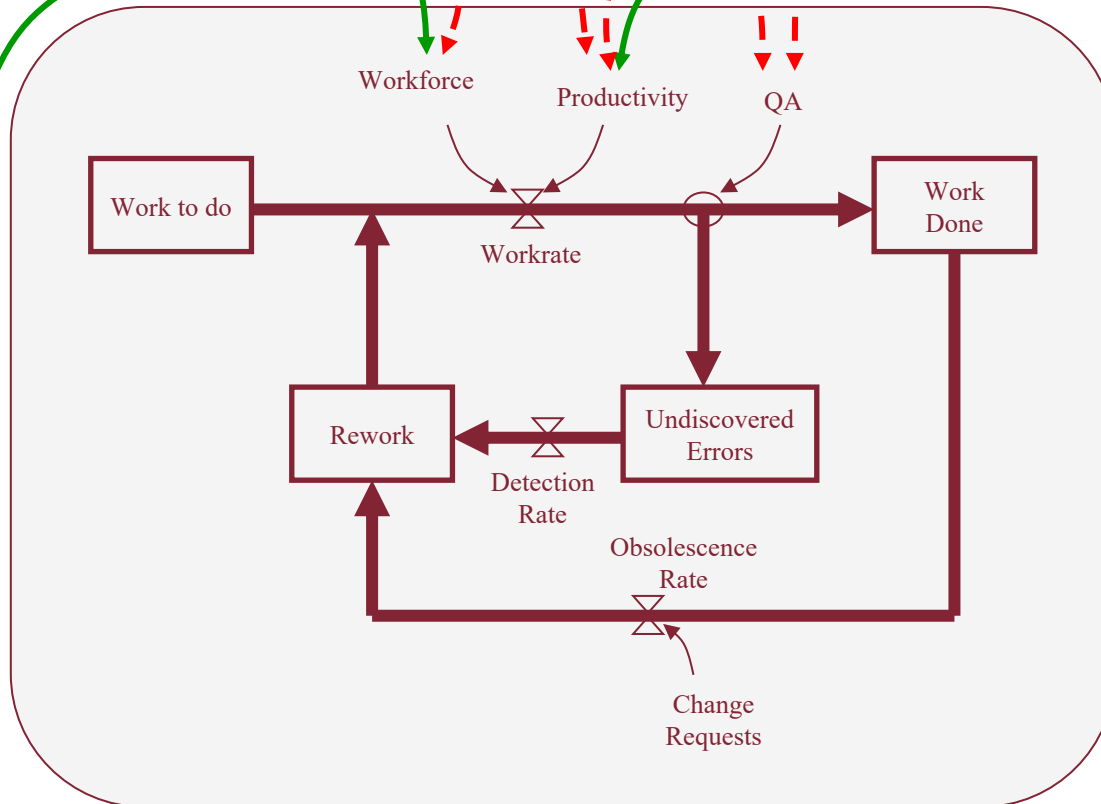
*Work out-of-sequence,  
Workplace congestion,  
Coordination problems,  
Low Morale*

*Fatigue, Stress,  
Low Morale*

*Overtime*

*Hiring*

*Schedule  
Pressure*



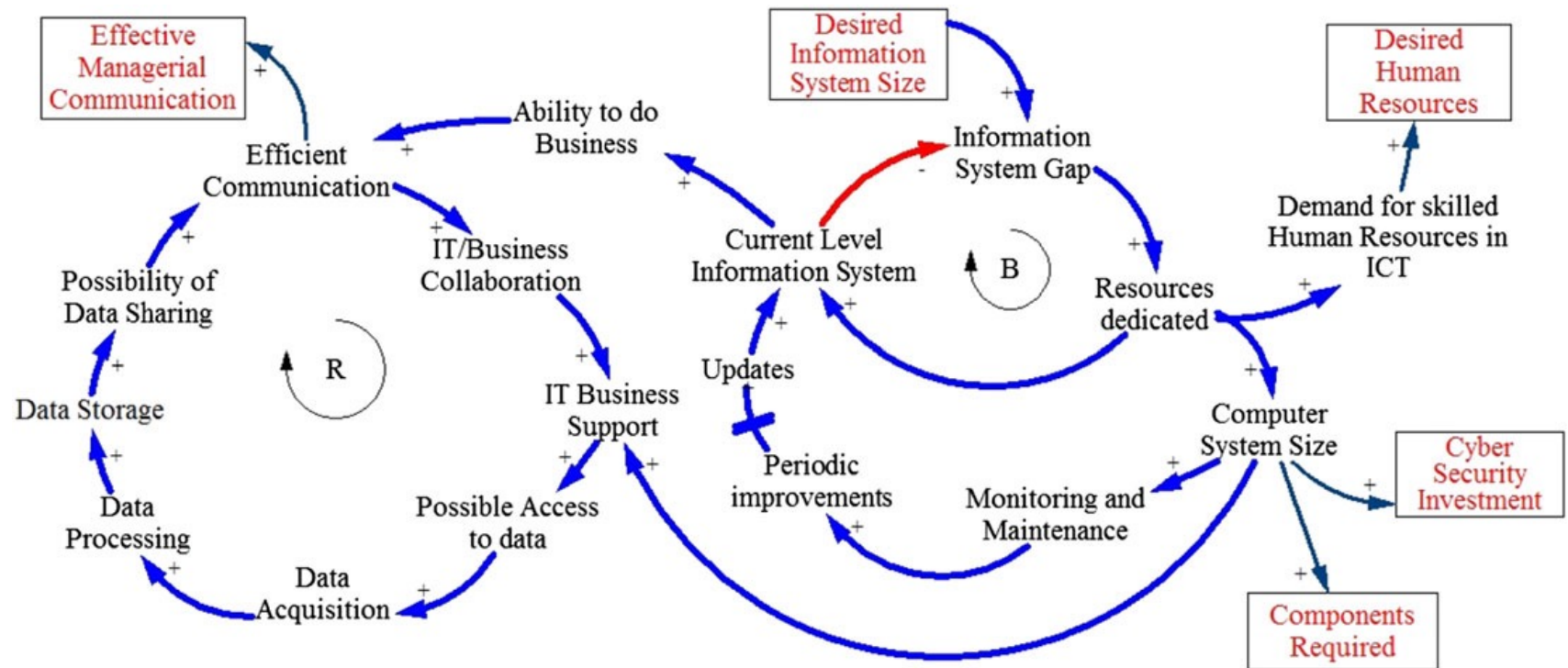
ITASEC 2020

Ancona - Febr. 6th 2020

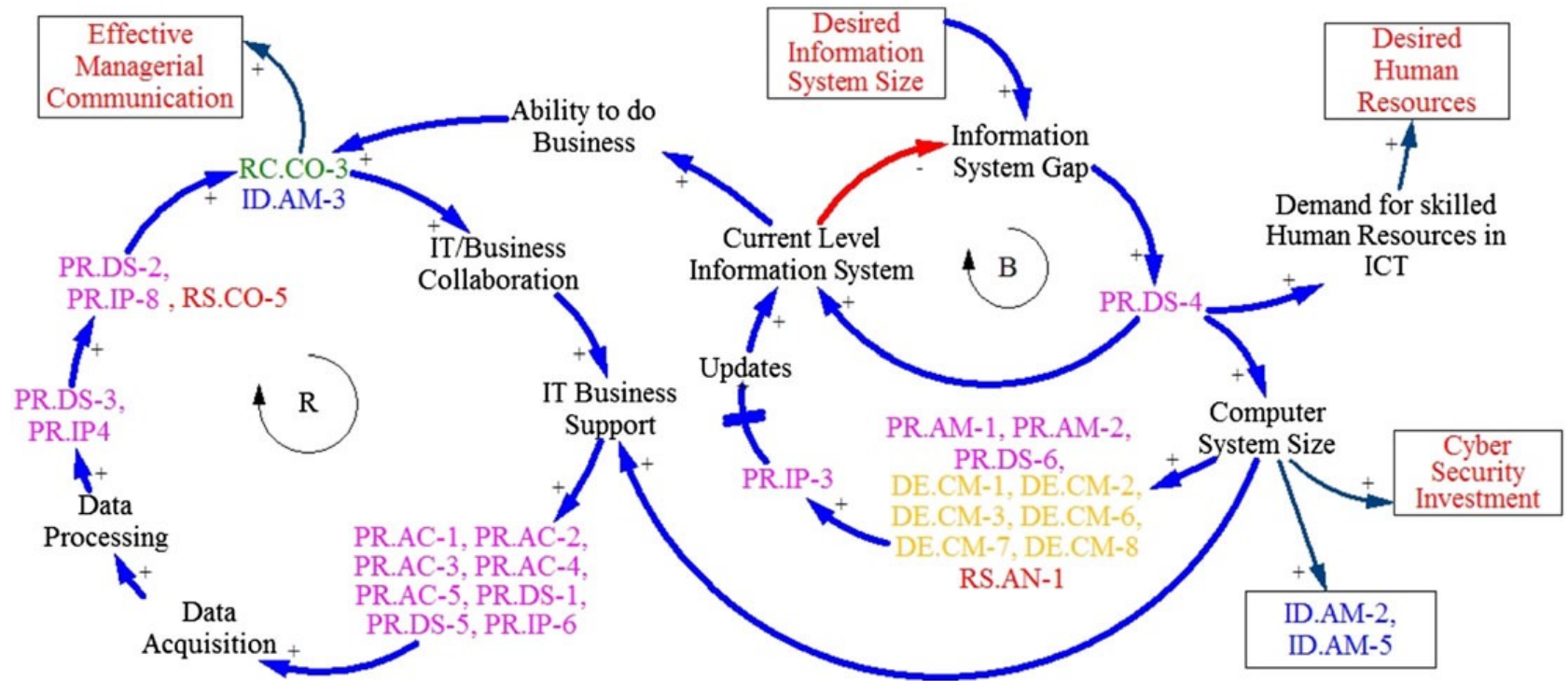
Pagina 23

**Apparent Progress**

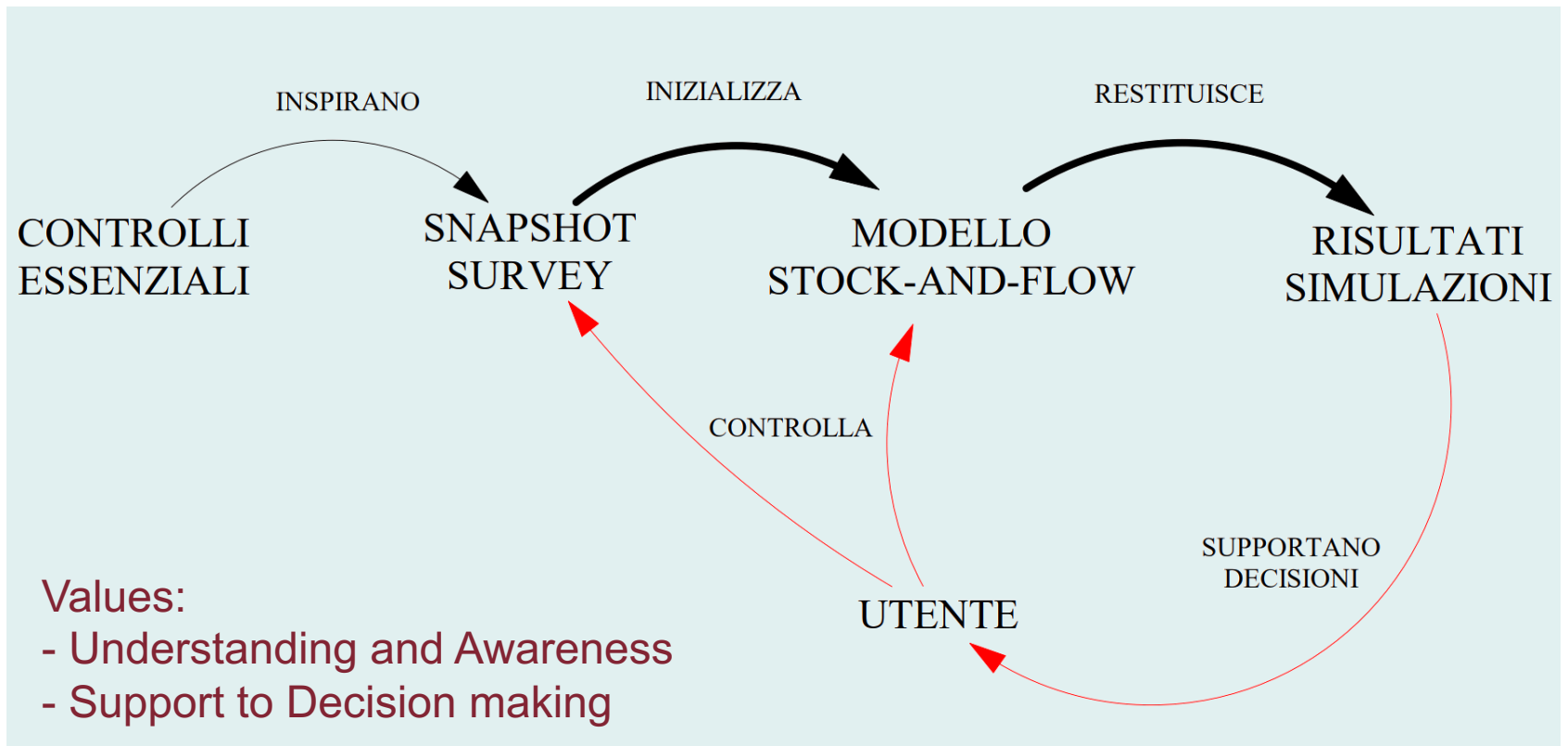
# Let's see one of the main sectors from the Bubble Diagram



# And with the mapping of framework categories



# Tool structure



# Snapshot Survey

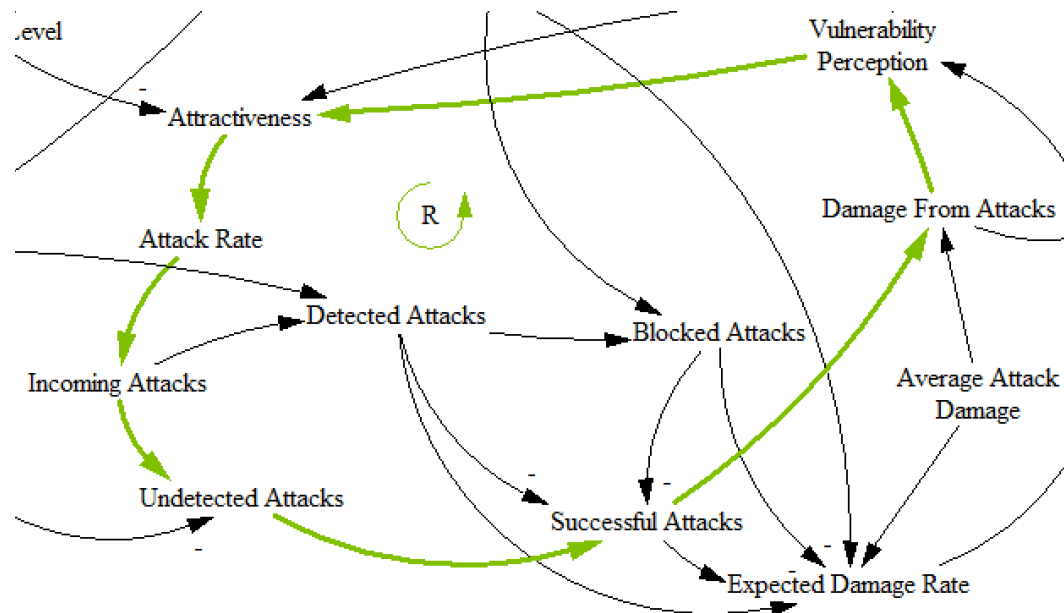
- Based on the 2016 Report on Cyberessentials
- **24 easy questions** on organizational aspects connected to IT security and cybersecurity
- **Does not require specific competences**
- Currently distributed as an excel file
- Provides back an immediate evaluation on the status of IT defenses for the SME
- For specific scores on the categories **Identify, Detect, Protect e Respond** easily allow the identification of potential vulnerabilities
- **Automatically produces the data needed by the SD model to be setup with the current organizational parameters**

15. Employees are aware and trained to understand cybersecurity risks and the practices needed for safely operate the business' IT systems. 0: No 1: Partially 3: Completely	0	8	0
task, is in charge of the initial set up for all systems and devices. 0: No 1: Yes	1	3	3
17. Default access credentials are always replaced. 0: No 1: Yes	1	6	6
18. Critical information, data and systems, identified at #3, are periodically backed up. 0: Never 1: Sporadically 3: At least twice a quarter 4: At least twice a month	1	3	3
19. Backups are safely stored and periodically checked. 0: No 1: Yes	0	3	0
20. Networks and systems are protected against unauthorized accesses using proper tools, such as firewalls. 0: No 1: Yes	1	8	8
21. All wireless networks are protected. 0: No 1: Yes (or, there are no wireless networks)	1	18	18
<b>Subscore</b>			<b>38 /100</b>
<b>Respond</b>	Value	Weight	Weighted Value
22. In the event of an accident (such as malware or other attacks being detected), those in charge of security are informed, and IT systems are secured by experienced personnel. 0: No 1: Yes	1	35	35
23. All software, firmware included, is updated to the latest version suggested by the manufacturer. 0: No 2: Occasional manual updates 4: Automatic or frequent updates	2	15	30
24. Obsolete software or devices that cannot be upgraded are disposed of. 0: No 1: Yes	0	5	0
<b>Subscore</b>			<b>65 /100</b>
<b>Total Score</b>			<b>103 /400</b> <b>25.75%</b>
<b>Initial State Input</b> {0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,1,1,0,1,1,1,2,0}			



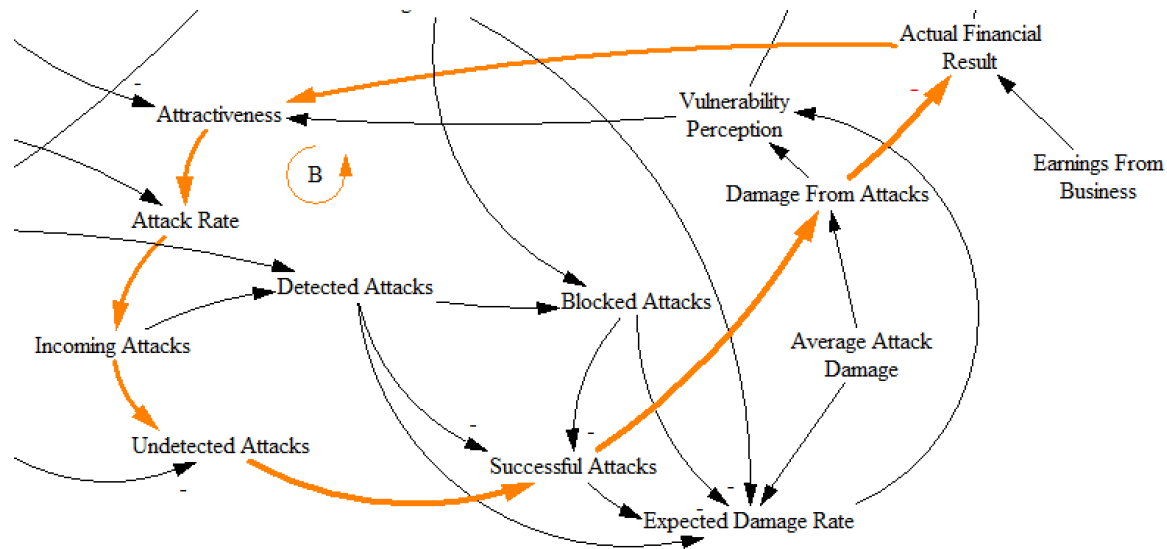


# Interesting Cycles (I)



- **Reinforcing Cycle: reputational damages**
- Snowball effects on reputation due to attacks
- Vulnerability perception from attackers increases, hence further increasing attacks and reputation loss

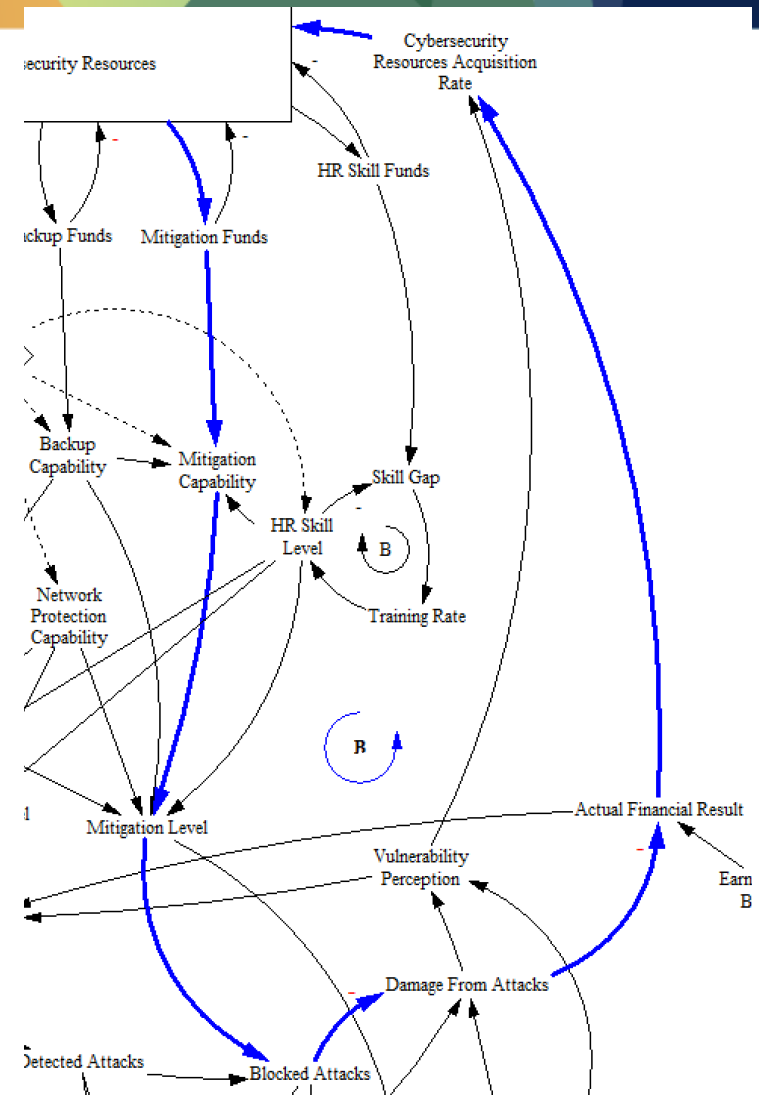
# Interesting Cycles (II)



- **Balancing loop: economic losses helps too!**
- Increasing attacks worsen the economic status of the company, hence making on a side less attractive too to potential new/old attackers

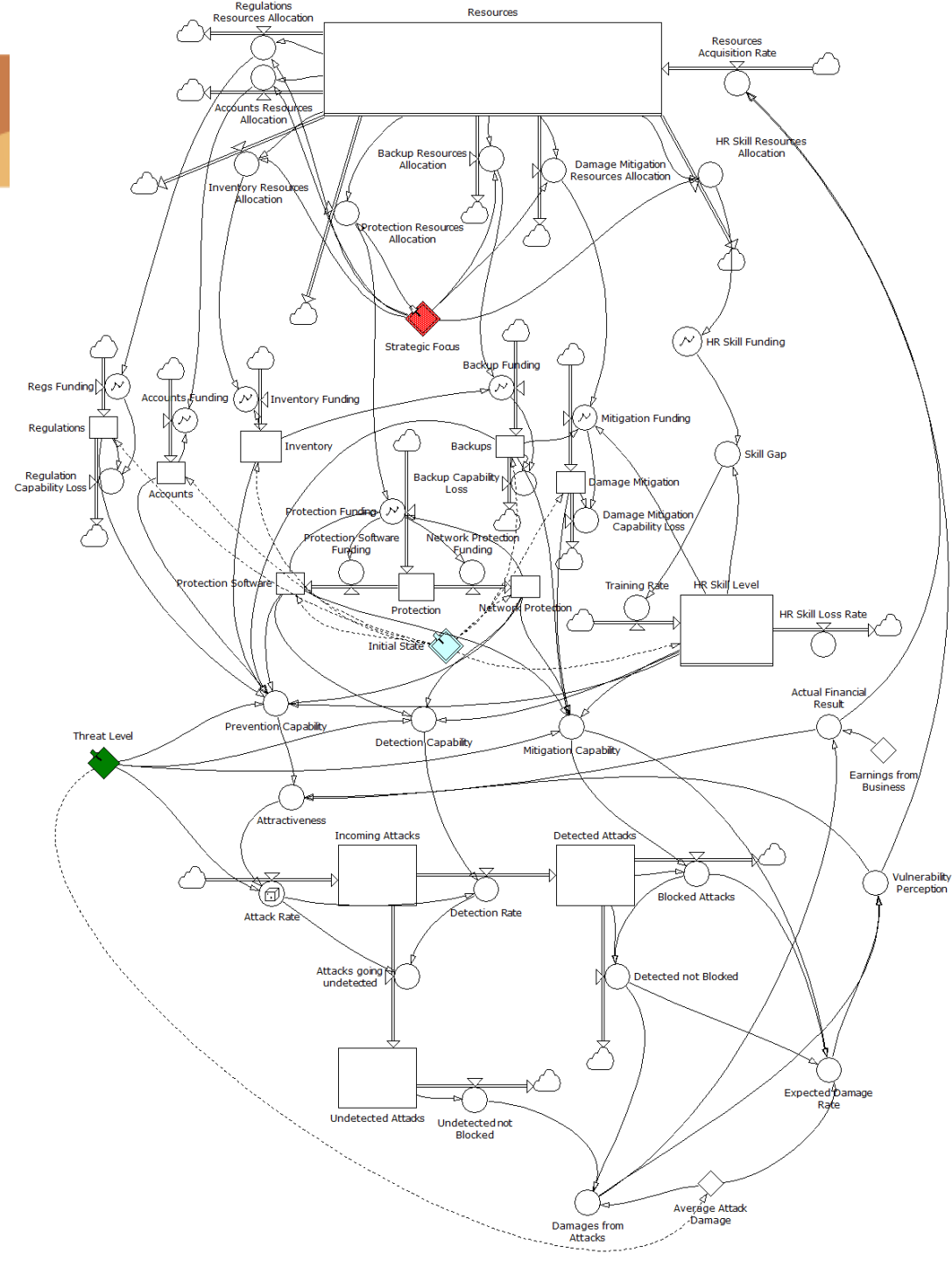
# Interesting Cycles (III)

- **Reinforcing cycle: IT and cyber defenses**
- Positive effect of investments in IT security
- Multiple cycles of this kind are present in the model (now just showing one of those, on *Mitigation*)
- Increasing investments on mitigation increases the *Mitigation Capability*, which in turn increases the attacks blocking capability, hence reducing economic losses
- Thus, the company can have further economic resources (not lost) to invest in defence
- **Virtuous Loop**

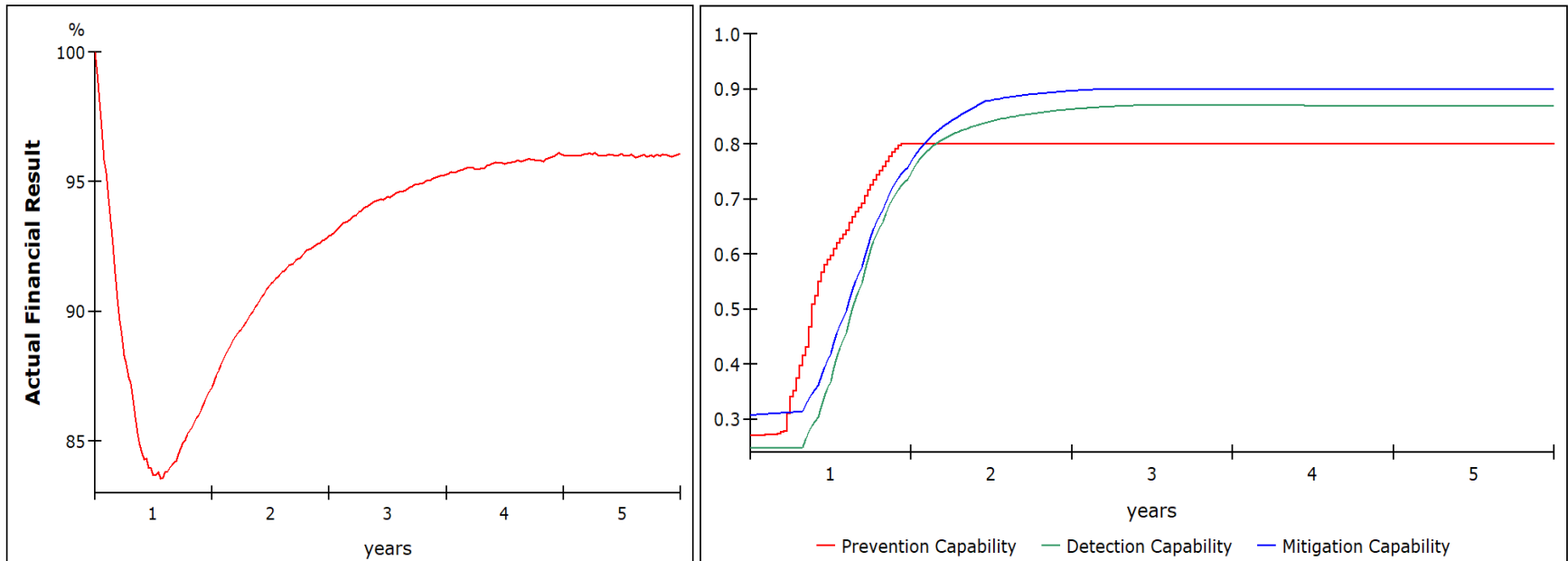


# Full SFD

- **Quantitative** model developed in PowerSim
- **Quite complex, even if still a proof of concept!**
- Three main **input variables**
- *Threat Level* defines the **level of risk** due to the scenario external environment (*Low, Medium, High*)
- *Initial State* allows to account for **different starting situations**, and uses the input from the Snapshot Survey scores
- *Strategic Focus* allows **prioritizing** investments in various macro-areas (*Regulations, Accounts, Inventory, Protection, Backup, Damage Mitigation, HR Skill*)

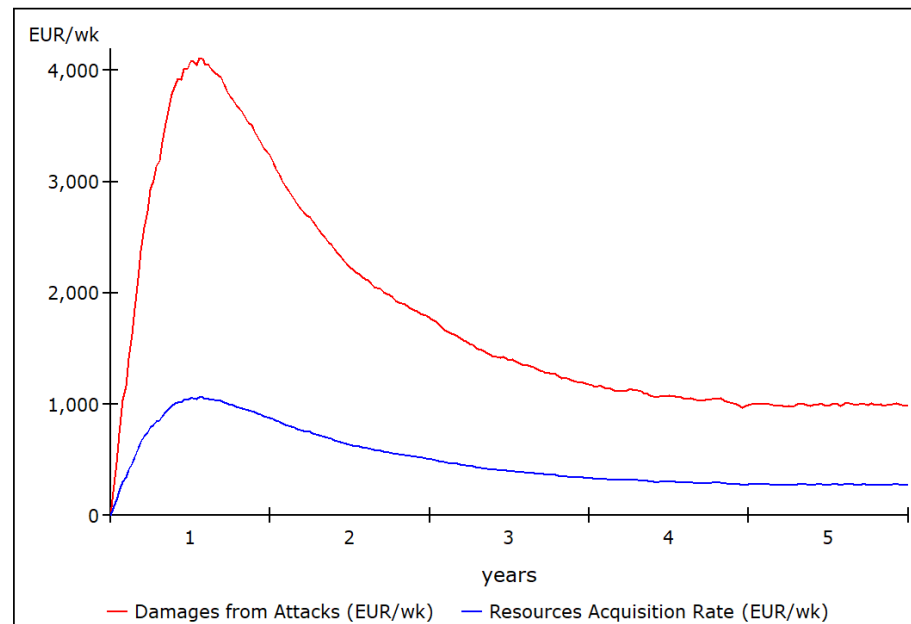


# Simulations: first scenario, Alpha Company (I)



- Alpha is a «typical» company that pays **low attention to IT and Cyber Security**
- 5 years simulation, **average risk level**
- Peak of loss ~16%, gradually reduced at around 4%
- In the first semester, ALPHA suffers severe economic losses, so they decide to invest in security
- Capability threshold reached between the second and third semester

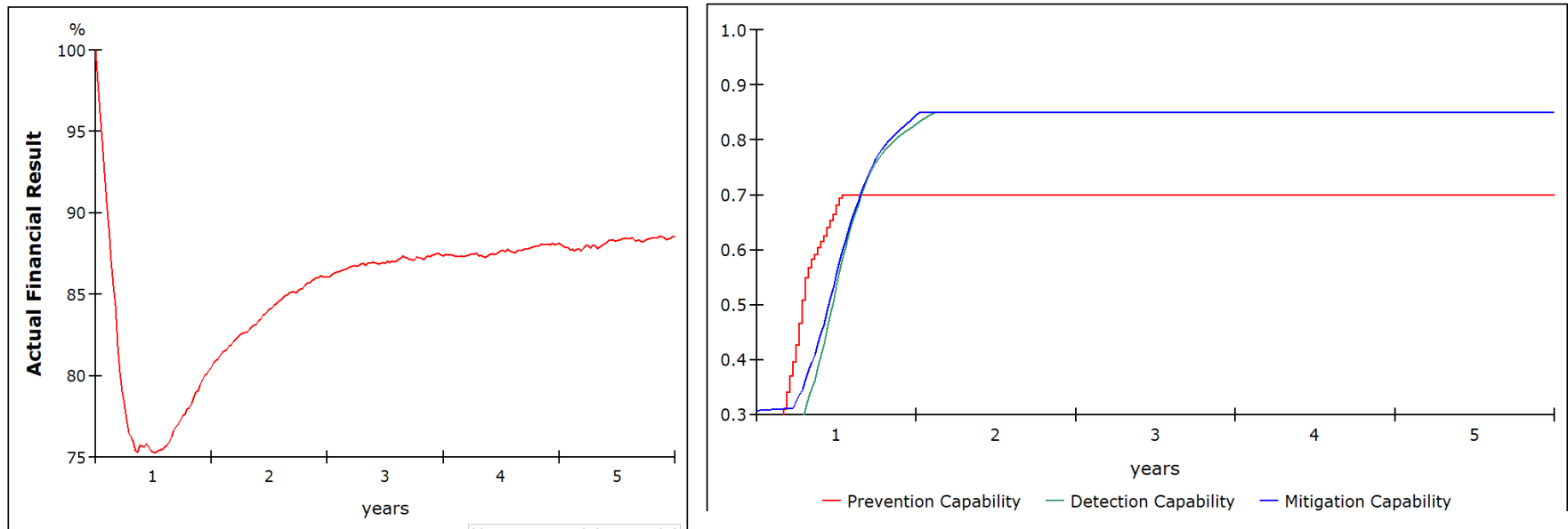
# Simulations: first scenario, Alpha Company (II)



- Suffered attacks (red) and IT Security investments (blue)
- Even in case of heavy losses, companies tend to invest carefully
- **However, by investing, they mature the awareness that ultimately it is convenient for them... but it takes time...!!! (perception delay)**

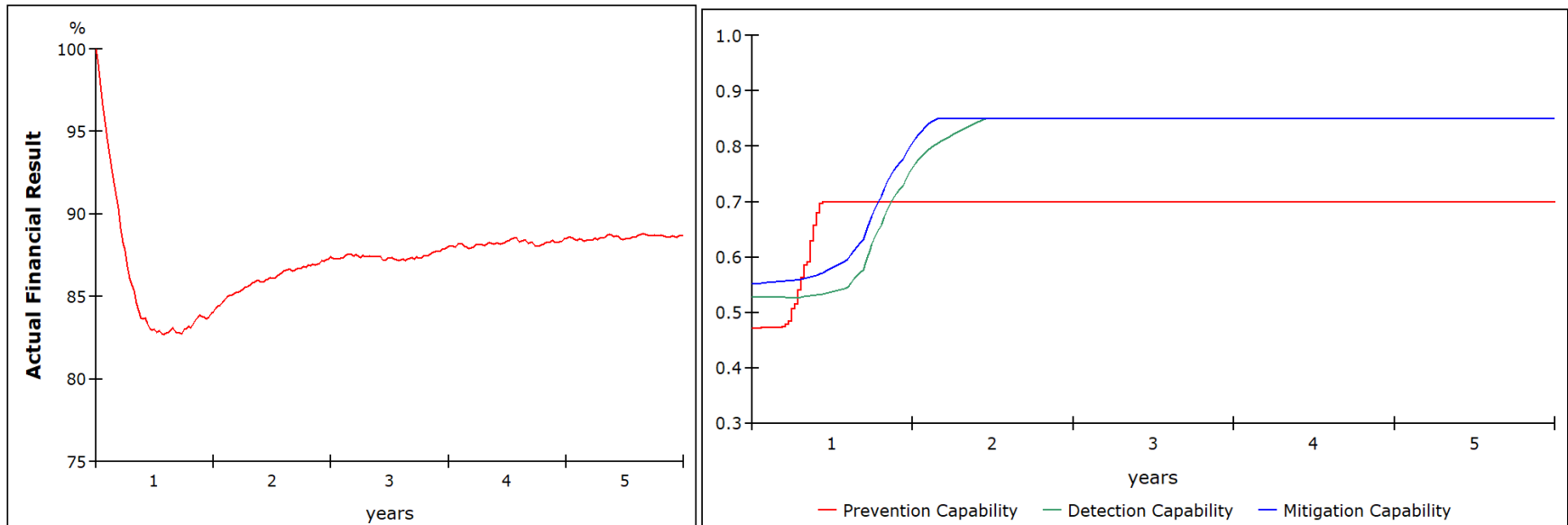


# Simulations: second scenario, still Alpha Company (III)



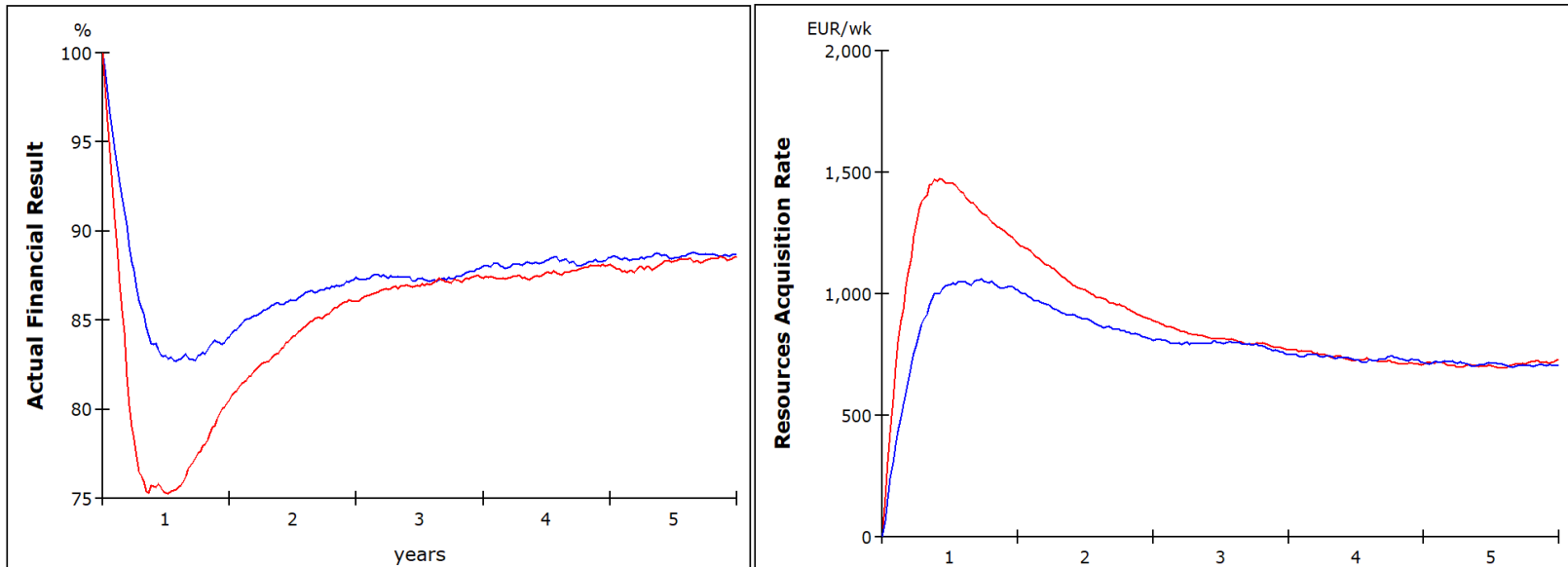
- Same company, **high risk level environment**
- Peak of loss at 25%, worst and slower recovery
- In a hostile environment, bad protection matters!!!
- Additional investments in order to compensate and anticipate future losses
- **Possible bankruptcy in the first years due to high losses!!!**

# Simulations: third scenario, Omega Company (IV)



- **Omega** has the same characteristics as Alpha but pays more attention to their IT defenses against attacks
- High risk level scenario
- Omega resists better
- In a counterintuitive way, defenses grow more gradually

# Confronting the two cases (V)



- High risk scenario confrontation
- Omega **almost** fully reduces losses and recovers quickly
- Also, Omega **spends less** even if in a critical situation, as it anticipated risk
- Possible competitive advantage of Omega over Alpha if in the same market...!!!

# Not only an application but a «needed evolution» of the FW

## Conclusions

- Tool to evaluate risks and investments in the cybersecurity field for SMEs (extendable to other types of organizations)
- Ease of use for SMEs in order to manage their improvements in IT/cyber security, by deciding where and how much to improve, thus managing at best the investments dedicated to such improvements in a more effective and aware approach
- Advantages also for third parties (i.e.: banks, insurance companies willing to define the risk level of a SME that wants to externalize their residual risk, etc.)
- Advantages following a Systems Thinking and System Dynamics approach (for this and other problems, sustainability on top, but also systemic relationships of risks in organizations)

## Developments and further research

- Unique tool integrating the assessment of current risk level by means of the Italian Framework (snapshot survey) and a System Dynamics model capable of simulating the evolution of risk, economic losses/investments, etc.
- Possibility to develop a graphical interface to evolve into a Decision Support System
- More details in the simulations, more evidence of economic aspects, etc.
- Extension to the systemic evaluation of risks in financial Institutions / Assessment of compliance / evaluation of social impacts of finance / DPIA
- Use of System Dynamics to evaluate future scenarios in the evolution of the cybersecurity market (as part of the ECHO Project – see next slide)

# Thank you!

Research funded with the support of the ECHO Project:

## European network of Cybersecurity centres and competence Hub for innovation and Operations

- ECHO is one of the four Pilot projects, launched by the European Commission, to establish and operate a Cybersecurity Competence Network.
- 48 months H2020 project, 30 partners from 15 EU member countries plus Ukraine, representing 13 existing cybersecurity competence centres and comprised of five research institutes in the cybersecurity domain; eleven large enterprises;



European network of Cybersecurity centres and competence Hub for innovation and Operations

*The ECHO project has received funding from the European Union's Horizon 2020 research and innovation programme, under the grant agreement no. 830943*

ECHO website: [www.echonetwork.eu](http://www.echonetwork.eu)

Twitter: [@ECHOcybersec](https://twitter.com/ECHOcybersec)

Linkedin: <https://www.linkedin.com/in/echo-cybersecurity-556a6717b/>

Contacts: Dr Ing Stefano ARMENIA – [s.armenia@unilink.it](mailto:s.armenia@unilink.it)