MIT Interdisciplinary Consortium for Improving Critical Infrastructure Cybersecurity – (IC)^3

Cyber Safety: A Systems Thinking and Systems Theory Approach to Managing Cyber Security Risks

Presented at the International Conference on Computer Security in a Nuclear World: Expert Discussion and Exchange, International Atomic Energy Agency, June 2, 2015, Vienna, Austria

IAEA
International Atomic Energy Agency
Atoms for Peace

Dr. Qi Van Eikema Hommes, Lecturer & Research Affiliate
Hamid Salim
Stuart Madnick, Professor
Michael Coden, CISSP, Associate Director MIT-(IC)^3

Massachusetts Institute of Technology

MITSloan MANAGEMENT

Presentation Outline

- $(IC)^3$
- Research Motivations
- Approaches
  - System-Theoretic Accident Model and Processes (STAMP)
    - Causal Analysis based on STAMP (CAST)
    - System Theoretic Process Analysis (STPA)
- Case Study
  - CAST Applied to the TJX Case
  - CAST Applied to Stuxnet
- Future Research Directions

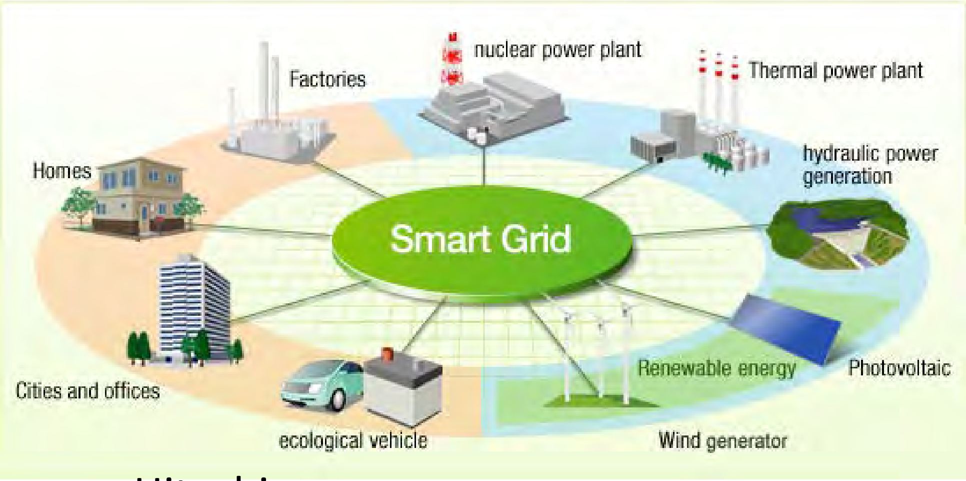
(IC)^3 is a Shared Research Consortium

Each member contributes to the annual research budget
All members share in the tools, models, methods, processes and procedures developed

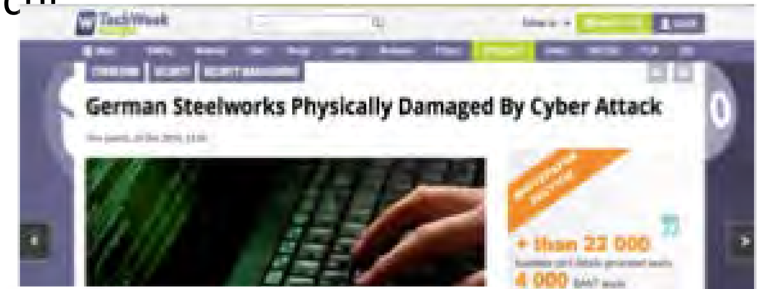
Join (IC)^3 at http://ic3.mit.edu

Research Motivations

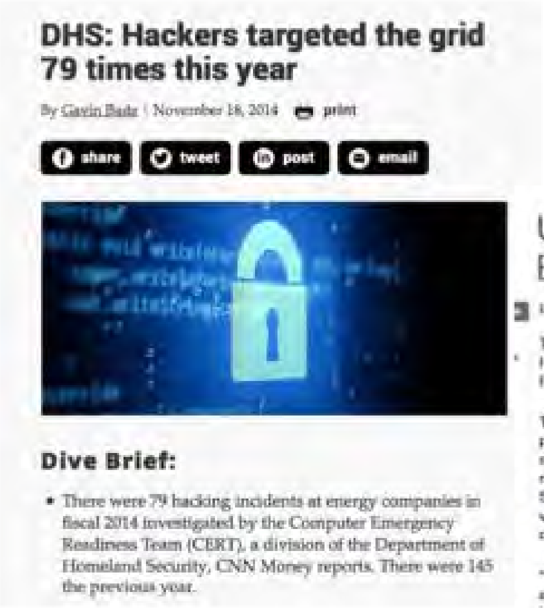
Cyber to Physical Risks With Major Consequences



Source: Hitachi



German Steelworks Physically Damaged By Cyber Attack

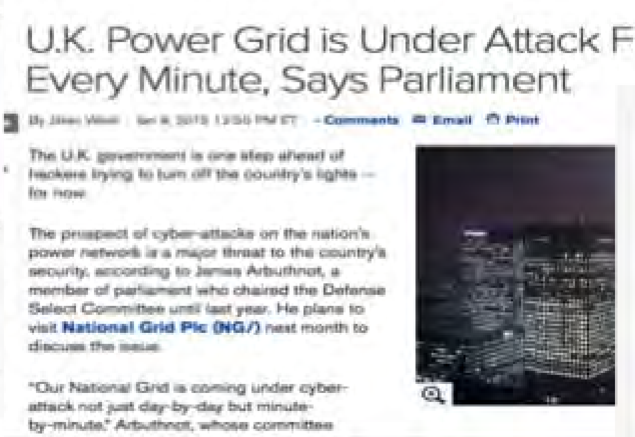


DHS: Hackers targeted the grid 79 times this year

By Gavin Bade | November 18, 2014 print

Dive Brief:

- There were 79 hacking incidents at energy companies in fiscal 2014 investigated by the Computer Emergency Readiness Team (CERT), a division of the Department of Homeland Security, CNN Money reports. There were 145 the previous year.



U.K. Power Grid is Under Attack From Hackers Every Minute, Says Parliament

By [illegible] Jan 8, 2015 12:50 PM ET - Comments Email Print

The U.K. government is one step ahead of hackers trying to turn off the country's lights -- for now.

The prospect of cyber-attacks on the nation's power network is a major threat to the country's security, according to James Arbuthnot, a member of parliament who chaired the Defense Select Committee until last year. He plans to visit National Grid Plc (NG/) next month to discuss the issue.

"Our National Grid is coming under cyber-attack not just day-by-day but minute-by-minute," Arbuthnot, whose committee

Most Violent Cyber Attack Noted To Date: 2008 Pipeline Explosion Caused By Remote Hacking

Reporting by Jordan Robertson and Michael Riley in Bloomberg is shedding new

Massachusetts Institute of Technology

$(IC)^3$

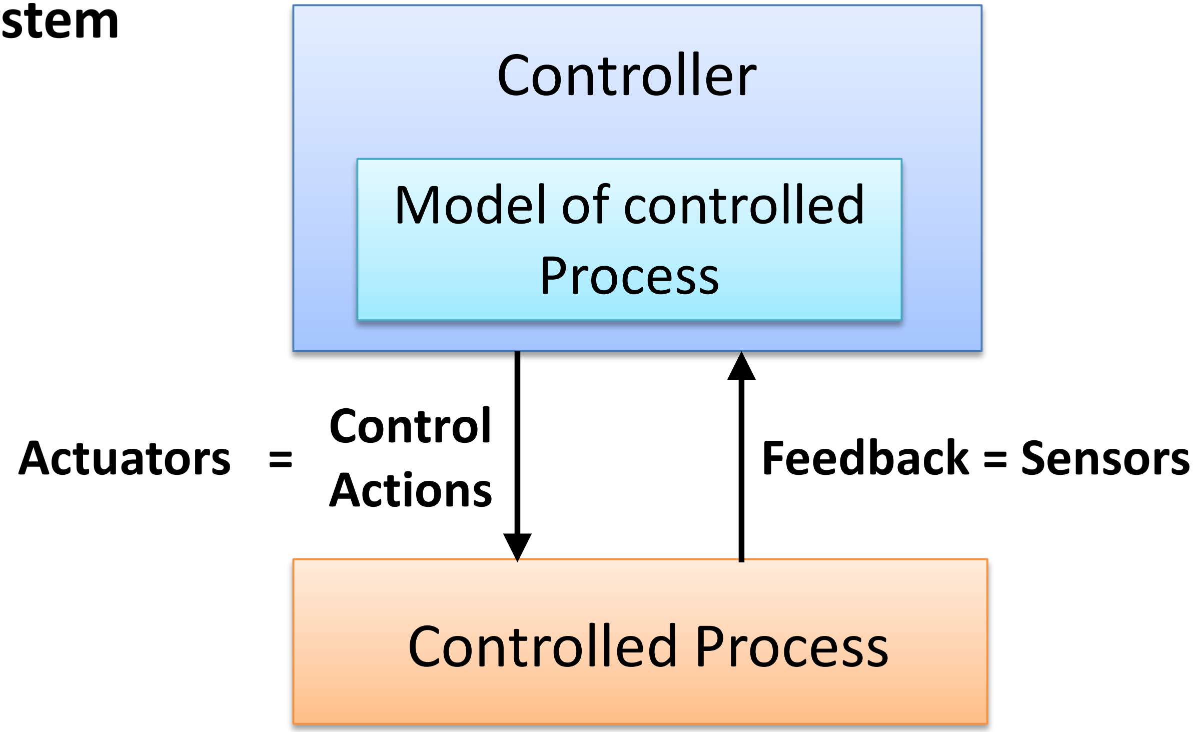
INTERDISCIPLINARY CONSORTIUM for IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY

MITSloan MANAGEMENT

System Theoretic Accident Model and Processes (STAMP)

Professor Nancy Leveson analyzes industrial accidents including Citichem Oakbridge, Challenger disaster, etc., developing STAMP:

- **Modeling the effects of complex system interactions by:**
- **Hierarchical Layers of Actuators/Controls and Sensors/Feedback**
- **Including the role of human actions and decisions as a part of the whole system**



Controller

Model of controlled Process

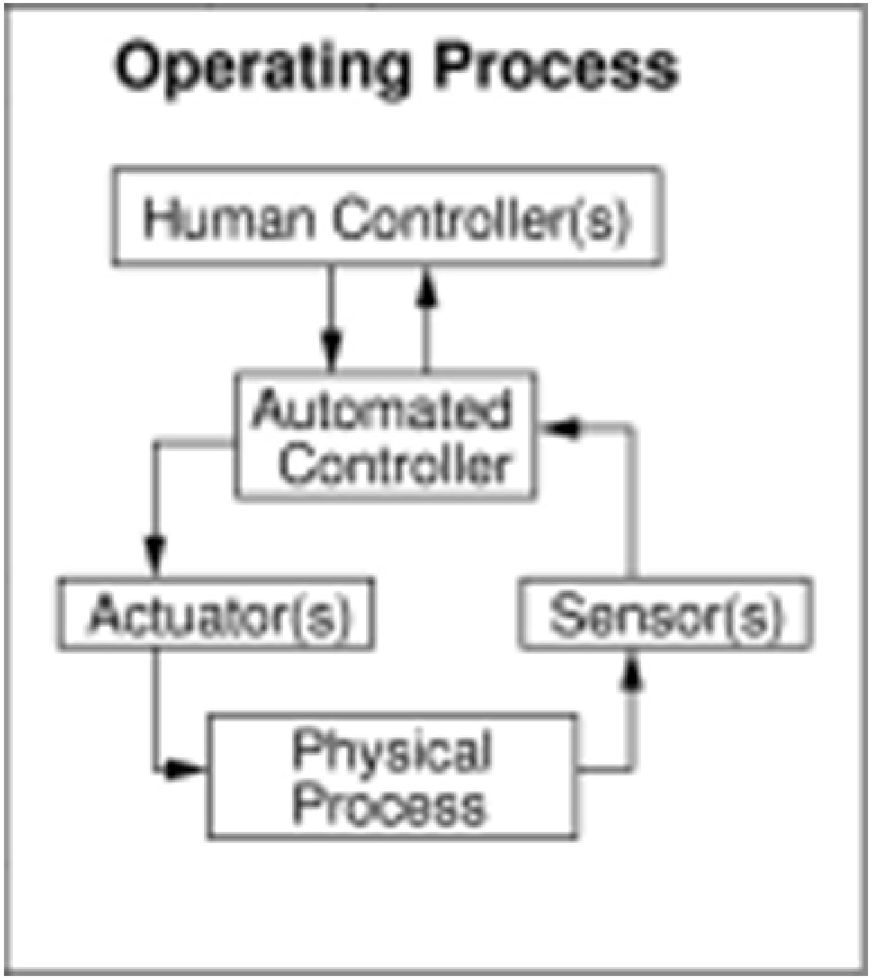
Actuators = Control Actions

Feedback = Sensors

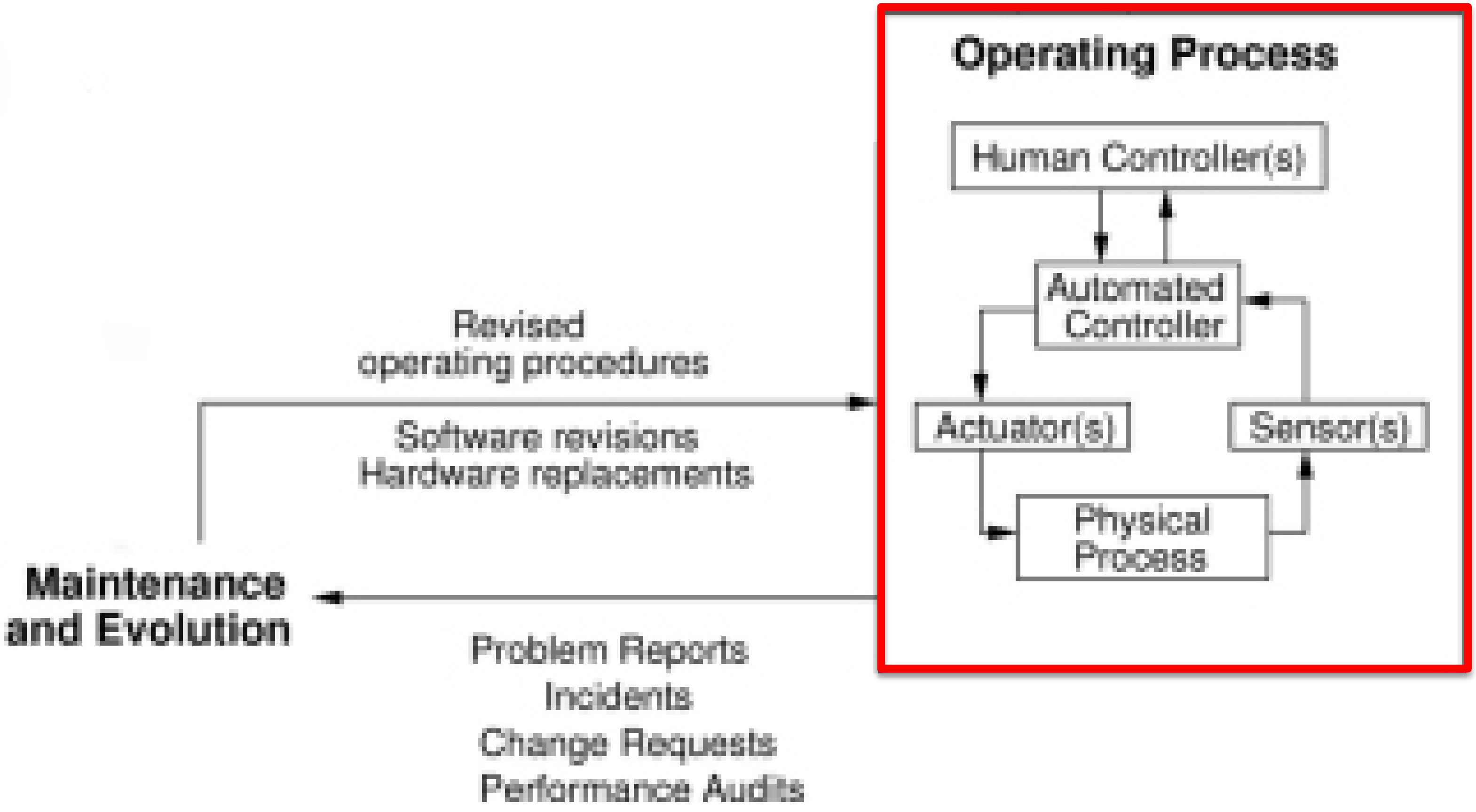
Controlled Process

Typical Industrial or Cyber Incident Investigation Model

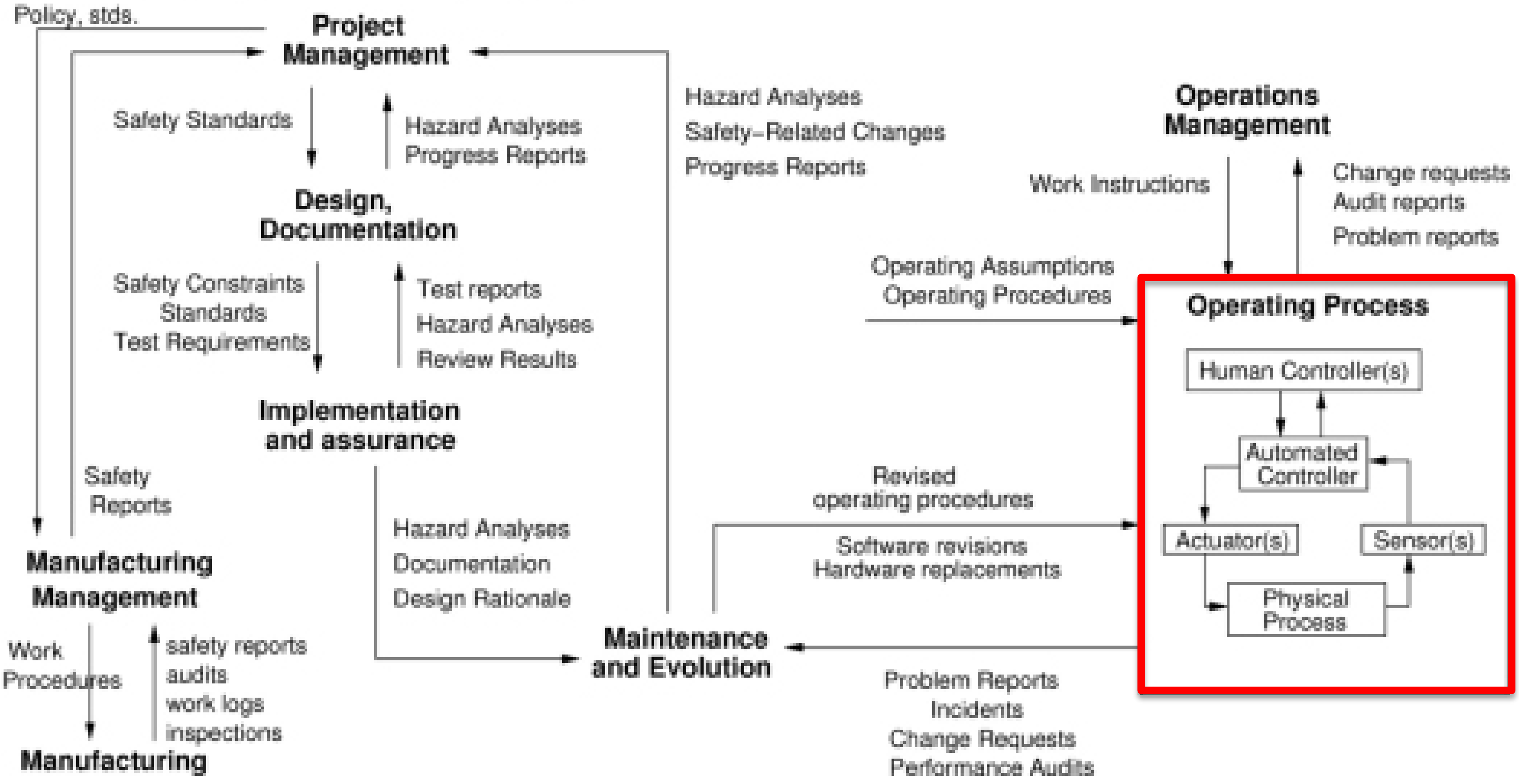
Investigation usually stops when a human error is found



Add Maintenance and Evolution Layers



Add Project Management and Operations Management Layers

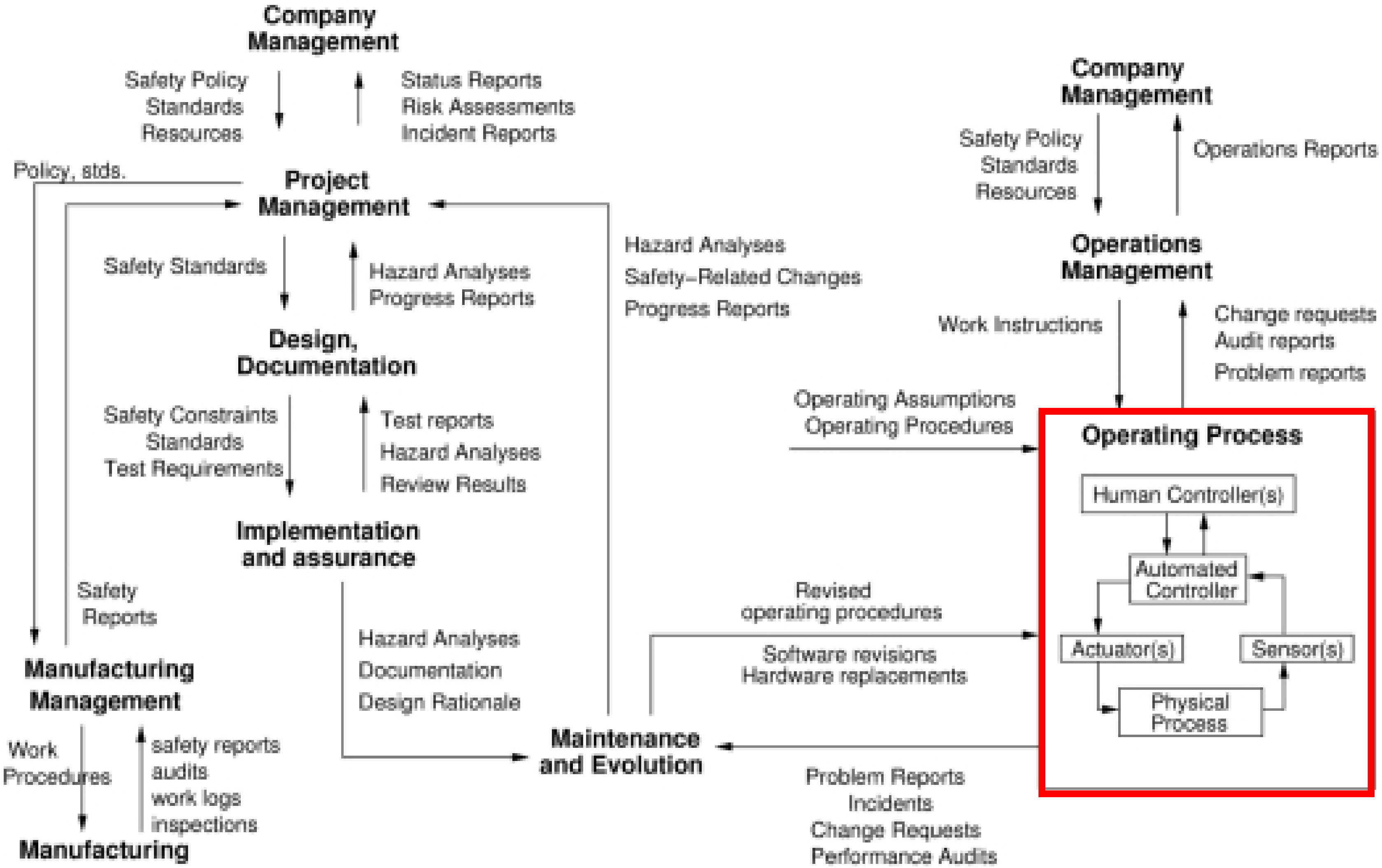


Massachusetts Institute of Technology

(IC)³ for INTERDISCIPLINARY CONSORTIUM for IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY

MITSloan MANAGEMENT

Add Company Management Layer



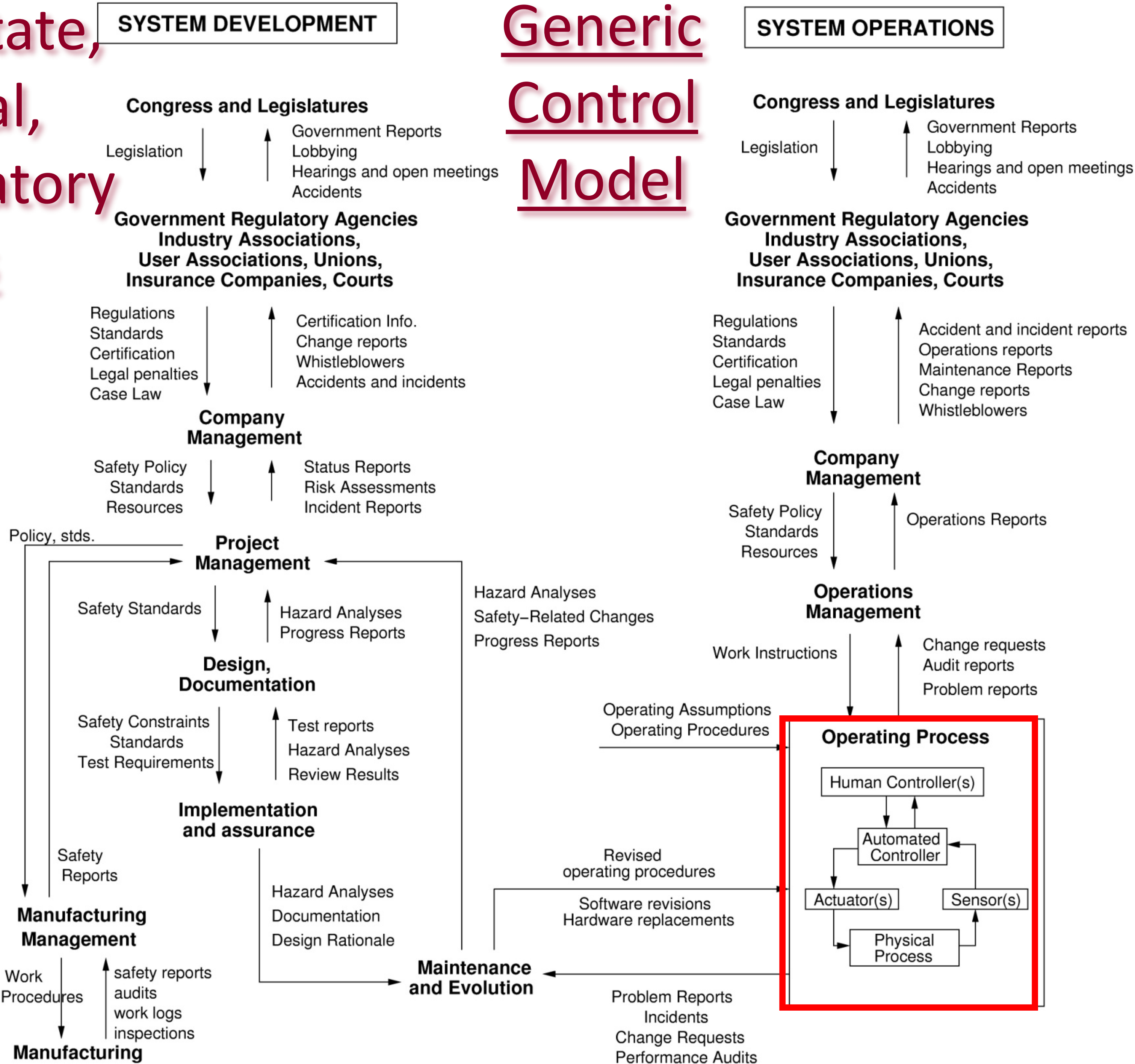
Massachusetts Institute of Technology

(IC)3 for INTERDISCIPLINARY CONSORTIUM IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY

MITSloan MANAGEMENT

Add State, Federal, Regulatory Layers

Generic Control Model



SYSTEM DEVELOPMENT

Congress and Legislatures

Legislation

Government Reports
Lobbying
Hearings and open meetings
Accidents

Government Regulatory Agencies
Industry Associations,
User Associations, Unions,
Insurance Companies, Courts

Regulations
Standards
Certification
Legal penalties
Case Law

Certification Info.
Change reports
Whistleblowers
Accidents and incidents

Company
Management

Safety Policy
Standards
Resources

Status Reports
Risk Assessments
Incident Reports

Policy, stds.

Project
Management

Safety Standards

Hazard Analyses
Progress Reports

Hazard Analyses
Safety–Related Changes
Progress Reports

Design,
Documentation

Safety Constraints
Standards
Test Requirements

Test reports
Hazard Analyses
Review Results

Implementation
and assurance

Safety
Reports

Hazard Analyses
Documentation
Design Rationale

Manufacturing
Management

Work
Procedures

safety reports
audits
work logs
inspections

Manufacturing

Maintenance
and Evolution

SYSTEM OPERATIONS

Congress and Legislatures

Legislation

Government Reports
Lobbying
Hearings and open meetings
Accidents

Government Regulatory Agencies
Industry Associations,
User Associations, Unions,
Insurance Companies, Courts

Regulations
Standards
Certification
Legal penalties
Case Law

Accident and incident reports
Operations reports
Maintenance Reports
Change reports
Whistleblowers

Company
Management

Safety Policy
Standards
Resources

Operations Reports

Operations
Management

Work Instructions

Change requests
Audit reports
Problem reports

Operating Assumptions
Operating Procedures

Operating Process

Human Controller(s)

Automated
Controller

Actuator(s)

Sensor(s)

Physical
Process

Revised
operating procedures

Software revisions
Hardware replacements

Problem Reports
Incidents
Change Requests
Performance Audits

Massachusetts
Institute of
Technology

(IC)³
for
INTERDISCIPLINARY CONSORTIUM
IMPROVING CRITICAL
INFRASTRUCTURE CYBERSECURITY

MITSloan
MANAGEMENT

The Approaches

STAMP = System Theoretic Accident Model And Processes

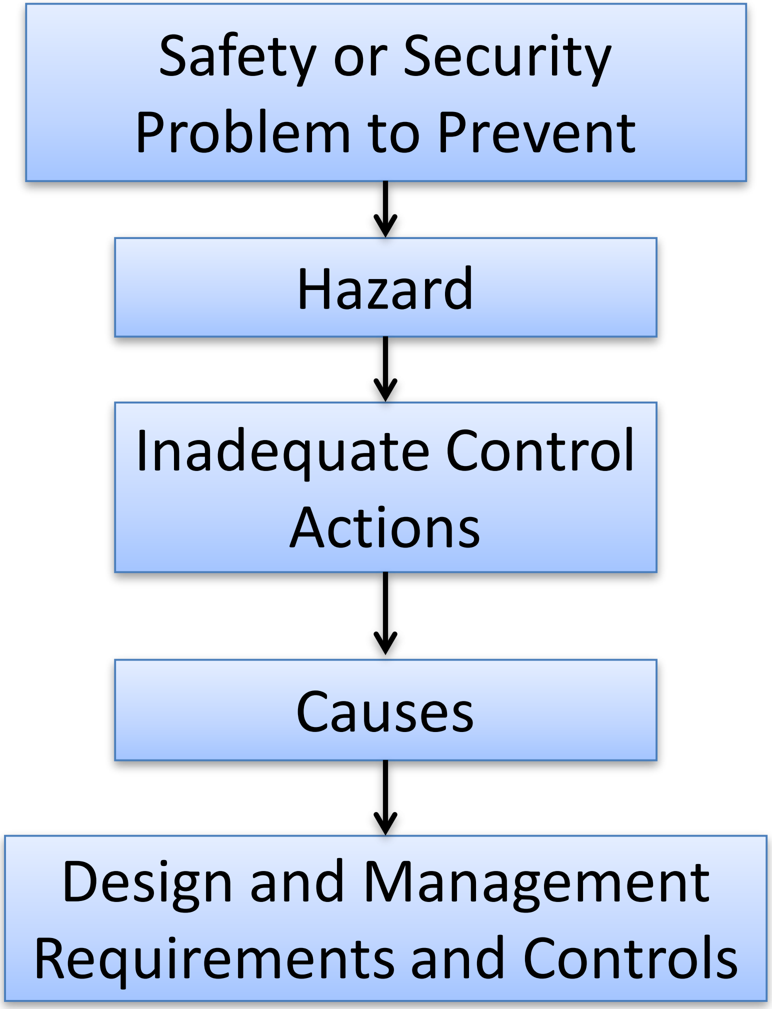
1. **CAST:** Causal Analysis using System Theory
   – Prove the model by looking backwards

2. **STPA:** System Theoretic Process Analysis
   – Apply the model looking forward for incident prevention

CAST Systematic Analysis Process

1	System and hazard definition
2	System level safety/security requirements
3	Draw hierarchical control structure
4	Proximate events
5	Analyze the physical system
6	Moving up the levels of the control structure
7	Coordination and communication
8	Dynamics and change over time
9	Generate recommendations.

STPA Systematic Incident Prevention Process


Safety or Security Problem to Prevent
Hazard
Inadequate Control Actions
Causes
Design and Management Requirements and Controls

Presentation Outline

- (IC)^3
- Research Motivations
- Approaches
  - – System-Theoretic Accident Model and Processes (STAMP)
    - Causal Analysis based on STAMP (CAST)
    - System Theoretic Process Analysis (STPA)
- Case Study
  - – CAST Applied to the TJX Case
  - – CAST Applied to Stuxnet
- Future Research Directions

TJX (TJ Maxx & Marshalls) Case Study

- TJX is a US-based major off-price retailer.
  - Revenues > $25 billion (FY2014)
- Victim of largest (by number of cards) cyber-attack in history, when announced in 2007.
- Cost to TJX > $170 million, per SEC filings.
- Cyber-attack launched from a store on Miami, FL in 2005 by exploiting Wi-Fi vulnerability.
- Hackers ultimately reached corporate payment servers and stole current transaction data.
- Cyber-attack lasted for over 1.5 years (According to the US ICS-CERT, based on all reported ICS cyber-attacks, the average time that cyber-attackers were inside the ICS system before being discovered was 243 days.)

Sources: Federal/State Court records (primary), TJX SEC Filings, Others (NYT, WSJ, Globe, FTC, Academic papers, Journal articles). ICS-CERT Oral Presentation, ABB Automation & Power World, March, 2015

CAST Step 1: Identify System and Hazards

- ***System***
  - TJX payment card processing system
- ***Hazards – at system level***
  - System allows for unauthorized access to customer information

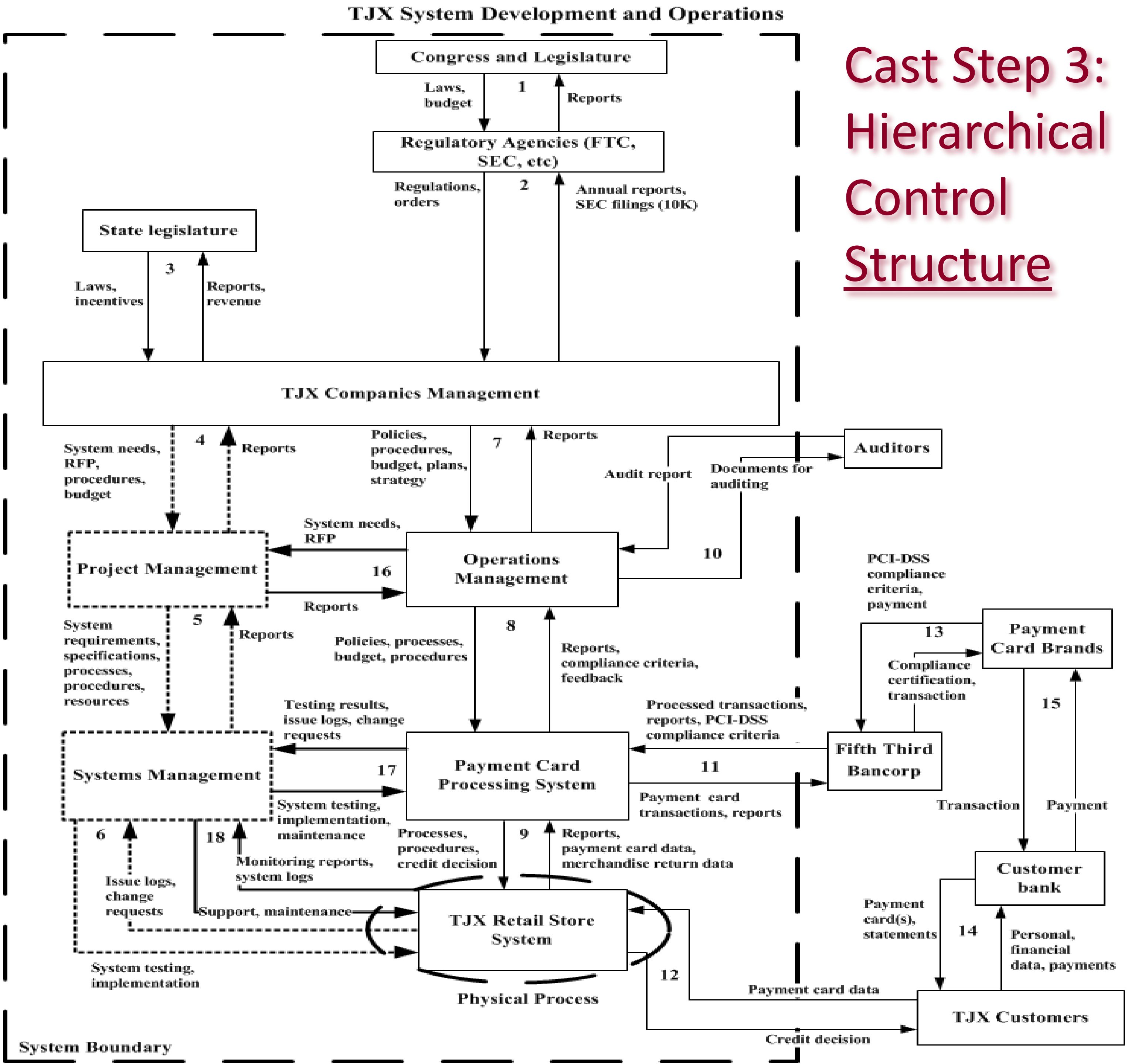
1	System and hazard definition
2	System level safety/security requirements
3	Draw control structure
4	Proximate events
5	Analyze the physical system
6	Moving up the levels of the control structure
7	Coordination and communication
8	Dynamics and change over time
9	Generate recommendations.

CAST Step 2:
Define System Security Requirements

- Protect customer information from unauthorized access.
- Provide adequate training to staff for managing security technology infrastructure.
- Minimize losses from unauthorized access to payment system.

1	System and hazard definition
2	System level safety/security requirements
3	Draw control structure
4	Proximate events
5	Analyze the physical system
6	Moving up the levels of the control structure
7	Coordination and communication
8	Dynamics and change over time
9	Generate recommendations.

Cast Step 3: Hierarchical Control Structure



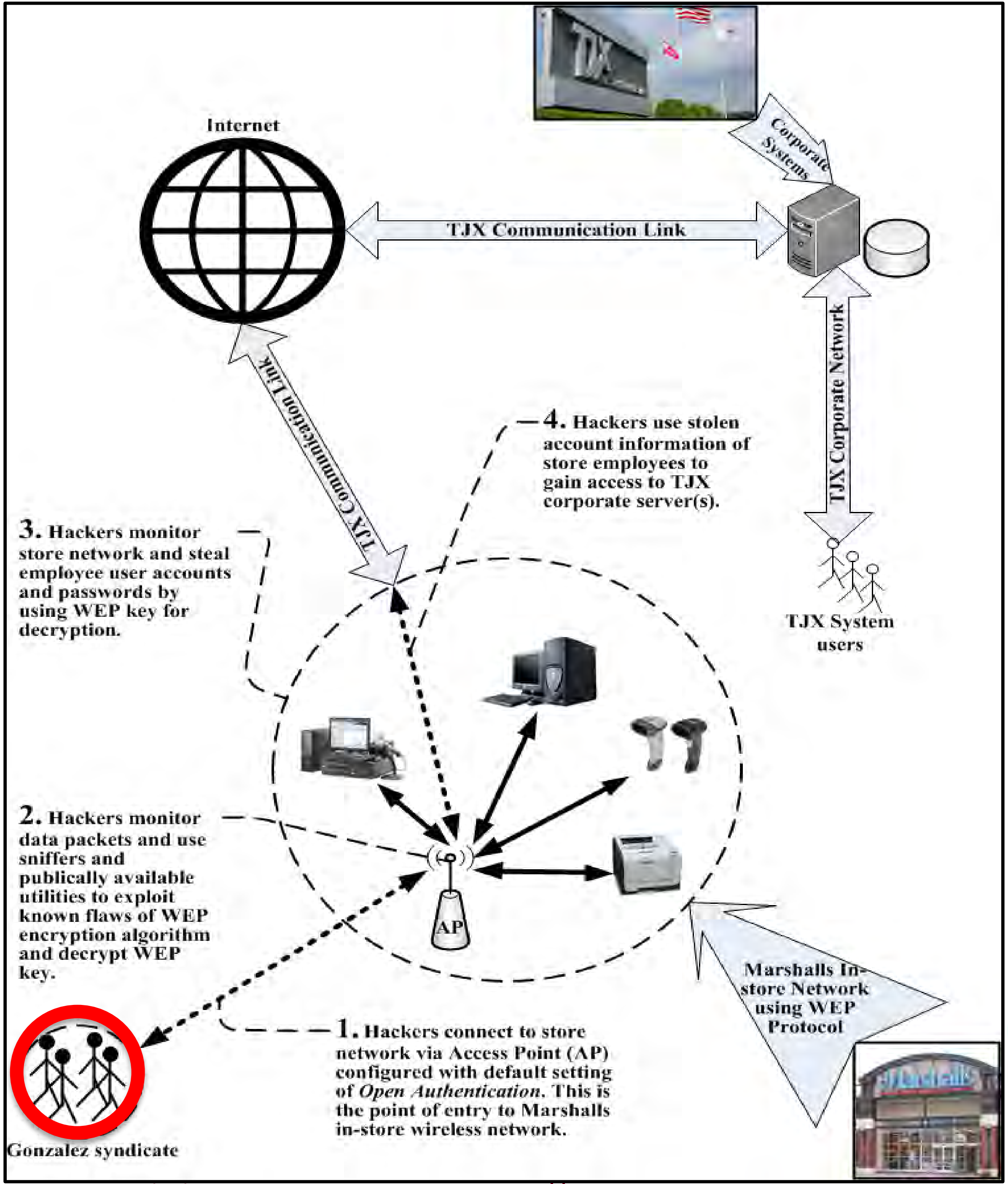
TJX System Development and Operations
Congress and Legislature
Laws, budget
1
Reports
Regulatory Agencies (FTC, SEC, etc)
Regulations, orders
2
Annual reports, SEC filings (10K)
State legislature
3
Laws, incentives
Reports, revenue
TJX Companies Management
System needs, RFP, procedures, budget
4
Reports
Policies, procedures, budget, plans, strategy
7
Reports
Auditors
Audit report
Documents for auditing
10
Project Management
System needs, RFP
16
Reports
Operations Management
System requirements, specifications, processes, procedures, resources
5
Reports
Policies, processes, budget, procedures
8
Reports, compliance criteria, feedback
PCI-DSS compliance criteria, payment
13
Payment Card Brands
Compliance certification, transaction
15
Testing results, issue logs, change requests
Processed transactions, reports, PCI-DSS compliance criteria
Systems Management
17
Payment Card Processing System
11
Fifth Third Bancorp
System testing, implementation, maintenance
Payment card transactions, reports
Transaction
Payment
6
18
Processes, procedures, credit decision
9
Reports, payment card data, merchandise return data
Customer bank
Issue logs, change requests
Monitoring reports, system logs
Support, maintenance
TJX Retail Store System
Payment card(s), statements
14
Personal, financial data, payments
System testing, implementation
12
Payment card data
Physical Process
TJX Customers
Credit decision
System Boundary

Proximal Event Chain

1	System and hazard definition
2	System level safety/security requirements
3	Draw control structure
4	Proximate events
5	Analyze the physical system
6	Moving up the levels of the control structure
7	Coordination and communication
8	Dynamics and change over time
9	Generate recommendations.

Breaching Marshalls' Store

1. **AP- Open authentication** vs Shared Key authentication.
2. **WEP** publically known **weak algorithm compromised.**
3. **Sniffers used** to monitor data packets.
4. Hackers steal store **employee account information** and **gain access to TJX corporate servers.**



4. Hackers use stolen account information of store employees to gain access to TJX corporate server(s).

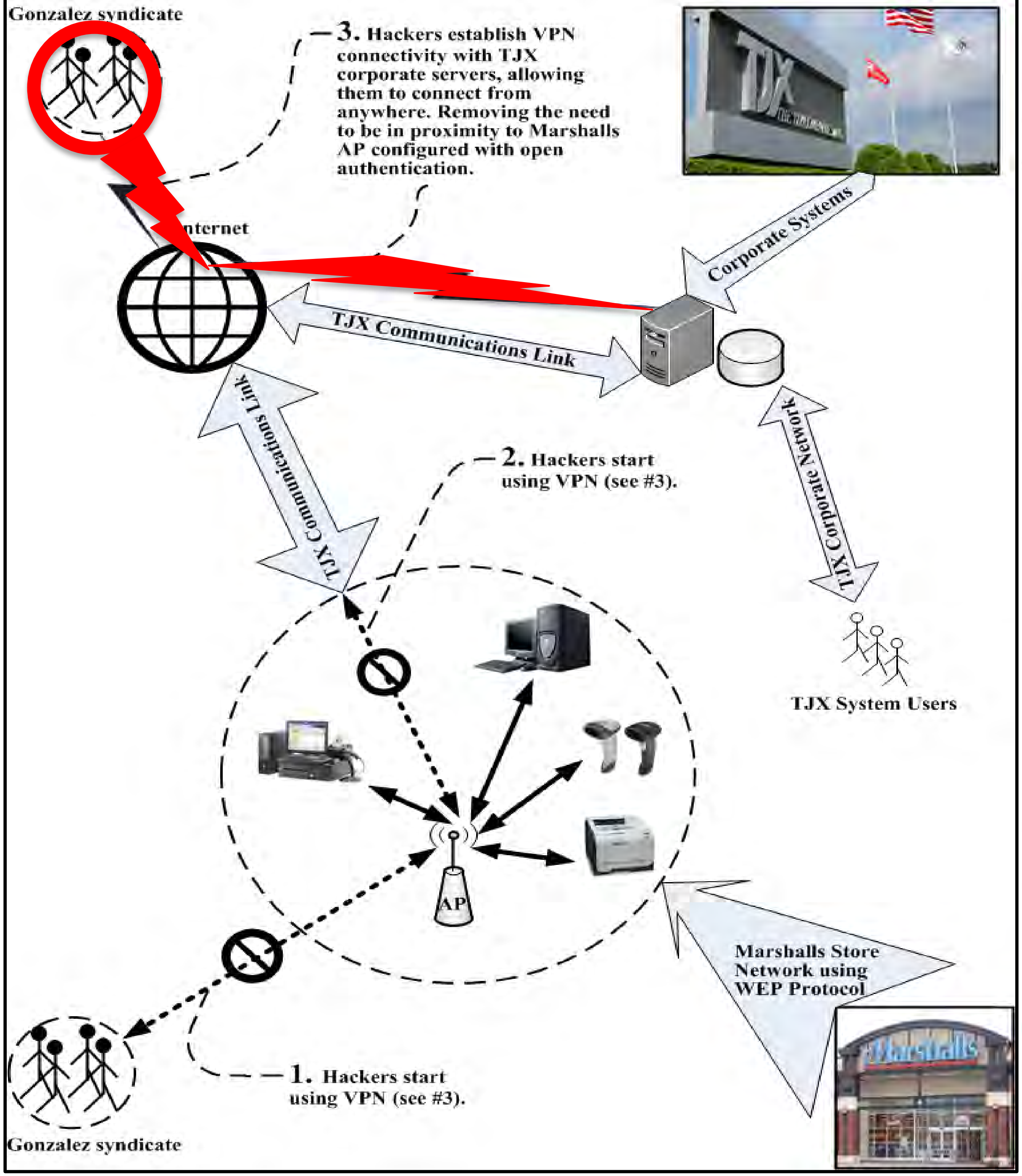
3. Hackers monitor store network and steal employee user accounts and passwords by using WEP key for decryption.

2. Hackers monitor data packets and use sniffers and publically available utilities to exploit known flaws of WEP encryption algorithm and decrypt WEP key.

1. Hackers connect to store network via Access Point (AP) configured with default setting of *Open Authentication*. This is the point of entry to Marshalls in-store wireless network.

Hackers Establish VPN Connection

1. Hackers use Marshalls AP to install VPN connection.
2. VPN is between TJX corporate server and hacker controlled servers in Latvia.
3. Code installed on TJX corporate payment processing server.
4. No longer using TJX network



3. Hackers establish VPN connectivity with TJX corporate servers, allowing them to connect from anywhere. Removing the need to be in proximity to Marshalls AP configured with open authentication.

2. Hackers start using VPN (see #3).

1. Hackers start using VPN (see #3).

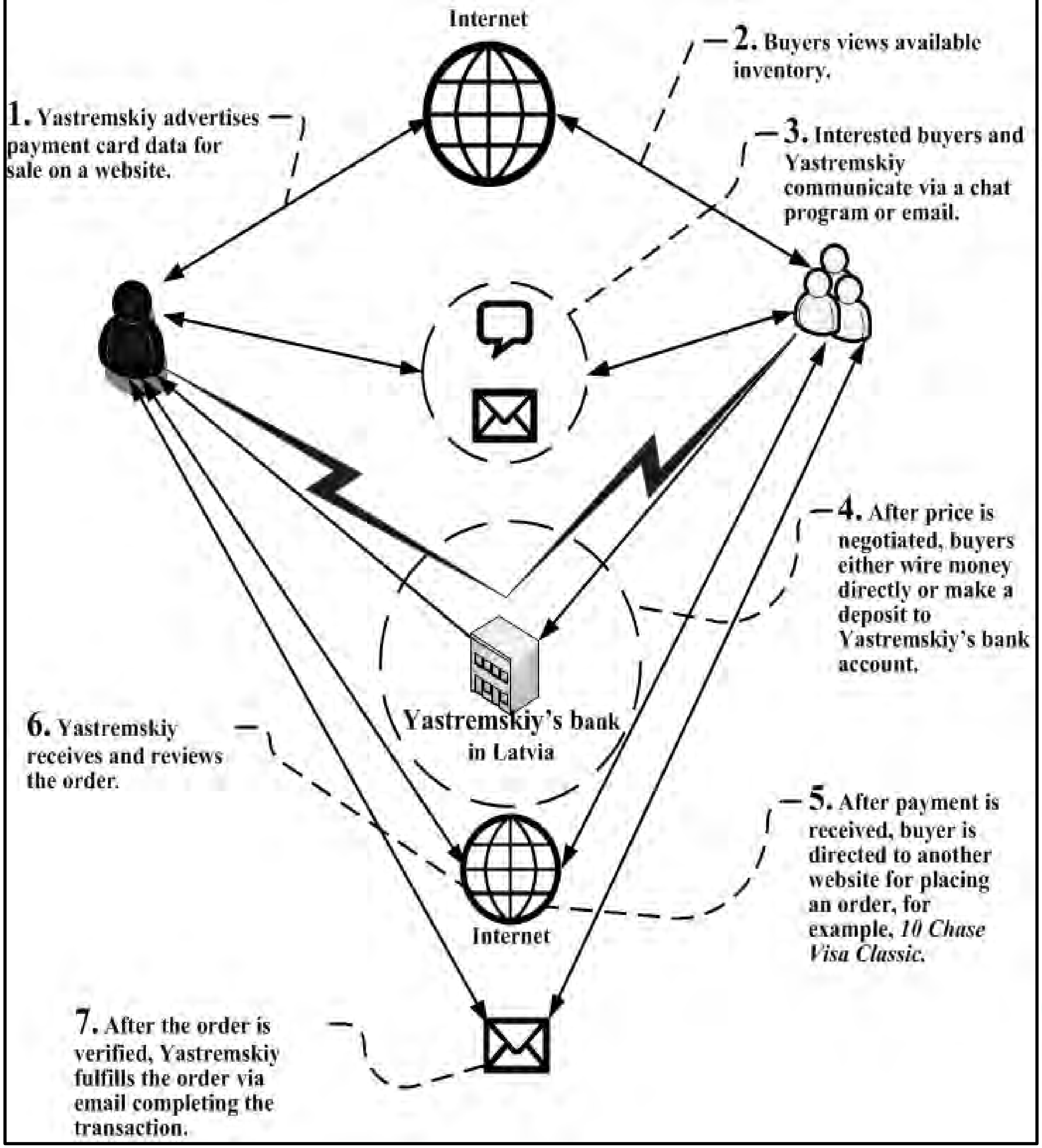
Massachusetts Institute of Technology

(IC)³ for INTERDISCIPLINARY CONSORTIUM IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY

MITSloan MANAGEMENT

Flow for Sales of Stolen Payment Card Information

Hackers are selling credit card data for almost 1.5 years


Internet
1. Yastremskiy advertises payment card data for sale on a website.
2. Buyers views available inventory.
3. Interested buyers and Yastremskiy communicate via a chat program or email.
4. After price is negotiated, buyers either wire money directly or make a deposit to Yastremskiy's bank account.
Yastremskiy's bank in Latvia
5. After payment is received, buyer is directed to another website for placing an order, for example, *10 Chase Visa Classic.*
6. Yastremskiy receives and reviews the order.
Internet
7. After the order is verified, Yastremskiy fulfills the order via email completing the transaction.

Massachusetts Institute of Technology

(IC)3 for INTERDISCIPLINARY CONSORTIUM IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY

MITSloan MANAGEMENT

Analyzing the Physical System

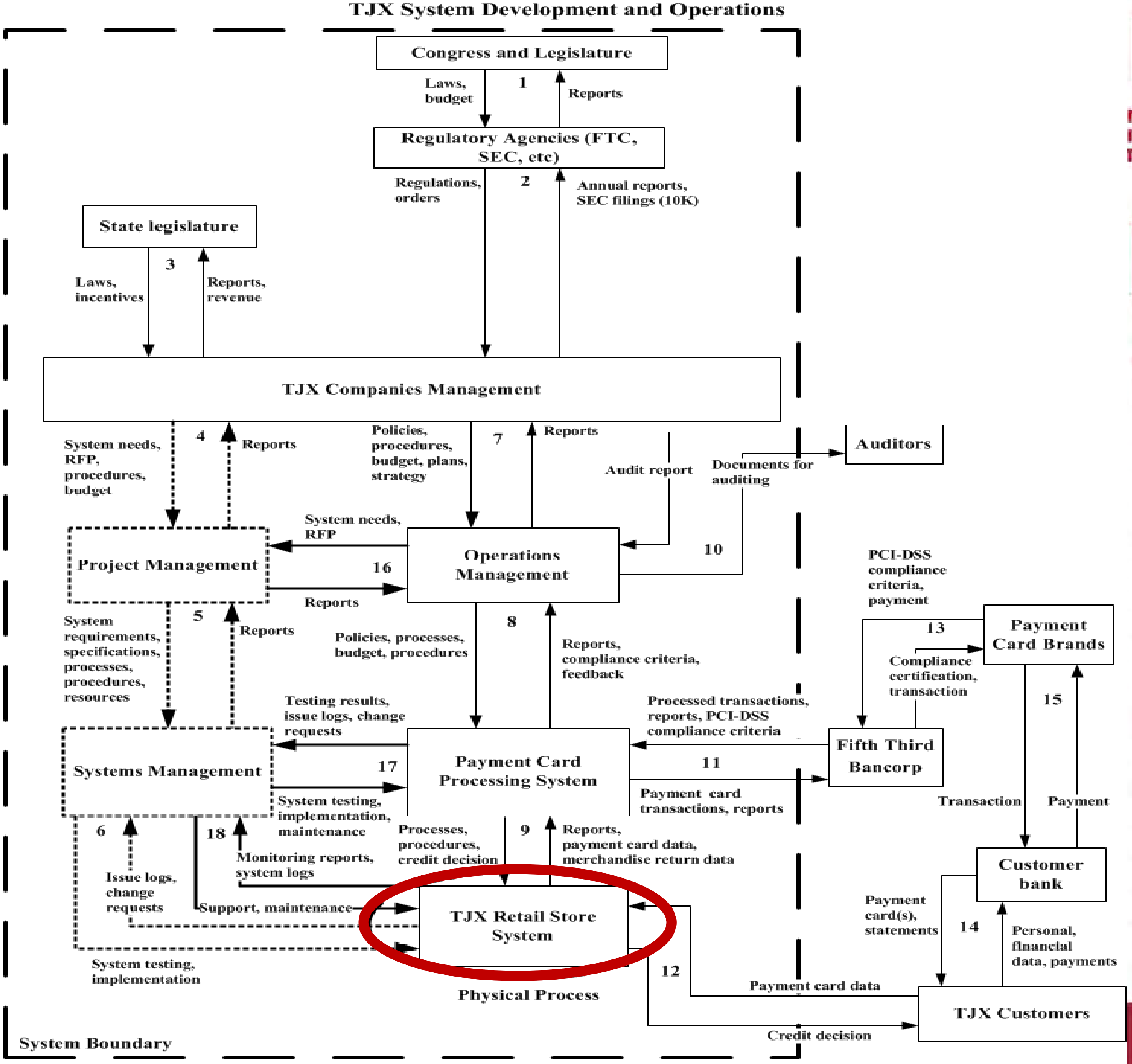
1	System and hazard definition
2	System level safety/security requirements
3	Draw control structure
4	Proximate events
5	Analyze the physical system
6	Moving up the levels of the control structure
7	Coordination and communication
8	Dynamics and change over time
9	Generate recommendations.

Massachusetts Institute of Technology

(IC)^3 for INTERDISCIPLINARY CONSORTIUM IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY

MITSloan MANAGEMENT

Cast Step 5: Analyzing the Physical Process (TJX Retail Store)



TJX System Development and Operations

Congress and Legislature

Laws, budget

1

Reports

Regulatory Agencies (FTC, SEC, etc)

Regulations, orders

2

Annual reports, SEC filings (10K)

State legislature

Laws, incentives

3

Reports, revenue

TJX Companies Management

System needs, RFP, procedures, budget

4

Reports

Policies, procedures, budget, plans, strategy

7

Reports

Audit report

Documents for auditing

Auditors

10

Project Management

System needs, RFP

16

Reports

Operations Management

System requirements, specifications, processes, procedures, resources

5

Reports

Policies, processes, budget, procedures

8

Reports, compliance criteria, feedback

PCI-DSS compliance criteria, payment

13

Payment Card Brands

Compliance certification, transaction

15

Testing results, issue logs, change requests

Processed transactions, reports, PCI-DSS compliance criteria

Systems Management

17

Payment Card Processing System

11

Fifth Third Bancorp

System testing, implementation, maintenance

Payment card transactions, reports

Transaction

Payment

6

18

Monitoring reports, system logs

Processes, procedures, credit decision

9

Reports, payment card data, merchandise return data

Customer bank

Issue logs, change requests

Support, maintenance

TJX Retail Store System

Payment card(s), statements

14

Personal, financial data, payments

System testing, implementation

12

Payment card data

Physical Process

TJX Customers

Credit decision

System Boundary

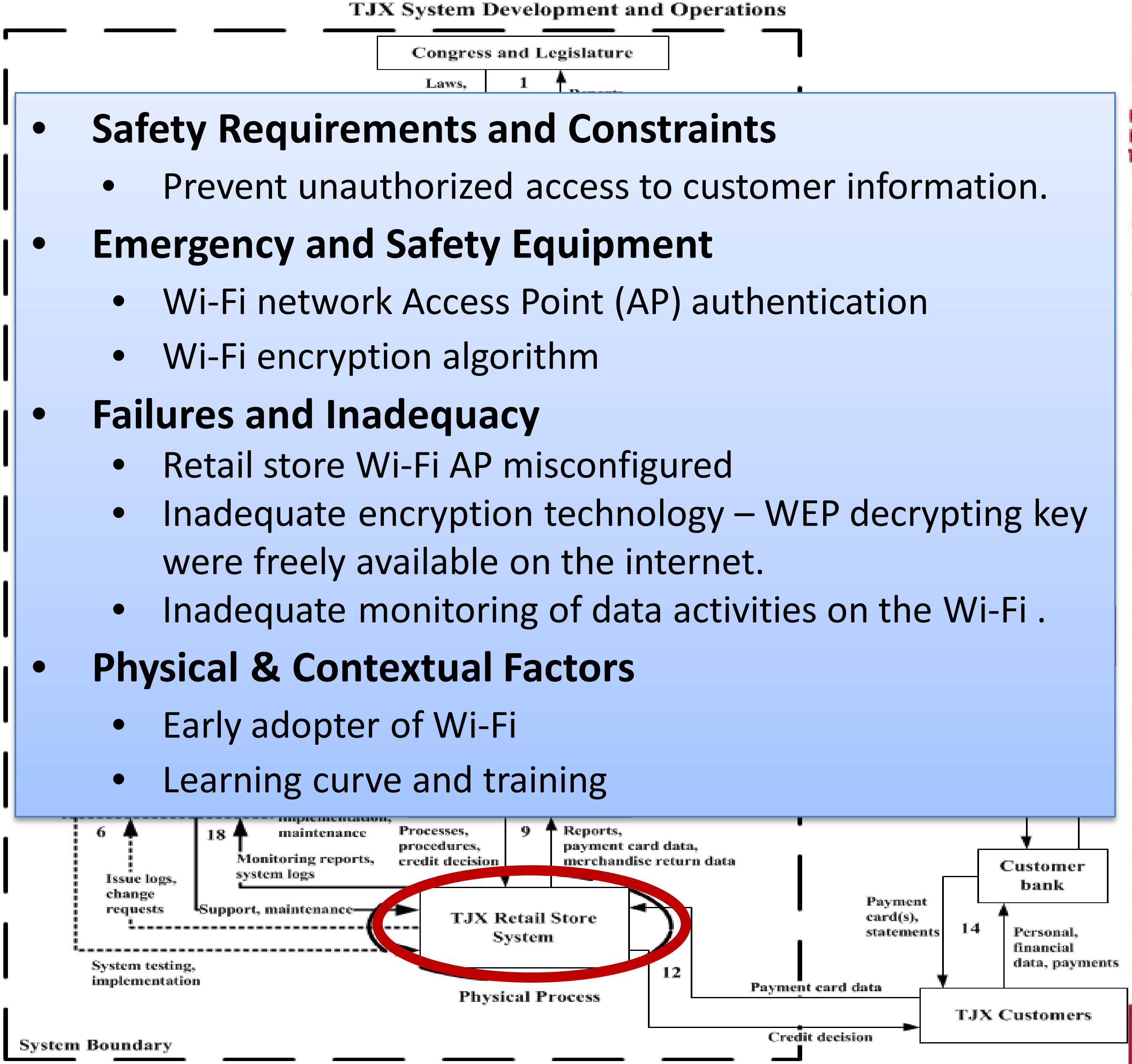
Legend:

- Each **number** indicates a unique loop.
- Bold-dashed **square** indicates TJX system boundary.
- Bold-dashed **oval** indicates the physical system.
- **Downward arrow** represents reference channel for imposing safety constraints.
- **Upward arrow** represents feedback channel and reports the effectiveness of constraints.

Cast Step 5: Analyzing the Physical Process (TJX Retail Store)

Four Key Areas:

1. **Safety Requirements & Constraints**
2. **Emergency & Safety Equipment**
3. **Failures & Inadequacy**
4. **Physical & Contextual Factors**



- **Safety Requirements and Constraints**
  - Prevent unauthorized access to customer information.
- **Emergency and Safety Equipment**
  - Wi-Fi network Access Point (AP) authentication
  - Wi-Fi encryption algorithm
- **Failures and Inadequacy**
  - Retail store Wi-Fi AP misconfigured
  - Inadequate encryption technology – WEP decrypting key were freely available on the internet.
  - Inadequate monitoring of data activities on the Wi-Fi .
- **Physical & Contextual Factors**
  - Early adopter of Wi-Fi
  - Learning curve and training

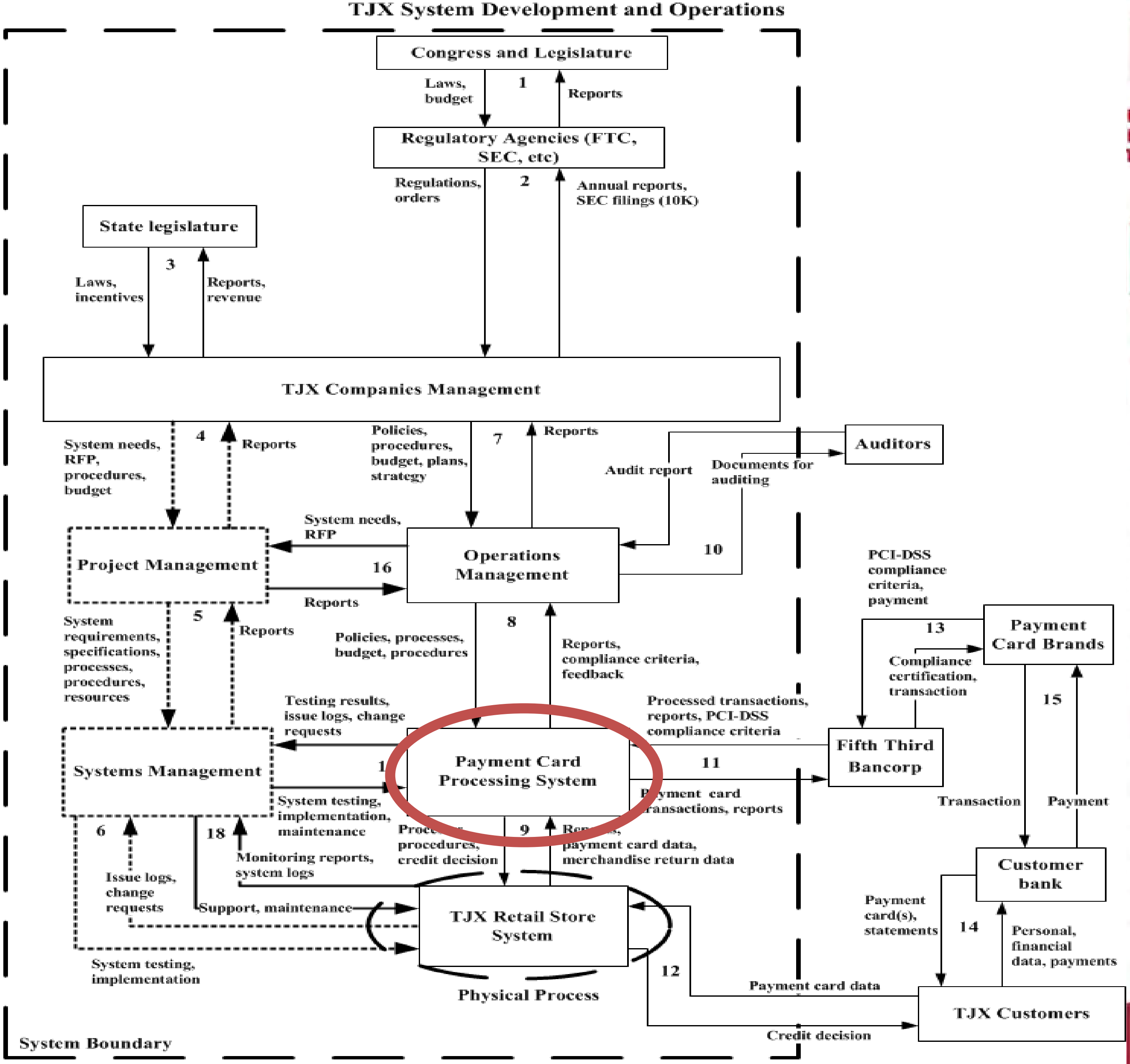
Legend:
- Each **number** indicates a unique loop.
- Bold-dashed **square** indicates TJX system boundary.
- Bold-dashed **oval** indicates the physical system.
- **Downward arrow** represents reference channel for imposing safety constraints.
- **Upward arrow** represents feedback channel and reports the effectiveness of constraints.

Analyzing the Control Structure

1	System and hazard definition
2	System level safety/security requirements
3	Draw control structure
4	Proximate events
5	Analyze the physical system
6	Moving up the levels of the control structure
7	Coordination and communication
8	Dynamics and change over time
9	Generate recommendations.

Step 6: Analysis of Higher Levels of the Hierarchical Safety Control Structure

Payment Card Processing System



TJX System Development and Operations

Congress and Legislature

Laws, budget

1

Reports

Regulatory Agencies (FTC, SEC, etc)

Regulations, orders

2

Annual reports, SEC filings (10K)

State legislature

Laws, incentives

3

Reports, revenue

TJX Companies Management

System needs, RFP, procedures, budget

4

Reports

Policies, procedures, budget, plans, strategy

7

Reports

Auditors

Audit report

Documents for auditing

System needs, RFP

Project Management

16

Reports

Operations Management

10

System requirements, specifications, processes, procedures, resources

5

Reports

8

Policies, processes, budget, procedures

Reports, compliance criteria, feedback

PCI-DSS compliance criteria, payment

Payment Card Brands

13

Compliance certification, transaction

15

Testing results, issue logs, change requests

Processed transactions, reports, PCI-DSS compliance criteria

Systems Management

1

Payment Card Processing System

11

Fifth Third Bancorp

System testing, implementation, maintenance

Payment card transactions, reports

Transaction

Payment

6

18

Processes, procedures, credit decision

9

Reports, payment card data, merchandise return data

Customer bank

Monitoring reports, system logs

Issue logs, change requests

Support, maintenance

TJX Retail Store System

Payment card(s), statements

14

Personal, financial data, payments

System testing, implementation

12

Physical Process

Payment card data

TJX Customers

Credit decision

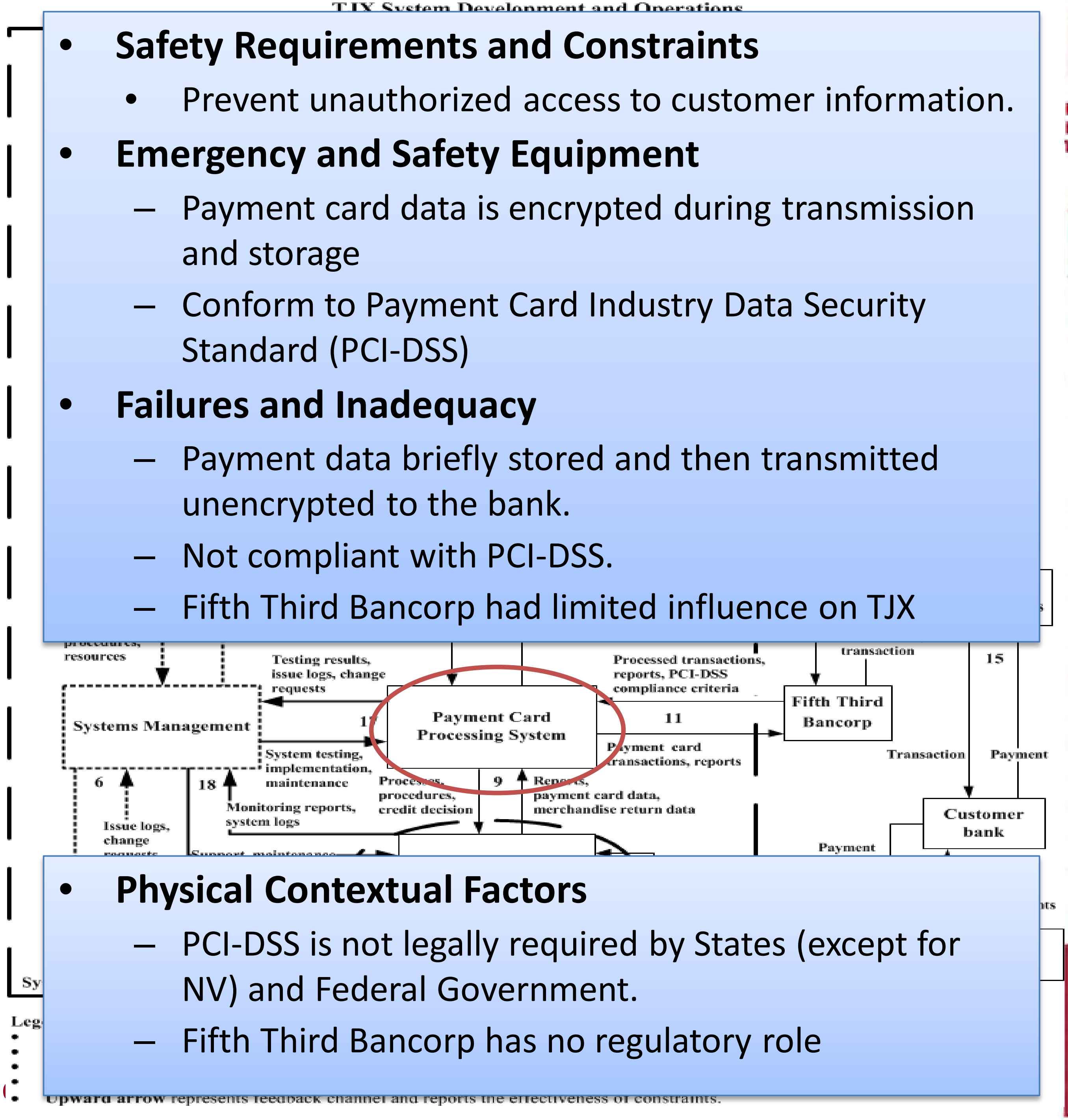
System Boundary

Legend:

- Each **number** indicates a unique loop.
- Bold-dashed **square** indicates TJX system boundary.
- Bold-dashed **oval** indicates the physical system.
- **Downward arrow** represents reference channel for imposing safety constraints.
- **Upward arrow** represents feedback channel and reports the effectiveness of constraints.

Step 6: Analysis of Higher Levels of the Hierarchical Safety Control Structure

Payment Card Processing System

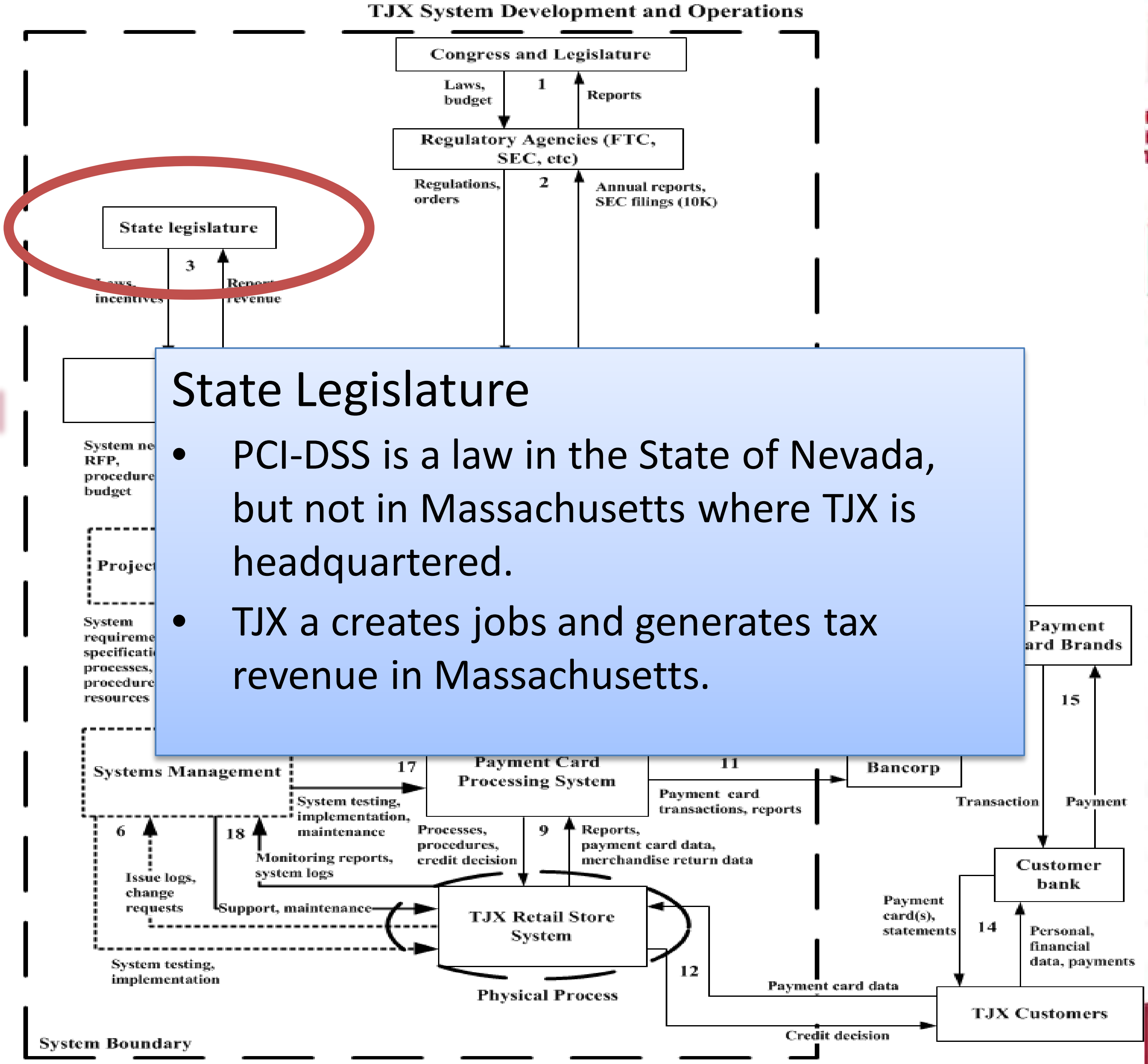

TJX System Development and Operations
procedures, resources
Testing results, issue logs, change requests
Processed transactions, reports, PCI-DSS compliance criteria
transaction
15
Systems Management
17
Payment Card Processing System
11
Fifth Third Bancorp
System testing, implementation, maintenance
Payment card transactions, reports
Transaction
Payment
6
18
Processes, procedures, credit decision
9
Reports, payment card data, merchandise return data
Monitoring reports, system logs
Issue logs, change requests
Support, maintenance
Customer bank
Payment
Sy
Leg
Upward arrow represents feedback channel and reports the effectiveness of constraints.

- **Safety Requirements and Constraints**
  - Prevent unauthorized access to customer information.
- **Emergency and Safety Equipment**
  - Payment card data is encrypted during transmission and storage
  - Conform to Payment Card Industry Data Security Standard (PCI-DSS)
- **Failures and Inadequacy**
  - Payment data briefly stored and then transmitted unencrypted to the bank.
  - Not compliant with PCI-DSS.
  - Fifth Third Bancorp had limited influence on TJX

- **Physical Contextual Factors**
  - PCI-DSS is not legally required by States (except for NV) and Federal Government.
  - Fifth Third Bancorp has no regulatory role

Step 6: Analysis of Higher Levels of the Hierarchical Safety Control Structure

State Legislature


TJX System Development and Operations
Congress and Legislature
Laws, budget
1
Reports
Regulatory Agencies (FTC, SEC, etc)
Regulations, orders
2
Annual reports, SEC filings (10K)
State legislature
3
Laws, incentives
Report, revenue
System needs, RFP, procedures, budget
Project
System requirements, specifications, processes, procedures, resources
Payment Card Brands
15
Systems Management
17
Payment Card Processing System
11
Bancorp
System testing, implementation, maintenance
Payment card transactions, reports
Transaction
Payment
6
18
Processes, procedures, credit decision
9
Reports, payment card data, merchandise return data
Customer bank
Monitoring reports, system logs
Issue logs, change requests
Support, maintenance
TJX Retail Store System
Payment card(s), statements
14
Personal, financial data, payments
System testing, implementation
12
Payment card data
Physical Process
TJX Customers
Credit decision
System Boundary

State Legislature

- PCI-DSS is a law in the State of Nevada, but not in Massachusetts where TJX is headquartered.
- TJX a creates jobs and generates tax revenue in Massachusetts.

Legend:
- Each **number** indicates a unique loop.
- Bold-dashed **square** indicates TJX system boundary.
- Bold-dashed **oval** indicates the physical system.
- **Downward arrow** represents reference channel for imposing safety constraints.
- **Upward arrow** represents feedback channel and reports the effectiveness of constraints.

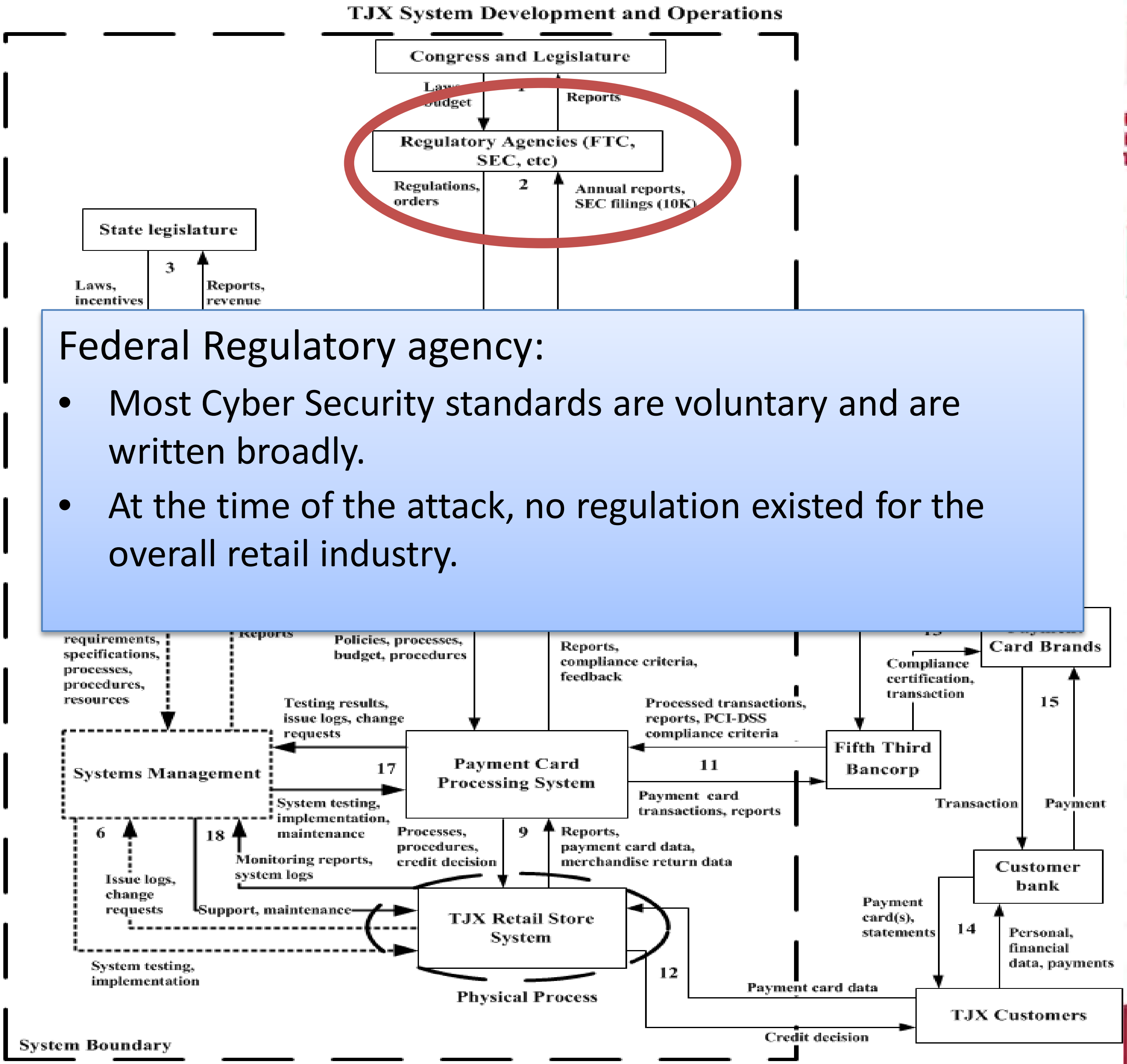
Massachusetts Institute of Technology

(IC)³ for IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY INTERDISCIPLINARY CONSORTIUM

MITSloan MANAGEMENT

Step 6: Analysis of Higher Levels of the Hierarchical Safety Control Structure

Regulatory Agencies: FTC, SEC, etc.


TJX System Development and Operations
Congress and Legislature
Laws, budget
1
Reports
Regulatory Agencies (FTC, SEC, etc)
Regulations, orders
2
Annual reports, SEC filings (10K)
State legislature
3
Laws, incentives
Reports, revenue
requirements, specifications, processes, procedures, resources
Reports
Policies, processes, budget, procedures
Reports, compliance criteria, feedback
13
Payment Card Brands
Compliance certification, transaction
15
Testing results, issue logs, change requests
Processed transactions, reports, PCI-DSS compliance criteria
Systems Management
17
Payment Card Processing System
11
Fifth Third Bancorp
System testing, implementation, maintenance
Payment card transactions, reports
Transaction
Payment
6
18
Processes, procedures, credit decision
9
Reports, payment card data, merchandise return data
Customer bank
Monitoring reports, system logs
Issue logs, change requests
Support, maintenance
TJX Retail Store System
Payment card(s), statements
14
Personal, financial data, payments
System testing, implementation
12
Physical Process
Payment card data
TJX Customers
Credit decision
System Boundary

Federal Regulatory agency:

- Most Cyber Security standards are voluntary and are written broadly.
- At the time of the attack, no regulation existed for the overall retail industry.

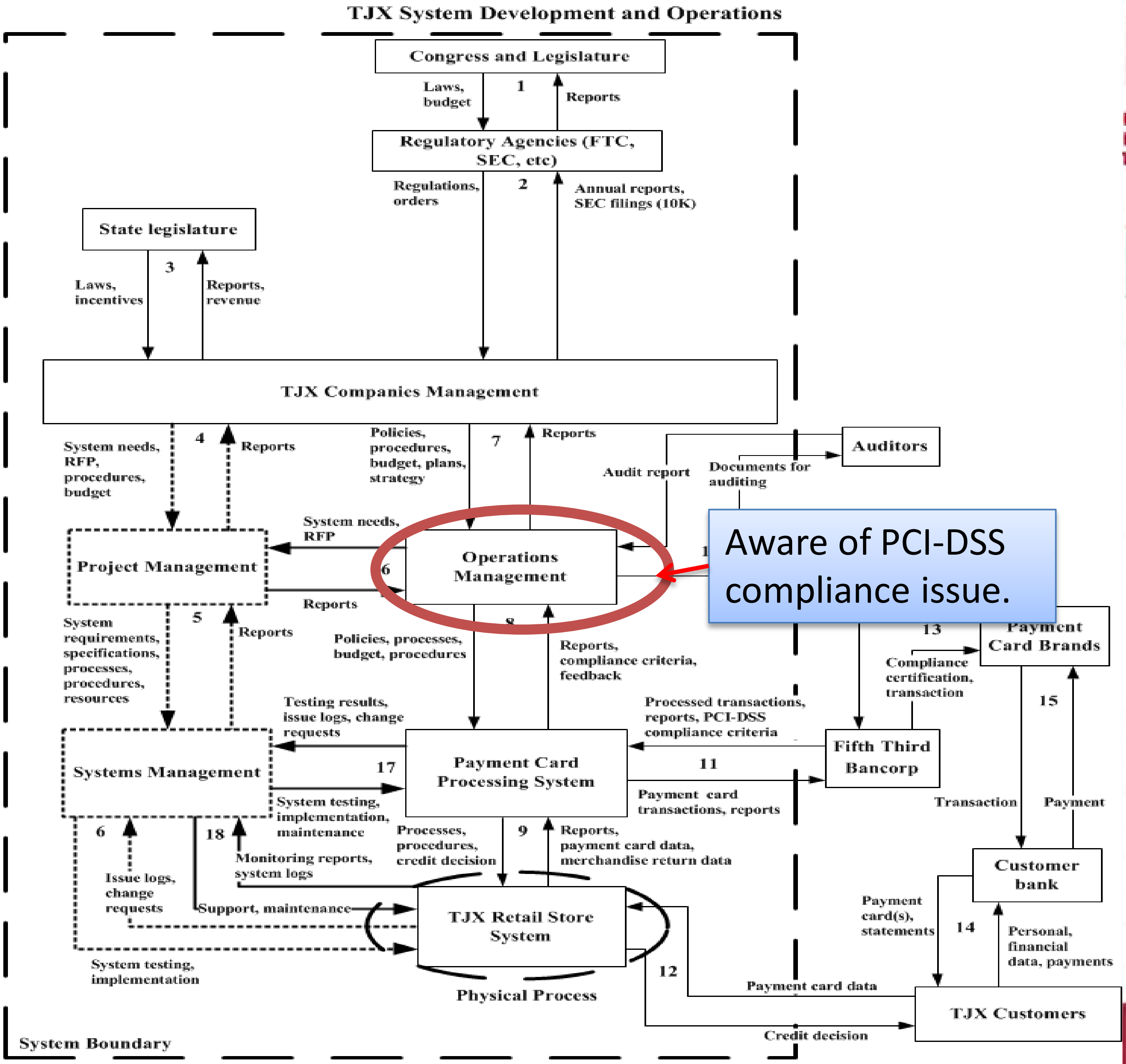
Legend:

- Each **number** indicates a unique loop.
- Bold-dashed **square** indicates TJX system boundary.
- Bold-dashed **oval** indicates the physical system.
- **Downward arrow** represents reference channel for imposing safety constraints.
- **Upward arrow** represents feedback channel and reports the effectiveness of constraints.

Coordination and Communication

1	System and hazard definition
2	System level safety/security requirements
3	Draw control structure
4	Proximate events
5	Analyze the physical system
6	Moving up the levels of the control structure
7	Coordination and communication
8	Dynamics and change over time
9	Generate recommendations.

Step 7: Coordination and Communication



TJX System Development and Operations

Congress and Legislature

Laws, budget

1

Reports

Regulatory Agencies (FTC, SEC, etc)

Regulations, orders

2

Annual reports, SEC filings (10K)

State legislature

Laws, incentives

3

Reports, revenue

TJX Companies Management

System needs, RFP, procedures, budget

4

Reports

Policies, procedures, budget, plans, strategy

7

Reports

Audit report

Documents for auditing

Auditors

Project Management

System needs, RFP

6

Operations Management

Reports

System requirements, specifications, processes, procedures, resources

5

Reports

Policies, processes, budget, procedures

8

Reports, compliance criteria, feedback

13

Payment Card Brands

Compliance certification, transaction

15

Processed transactions, reports, PCI-DSS compliance criteria

Fifth Third Bancorp

Testing results, issue logs, change requests

Systems Management

17

Payment Card Processing System

11

Payment card transactions, reports

Transaction

Payment

System testing, implementation, maintenance

6

18

Monitoring reports, system logs

Processes, procedures, credit decision

9

Reports, payment card data, merchandise return data

Customer bank

Issue logs, change requests

Support, maintenance

TJX Retail Store System

Payment card(s), statements

14

Personal, financial data, payments

System testing, implementation

12

Payment card data

Physical Process

TJX Customers

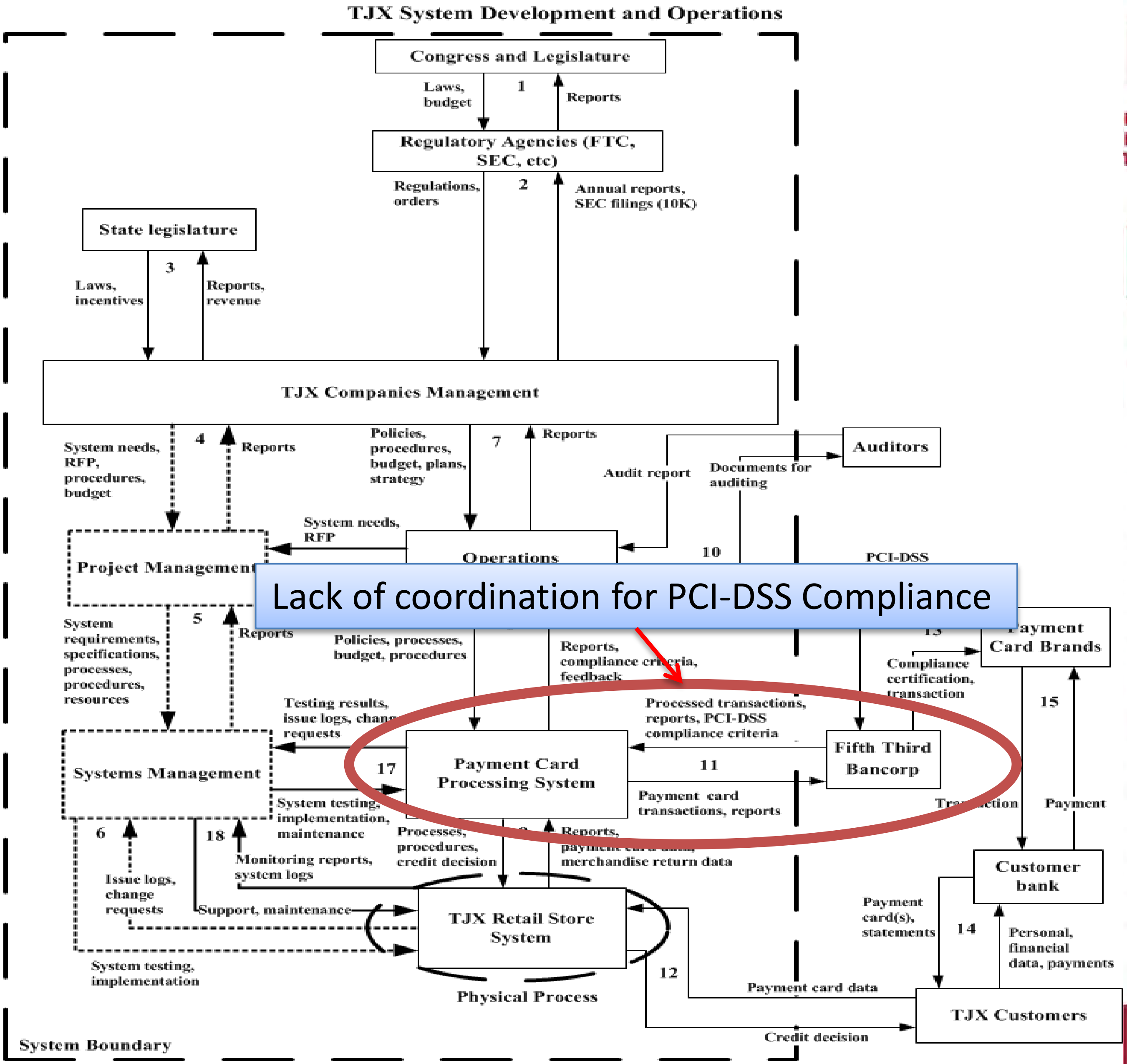
Credit decision

System Boundary

Aware of PCI-DSS compliance issue.

Legend:
- Each **number** indicates a unique loop.
- Bold-dashed **square** indicates TJX system boundary.
- Bold-dashed **oval** indicates the physical system.
- **Downward arrow** represents reference channel for imposing safety constraints.
- **Upward arrow** represents feedback channel and reports the effectiveness of constraints.

Step 7: Coordination and Communication

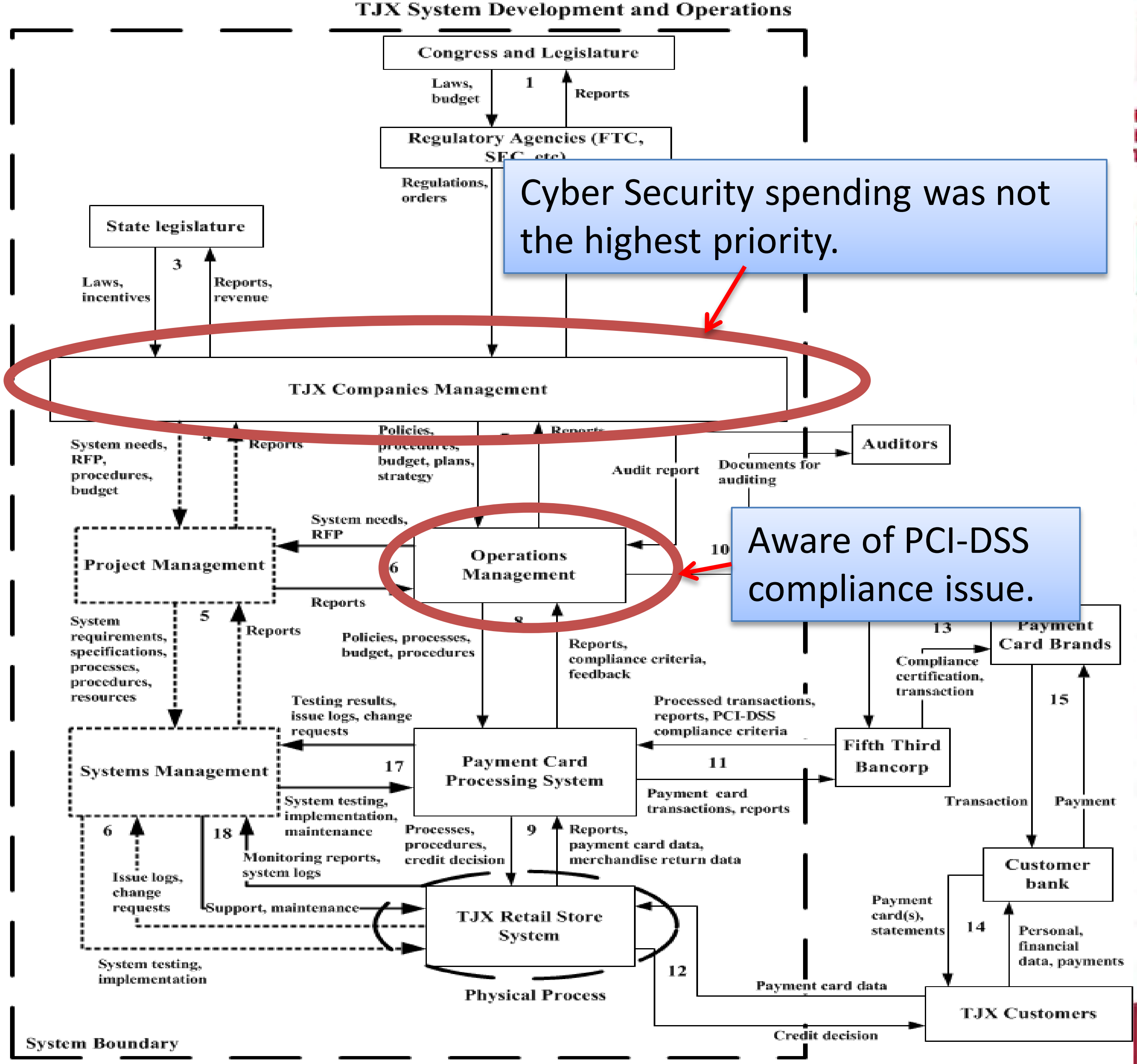


TJX System Development and Operations
Congress and Legislature
Laws, budget
1
Reports
Regulatory Agencies (FTC, SEC, etc)
Regulations, orders
2
Annual reports, SEC filings (10K)
State legislature
Laws, incentives
3
Reports, revenue
TJX Companies Management
System needs, RFP, procedures, budget
4
Reports
Policies, procedures, budget, plans, strategy
7
Reports
Audit report
Documents for auditing
Auditors
Project Management
System needs, RFP
Operations
10
PCI-DSS
System requirements, specifications, processes, procedures, resources
5
Reports
Policies, processes, budget, procedures
Reports, compliance criteria, feedback
13
Payment Card Brands
Compliance certification, transaction
Testing results, issue logs, change requests
Processed transactions, reports, PCI-DSS compliance criteria
15
Systems Management
17
Payment Card Processing System
11
Fifth Third Bancorp
System testing, implementation, maintenance
Payment card transactions, reports
Transaction
Payment
6
18
Processes, procedures, credit decision
9
Reports, payment card data, merchandise return data
Issue logs, change requests
Monitoring reports, system logs
Customer bank
Support, maintenance
TJX Retail Store System
Payment card(s), statements
14
Personal, financial data, payments
System testing, implementation
12
Physical Process
Payment card data
TJX Customers
Credit decision
System Boundary

Lack of coordination for PCI-DSS Compliance

Legend:
- Each **number** indicates a unique loop.
- Bold-dashed **square** indicates TJX system boundary.
- Bold-dashed **oval** indicates the physical system.
- **Downward arrow** represents reference channel for imposing safety constraints.
- **Upward arrow** represents feedback channel and reports the effectiveness of constraints.

Step 7: Coordination and Communication


TJX System Development and Operations
Congress and Legislature
Laws, budget
1
Reports
Regulatory Agencies (FTC, SEC, etc)
Regulations, orders
State legislature
3
Laws, incentives
Reports, revenue
TJX Companies Management
System needs, RFP, procedures, budget
4
Reports
Policies, procedures, budget, plans, strategy
7
Reports
Auditors
Audit report
Documents for auditing
System needs, RFP
Project Management
6
Operations Management
Reports
10
5
Reports
System requirements, specifications, processes, procedures, resources
Policies, processes, budget, procedures
8
Reports, compliance criteria, feedback
13
Payment Card Brands
Compliance certification, transaction
15
Testing results, issue logs, change requests
Processed transactions, reports, PCI-DSS compliance criteria
Fifth Third Bancorp
Systems Management
17
Payment Card Processing System
11
System testing, implementation, maintenance
Payment card transactions, reports
Transaction
Payment
6
18
Processes, procedures, credit decision
9
Reports, payment card data, merchandise return data
Monitoring reports, system logs
Issue logs, change requests
Support, maintenance
TJX Retail Store System
Customer bank
Payment card(s), statements
14
Personal, financial data, payments
System testing, implementation
12
Payment card data
Physical Process
TJX Customers
Credit decision
System Boundary

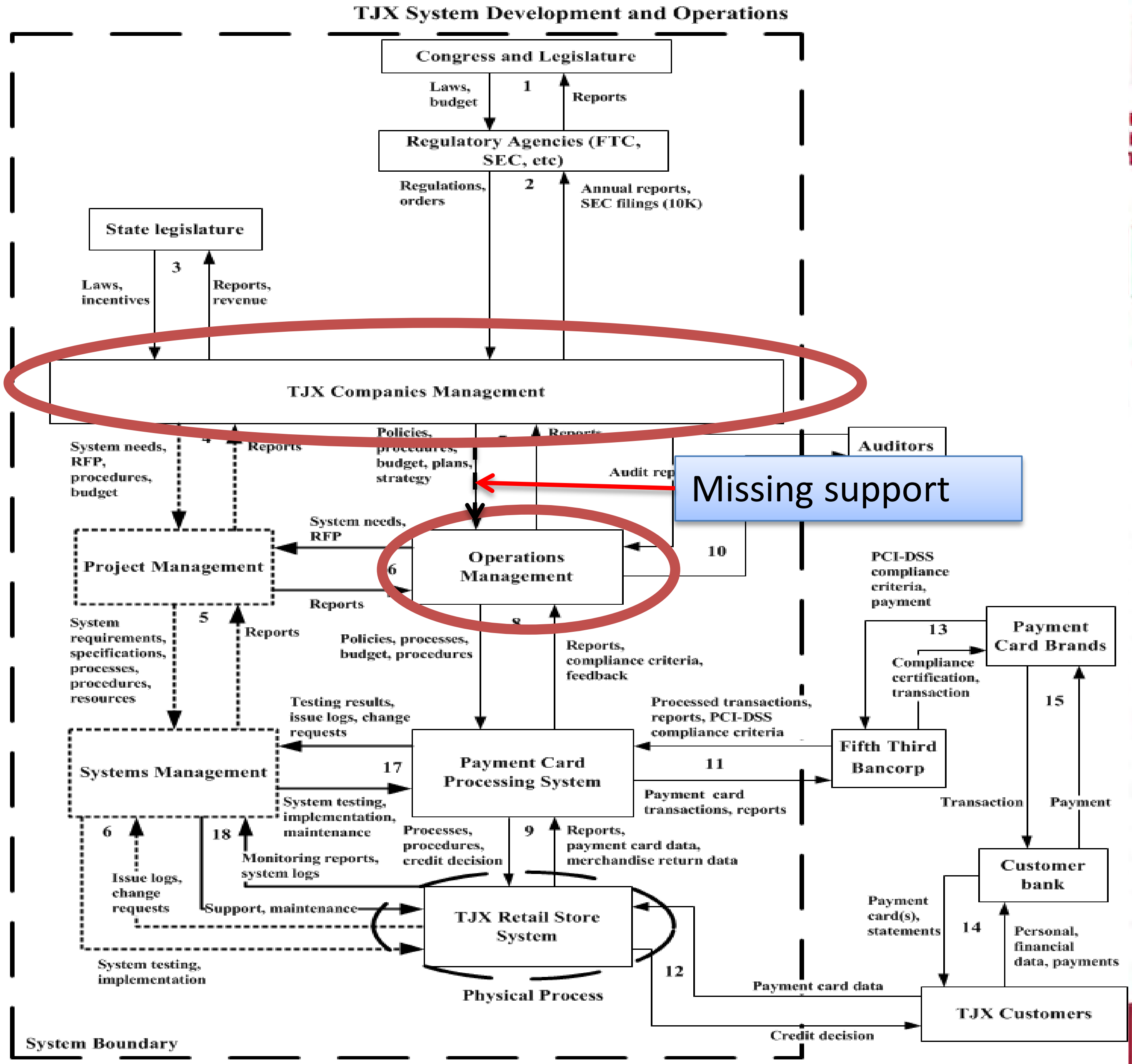
Cyber Security spending was not the highest priority.

Aware of PCI-DSS compliance issue.

Legend:

- Each **number** indicates a unique loop.
- Bold-dashed **square** indicates TJX system boundary.
- Bold-dashed **oval** indicates the physical system.
- **Downward arrow** represents reference channel for imposing safety constraints.
- **Upward arrow** represents feedback channel and reports the effectiveness of constraints.

Step 7: Coordination and Communication


TJX System Development and Operations

Congress and Legislature

Laws, budget

1

Reports

Regulatory Agencies (FTC, SEC, etc)

Regulations, orders

2

Annual reports, SEC filings (10K)

State legislature

Laws, incentives

3

Reports, revenue

TJX Companies Management

System needs, RFP, procedures, budget

4

Reports

Policies, procedures, budget, plans, strategy

Reports

Auditors

Audit rep

Missing support

Project Management

System needs, RFP

6

Operations Management

Reports

10

PCI-DSS compliance criteria, payment

System requirements, specifications, processes, procedures, resources

5

Reports

Policies, processes, budget, procedures

8

Reports, compliance criteria, feedback

Payment Card Brands

13

Compliance certification, transaction

15

Testing results, issue logs, change requests

Processed transactions, reports, PCI-DSS compliance criteria

Systems Management

17

Payment Card Processing System

11

Fifth Third Bancorp

System testing, implementation, maintenance

Payment card transactions, reports

Transaction

Payment

6

18

Processes, procedures, credit decision

9

Reports, payment card data, merchandise return data

Customer bank

Issue logs, change requests

Monitoring reports, system logs

Support, maintenance

TJX Retail Store System

Payment card(s), statements

14

Personal, financial data, payments

System testing, implementation

12

Physical Process

Payment card data

TJX Customers

Credit decision

System Boundary

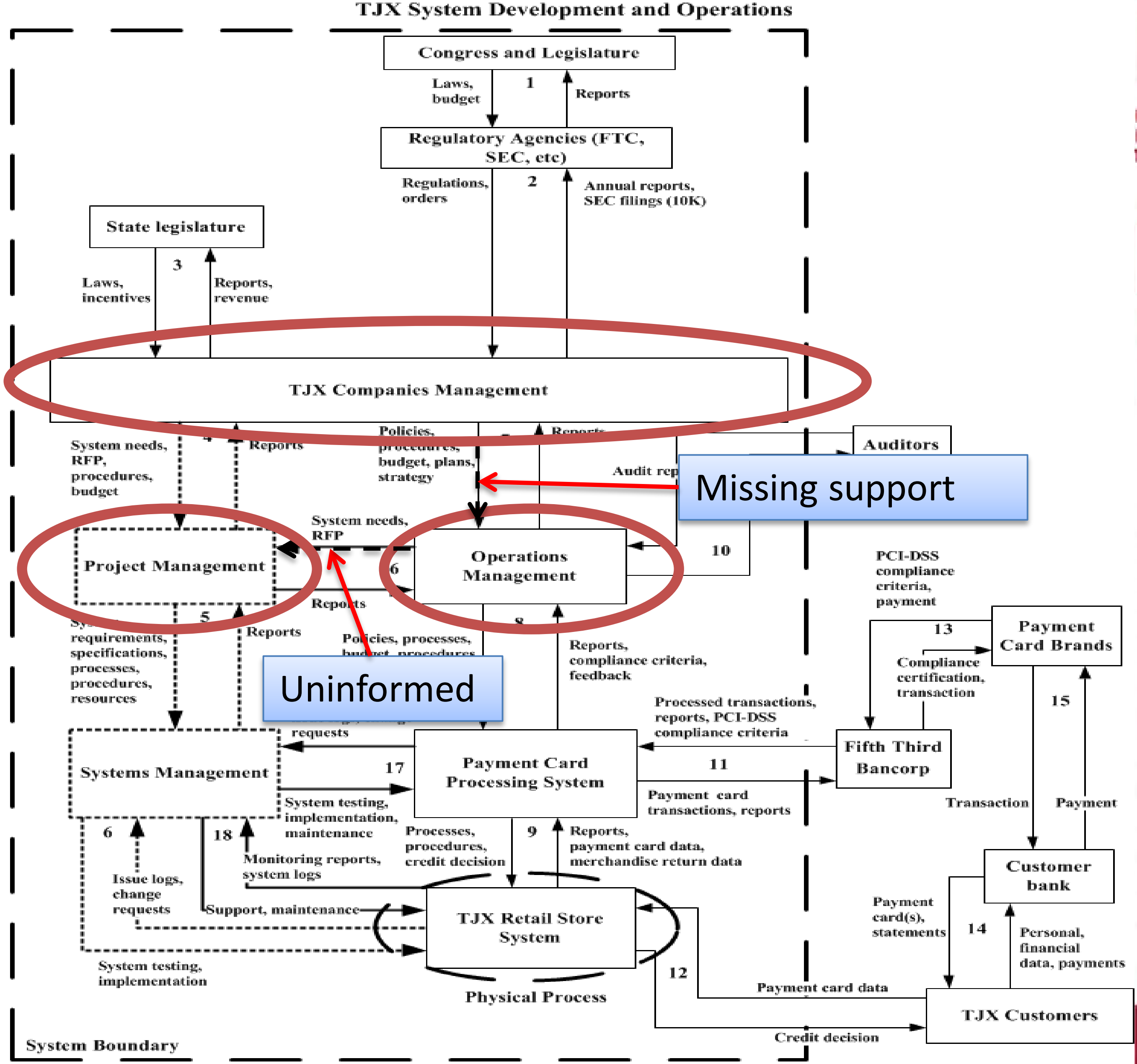
Legend:
- Each **number** indicates a unique loop.
- Bold-dashed **square** indicates TJX system boundary.
- Bold-dashed **oval** indicates the physical system.
- **Downward arrow** represents reference channel for imposing safety constraints.
- **Upward arrow** represents feedback channel and reports the effectiveness of constraints.

Massachusetts Institute of Technology

(IC)³ for INTERDISCIPLINARY CONSORTIUM IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY

MITSloan MANAGEMENT

Step 7: Coordination and Communication


TJX System Development and Operations
Congress and Legislature
Laws, budget
1
Reports
Regulatory Agencies (FTC, SEC, etc)
Regulations, orders
2
Annual reports, SEC filings (10K)
State legislature
3
Laws, incentives
Reports, revenue
TJX Companies Management
System needs, RFP, procedures, budget
4
Reports
Policies, procedures, budget, plans, strategy
7
Reports
Audit rep
Auditors
Project Management
System needs, RFP
6
Operations Management
Reports
10
5
System requirements, specifications, processes, procedures, resources
Reports
Policies, processes, budget, procedures
8
Reports, compliance criteria, feedback
requests
PCI-DSS compliance criteria, payment
Payment Card Brands
13
Compliance certification, transaction
15
Processed transactions, reports, PCI-DSS compliance criteria
Fifth Third Bancorp
Systems Management
17
Payment Card Processing System
11
Payment card transactions, reports
Transaction
Payment
System testing, implementation, maintenance
6
18
Processes, procedures, credit decision
9
Reports, payment card data, merchandise return data
Customer bank
Monitoring reports, system logs
Issue logs, change requests
Support, maintenance
TJX Retail Store System
Payment card(s), statements
14
Personal, financial data, payments
System testing, implementation
12
Physical Process
Payment card data
TJX Customers
Credit decision
System Boundary

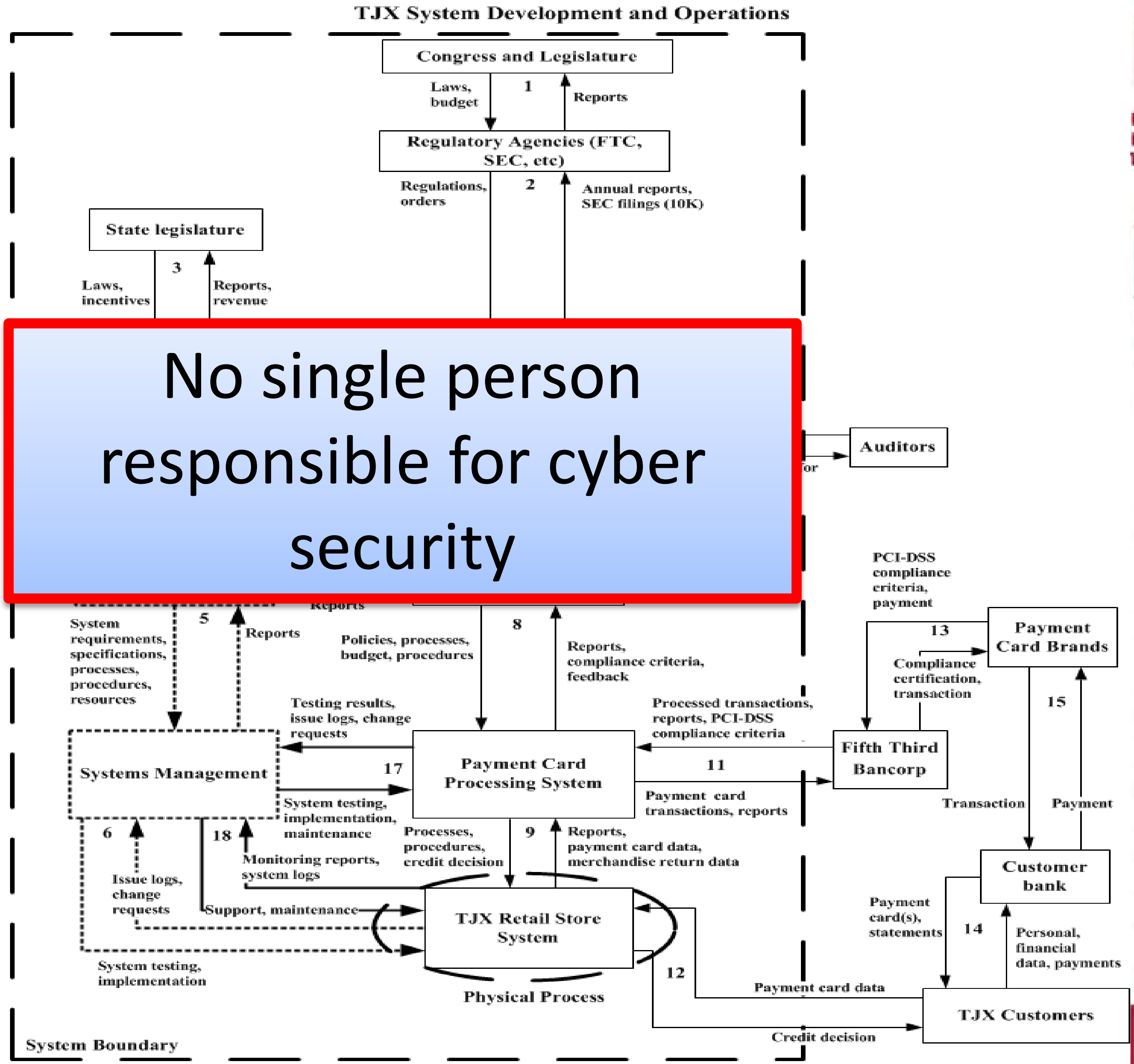
Missing support

Uninformed

Legend:

- Each **number** indicates a unique loop.
- Bold-dashed **square** indicates TJX system boundary.
- Bold-dashed **oval** indicates the physical system.
- **Downward arrow** represents reference channel for imposing safety constraints.
- **Upward arrow** represents feedback channel and reports the effectiveness of constraints.

Step 7: Coordination and Communication


TJX System Development and Operations
Congress and Legislature
Laws, budget
1
Reports
Regulatory Agencies (FTC, SEC, etc)
Regulations, orders
2
Annual reports, SEC filings (10K)
State legislature
Laws, incentives
3
Reports, revenue
Auditors
for
PCI-DSS compliance criteria, payment
Reports
System requirements, specifications, processes, procedures, resources
5
Reports
Policies, processes, budget, procedures
8
Reports, compliance criteria, feedback
13
Payment Card Brands
Compliance certification, transaction
Processed transactions, reports, PCI-DSS compliance criteria
15
Testing results, issue logs, change requests
Systems Management
17
Payment Card Processing System
11
Fifth Third Bancorp
Payment card transactions, reports
Transaction
Payment
System testing, implementation, maintenance
6
18
Processes, procedures, credit decision
9
Reports, payment card data, merchandise return data
Customer bank
Monitoring reports, system logs
Issue logs, change requests
Support, maintenance
TJX Retail Store System
Payment card(s), statements
14
Personal, financial data, payments
System testing, implementation
12
Payment card data
Physical Process
TJX Customers
Credit decision
System Boundary

No single person responsible for cyber security

Legend:

- Each **number** indicates a unique loop.
- Bold-dashed **square** indicates TJX system boundary.
- Bold-dashed **oval** indicates the physical system.
- **Downward arrow** represents reference channel for imposing safety constraints.
- **Upward arrow** represents feedback channel and reports the effectiveness of constraints.

Massachusetts Institute of Technology

(IC)³ for INTERDISCIPLINARY CONSORTIUM IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY

MITSloan MANAGEMENT

Dynamic Migration to High Risk State

1	System and hazard definition
2	System level safety/security requirements
3	Draw control structure
4	Proximate events
5	Analyze the physical system
6	Moving up the levels of the control structure
7	Coordination and communication
8	Dynamics and change over time
9	Generate recommendations.

CAST Step 8: Dynamics and Migration to a High-Risk State

- Initially cyber security risk was low because vulnerabilities were unknown to everyone – experts, businesses, and hackers.
- Flaws in managerial decision making process.
  - Information availability: recent experiences strongly influence the decision (i.e., no break-ins so far.)

CAST Step 8: Dynamics and Migration to a High-Risk State (Cont.)

"My understanding is that we can be PCI-compliant without the planned FY07 upgrade to WPA technology for encryption because most of our stores do not have WPA capability without some changes. WPA is clearly best practice and may ultimately become a requirement for PCI compliance sometime in the future. ***I think we have an opportunity to defer some spending from FY07's budget by removing the money for the WPA upgrade, but would want us all to agree that the risks are small or negligible." – TJX CIO, Nov. 2005***

- Above is a message from CIO in November 2005 to his staff, requesting agreement on his belief that cyber security risk is low.
- There were only two opposing views, a majority of his staff agreed.
- **This confirmation trap led to postponing upgrades.**

Comparison of Results from FTC and CPC Investigations and STAMP/CAST Analysis

No.	Recommendation	CPC	FTC	STAMP /CAST
1	Create an executive level role for managing cyber security risks.	No	*	Yes
2	PCI-DSS integration with TJX processes.	No	No	Yes
3	Develop a safety culture.	No	No	Yes
4	Understand limitations of PCI-DSS and standards in general.	No	No	Yes
5	Review system architecture.	No	No	Yes
6	Upgrade encryption technology.	Yes	No	Yes
7	Implement vigorous monitoring of systems.	Yes	No	Yes
8	Implement information security program.	No	Yes	Yes

CPC = Canadian Privacy Commission

FTC = Federal Trade Commission

* = Indicates recommendations that are close to STAMP/CAST based analysis but also has differences.

Research Contributions

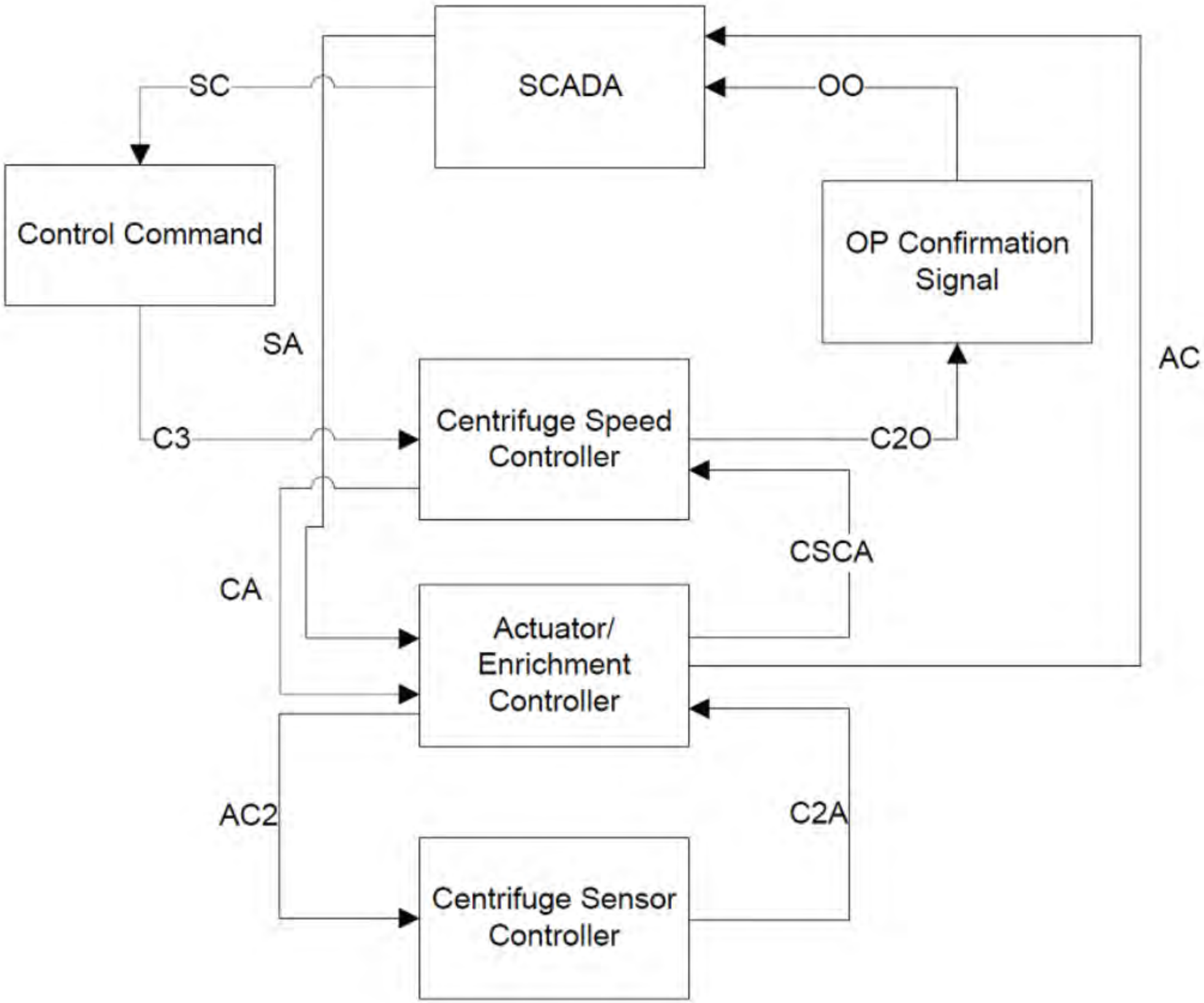
1. Highlighted need for systematic thinking and systems engineering approach to cyber security.
2. Tested STAMP/CAST as a new approach for managing cyber security risks.
3. Discovered new insights when applying STAMP/CAST to the TJX case.
4. Recommendations provide a basis for preventing similar events in the future.
5. The US Air Force has successfully implemented, and is implementing STPA as a cyber security measure
6. STAMP/CAST/STPA is compatible with the NIST Cybersecurity Framework, UK Cyber Essentials, IEC-62443 and other Cybersecurity standards

Massachusetts Institute of Technology

(IC)^3 for INTERDISCIPLINARY CONSORTIUM IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY

MITSloan MANAGEMENT

Application to Cyber Physical System (Stuxnet Example)


SCADA
SC
OO
Control Command
OP Confirmation Signal
SA
AC
C3
Centrifuge Speed Controller
C2O
CSCA
CA
Actuator/ Enrichment Controller
AC2
C2A
Centrifuge Sensor Controller

Massachusetts Institute of Technology

(IC)³ for Interdisciplinary Consortium Improving Critical Infrastructure Cybersecurity

MITSloan Management

Future Research Directions

- Continue applying CAST for Cyber Security attack analysis and generate comprehensive list of recommendations that include:
    - Improvements to mitigate technology vulnerabilities
    - Ways to address systemic issues related to management, decision making, culture, policy and regulation.
- Apply the System Theoretic Process Analysis (STPA) approach to identify system vulnerability prior to an attack.
    - – (IC)^3 has started a project to ensure the cyber security of complex power grids, working with major grid operators in the US, Dubai, and Singapore.

MIT Interdisciplinary Consortium for Improving Critical Infrastructure Cybersecurity – (IC)^3

Questions?

Michael Coden, CISSP, Associate Director MIT-(IC)^3
mcoden@mit.edu
http://ic3.mit.edu

Presented at the International Conference on Computer Security in a Nuclear World: Expert Discussion and Exchange, International Atomic Energy Agency, June 2, 2015, Vienna, Austria