Daniel Alberto Sepúlveda Estay - DTU Orbit (31/03/2019)

Daniel Alberto Sepúlveda Estay

Research areas
Cyber Risk and Security in the Global Supply Chain
System Dynamics and Quantitative Methods

Research and teaching information
Guest Lecturer for the Course "Supply Chain Management and Advanced Planning" at DTU

Organisations

Postdoc, Department of Technology, Management and Economics
15/10/2014 → present
dasep@dtu.dk
VIP

Management Science
26/03/2019 → present
VIP

Transport DTU
26/03/2019 → present
VIP

Operations Management
26/03/2019 → present
VIP

Transport DTU
16/03/2017 → 26/03/2019 Former
VIP

Operations Management
31/05/2016 → 31/05/2016 Former
VIP

Management Science
11/11/2014 → 26/03/2019 Former
VIP

Operations Management
26/04/2017 → 26/03/2019 Former
VIP

Research outputs:

An Impact-Wave Analogy for Managing Cyber Risks in Supply Chains
Supply chains are dependent on Information Technology (IT) and cyberspace processes. Yet, despite the advantages of its increased connectivity and systems integration with suppliers and customers, this also opens the door to new risks from and to supply chain partners. Literature in this nascent research area is limited, with few frameworks available to complement traditional risk management methods. This paper shows the current results of a literature review on the field of supply chain cyber risk management (SCCRM), with the aim of gathering and structuring its extant literature and proposing a taxonomy that will give a better overview of the approaches found in the scientific literature. This taxonomy is then used to propose a novel SCCRM framework. Finally, a novel Impact-Wave analogy is presented to provide a graphical understanding of the application of this framework.

General information
State: Published
Organisations: Department of Management Engineering, Management Science, Operations Management, Technical University of Denmark
Contributors: Guerra, P., Sepúlveda Estay, D. A.
Number of pages: 5
Publication date: 2019
An Impact-Wave Analogy for Managing Cyber Risks in Supply Chains

Supply chains are dependent on Information Technology (IT) and cyberspace processes. Yet, despite the advantages of its increased connectivity and systems integration with suppliers and customers, this also opens the door to new risks from and to supply chain partners. Literature in this nascent research area is limited, with few frameworks available to complement traditional risk management methods. This paper shows the current results of a literature review on the field of supply chain cyber risk management (SCCRM), with the aim of gathering and structuring its extant literature and proposing a taxonomy that will give a better overview of the approaches found in the scientific literature. This taxonomy is then used to propose a novel SCCRM framework. Finally, a novel Impact-Wave analogy is presented to provide a graphical understanding of the application of this framework.

CyberShip: An SDN-based Autonomic Attack Mitigation Framework for Ship Systems

The use of Information and Communication Technology (ICT) in the ship communication network brings new security vulnerabilities and make communication links a potential target for various kinds of cyber physical attacks, which results in the degradation of the performance. Moreover, crew members are burdened with the task of configuring the network devices with low-level device specific syntax for mitigating the attacks. Heavy reliance on the crew members and additional software and hardware devices makes the mitigation difficult and time consuming process. Recently, the emergence of Software-Defined Networking (SDN) offers a solution to reduce the complexity in the network management tasks.

To explore the advantages of using SDN, we propose a framework based on SDN and a use case to mitigate the attacks in an automated way for improved resilience in the ship communication network.
Danish Maritime Fund (DMF) with the objective of proposing a framework for improving the resilience of the shipping industry.

General information
State: Published
Organisations: Department of Management Engineering, Management Science, Transport DTU, Operations Management, Department of Applied Mathematics and Computer Science, Cyber Security
Contributors: Sahay, R., Sepúlveda Estay, D. A.
Number of pages: 25
Publication date: 2018

Publication information
Original language: English
Electronic versions:

180404_cybership_report_WP2.pdf
Source: PublicationPreSubmission
Source-ID: 149384338
Research output: Research › Report – Annual report year: 2018

Work Package 3 and 4 Report - Cyber resilience for the shipping industry
This report describes the current state of the research performed as a part of the CyberShip project for its work packages #3 and #4. Work package #3 defines measures of prevention to cyber-attacks, which include frameworks for the strategic and tactical understanding of the effects of a cyber attack, and a number of frameworks that can be used to structure and analyze the existing risk to a cyber attack in a CyberShip system as defined in work package #2. Work Package #4 defines measure of reaction to cyber-attacks and is developed through the use of software-defined networks (SDN) on a simplified Cybership systems to reflect the potential of using such a technology on a complete CyberShip system. This reports provides a theoretical and methodological foundation to be applied in the development of case studies, subject of work package #5.

General information
State: Published
Organisations: Operations Management, Transport DTU, Management Science, Department of Management Engineering, Cyber Security, Department of Applied Mathematics and Computer Science
Contributors: Sahay, R., Sepúlveda Estay, D. A.
Number of pages: 30
Publication date: 2018

Publication information
Original language: English
Source: PublicationPreSubmission
Source-ID: 159336693
Research output: Research › Report – Annual report year: 2018

A system dynamics case study of resilient response to IP theft from a cyber- attack
Undesirable changes in supply chain physical operations derived from disruptions in the transmission or storage of digital information are reported daily despite the Information Technology (IT) protection available. Once a disruption materializes, the company losses will depend on the coherence and swiftness of the supply chain response (resilience). However, current resilience frameworks are qualitative, do not address evolution over time as a relevant aspect, and thus do not provide indications on how to design a resilient response. This paper contributes to closing this gap by developing a system dynamics model from an actual case of resilient response after a cyber-attack. Both casespecific and generic structures are extracted from the case data analysis, and a reaction mechanism is proposed that results in the observed behavior. The identification of these structures should eventually aid decision makers in the process of designing a resilient supply chain response.

General information
State: Published
Organisations: Department of Management Engineering, Management Science, Transport DTU, Operations Management
Contributors: Sepúlveda Estay, D. A., Khan, O.
Pages: 1291-1295
Publication date: 2017

Host publication information
Title of host publication: Proceedings of the 2017 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM)
Publisher: IEEE
Managing cyber-risk and security in the global supply chain: a systems analysis approach to risk, structure and behaviour

The threat of cyber-attacks continues to grow and disrupt global supply chains, exposing companies to disruptions that severely affect or completely halt normal operations. This impacts business performance negatively through the company’s bottom line and reputation, even resulting in long-term legal ramifications. As a result, little information about attacks and their consequences is published. Supply chains continue to prepare for cyber-attacks through a mix of traditional risk and resilience frameworks, protecting their networks through patches, firewalls and antiviruses, or financially through insurance. Yet these approaches are not giving the expected results, as reflected by the steady increase in disruptions from cyber-attacks. This thesis investigates and proposes tools for managing cyber-risks in the supply chain, derived from an analysis that follows three main steps. In step one, existing knowledge about supply chain cyber-resilience is analysed through a systematic literature review, and gaps are identified. Two of the identified gaps are addressed in detail, 1) insufficient understanding of the particular characteristics cyber-risks and how these compare to other supply chain risks for effective risk management, and 2) insufficient address by current methods to aspects of compartmentalization, static focus and history-dependence in the management of supply chain cyber-risk and cyber-resilience. Step two of this thesis explores the first gap by identifying the particular characteristics of cyber-risks from cyber-attack report data. Finally in step three methods based on systems thinking are applied to case studies to evaluate the degree to which these methods address compartmentalization, dynamics and history dependency in their application to the management of cyber-risk and cyber-resilience. The findings of the research are in three main domains. First, the research reveals relevant gaps in the traditional methods available for the management of cyber risks, in areas such as their consideration of dynamic behaviour, inadequate or difficult reporting of events, their dependence on historical data to manage unknown or new attacks, and a silo-approach for managing a problem that is cross-disciplinary. Second, relevant differences between cyber-risks and other supply chain risks are identified, in areas such as the capacity of disruptions from cyber risks to go undetected, the high reproduction fidelity of cyber-risks, the capacity of cyber risks to affect different geographical locations simultaneously, and the complexity of cyber-attacks. Finally, the research reveals that the novel use of methods based in systems thinking for managing cyber-risks at the same time address gaps found in traditional methods, and provide a foundation for thinking about cyber-risks not as an outside threat, but rather as the result of incomplete requirements to the supply chain design. This change in focus could allow supply chains to minimize losses by preparing the system for reaction to whatever cyber-risk leads to an operational disruption. The findings of the research have both industrial implications and academic implications. The industrial implications suggest supply chains can benefit from designing the behaviours they require through cross-disciplinary, simulation-based techniques. The academic implications suggest that researchers will benefit from 1) adjusting reporting times to match the quick development cycle of cyber-attacks, 2) consolidating a cross-disciplinary cyber-risk and resilience research community, and 3) expanding existing research methods by integrating dynamic systems thinking into data gathering and analysis.

A systems approach to cyber-risk management

General information
State: Published
Organisations: Department of Management Engineering, Management Science
Contributors: Sepúlveda Estay, D. A.
Number of pages: 620
Publication date: 2017

Publication information
Publisher: DTU Management Engineering
Original language: English
Electronic versions:
180411_PhD_Thesis_Complete_Printing.pdf
Source: PublicationPreSubmission
Source-ID: 146599845
Research output: Research › Ph.D. thesis – Annual report year: 2018
Control Structures in supply chains as a way to manage unpredictable cyber-risks

Supply chain growth, and their dependence on Information Technology (IT), is making cyber risks an increasingly unmanageable threat through traditional risk assessment methods. Systemic analysis methods have been identified as alternatives to traditional methods. This paper analyzes the application of a systemic risk analysis methodology to understand cyber risks in the supply chain. A generic supply chain is analyzed, and information flows, dynamic structures and the influence of cyber-attack on these are identified. This paper argues that a systemic approach is more efficient in detecting vulnerabilities, enabling an evolving disruption response process and culture in the supply chain.

General information
State: Published
Organisations: Department of Management Engineering, Management Science, Aalborg University
Contributors: Sepúlveda Estay, D. A., Khan, O.
Number of pages: 10
Publication date: 2016
Peer-reviewed: Yes
Electronic versions:
160619_Full_Paper.pdf
Source: PublicationPreSubmission
Source-ID: 126263311
Research output: Research - peer-review » Paper – Annual report year: 2016

Hackeando los ciber-riesgos en la cadena de suministro: Para entender los controles correctos, hay que mirar el sistema

Si se consideran tanto la creciente complejidad de las redes de abastecimiento, como la consecuente exposición de estas redes a interrupciones inesperadas ocasionadas por ciber-ataques, se requiere una forma más amplia para entender los ciber-riesgos en las cadenas de suministro. En este artículo se describen algunas de las razones por las que los métodos de evaluación de riesgos actuales son insuficientes, se proporciona una analogía para entender los efectos dinámicos en una empresa, se describe en términos generales lo que significa entender los ciber-riesgos desde el punto de vista de teoría de control, y se enuncia una nueva forma de entender la resiliencia en la cadena de suministro. Nuestro trabajo propone un cambio foco desde la confiabilidad de los componentes individuales en la cadena de suministro, hacia el control y un entendimiento más profundo del sistema.

General information
State: Published
Organisations: Department of Management Engineering, Management Science
Contributors: Sepúlveda Estay, D. A., Khan, O.
Publication date: 2016
Peer-reviewed: Unknown

Publication information
Journal: Logistec
Issue number: 05 Enero 2016
Original language: Spanish
Electronic versions:
HACEANDO.pdf
URLs:
Extending supply chain risk and resilience frameworks to manage cyber risk

This paper proposes two complementary tools for the description and quantification of dynamic effects arising from supply chain cyber-attacks. The first tool proposes a comprehensive analysis of the problem space through system dynamics methods, to identify explicitly mental models regarding aspects such as stakeholders, relevant relationships, feedback effects and potential policy levers. The second tool is proposed as a way of transitioning towards a dynamic analysis of the problem of cyber-attacks on supply chains, and is complementary to existing risk analysis tools.

General information
State: Published
Organisations: Department of Management Engineering, Management Science
Contributors: Sepúlveda Estay, D. A., Khan, O.
Number of pages: 10
Publication date: 2015
Peer-reviewed: Yes
Event: Paper presented at 22nd EurOMA Conference, Neuchâtel, Switzerland.
Keywords: Supply chain, Cyber-risk, Resilience
Electronic versions:
Hacking_cyber_risks.pdf
Source: PublicationPreSubmission
Source-ID: 112536415
Research output: Research - peer-review › Paper – Annual report year: 2015

Hacking cyber-risks back in their tracks: to identify the right supply chain controls, look at the system

A more comprehensive way of looking at cyber-risks in supply chains is required, when considering the increasing complexity of the supply networks and the exposure to unexpected disruptions, caused by cyber-attacks. This article describes some of the reasons why current risk assessment methods are insufficient. The article provides an analogy for understanding the dynamic effects in a company. It describes in general terms what it means to understand cyber-risks from the control perspective, and it describes a new way to understand supply chain resilience. The focus is changed from the reliability of the supply chain components to the control and a deeper understanding of the supply chain system.

General information
State: Published
Organisations: Department of Management Engineering, Management Science
Contributors: Sepúlveda, D., Khan, O.
Pages: 32-35
Publication date: 2015
Peer-reviewed: Unknown

Publication information
Journal: Effektivitet
Issue number: 3
ISSN (Print): 0903-2266
Ratings:
ISI indexed (2013): ISI indexed no
ISI indexed (2012): ISI indexed no
ISI indexed (2011): ISI indexed no
Original language: English
Electronic versions:
Hacking_cyber_risks.pdf
URLs:
Source: PublicationPreSubmission
Source-ID: 119572568
Supply Chain Cyber-Resilience: Creating an Agenda for Future Research

Supply chains have become more vulnerable in recent years, and high-profile cyber-attacks that have crippled the supply chains of well-known companies reveal that the point of entry for hackers is often through the weakest link in the chain. Exacerbated by growing complexity and the need to be visible, these supply chains share vital streams of information every minute of the day, thereby becoming an easy and highly lucrative target for talented criminals, causing financial losses as well as damaging brand reputation and value. Companies must therefore invest in supply chain capabilities to withstand cyber-attacks (i.e., cyber-resilience) in order to guard against potential threats. They must also embrace the reality that this often-unknown dimension of risk is the "new normal". Although interest on this topic has grown in the business world, less has been reported by the academic community. One reason for this could be due to the convergence of two different disciplines, information technology and supply chains, where supply chain cyber-risk and cyber-resilience appear to have a natural fit. The topic of cyber-resilience in supply chains is still in early stages of development, and this is one of the first journals to focus a special issue on it. Currently, the closest academic literature is within the realms of supply chain risk and resilience, where numerous models and frameworks exist. In this article, this literature is explored to identify whether these models can incorporate the dimension of cyber-risk and cyber-resilience. In doing so, we create a research agenda for supply chain cyber-resilience and provide recommendations for both academia and practice.

Towards a supply chain cyber-risk and resilience research agenda - a systematic literature review

The increased dependence of supply chains on information technology has exacerbated the impact of cyber risks (Dedrick et al., 2008), ranging from the breach of data confidentiality, to the destruction of data and the disruption of supply operations.

There is a robust body of knowledge, which has allowed the development of models, frameworks, tools and techniques to understand and manage supply chain risk (Khan et al., 2007). However, the evaluation of cyber risks and resilience in the supply chain has been less explored.

The purpose of this paper is to contribute to the gap in theory through a systematic review of the literature (Tranfield et al., 2003). Specifically the focus is on 1) developing a definition for cyber resilience in the supply chain, and 2) suggesting a research agenda for this area.

General information
State: Published
Organisations: Department of Management Engineering, Management Science
Tradeoffs between alleviating emergency department crowding and return visits

General information
State: Published
Organisations: Department of Management Engineering, Management Science, Beth Israel Deaconess Medical Center
Number of pages: 1
Publication date: 2014
Peer-reviewed: No
Event: Poster session presented at 6th Danish Emergency Medicine Conference, Odense, Denmark.
Electronic versions:
Tradeoffs_between_alleviating_emergency_department.pdf
Source: PublicationPreSubmission
Source-ID: 103045484
Research output: Research › Poster – Annual report year: 2014

Projects:

Development of a Massive Open Online Course (MOOC)
Kirchner, K., PI, Department of Management Engineering, Management Science, Implementation and Performance Management
Jacobsen, P., Project Participant, Operations Management, Transport DTU, Management Science, Department of Management Engineering
Sepúlveda Estay, D. A., Project Participant, Operations Management, Transport DTU, Management Science, Department of Management Engineering
26/10/2018 → …
Nature of activity type: Teaching
Project: Research › Teaching

CyberShip: Cyber Resilience for the Shipping Industry (CyberShip)
The shipping industry has become more vulnerable to cyber-attacks in recent years, because of its dependence on information technology and increasingly complex networks. Cyber systems are incorporated into almost every facet of maritime operations, such as financial and human resources management, security systems, navigation (Global Navigation Satellite Systems (GNSS), Automatic Identification System (AIS), Electronic Chart Display Systems (ECDIS), etc.), communications, electronic certificates, cargo tracking, pre-arrival processing and other key systems and equipment. All maritime structures (including ships and offshore facilities) as well as the connected infrastructure (e.g. offices of shipping companies, ports etc) are vulnerable. Currently, the awareness regarding cyber security aspects is either at a very low level or completely disregarded. The issue of cyber security has been brought into the attention of the International Maritime Organization (IMO), and industry associations such as BIMCO and others. As a result of this guidelines for tackling cyber security problems have been developed. This project is aimed at providing shipping companies and regulators with a reference framework and decision support model to better cope with disruptions originating from a cyber-attack.
Barfod, M. B., Project Manager, Department of Management Engineering, Management Science, Transport DTU, Operations Management
Psaraftis, H. N., Project Participant, Department of Management Engineering, Management Science, Transport DTU, Operations Management
Jensen, C. D., Project Participant, Department of Applied Mathematics and Computer Science, Cyber Security, Copenhagen Center for Health Technology
Sepúlveda Estay, D. A., Project Participant, Department of Management Engineering, Management Science, Transport DTU, Operations Management
Sahay, R., Project Participant, Department of Applied Mathematics and Computer Science, Cyber Security
01/09/2017 → 31/08/2019
Documents:
Activities:

2019 STAMP Workshop
Daniel Alberto Sepúlveda Estay (Speaker)
Nancy Leveson (Speaker)
John Thomas (Lecturer)
Rishikesh Sahay (Speaker)

Department of Management Engineering
Management Science
Transport DTU
Cyber Security

Department of Applied Mathematics and Computer Science

Description
MIT STAMP/STPA Workshop took place during March 25-29, 2019 in Cambridge, MA, USA.

STAMP is an accident causality model based on systems theory and systems thinking. STAMP integrates into engineering analysis the causal factors in our increasingly complex systems such as software, human-decision making and human factors, new technology, social and organizational design, and safety culture.

STPA is a powerful new hazard analysis technique based on STAMP while CAST is the equivalent for accident/incident analysis. These tools are now used globally in almost every industry. Newer tools, such of those for doing early concept analysis (STECA) security analysis (STPA-Sec) and leading indicators have been developed. This free workshop will provide attendees with the opportunity to learn how to use these new tools, to meet with users and to hear about applications, evaluations, and the latest developments in this powerful new approach to system safety engineering and to cyber security.

Degree of recognition: International

Documents:
190325-STAMP_Presentation

Links:

Related external organisation

Massachusetts Institute of Technology
02139, Cambridge, Massachusetts, United States
Activity: Talks and presentations › Conference presentations

Lecturer - Production and Scheduling
Period: 4 Feb 2019 → 20 May 2019
Daniel Alberto Sepúlveda Estay (Lecturer)
Commercial ships are equipped with intelligent devices which continuously collect data from the environment and other ships, and provide these data to controllers that manage these devices and make decisions based on this data. However, the increased deployment of such intelligent devices also increases the potential security risks.

This project aims to map the information systems (IT and OT) that exist on a ship, identify and categorize the risks in these systems, and provide measures and processes to improve the reaction and recovery (resilience) in a shipping operation after a cyber-attack.

Degree of recognition: International
Documents:
- NATO workshop Invitation
- Poster Presentation
- NATO Rovaniemi ARW Group Photo

Related event

NATO Advanced Research Workshop: NARW 2019
27/01/2019 → 30/03/2019
Rovaniemi, Finland
Activity: Talks and presentations › Talks and presentations in private or public companies and organisations

Managing cyber-risk and security in the global supply chain
Period: 8 Jan 2019
Daniel Alberto Sepúlveda Estay (Guest lecturer)
Department of Management Engineering
An Impact-Wave Analogy for Managing Cyber Risks in Supply Chains

Period: 17 Dec 2018
Daniel Alberto Sepúlveda Estay (Guest lecturer)
Department of Management Engineering
Management Science
Transport DTU
Operations Management

Description
Supply chains are dependent on Information Technology (IT) and cyberspace processes. Yet, despite the advantages of its increased connectivity and systems integration with suppliers and customers, this also opens the door to new risks from and to supply chain partners. Literature in this nascent research area is limited, with few frameworks available to complement traditional risk management methods. This presentation based on a conference paper of the same title shows the current results of a literature review on the field of supply chain cyber risk management (SCCRM), with the aim of gathering and structuring its extant literature and proposing a taxonomy that will give a better overview of the approaches found in the scientific literature. This taxonomy is then used to propose a novel SCCRM framework. Finally, a novel Impact-Wave analogy is presented to provide a graphical understanding of the application of this framework.

Degree of recognition: International
Documents:
IEEE-IEEM18-P-0561
Links:

Related event
2018 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM)
16/12/2018 → 19/12/2018
Bangkok, Thailand
Activity: Talks and presentations › Conference presentations

Guest Lecturer - Course 42457 Supply Chain Management
Period: 4 Sep 2018 → 25 Sep 2018
Daniel Alberto Sepúlveda Estay (Guest lecturer)
Department of Management Engineering
Transport DTU
Management Science
Operations Management
Description
Delivered the following topics

1.- Supply Chain Distribution Game
2.- Supply Chain Coordination
3.- Supply Chain production strategies

Related event

Supply Chain Management Course 42457 E18
03/09/2018 → 15/12/2018
Kongens Lyngby, Denmark
Activity: Talks and presentations › Guest lectures, external teaching and course activities at other universities

Lecturer - Production and Planning course 42582
Period: 4 Sep 2018 → 20 Dec 2018
Daniel Alberto Sepúlveda Estay (Guest lecturer)
Department of Management Engineering
Transport DTU
Management Science
Operations Management

Description
Topics covered:
1.- Supply Chain Management Game
2.- Quality Management
3.- Inventory Management
Degree of recognition: National
Documents:
IMG_20180910_092932
IMG_20180910_093038
IMG_20180910_093306
IMG_20180910_093630

Related event

Course 42582 Production and Planning (Produktion og Planlægning)
03/09/2018 → 15/12/2018
Kongens Lyngby, Denmark
Activity: Talks and presentations › Guest lectures, external teaching and course activities at other universities

Internal Examiner
Period: 6 Jun 2018
Daniel Alberto Sepúlveda Estay (External examiner)
Department of Management Engineering
Transport DTU
Management Science
Operations Management

Description
MSc. Thesis examiner for Student Pablo Guerra (s150907)
Degree of recognition: National
Documents:
IMG_20180606_113343
Activity: Examinations and supervision › Internal examination
Guest Lecturer - Supply Chain Management Game  
Period: 7 Mar 2018  
Daniel Alberto Sepúlveda Estay (Guest lecturer)  
Diana Cordes Feibert (Lecturer)  
Department of Management Engineering  
Transport DTU  
Management Science  
Operations Management  

Description  
Topic covered:  
1.- Supply Chain Management Game  
Degree of recognition: National  
Documents:  
IMG_20180307_140758  
IMG_20180307_140733  
IMG_20180307_155331  

Related event  
Course 41713: Produktionsteknologi og produktionsstyring  
01/01/2018 → 20/05/2018  
Kongens Lyngby, Denmark  
Activity: Talks and presentations › Guest lectures, external teaching and course activities at other universities

Guest Lecturer - Supply Chain Management  
Period: 14 Feb 2018  
Daniel Alberto Sepúlveda Estay (Guest lecturer)  
Omera Khan (Lecturer)  
Department of Management Engineering  
Transport DTU  
Management Science  
Operations Management  

Description  
Delivered topics:  
1.- Supply Chain Distribution Game  
Degree of recognition: National  
Documents:  
All4  
Team3a  
Team1b  
Team2b  
Team4c  

Related event  
Supply Chain Management  
01/01/2018 → 20/05/2018  
Copenhagen, Denmark  
Activity: Talks and presentations › Guest lectures, external teaching and course activities at other universities

A System Dynamics Case Study of Resilient Response to IP Theft from a Cyber-attack  
Period: 12 Dec 2017  
Daniel Alberto Sepúlveda Estay (Speaker)  
Operations Management
Undesirable changes in supply chain physical operations derived from disruptions in the transmission or storage of digital information are reported daily despite the Information Technology (IT) protection available. Once a disruption materializes, the company losses will depend on the coherence and swiftness of the supply chain response (resilience). However, current resilience frameworks are qualitative, do not address evolution over time as a relevant aspect, and thus do not provide indications on how to design a resilient response. This paper contributes to closing this gap by developing a system dynamics model from an actual case of resilient response after a cyber-attack. Both case-specific and generic structures are extracted from the case data analysis, and a reaction mechanism is proposed that results in the observed behavior. The identification of these structures should eventually aid decision makers in the process of designing a resilient supply chain response.

Degree of recognition: International

Documents:
ieem2017_P-0663-Oral

Related event

2017 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM)
10/12/2017 → 13/12/2017
Singapore, Singapore
Activity: Talks and presentations › Conference presentations

MADE Danish Manufacturing Association Conference
Period: 15 Jun 2017
Daniel Alberto Sepúlveda Estay (Speaker)
Department of Management Engineering
Management Science
Operations Management
Transport DTU

Description
Supply Chain Cyber resilience - The New Normal
Documents:
170515b_MADE_Final

Related event

MADE Danish Manufacturing Association Conference
15/06/2017 → 15/06/2017
Activity: Talks and presentations › Conference presentations

Teaching Assistant for course 15.872 System Dynamics II
Period: 15 Apr 2017 → 2 Jun 2017
Daniel Alberto Sepúlveda Estay (Guest lecturer)
Bradley Morrison (Lecturer)
Department of Management Engineering
Management Science
Transport DTU

Description
15.871 and 872 introduce you to system dynamics modeling for the analysis of business policy and strategy. You will learn to visualize a business organization in terms of the structures and policies that create dynamics and regulate performance. System dynamics allows us to create ‘microworlds,’ management flight simulators where space and time can be compressed, slowed, and stopped so we can experience the long-term side effects of decisions, systematically explore new strategies, and develop our understanding of complex systems. In these system dynamics courses we use
simulation models, case studies, and management flight simulators to develop principles of policy design for successful management of complex strategies. Case studies of successful strategy design and implementation using system dynamics will be stressed. We consider the use of systems thinking to promote effective organizational learning. The principal purpose of modeling is to improve our understanding of the ways in which an organization’s performance is related to its internal structure and operating policies as well as those of customers, competitors, suppliers, and other stakeholders.

During the course students use several simulation models to explore such strategic issues as fluctuating sales, production and earnings; market growth and stagnation; the diffusion of new technologies; the use and reliability of forecasts; the rationality of business decision making; and applications in health care, energy policy, environmental sustainability, and other topics.

Students learn to recognize and deal with situations where policy interventions are likely to be delayed, diluted, or defeated by unanticipated reactions and side effects. You will have a chance to use state of the art software for computer simulation and gaming. Assignments give hands-on experience in developing and testing computer simulation models in diverse settings.

Degree of recognition: National

Documents:
Syllabus for course 15.872 System Dynamics II

Related event

15.872 System Dynamics II
15/04/2017 → 02/06/2017
Activity: Talks and presentations › Guest lectures, external teaching and course activities at other universities

2017 STAMP Workshop
Period: 27 Mar 2017 → 30 Mar 2017
Daniel Alberto Sepúlveda Estay (Speaker)
Nancy Leveson (Speaker)
John Thomas (Lecturer)
Department of Management Engineering
Management Science
Transport DTU

Description
MIT STAMP/STPA Workshop took place during March 27-30, 2017.

STAMP is an accident causality model based on systems theory and systems thinking. STAMP integrates into engineering analysis the causal factors in our increasingly complex systems such as software, human-decision making and human factors, new technology, social and organizational design, and safety culture.

STPA is a powerful new hazard analysis technique based on STAMP while CAST is the equivalent for accident/incident analysis. These tools are now used globally in almost every industry. Newer tools, such of those for doing early concept analysis (STECA) security analysis (STPA-Sec) and leading indicators have been developed. This free workshop will provide attendees with the opportunity to learn how to use these new tools, to meet with users and to hear about applications, evaluations, and the latest developments in this powerful new approach to system safety engineering and to cyber security.

Degree of recognition: International

Documents:
170330_Workshop_presentation_Sepulveda

Related external organisation

Massachusetts Institute of Technology
02139, Cambridge, Massachusetts, United States
Activity: Talks and presentations › Conference presentations

Webinar: Recovery of Operations from Cyberattacks - a structure for response
Period: 15 Mar 2017
Daniel Alberto Sepúlveda Estay (Speaker)
Cyber attacks on supply chains are a constant threat to organizations. News media are regularly reporting cyber attacks to supply chains that result in data theft or denial of service. Examples abound, such as the theft of credit card data for 70 million customers from Target in 2013, and a sophisticated distributed attack that blocked the websites of major companies in the east-US such as Amazon, Starbucks and PayPal, during most the 21st of October 2016. Although relevant, this coverage often overshadows cyber-attacks that affect supply chain operations, which continue to occur without media attention. This is giving hackers free range to refine and practice their techniques for increased penetration and damage, resulting in a whole different range of disruptions such as container theft, intervention of plant operation, or misallocation of payments, for example. The MIT Center for Transportation & Logistics (CTL) will host a webinar to address hacker-related vulnerabilities in supply chain operations. At the root of this problem lies the structure of data exchanges between supply chain partners. Key questions for supply chain managers include: How does your supply chain manage these data exchanges? How much are you assigning these problems to IT even though they have direct impact on operations? How does your supply chain prevent these attacks, or react when these attacks happen? Is your supply chain merely relying on external insurance, or do you understand how these exchanges can be designed and controlled in cases of attack for improved recovery? Dr. Jim Rice and Daniel Sepulveda, PhD student, will address these questions, and talk about research findings that offer a deeper understanding of the structures that supply chains can use to improve their response from hacker attacks so as to minimize operational disruption and allow a more efficient recovery.

Chairman: James Blanley Rice. Center for Transportation and Logistics at the Massachusetts Institute of Technology
Degree of recognition: International
Documents:
170315_Webinar_Daniel_Sepulveda
MIT-CTL-Webinar_registration_page
Links:
https://www.youtube.com/watch?v=zsmpjNRcIfl (Cyber attacks on supply chains are a constant threat to organizations. News media are regularly reporting cyber attacks to supply chains that result in data theft or denial of service. Examples abound, such as the theft of credit card data for 70 million customers from Target in 2013, and a sophisticated distributed attack that blocked the websites of major companies in the east-US such as Amazon, Starbucks and PayPal, during most the 21st of October 2016. Although relevant, this coverage often overshadows cyber-attacks that affect supply chain operations, which continue to occur without media attention. This is giving hackers free range to refine and practice their techniques for increased penetration and damage, resulting in a whole different range of disruptions such as container theft, intervention of plant operation, or misallocation of payments, for example. The MIT Center for Transportation & Logistics (CTL) will host a webinar to address hacker-related vulnerabilities in supply chain operations. At the root of this problem lies the structure of data exchanges between supply chain partners. Key questions for supply chain managers include: How does your supply chain manage these data exchanges? How much are you assigning these problems to IT even though they have direct impact on operations? How does your supply chain prevent these attacks, or react when these attacks happen? Is your supply chain merely relying on external insurance, or do you understand how these exchanges can be designed and controlled in cases of attack for improved recovery? Dr. Jim Rice and Daniel Sepulveda, PhD student, will address these questions, and talk about research findings that offer a deeper understanding of the structures that supply chains can use to improve their response from hacker attacks so as to minimize operational disruption and allow a more efficient recovery.)

Related event
Webinar: Recovery of Operations from Cyberattacks - a structure for response
15/03/2017 → …
Cambridge, United States
Activity: Talks and presentations › Conference presentations

35th International Conference on the System Dynamics Society (Event)
Period: 1 Mar 2017 → 30 Apr 2017
Daniel Alberto Sepúlveda Estay (Reviewer)
Department of Management Engineering
Management Science
Description
2017 marks the 60th anniversary of the founding of the field of System Dynamics. It is thus fitting that we hold the 60th anniversary conference in Cambridge, next to the MIT campus where Jay Forrester developed the field. Today, System Dynamics is used around the world, from K-12 classrooms through doctoral programs, in scholarly research across many disciplines, and in applications from organizational change to climate change, from medicine to management. We will celebrate the accomplishments of the past six decades and explore future directions by showcasing the best work in dynamic modeling being done today.

There will be plenary presentations showcasing important work in the field, along with parallel and poster sessions, making available the most current research, applications, and work in progress. There is a full day of skill-building workshops covering a range of topics from basic software use to advanced analysis techniques. In addition, there will be interest group sessions, student colloquia, the modeling assistance workshop, vendor displays, demonstrations, and more. The conference schedule will provide time for social and professional interaction.

The Society's annual international conference is held alternately in North America and Europe, with occasional appearances in Asia and the Pacific Rim. These conferences, and the meetings of local chapters and interest groups, introduce newcomers to the field, keep practitioners aware of current developments, and provide unparalleled networking opportunities
Degree of recognition: International

Related event
35th International Conference on the System Dynamics Society
16/07/2017 → 20/07/2017
Cambridge, United States
Activity: Research › Peer review of manuscripts

Teaching Assistant for course 15.871 Introduction to System Dynamics
Period: 7 Jan 2017 → 15 Apr 2017
Daniel Alberto Sepúlveda Estay (Participant)
Department of Management Engineering
Management Science
Transport DTU

Description
15.871 and 872 introduce you to system dynamics modeling for the analysis of business policy and strategy. You will learn to visualize a business organization in terms of the structures and policies that create dynamics and regulate performance. System dynamics allows us to create ‘microworlds,’ management flight simulators where space and time can be compressed, slowed, and stopped so we can experience the long-term side effects of decisions, systematically explore new strategies, and develop our understanding of complex systems. In these system dynamics courses we use simulation models, case studies, and management flight simulators to develop principles of policy design for successful management of complex strategies. Case studies of successful strategy design and implementation using system dynamics will be stressed. We consider the use of systems thinking to promote effective organizational learning. The principal purpose of modeling is to improve our understanding of the ways in which an organization’s performance is related to its internal structure and operating policies as well as those of customers, competitors, suppliers, and other stakeholders.

During the course students use several simulation models to explore such strategic issues as fluctuating sales, production and earnings; market growth and stagnation; the diffusion of new technologies; the use and reliability of forecasts; the rationality of business decision making; and applications in health care, energy policy, environmental sustainability, and other topics.

Students learn to recognize and deal with situations where policy interventions are likely to be delayed, diluted, or defeated by unanticipated reactions and side effects. You will have a chance to use state of the art software for computer simulation and gaming. Assignments give hands-on experience in developing and testing computer simulation models in diverse settings.
Degree of recognition: National
Documents:
Syllabus for course 15.871 Introduction to System Dynamics
Activity: Other
Teaching Assistant for course 15.871 Introduction to System Dynamics
Period: 7 Jan 2017 → 15 Apr 2017
Daniel Alberto Sepúlveda Estay (Lecturer)
Bradley Morrison (Lecturer)
Department of Management Engineering
Management Science
Transport DTU

Description
15.871 and 872 introduce you to system dynamics modeling for the analysis of business policy and strategy. You will learn to visualize a business organization in terms of the structures and policies that create dynamics and regulate performance. System dynamics allows us to create ‘microworlds,’ management flight simulators where space and time can be compressed, slowed, and stopped so we can experience the long-term side effects of decisions, systematically explore new strategies, and develop our understanding of complex systems. In these system dynamics courses we use simulation models, case studies, and management flight simulators to develop principles of policy design for successful management of complex strategies. Case studies of successful strategy design and implementation using system dynamics will be stressed. We consider the use of systems thinking to promote effective organizational learning.

The principal purpose of modeling is to improve our understanding of the ways in which an organization’s performance is related to its internal structure and operating policies as well as those of customers, competitors, suppliers, and other stakeholders.

During the course students use several simulation models to explore such strategic issues as fluctuating sales, production and earnings; market growth and stagnation; the diffusion of new technologies; the use and reliability of forecasts; the rationality of business decision making; and applications in health care, energy policy, environmental sustainability, and other topics.

Students learn to recognize and deal with situations where policy interventions are likely to be delayed, diluted, or defeated by unanticipated reactions and side effects. You will have a chance to use state of the art software for computer simulation and gaming. Assignments give hands-on experience in developing and testing computer simulation models in diverse settings.

Degree of recognition: National
Documents:
Syllabus for course 15.871 Introduction to System Dynamics

Related external organisation

Massachusetts Institute of Technology
02139, Cambridge, Massachusetts, United States
Activity: Talks and presentations › Guest lectures, external teaching and course activities at other universities

Massachusetts Institute of Technology
Period: 17 Sep 2016 → 2 Jun 2017
Daniel Alberto Sepúlveda Estay (Visiting researcher)
Department of Management Engineering
Management Science

Description
Visiting PhD Researcher: Cyber risk and Security in the Global Supply Chain

Visiting: Center for Transportation and Logistics at the Massachusetts Institute of Technology

Documents:
MIT-CTL-Visiting PhD student webpage
MIT-CTL-Research_Page

Links:
http://ctl.mit.edu/about/bio/daniel-sepulveda-estay (Researcher profile page in the webpage of Center for Transport and Logistics at the Massachusetts Institute of Technology.)
http://ctl.mit.edu/mapping-supply-chain-response-cyber-attacks (Research Introduction webpage in the webpage of the Center for Transportation and Logistics at the Massachusetts Institute of Technology)

Activity: Visiting an external institution › Visiting another research institution
Leaders in Supply Chain: Cyber Security
Period: 11 May 2016
Daniel Alberto Sepúlveda Estay (Keynote speaker)
Department of Management Engineering
Management Science

Description
Key Note Speaker: Leaders in Supply Chain: Cyber Security
Delivered the key Note titled: "Systems approach to Cyber risks"
Links:
https://www.ciltuk.org.uk/Events/EventDetails.aspx?dateid=2350 (Webpage at the Chartered Institute for Transport and Logistics about the Key note speech)

Related event
Leaders in Supply Chain: Cyber Security
11/05/2016 → …
Activity: Talks and presentations › Conference presentations

PhD Project Pitch Video: Cyber risk and security in the global supply chain
Period: 21 Mar 2016
Daniel Alberto Sepúlveda Estay (Participant)
Department of Management Engineering
Management Science

Description
A 1 minute pitch of the PhD project "Cyber risk and Security in the global supply chain"
Links:
https://www.youtube.com/watch?v=6_fd2SXc4LE
Activity: Other

34th International Conference of the System Dynamics Society (Event)
Period: 1 Mar 2016 → 31 May 2016
Daniel Alberto Sepúlveda Estay (Member)
Department of Management Engineering
Management Science
Degree of recognition: International
Documents:
34th International System Dynamics Conference Booklet 2016

Related event
34th International Conference of the System Dynamics Society
17/07/2016 → 21/07/2016
Delft, Netherlands
Activity: Membership › Membership in review committee

Guest Lecturer - ISCM Program RHUL: Supply Chain Distribution Game and Matching Supply And Demand lectures
Period: 18 Nov 2015
Daniel Alberto Sepúlveda Estay (Guest lecturer)
Department of Management Engineering
Management Science

Description
Delivered two lectures as Guest lecturer in the International Masters of Supply Management program at the Royal Holloway University of London.

Related external organisation

Royal Holloway University of London
Egham, United Kingdom

Activity: Talks and presentations › Guest lectures, external teaching and course activities at other universities

33rd International conference of the System Dynamics Society (Event)
Daniel Alberto Sepúlveda Estay (Member)
Department of Management Engineering
Management Science

Description
33rd International conference of the System Dynamics Society
Degree of recognition: International
Documents:
33rd International System Dynamics Conference Booklet 2015

Related event

33rd International conference of the System Dynamics Society
19/07/2015 → 23/07/2015
Cambridge, United States
Activity: Membership › Membership in review committee

Food and Agriculture Organization of the United Nations (External organisation)
Daniel Alberto Sepúlveda Estay (Member)
Department of Management Engineering
Management Science

Description
Meeting Urban Food Needs (MUFN) UN FAO & System Dynamics Italian Chapter (SYDIC)
Degree of recognition: International

Related external organisation

Food and Agriculture Organization of the United Nations
Italy
Activity: Membership › Membership in review committee

Lecturer - Supply Chain Management and Advanced Planning
Period: 18 Nov 2014
Daniel Alberto Sepúlveda Estay (Invited speaker)
Department of Management Engineering
Management Science

Description
Lecture on Supply Networks and Oursourcing

Related event

Supply Chain Management and Advanced Planning
02/09/2014 → …
Lyngby, Denmark
Activity: Talks and presentations › Conference presentations
32nd International Conference in System Dynamics (Event)
Period: 1 Apr 2014 → 30 May 2014
Daniel Alberto Sepúlveda Estay (Member)

Department of Management Engineering
Management Science

Description
Submission Reviewer for the 32nd International Conference in System Dynamics
Degree of recognition: International

Documents:
32nd International System Dynamics Conference Abstracts and Booklet 2014

Related event
32nd International Conference in System Dynamics
20/07/2014 → 24/07/2014
Delft, Netherlands
Activity: Membership › Membership in review committee

Online Tutorial: Loop Eigenvalue Elasticity Analysis of System Dynamics Models
Period: 2014 → …
Daniel Alberto Sepúlveda Estay (Participant)
Department of Management Engineering
Management Science
Transport DTU
Operations Management

Description
System Dynamics models are composed of different flow and state variables, with multiple interactions. In the process of identifying the relevant structure that leads to the observed behavior, the method of "Loop Eigenvalue Elasticity Analysis" (LEEA) can be very useful in quickly identifying the modes loops most relevant over time for this behavior.

The method was originally proposed by Kampmann and Oliva in 2006. This video is a tutorial that shows the implementation of such method when applied to a specific example.

The video first discusses the theory behind the analysis, then describes step by step the process of data gathering and processing, to finally describe the analysis of results.

In order to reproduce what is shown in the video, both VENSIM and Mathematica software packages are required.

Degree of recognition: International

Links:
https://www.youtube.com/watch?v=6eGmJKzPFYo (Tutorial about Loop Eigenvalue Elasticity Analysis (LEEA))
Activity: Other

Press clippings:

The best protection is a lean organization
Daniel Alberto Sepúlveda Estay
01/08/2018
Department of Management Engineering, Management Science, Transport DTU, Operations Management

Media coverage (1)

Det bedste forsvar er en smidig organisation
Daniel Alberto Sepúlveda Estay
01/08/2018
DYNAMO (National), Denmark, Print
Lotte Krull
Cyber attacks on supply chains are a constant threat to organizations. News media are regularly reporting cyber attacks to supply chains that result in data theft or denial of service. Examples abound, such as the theft of credit card data for 70 million customers from Target in 2013, and a sophisticated distributed attack that blocked the websites of major companies in the east-US such as Amazon, Starbucks and PayPal, during most the 21st of October 2016. Although relevant, this coverage often overshadows cyber-attacks that affect supply chain operations, which continue to occur without media attention. This is giving hackers free range to refine and practice their techniques for increased penetration and damage, resulting in a whole different range of disruptions such as container theft, intervention of plant operation, or misallocation of payments, for example.

The MIT Center for Transportation & Logistics (CTL) will host a webinar to address hacker-related vulnerabilities in supply chain operations. At the root of this problem lies the structure of data exchanges between supply chain partners. Key questions for supply chain managers include:

How does your supply chain manage these data exchanges?
How much are you assigning these problems to IT even though they have direct impact on operations?
How does your supply chain prevent these attacks, or react when these attacks happen?
Is your supply chain merely relying on external insurance, or do you understand how these exchanges can be designed and controlled in cases of attack for improved recovery?

Dr. Jim Rice and Daniel Sepulveda, PhD student, will address these questions, and talk about research findings that offer a deeper understanding of the structures that supply chains can use to improve their response from hacker attacks so as to minimize operational disruption and allow a more efficient recovery.

Department of Management Engineering, Management Science, Center for Transportation and Logistics at the Massachusetts Institute of Technology

Media contribution (1)

Webinar: Recovery of Operations From Hacker Attacks: A Structure for Response
15/03/2017

Webinar (International), United States, Web
Christine Adams / Daniel Sepulveda
44:40
https://www.youtube.com/watch?v=zsmpjNRclfI&t=152s

Cyber attacks on supply chains are a constant threat to organizations. News media are regularly reporting cyber attacks to supply chains that result in data theft or denial of service. Examples abound, such as the theft of credit card data for 70 million customers from Target in 2013, and a sophisticated distributed attack that blocked the websites of major companies in the east-US such as Amazon, Starbucks and PayPal, during most the 21st of October 2016. Although relevant, this coverage often overshadows cyber-attacks that affect supply chain operations, which continue to occur without media attention. This is giving hackers free range to refine and practice their techniques for increased penetration and damage, resulting in a whole different range of disruptions such as container theft, intervention of plant operation, or misallocation of payments, for example. The MIT Center for Transportation & Logistics (CTL) will host a webinar to address hacker-related vulnerabilities in supply chain operations. At the root of this problem lies the structure of data exchanges between supply chain partners. Key questions for supply chain managers include:

How does your supply chain manage these data exchanges?
How much are you assigning these problems to IT even though they have direct impact on operations?
How does your supply chain prevent these attacks, or react when these attacks happen?
Is your supply chain merely relying on external insurance, or do you understand how these exchanges can be designed and controlled in cases of attack for improved recovery?

Dr. Jim Rice and Daniel Sepulveda, PhD student, will address these questions, and talk about research findings that offer a deeper understanding of the structures that supply chains can use to improve their response from hacker attacks so as to minimize operational disruption and allow a more efficient recovery.

Daniel Alberto Sepúlveda Estay & James Blanley Rice