STPA FOR UNDERSTANDING THE CYBER RISKS IN A PHYSICAL SUPPLY CHAIN

STAMP WORKSHOP, MIT, MARCH 29, 2017

CYBER-TC CASE STUDY

Daniel Sepulveda, MSc.
dasep@dtu.dk

Omera Khan, PhD.
DTU/ Aalborg University

DTU
Technical University of Denmark

Part 1

BACKGROUND

CYBER-ATTACK

- "…offensive maneuver that targets computer information systems to either steal, alter, or destroy…"

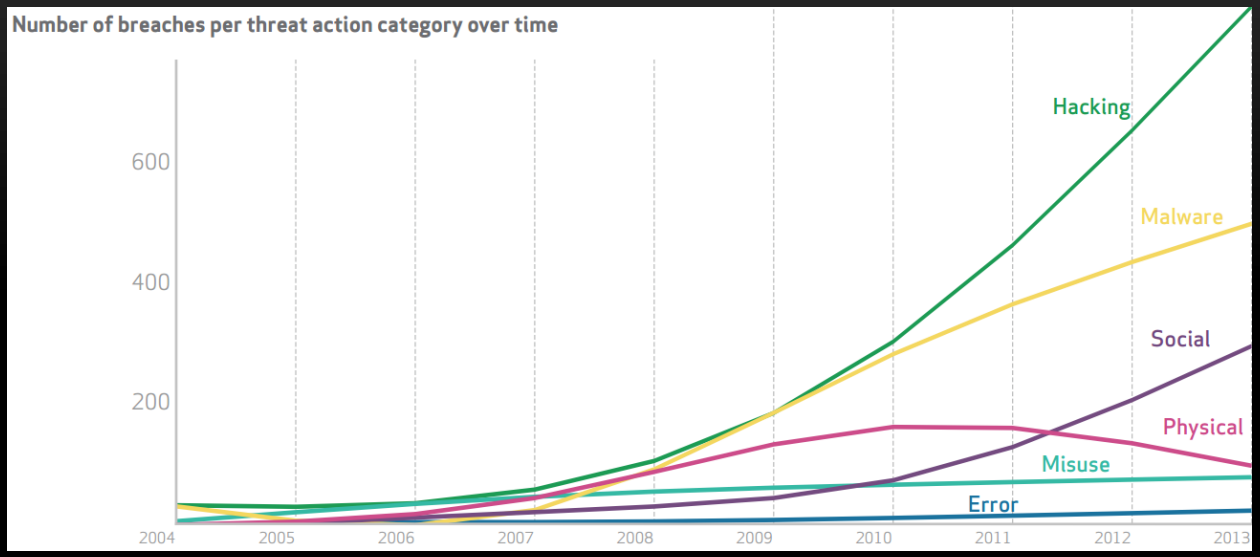
= IT

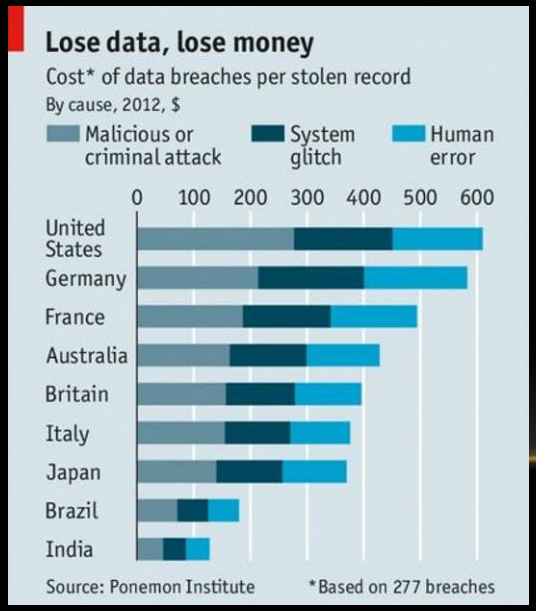
THE DAWN OF THE STUXNET

- Worm discovered in 2010
- Highly advanced (6-zero-day)
- Internet not required
- Targets highly specialized hardware in nuclear plants
- Effects: over 20% of centrifuges damaged
- Had a turn-off date: 24 June 2012

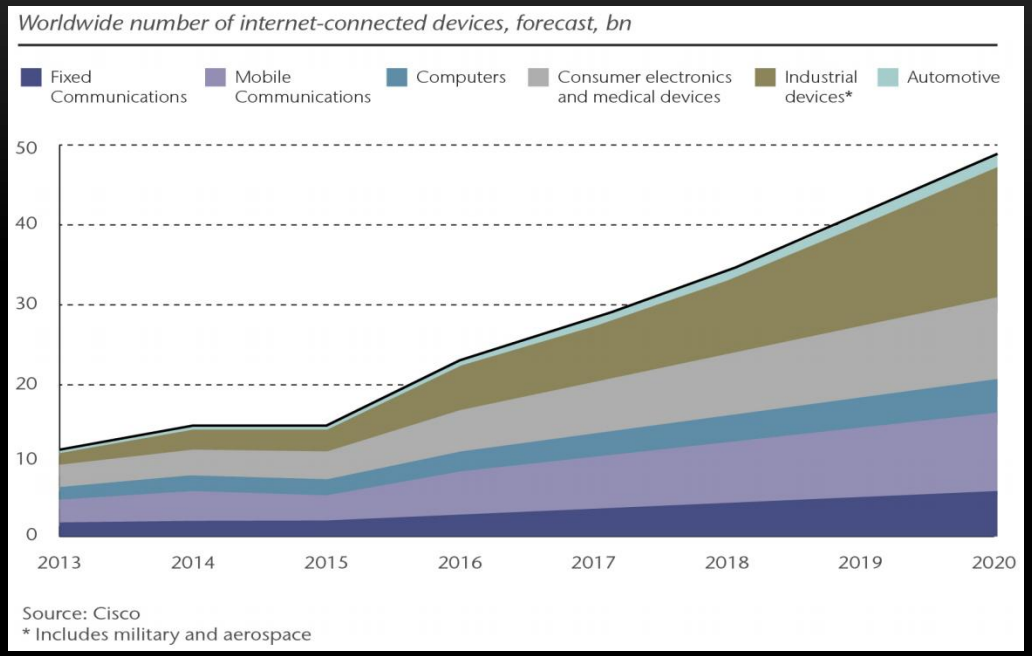
DTU

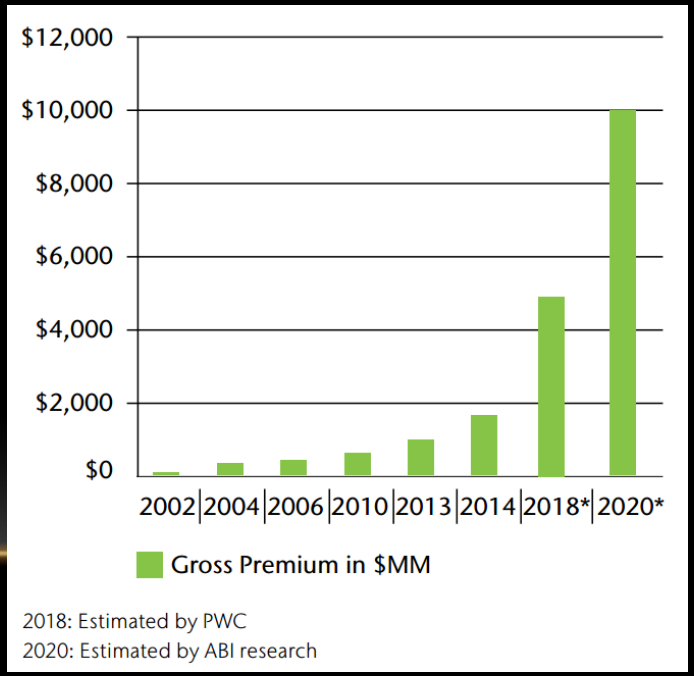
INCREASING PROBLEM





INCREASING PROBLEM



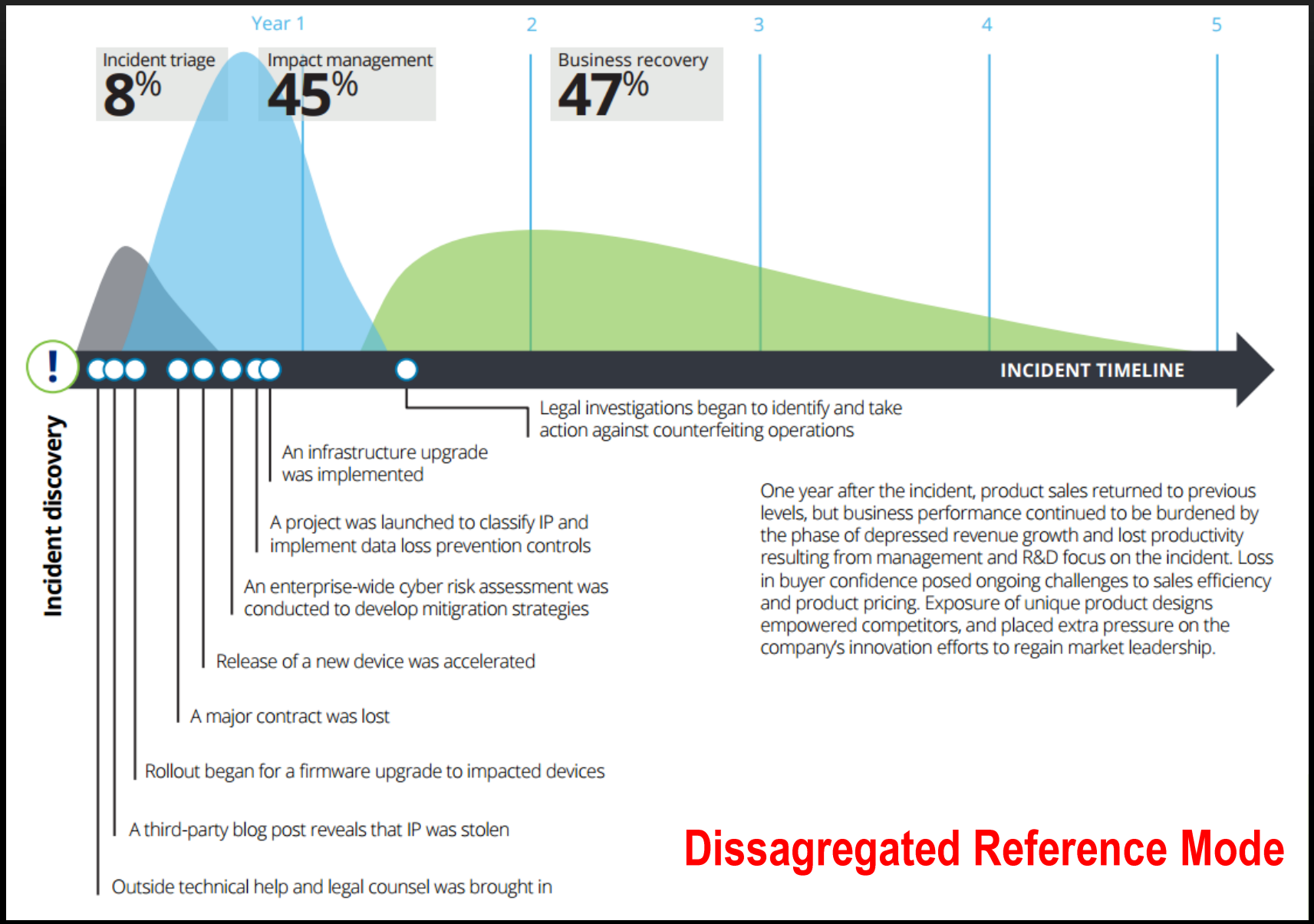


EXAMPLES OF CYBER ATTACKS TO SUPPLY CHAINS

- Purchase Orders activation
  - Hacker purchase order activated by supplier. Resulting erroneous delivery and payment due.
- Product Delivery
  - Product delivered to wrong hacker transport
  - Wrong product delivered due to hacker intervention
  - Late/No delivery due to hacker intervention
- Payments
  - Payment instructed to hacker account instead of supplier account
- New product activation
  - Loss of IP

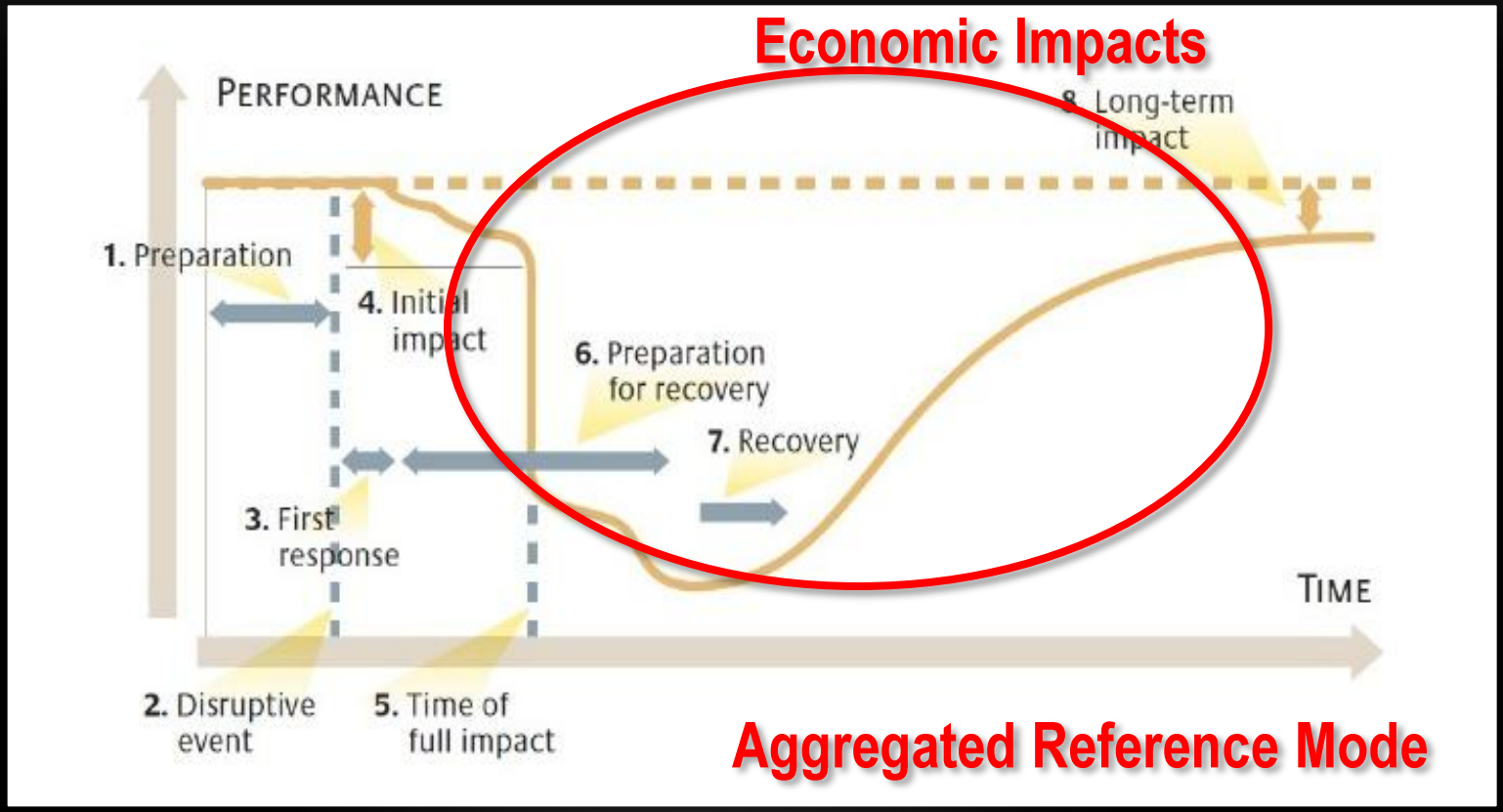
DTU

TIMELINE FOR A CYBER-ATTACK

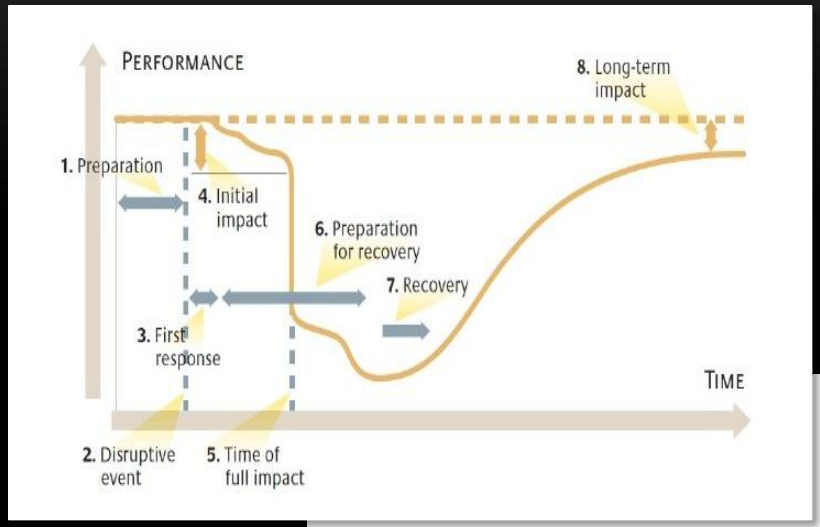


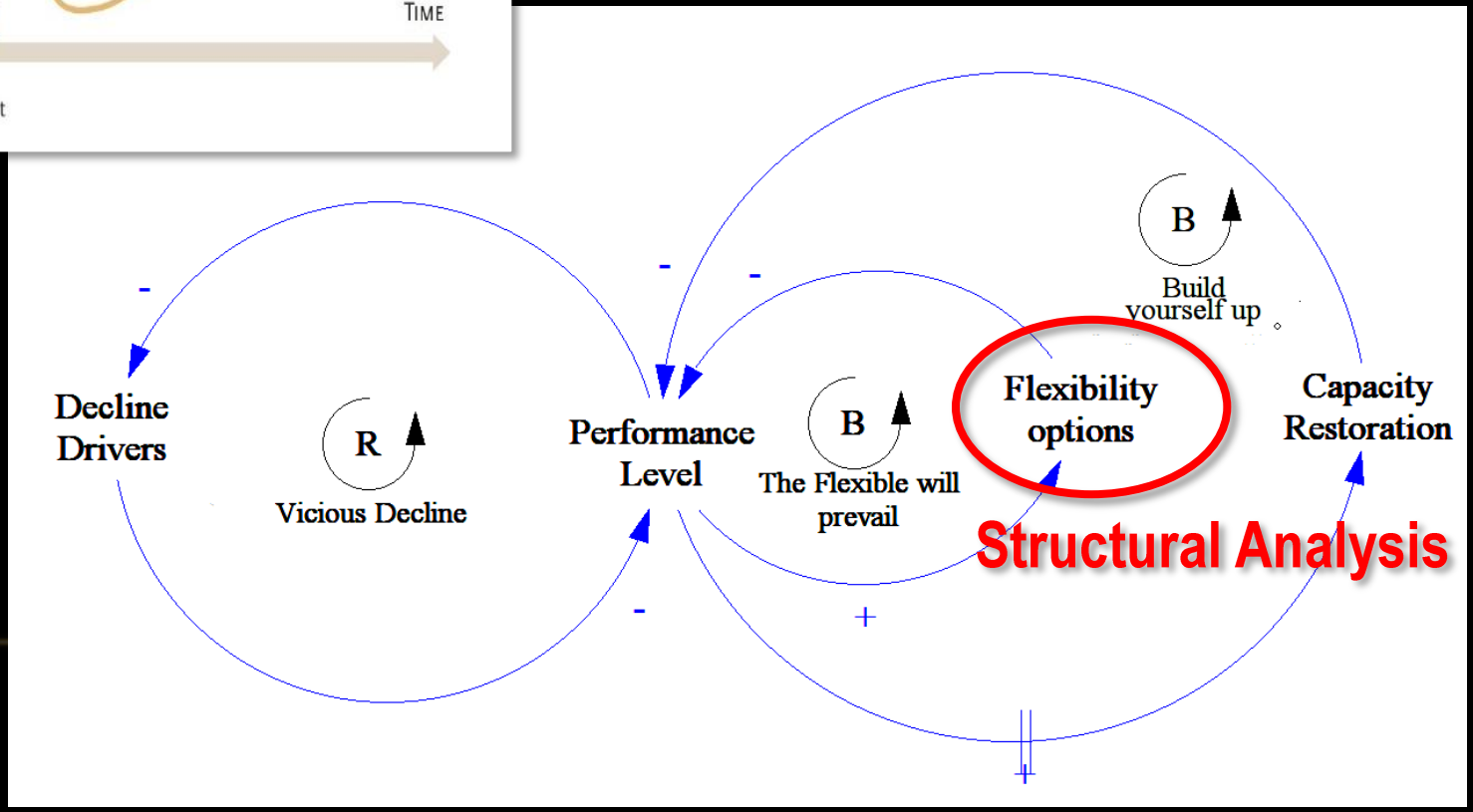
Dissagregated Reference Mode

DISRUPTION CURVE



REACTION ANALYSIS



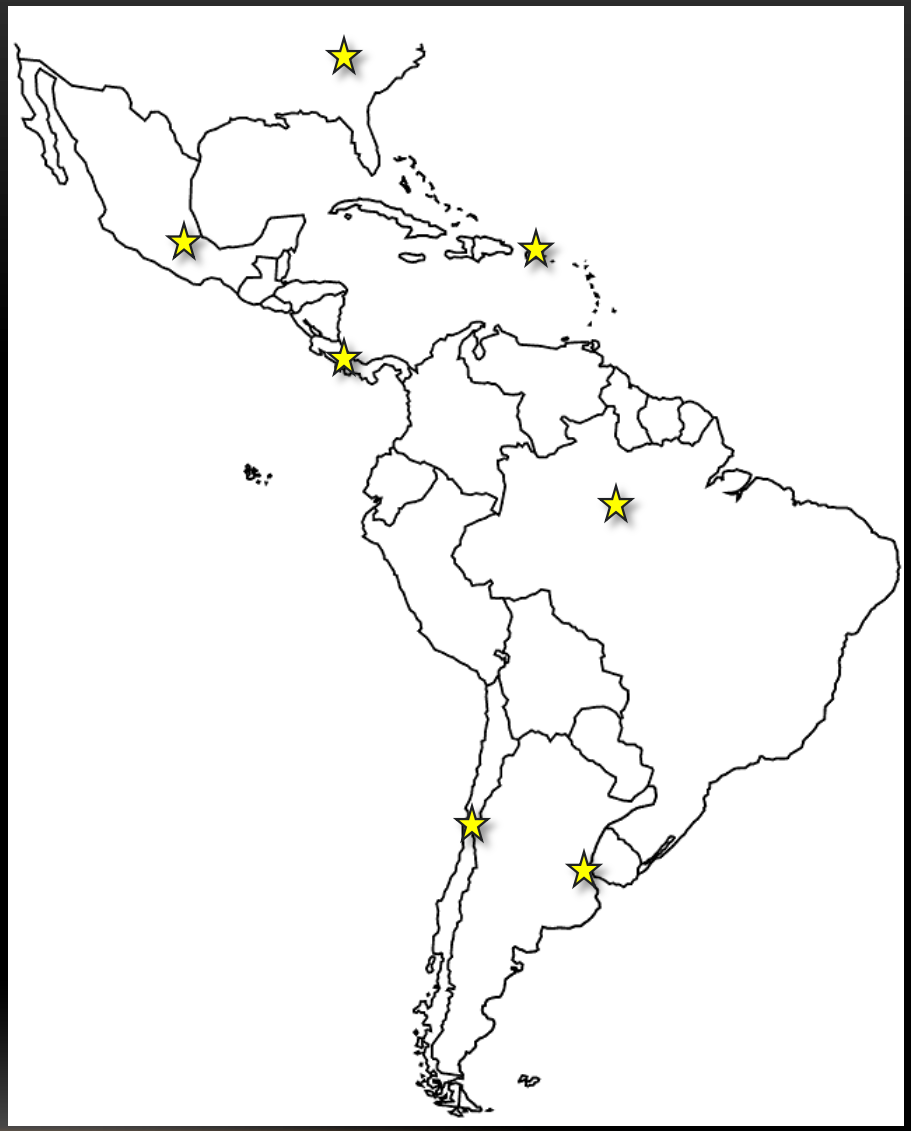


Part 2

PROBLEM DESCRIPTION

TC ORGANIZATION

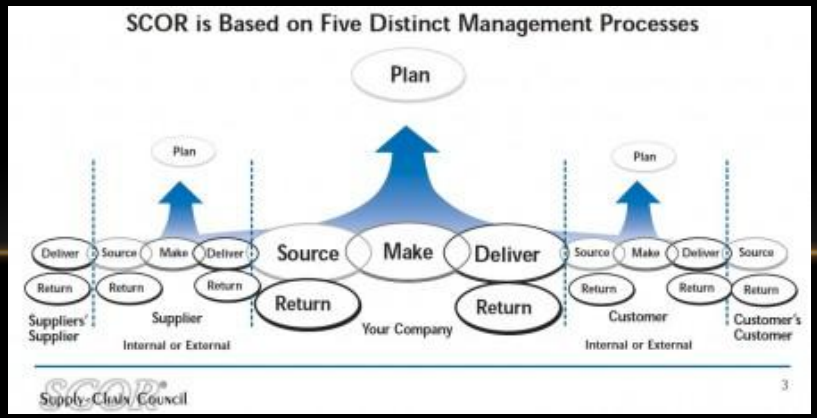
- Beverage Manufacturer
  - 22 manuf. Plants worldwide
  - 7 manuf. America
- 54 - 70 new products launched per year
- Distributed Purchasing Organization since 2007
- Lean Manufacturing Implemented 2008
- 99.5% operational service level requirement
- Products purchased: Liquid and Solid ingredients, containers (plastic, cardboard)



DTU

INTEREST ON STPA

1. Organizational requirement: Include cyber risks in procedures
2. Opportunity for comparison with traditional approach:
   - Supply Procedure / Supplier Evaluation
   - SCOR-derived process analysis
     - Supply Chain Operations Reference
   - Causal Chain (FMEA)
3. Search for supplier safety modularization



SYSTEM DEFINITION (STPA-SEC)

A system to safely and timely purchase the correct products…

by means of an cost-effective relationship with our supplier and their transport…

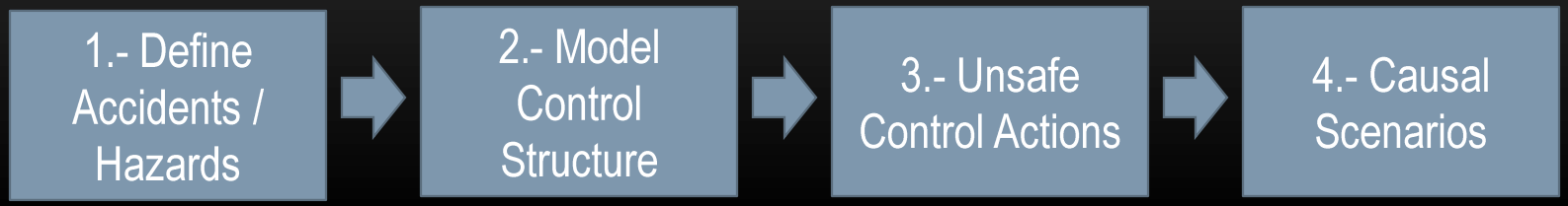
in order to contribute to the company's bottom line and reputation

DTU

Part 3

MODEL DEVELOPMENT

STPA PROCESS

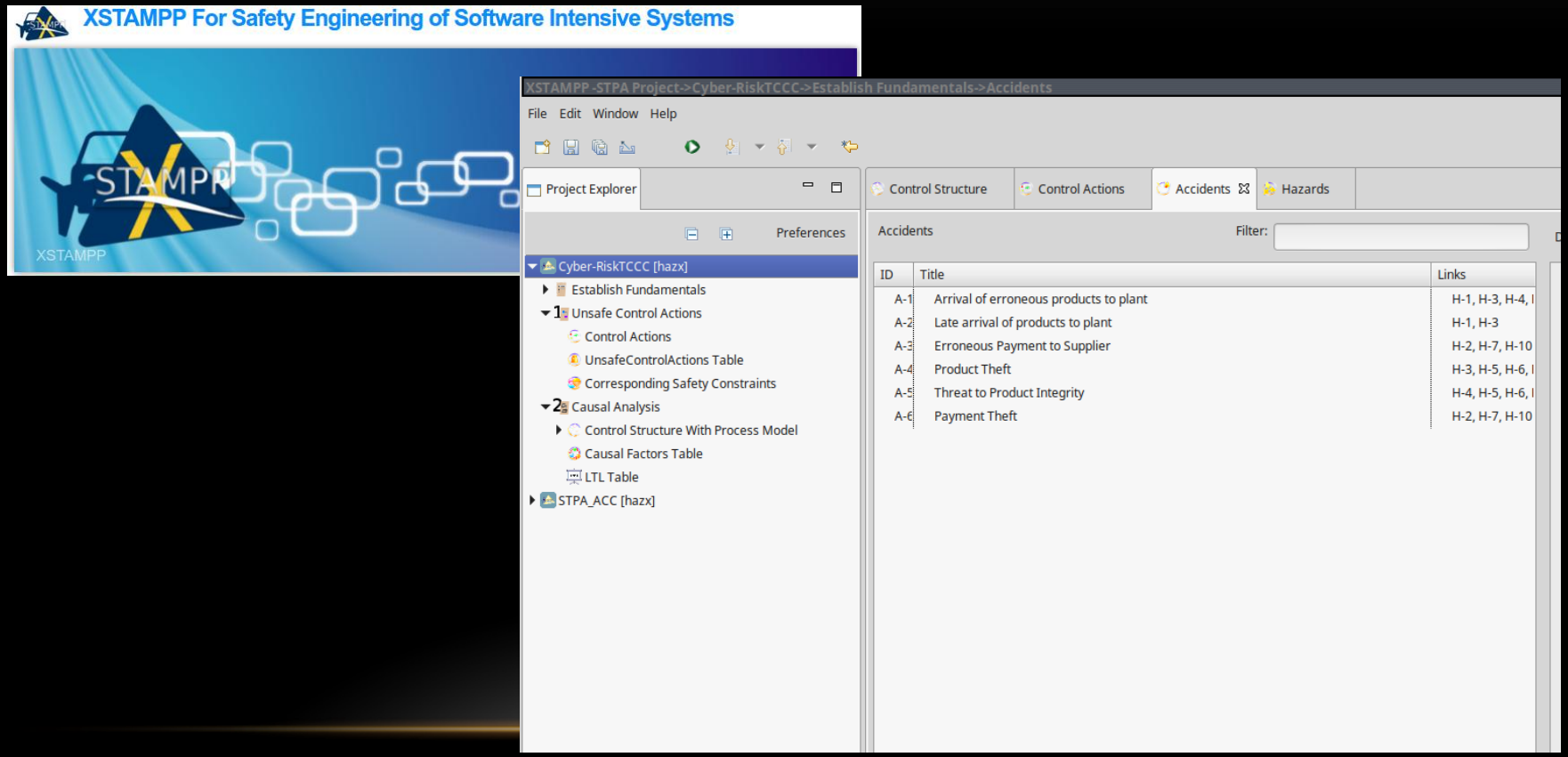


1. Identify Accidents and Hazards
2. Model the control structure of the system
3. Identify Unsafe Control Actions
4. Identify Causal factors and generate scenarios
    - Causal scenarios for each unsafe control actions
    - **Among these: cyber attacks**

DTU

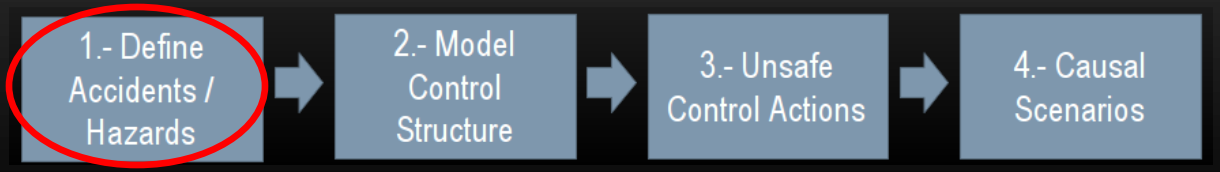
SOFTWARE USED

- XSTAMPP: http://www.xstampp.de/ from Stuttgart University



DTU

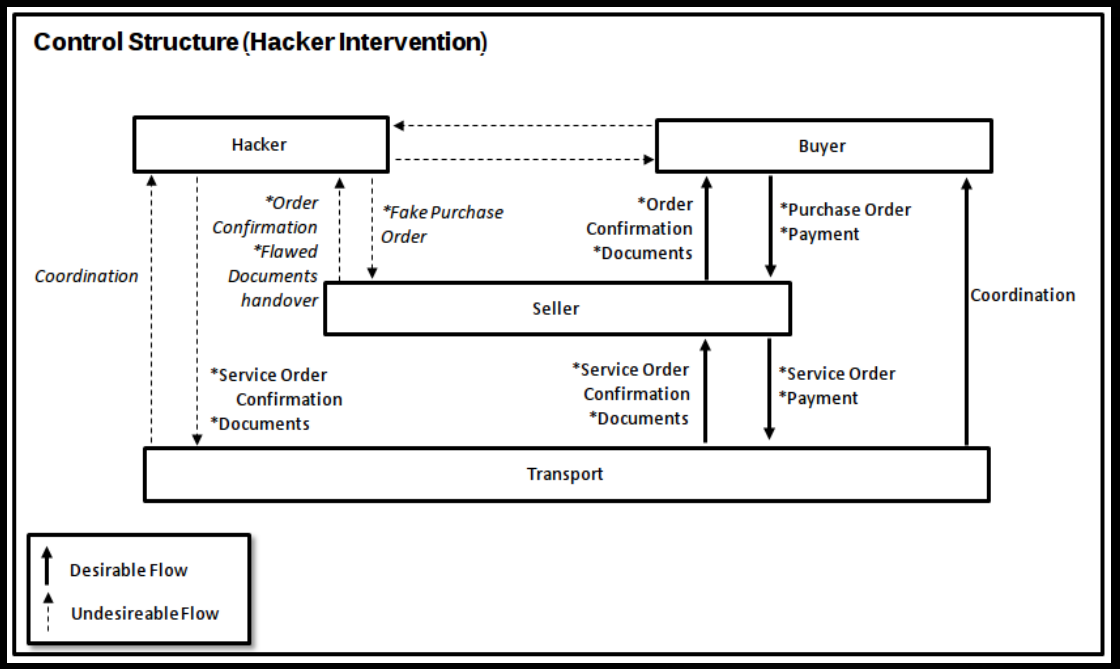
CYBER-TC CASE STUDY



- Accidents
  - A1: Erroneous arrival of product
  - A2: Erroneous payment to supplier
  - A4: Product loss
  - A5: Product integrity compromised
  - A6: Payment loss
- Hazards
  - H1: Inability to initiate procurement process
  - H2: Inability to perform physical transport
  - H3: Inability to confirm product integrity
  - H4: Inability to pay correctly

DTU

CONTROL STRUCTURE WITH HACKER



Problems:

- Disruptions without a hacker
- Double Analysis in context Causal Scenario
- Double Flow representation

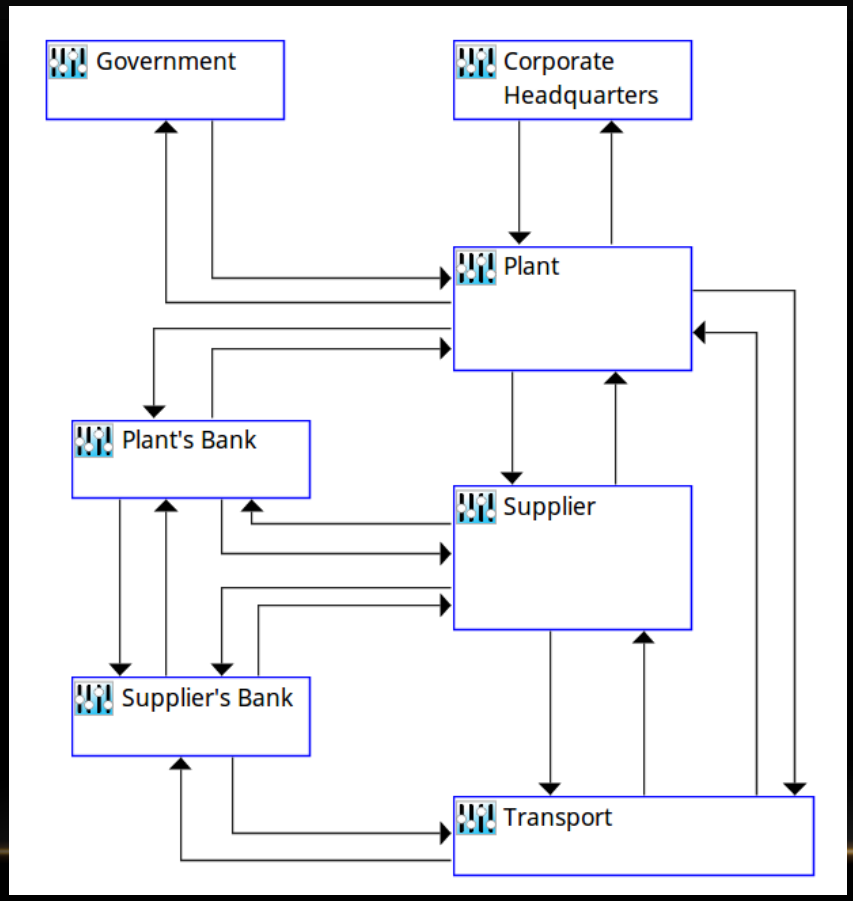
Option:

- Cyber attacks / Disruptions in Causal Scenarios

DTU

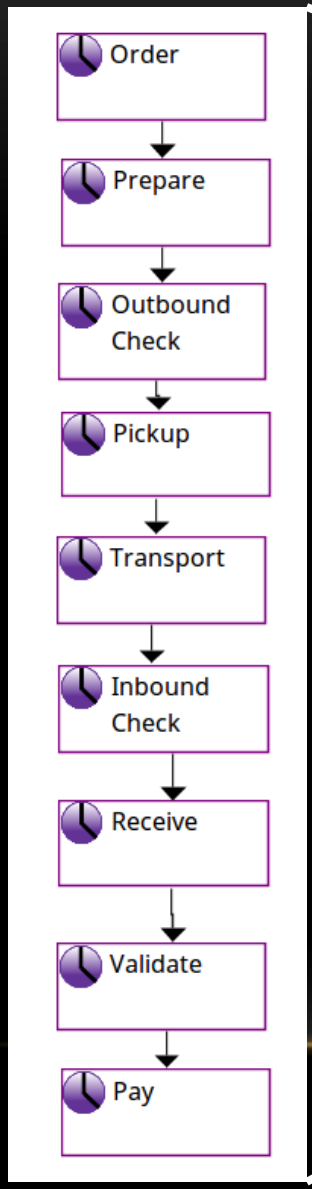
HIGH LEVEL CONTROL STRUCTURE

1.- Define Accidents / Hazards → 2.- Model Control Structure → 3.- Unsafe Control Actions → 4.- Causal Scenarios

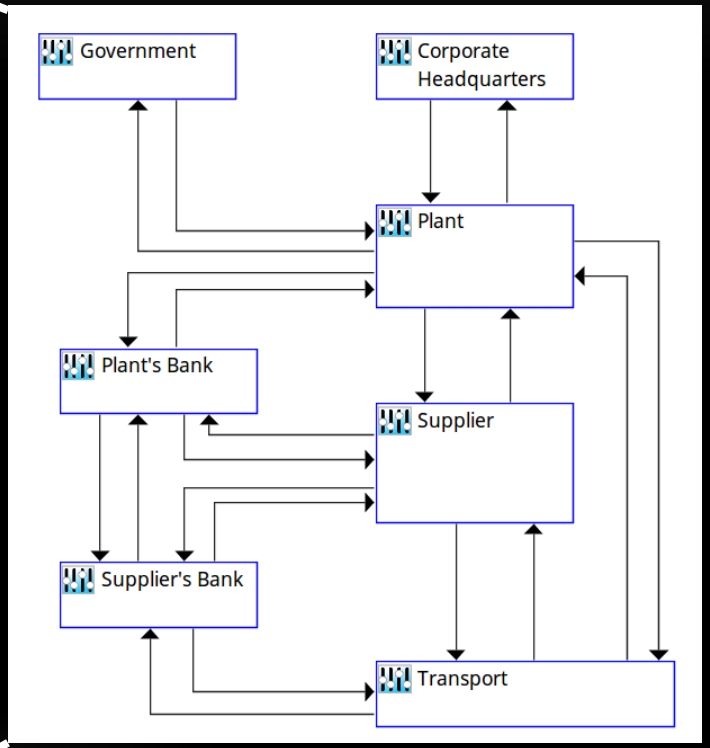


DTU

CONTROLLED PROCESS



1.- Define Accidents / Hazards → 2.- Model Control Structure → 3.- Unsafe Control Actions → 4.- Causal Scenarios

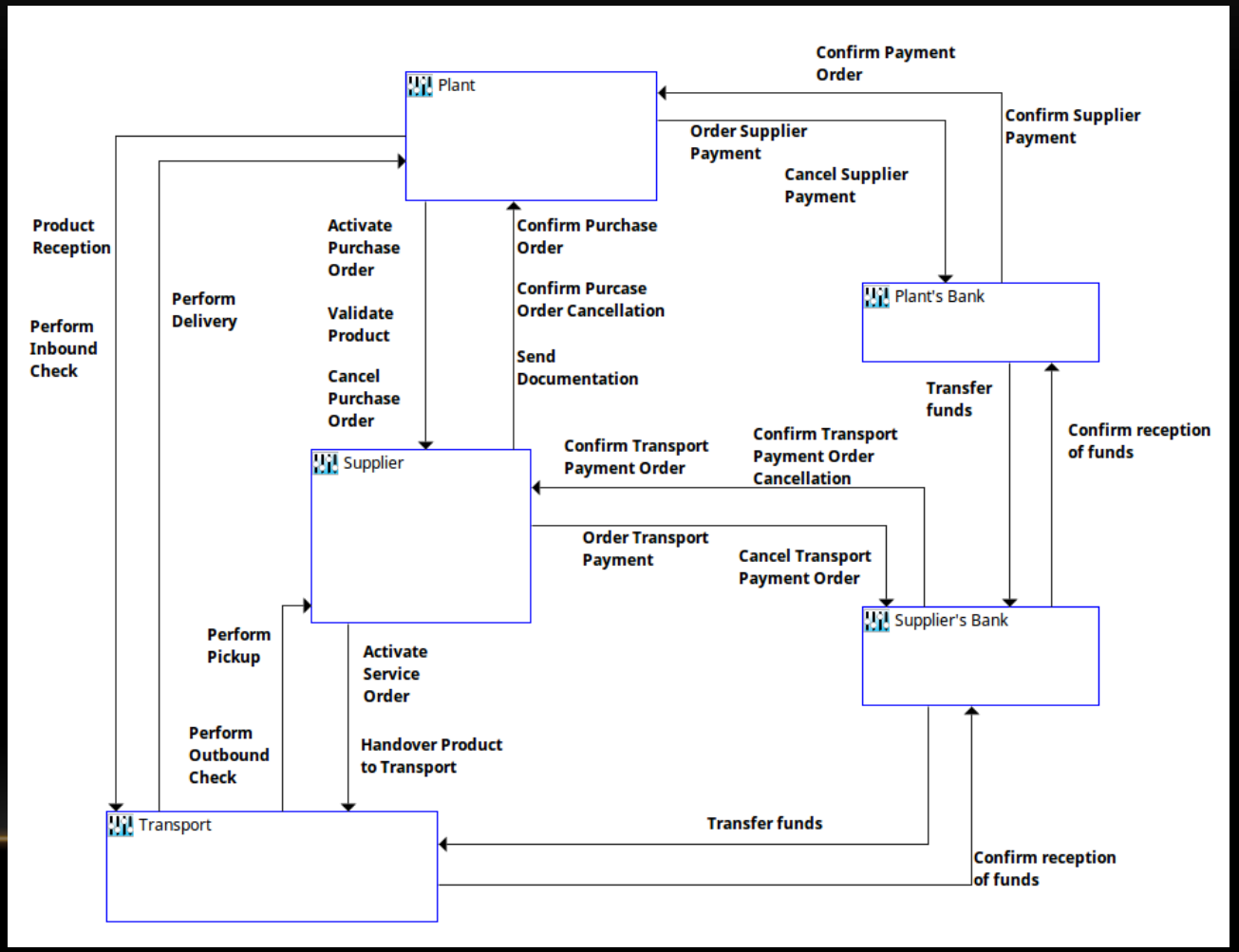


DTU

CONTROL ACTIONS

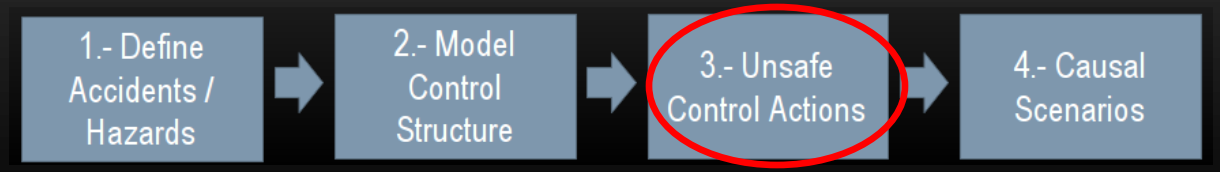
1.- Define Accidents / Hazards → **2.- Model Control Structure** → 3.- Unsafe Control Actions → 4.- Causal Scenarios

- From Procedures
- 31 Control Actions



DTU

UNSAFE CONTROL ACTIONS

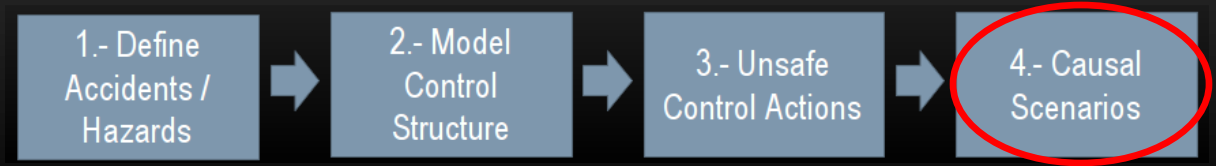


- 106 Unsafe Control Actions

Control Action	Not providing causes hazard	Providing causes hazard	Wrong timing or order causes hazard	Stopped too soon or Applied too long
Confirm payment order	UCA1.18	UCA1.19		
	Not providing when there has been a Supplier Payment order is hazardous	Providing when there has not been a Supplier payment order is hazardous	Providing before there has been a Supplier payment order is hazardous	Add stopped too soon UCA
	[H-4]	[H-4]	Not Hazardous	
	Add not given UCA	Add given incorrectly UCA	Add wrong timing UCA	
Order Supplier payment	UCA1.10	UCA1.11	UCA1.10	
	Not providing when there has been confirmation of product reception and validation is hazardous	Providing when there has not been a product reception is hazardous	Providing before there has been product reception is hazardous	Add stopped too soon UCA
	[H-2] [H-4]	[H-2] [H-3]	[H-2] [H-3]	
	Add not given UCA	UCA1.12	UCA1.11	
		Providing when there has not been product validation is hazardous	Providing before there has been product validation is hazardous	
		[H-2] [H-3]	[H-2] [H-3]	
		UCA1.17		
		Providing when there jas not been a suppier payment data confirmation is hazardous	Click to edit	
		[H-4]	Not Hazardous	
		Add given incorrectly UCA	Add wrong timing UCA	
Cancel supplier payment	UCA1.13	UCA1.14		
	Not providing when there has not been product reception is hazardous	Providing when there has been product validation, reception and supplier data confirmation is hazardous	Add wrong timing UCA	Add stopped too soon UCA
	[H-2] [H-3]	[H-4]		
	UCA1.15			
	Not providing when there has not been prodict validation is hazardous	Add given incorrectly UCA		
	[H-2] [H-3]			
	UCA1.16			
	Not providing when there has not been a supplier payment data confirmation is hazardous			
	[H-4]			
	Add not given UCA			

DTU

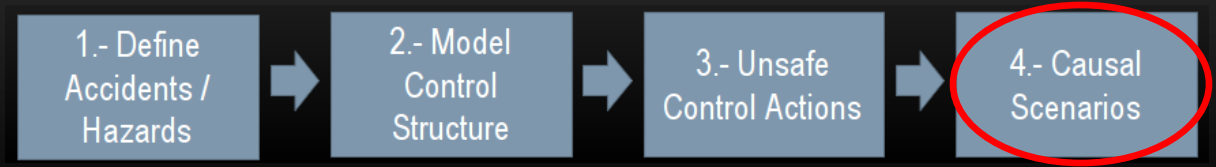
CAUSAL SCENARIOS - EXAMPLES



Controller	UCA	Causal Scenarios
Plant	UCA 1.12: Order supplier payment when there has not been product validation is hazardous.	1) Quality / Warehouse /Finance did not know the process 2) Quality / Warehouse / Finance did now know where to find the process 3) There was not central controller for confirmations before payment 4) Pressure to achieve daily goals 5) Pressure from Supplier 6) Pressure from Transport 7) Payment order has activated externally to bank 8) Product has been compromised by Hacker 9) Payment data has been changed by hacker
	UCA 1.13: Order supplier payment when there has not been product reception is hazardous.	
	UCA 1.14: Order supplier payment when there has not been supplier payment data is hazardous.	

DTU

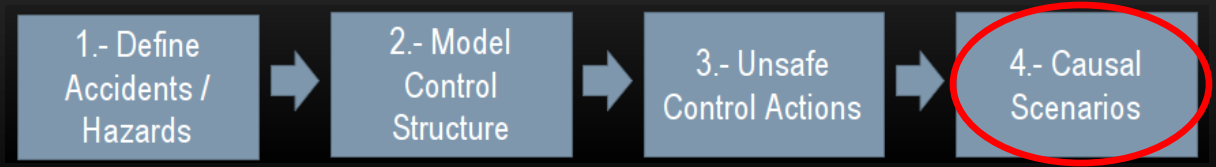
CAUSAL SCENARIOS - EXAMPLES



- Recommendations examples
  - Identify an organizational role to finance for controlling confirmations before payment
  - Generate payment order validation process with Bank
  - Training to Quality/ Warehouse/ Finance about the procedures
  - Develop process-pressure dynamic indicators
  - Implement gatekeeping at the bank

DTU

CAUSAL SCENARIOS - EXAMPLES



Controller	UCA	Causal Scenarios
Supplier	UCA 1.26 Confirming Purchase Order when purchase order source has not been validated is hazardous	1) Supplier is not aware of a validation requirement 2) Supplier does not consider validation important / No incentives 3) Internal supplier pressure to react quickly 4) Plant pressure to react quickly 5) Purchase Order has been activated by hacker 6) Supplier considers purchase order as validation

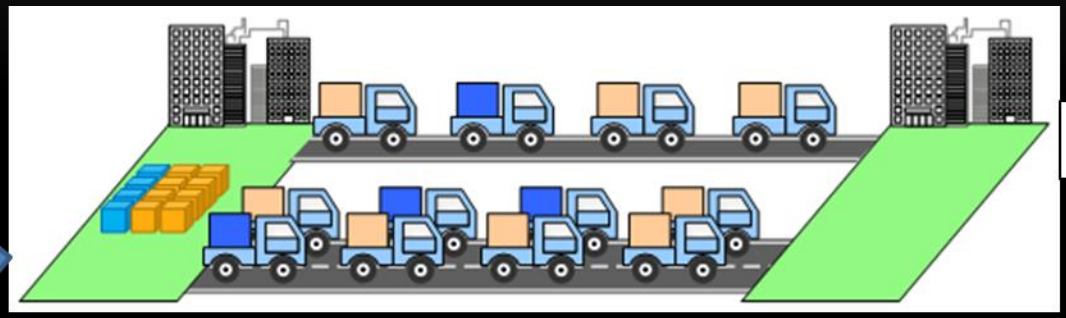
Controller	UCA	Causal Scenarios
Transport	UCA 1.43 Not performing outbound check when there is deficient documentation is hazardous	1) Transport does not know the outbound check requirement 2) Transport does not consider validation important / No incentives 3) Supplier pressure 4) Plant pressure 5) Internal transport pressure 5) Documentation has been adulterated by hacker 6) Product at the supplier has been adultrated by hacker

DTU

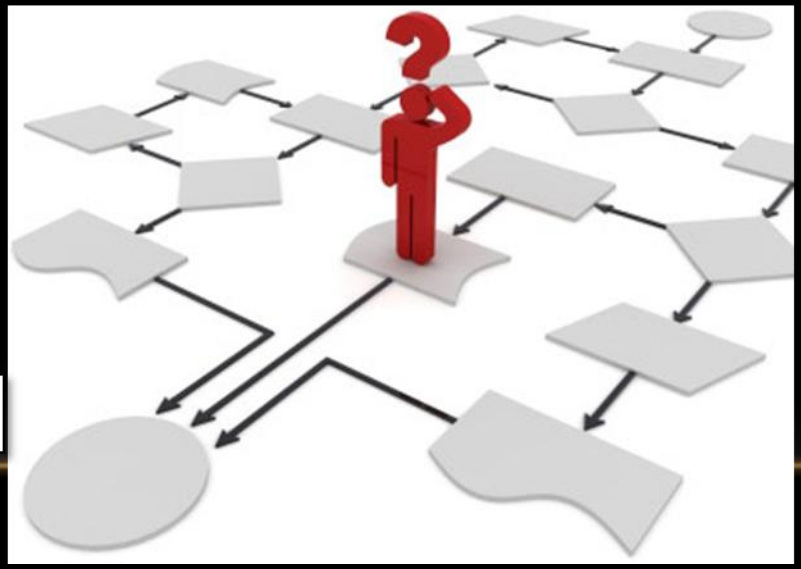
Part 4

CONCLUSIONS

SUPPLY CHAIN



physical operations



Information flows

COMMENTS WITH RESPCT TO XSTAMPP

- Pros
  - Sequential structured way of process analysis
  - Simplified sharing
  - Fast learning curve to new team members
- Cons
  - Safety constraints are nor linked to a hazards (they are to UCA)
  - Visualization problems (e.g., Control Actions column size control)
  - Trouble with control structure representations
  - Problems with table visualization (UCA) – loss of column titles

DTU

NEXT STEPS

- Explore Modularity
- Translation into procedure requirements
- Including internal controllers within each organization
- Data gathering for supply chains in other plants
- Adjust the supplier certification process to motivate required control structures

DTU

THANK YOU

DANIEL SEPULVEDA-ESTAY
DASEP@DTU.DK
+45 9187 6715