SMART WATER SUMMIT

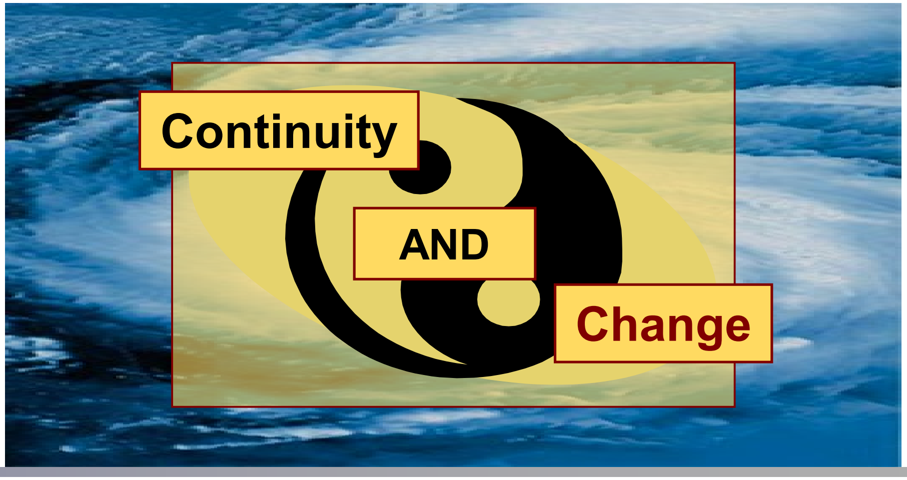
Continuity & Change:

Assuring Proactive Security Among Automation & Digitization

S. Massoud Amin, D.Sc.

Professor of Electrical & Computer Engineering
University Distinguished Teaching Professor
University of Minnesota

Fellow, IEEE and ASME



Keynote address at the Smart Water Summit (SWS), Scottsdale, AZ

25 August2019

Context – June 27, 2019

- **Post Ukraine: "Senate passes cybersecurity bill to decrease grid digitization, move toward manual control…":**
- The U.S. Senate on June 27, 2019 passed a bipartisan cybersecurity bill that will study ways to replace automated systems with low-tech redundancies to protect the country's electric grid from hackers.
- The Securing Energy Infrastructure Act (SEIA) establishes a two-year pilot program to identify new classes of security vulnerabilities and to research and test solutions, including "analog and nondigital control systems." The U.S. Department of Energy would be required to report back to Congress on its findings.
- The SEIA legislation was included in the National Defense Authorization Act for Fiscal Year 2020. A companion bill has been introduced by bipartisan sponsors in the House of Representatives.

SWS
SMART WATER SUMMIT

Source: https://www.utilitydive.com/news/senate-passes-cybersecurity-bill-to-decrease-grid-digitization-move-toward/557959/

Key Industry/Societal Trends

- Transitioning from Devices/Systems to Holistic Solutions
- Success = Technology, Standards, Policy, Culture, Mission
- Electrical Power, Energy & Water, Distribution Infrastructures' Resiliency
- Big Data, Analytics, AI/ML. Use of Social Media
- IoT … Smart Cities, Smart Homes, Smart Buildings, Smart Water…
- Convergence of IT and OT to Support Enterprise Data Management

» *Slow and Steady Energy Transition in the U.S., BUT→*

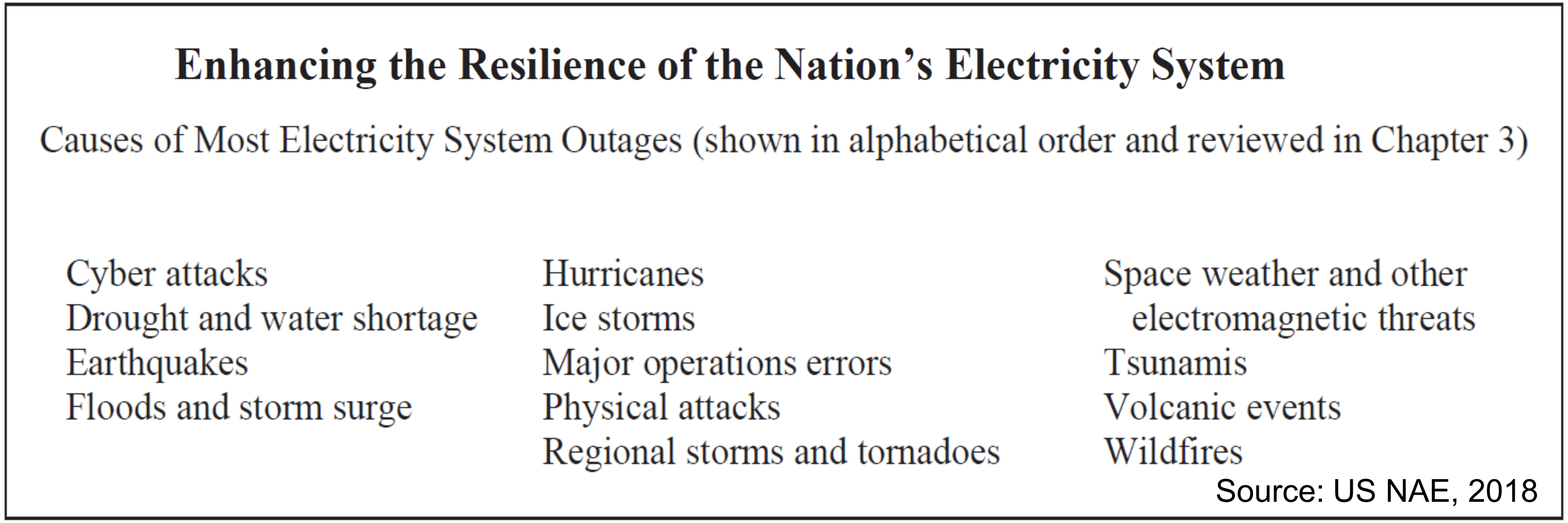
Cyber-Physical Systems

- Security (Cyber-physical, IT, OT and CI), and Security Methods/Approaches
- Resilience: Resiliency and assessments – destabilizers and countermeasures

Why Systems Fail?

- Natural hazards
- Malevolent acts
- Wearout and breakdown

- Human error
- Close-coupling of system elements
- Focus on a single outcome



Enhancing the Resilience of the Nation's Electricity System

Causes of Most Electricity System Outages (shown in alphabetical order and reviewed in Chapter 3)

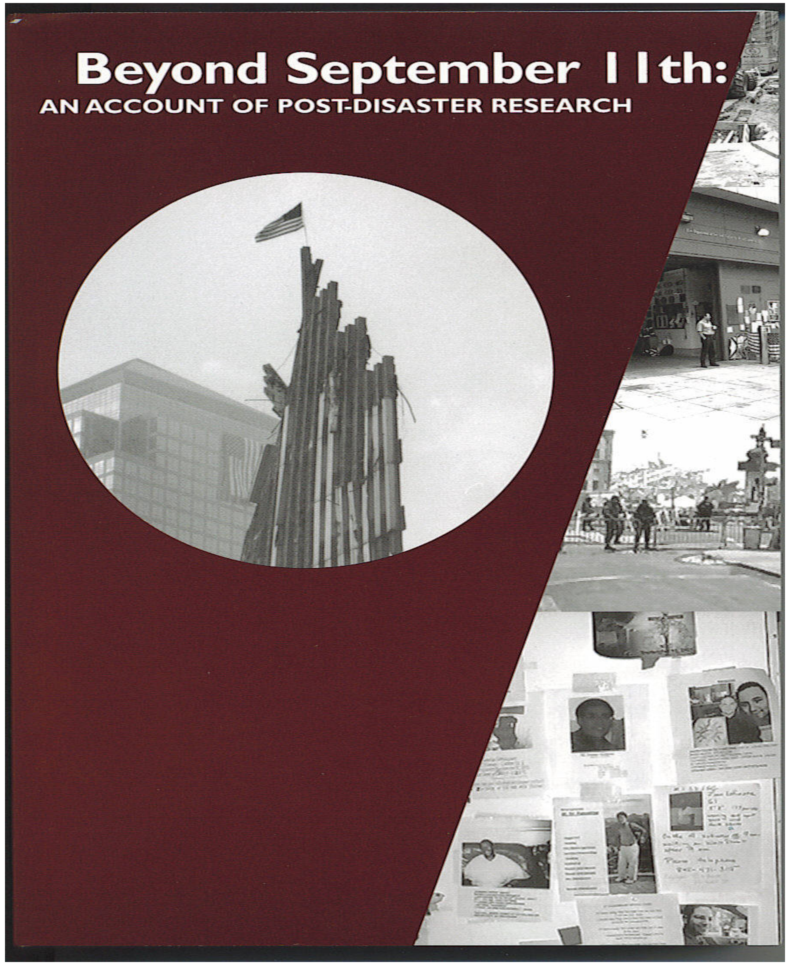
Cyber attacks
Drought and water shortage
Earthquakes
Floods and storm surge

Hurricanes
Ice storms
Major operations errors
Physical attacks
Regional storms and tornadoes

Space weather and other electromagnetic threats
Tsunamis
Volcanic events
Wildfires

Source: US NAE, 2018

Critical Features of Survivable Systems: Lessons from September 11



- ⌘ **resilience:** **ability to recover quickly**
- ⌘ **robustness:** **failure-resistant through design and/or construction**
- ⌘ **redundancy:** **duplicative capacity for service delivery**

Verizon, AT&T, ConEd, and MTA (among others) possessed all these attributes in equipment and people

Natural Hazards Research and Applications Information Center,
University of Colorado, Boulder, 2003

Resilience:

Precursor Detection for Situational Awareness and Proactive Actionable Intelligence

Fast modeling, and high-confidence look-ahead simulation, and validation of Complex Dynamical Systems

Critical System Dynamics and Resilience Capabilities

(January 1998- Present)

- Anticipation of disruptive events
- Look-ahead simulation capability
- Fast isolation and sectionalization
- Adaptive islanding
- Self-healing and restoration

re·sil·ience, *noun,* 1824:
The capability of a strained body to recover its size and shape after deformation caused especially by compressive stress;
An ability to recover from or adjust easily to misfortune or change

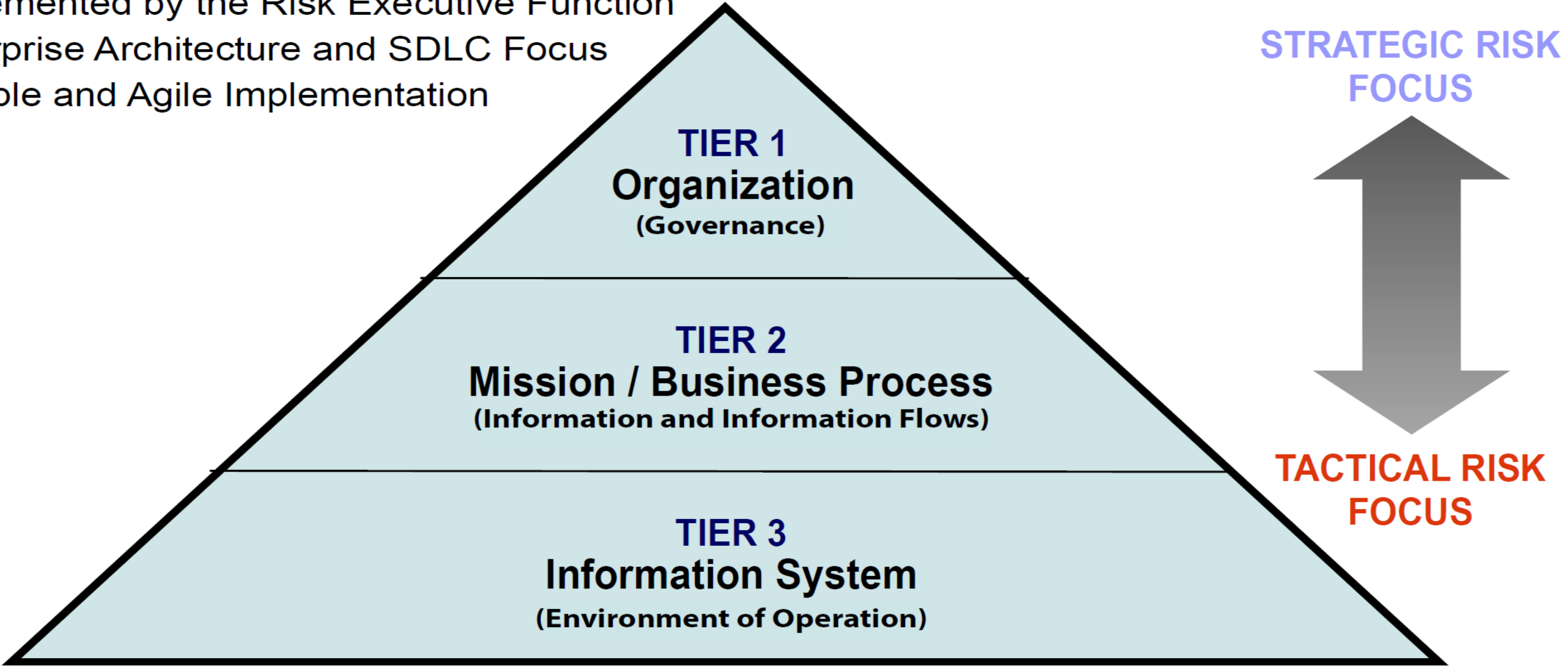
Resilience enables "Robustness": A system, organism or design may be said to be "robust" if it is capable of coping well with variations (internal or external and sometimes unpredictable) in its operating environment with minimal damage, alteration or loss of functionality.

SWS
SMART WATER SUMMIT

NIST: Enterprise-Wide Risk Management

- Multi-tiered Risk Management Approach
- Implemented by the Risk Executive Function
- Enterprise Architecture and SDLC Focus
- Flexible and Agile Implementation

Figure 1



Enterprise risk management (conceptual model)
Source: ***National Institute of Standards and Technology (NIST)***

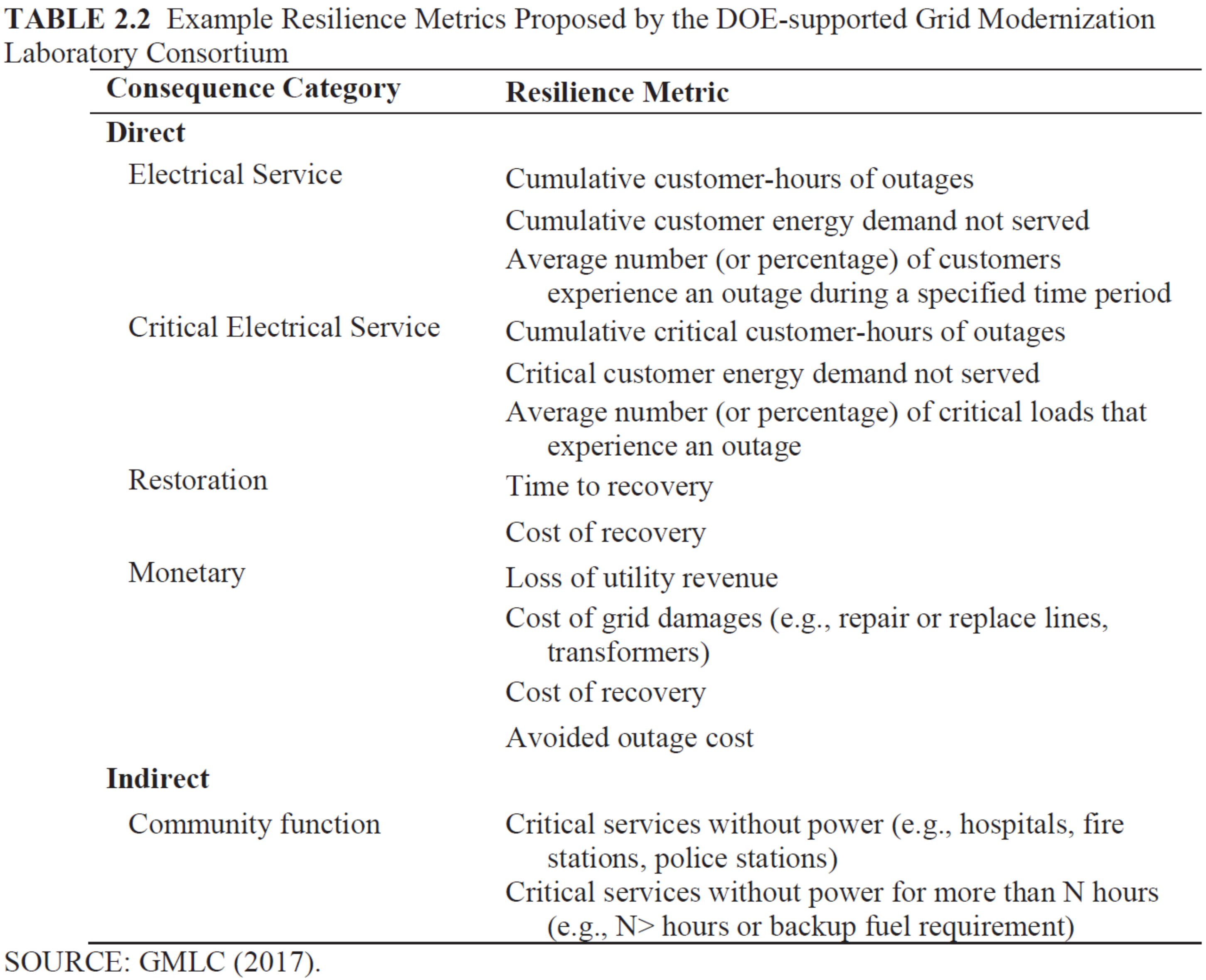


TABLE 2.2 Example Resilience Metrics Proposed by the DOE-supported Grid Modernization Laboratory Consortium

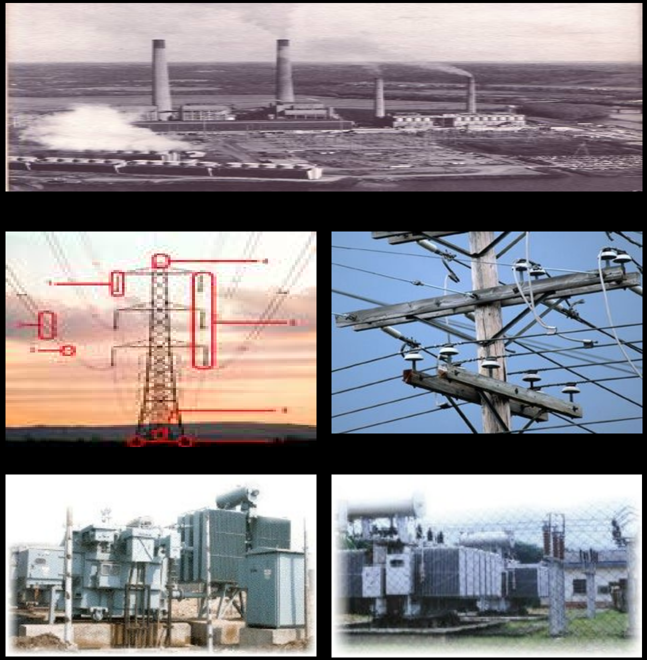
Consequence Category	Resilience Metric
Direct	
Electrical Service	Cumulative customer-hours of outages
	Cumulative customer energy demand not served
	Average number (or percentage) of customers experience an outage during a specified time period
Critical Electrical Service	Cumulative critical customer-hours of outages
	Critical customer energy demand not served
	Average number (or percentage) of critical loads that experience an outage
Restoration	Time to recovery
	Cost of recovery
Monetary	Loss of utility revenue
	Cost of grid damages (e.g., repair or replace lines, transformers)
	Cost of recovery
	Avoided outage cost
Indirect	
Community function	Critical services without power (e.g., hospitals, fire stations, police stations)
	Critical services without power for more than N hours (e.g., N> hours or backup fuel requirement)

SOURCE: GMLC (2017).

Interface of Smart Grid and Microgrids

- Fossil Fuel
- Long Distance Central Station
- An Aging Infrastructure
- Out of Capacity

- Renewable Power
- On-site
- Zero Energy Building
- Smart Grid



New Business Opportunities

- Turnkey Smart Buildings
- Web-enabled Energy Systems
- Residential DR
- Turnkey Perfect Power Retailing
- Turnkey AMI
- Commercial Perfect Power Retailing
- Enhanced Distribution Reliability Zones
- Entrepreneurial Microgrids

Utility Frustration

- “It’s all about the customer today and we know very little; and we have no regulatory incentive.”
- “Customer price transparency is the key with education and automation.”
- “Our infrastructure, policies and incentives are legacies of the 1930s.”

Cybersecurity

Changing Risks

Cyberspace

Cyber Activism

Cyber Insurance

Cyber War

Cyberattack

Cyber-Alert

Cyber Bullying

Cyber-ethics

Cyber crime

Cyber FININT

Cyberpower

Cybersecurity

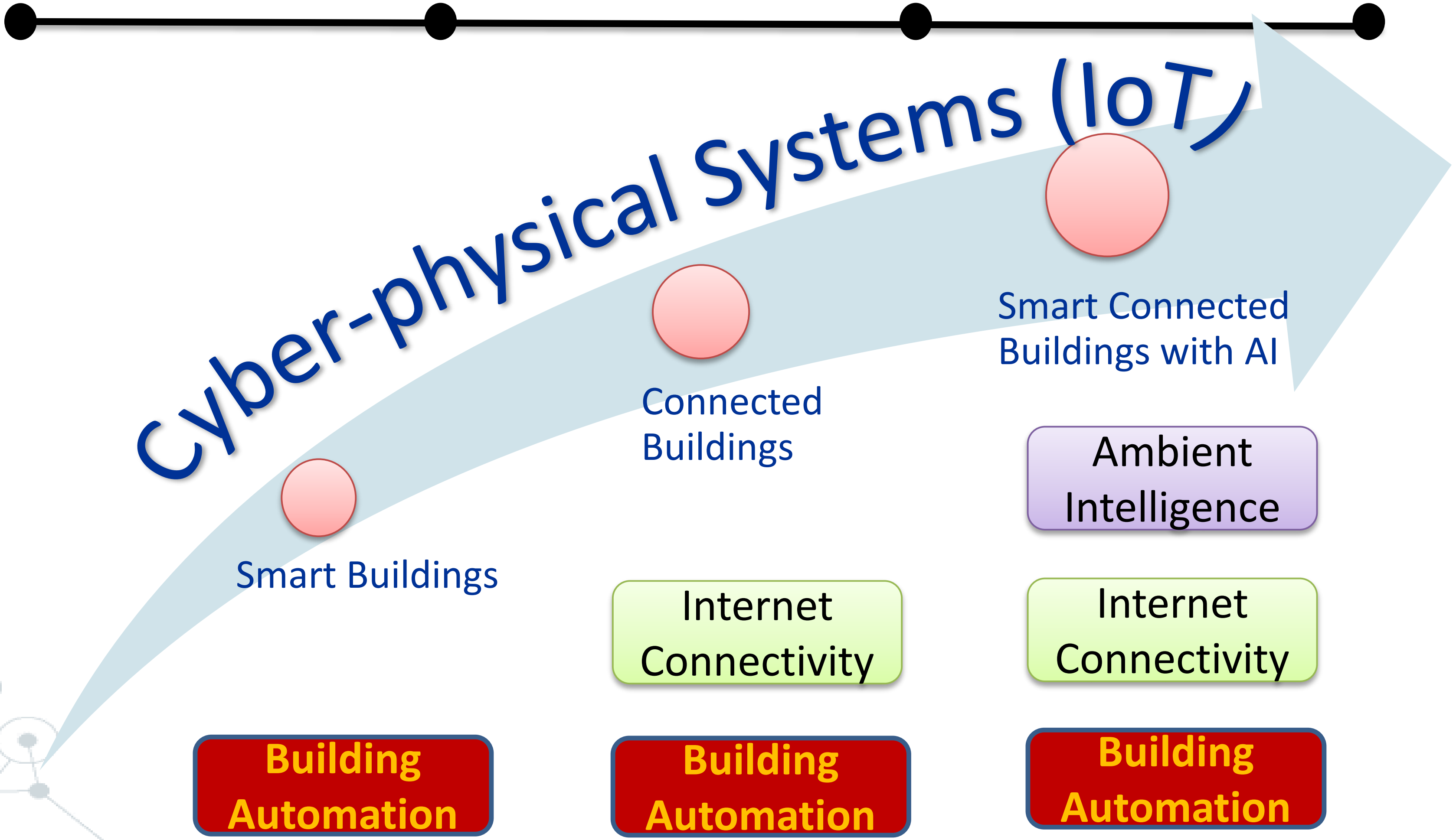
Cyber-Commerce

Cyber Espionage

Cyber Law

Cyber Communication

Example: Evolution of Building Technologies



Cyber-physical Systems (IoT)

Smart Buildings

Connected Buildings

Smart Connected Buildings with AI

Ambient Intelligence

Internet Connectivity

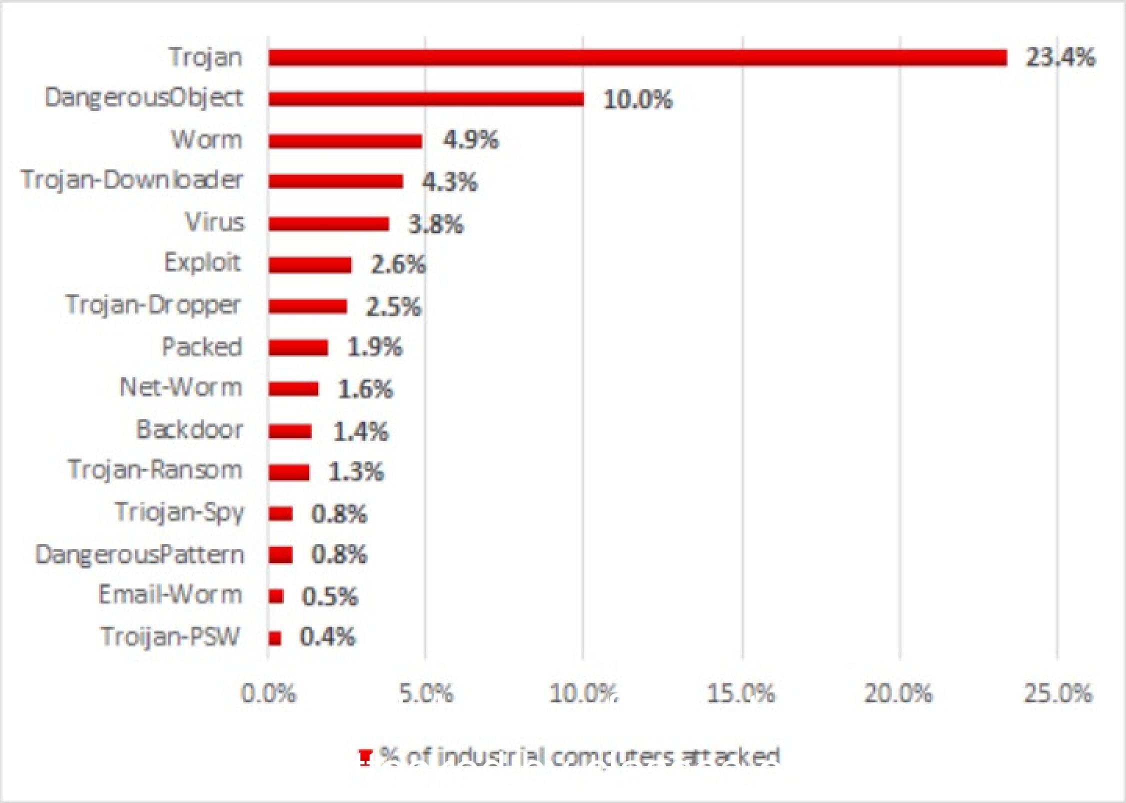
Internet Connectivity

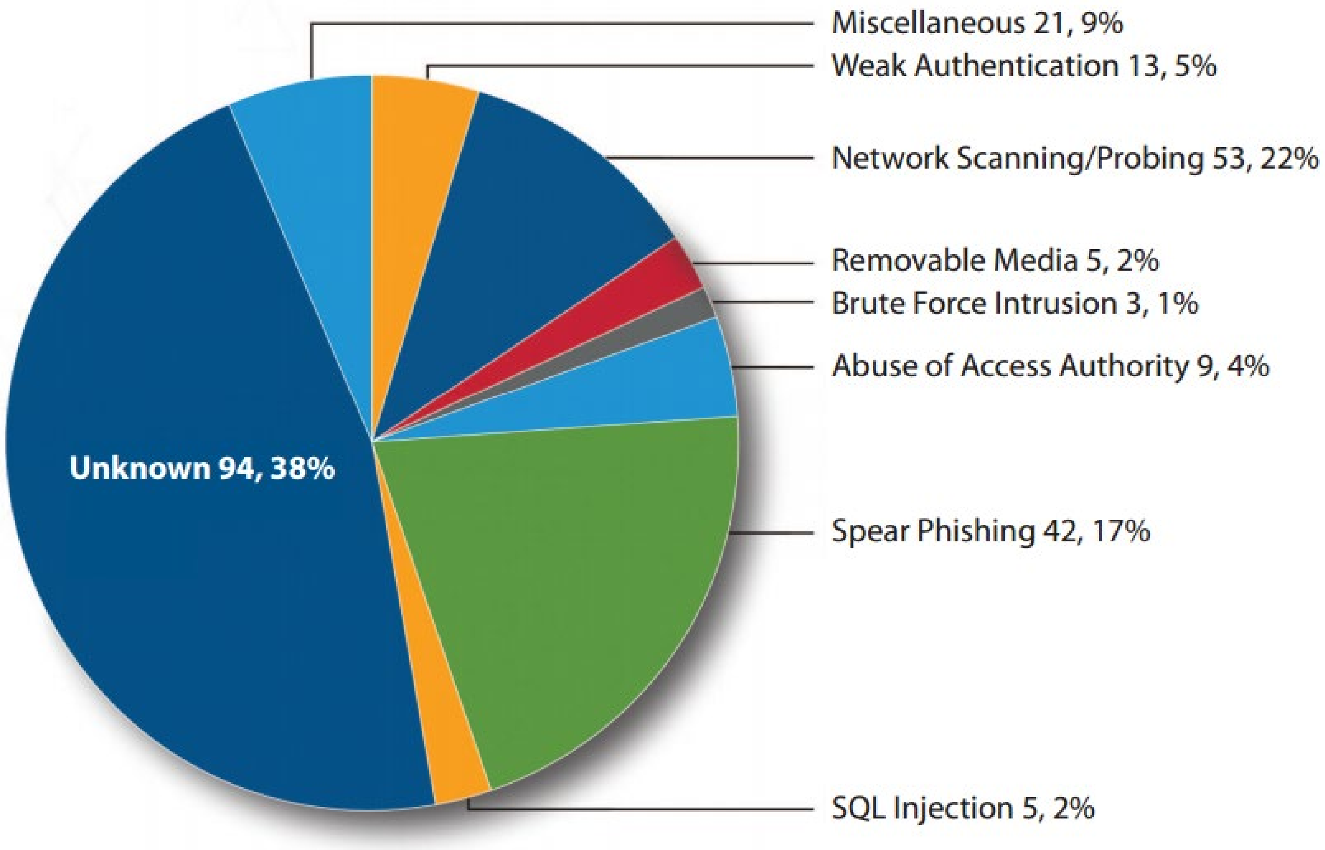
Building Automation

Building Automation

Building Automation

Threats and Risks





Network Topology

Common Protocols, Cloud, VPN, Process Automation, Power-System Automation

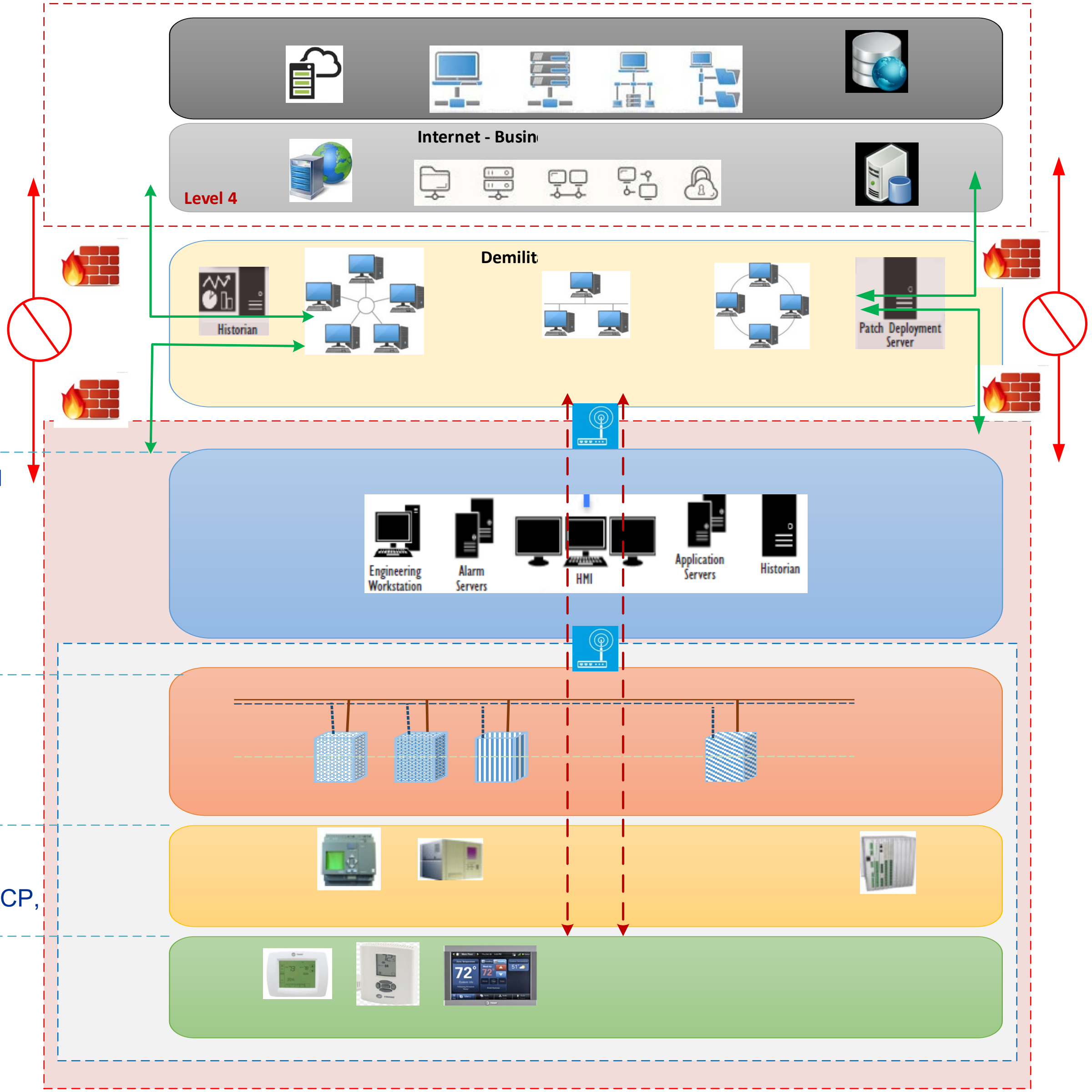
AS-i BSAP CC-Link Industrial Networks CIP CAN bus CANopen DeviceNet ControlNet DF-1 DirectNET EtherCAT Ethernet Global Data (EGD) Ethernet Powerlink EtherNet/IP Factory Instrumentation Protocol FINS FOUNDATION fieldbus H1 HSE GE SRTP HART Protocol Honeywell SDS HostLink INTERBUS MECHATROLINK MelsecNet Modbus Optomux PieP Profibus PROFINET IO RAPIEnet SERCOS interface SERCOS III Sinec H1 SynqNet TTEthernet

Common (IP, UDP) Protocols & Industrial Protocols, Industrial Control System, Process Automation, Power-System Automation

Common (IP, UDP) Protocols & Industrial Protocols , Industrial Control System

Industrial Protocols
(BACnet, BACnet MS/TP, BACnet/IP,
LON, Zigbee, Modbus RTU, Modbus/TCP,
DALI, Dynet, M-Bus, Profibus ...)

Fieldbus using Industrial Protocols
(IEBus, ANSI C12.18 IEC 61107
DLMS/IEC 62056 M-Bus Modbus,
ZigBee, M-Bus ...)



SMART WATER SUMMIT

Attack Scenario 1

(Air-gapped Network – IT/OT)

Attack Scenario 2

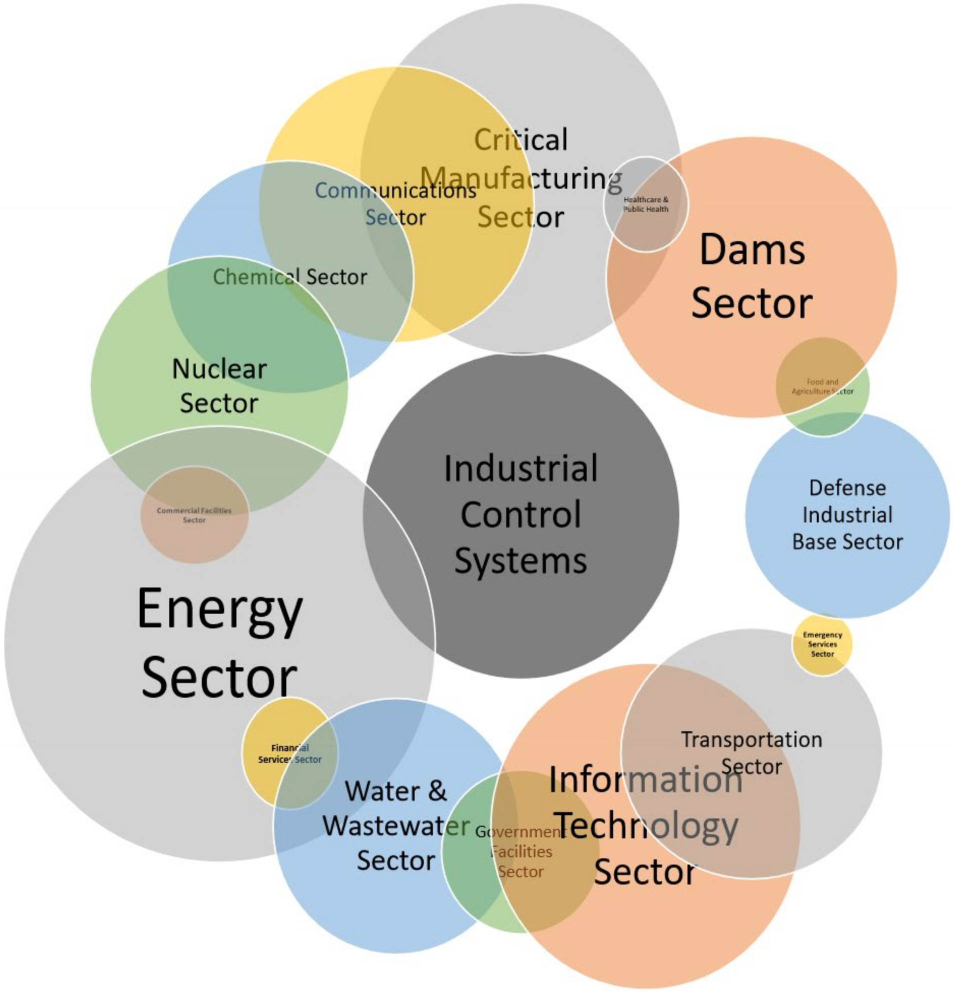
(All devices safe behind firewall)

Attack Scenario 3

(Well-planned distributed attacks)

Critical Infrastructure Interdependencies

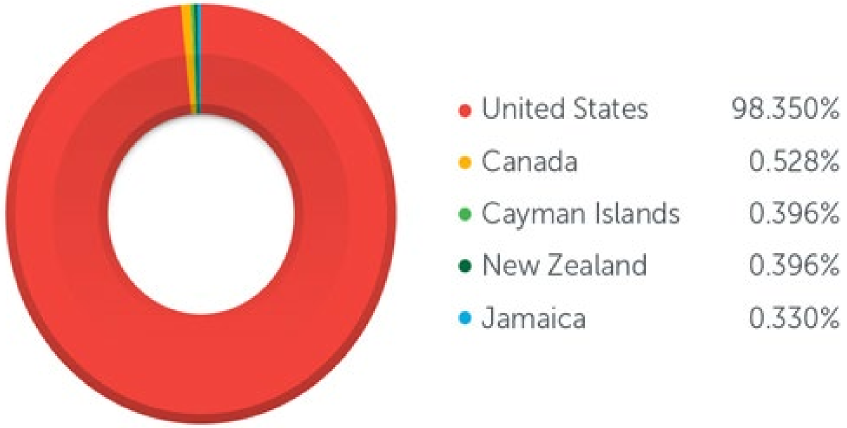
(Example: Risk/impact/loss due to cyberattack on ICS in the North American Power Grid)

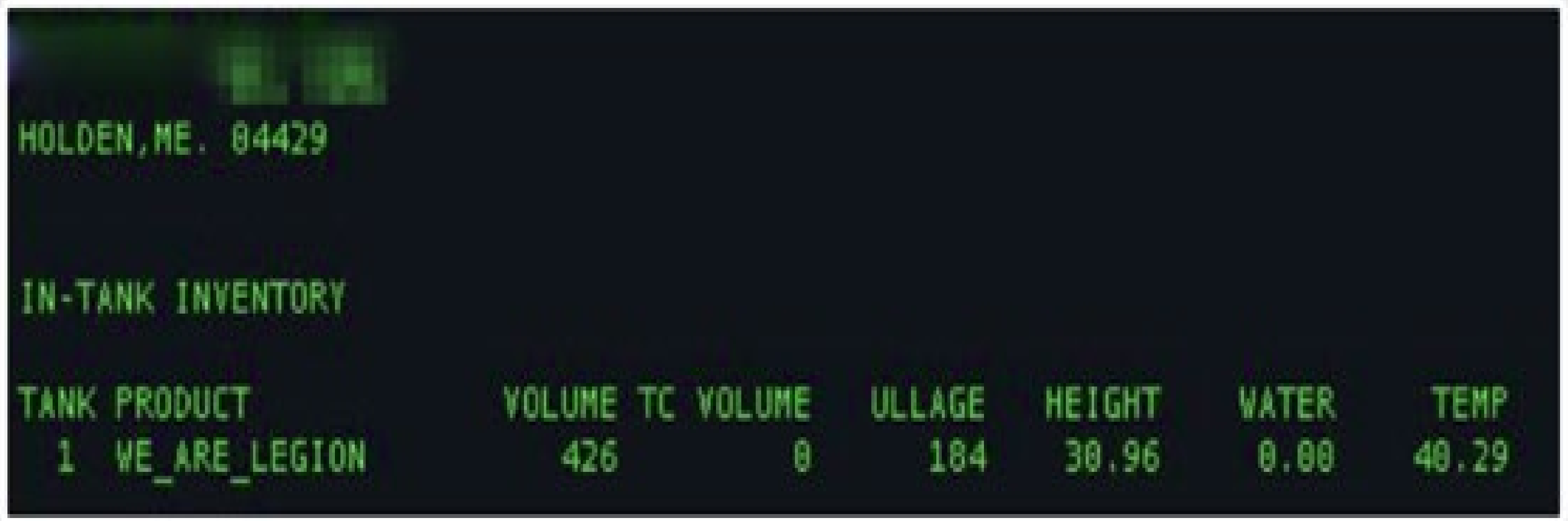

Critical Manufacturing Sector
Communications Sector
Healthcare & Public Health
Dams Sector
Chemical Sector
Nuclear Sector
Food and Agriculture Sector
Industrial Control Systems
Defense Industrial Base Sector
Commercial Facilities Sector
Energy Sector
Emergency Services Sector
Transportation Sector
Financial Services Sector
Water & Wastewater Sector
Government Facilities Sector
Information Technology Sector

Courtesy of: Prof. Massoud Amin, TLI

SMART WATER SUMMIT

GasPot 1





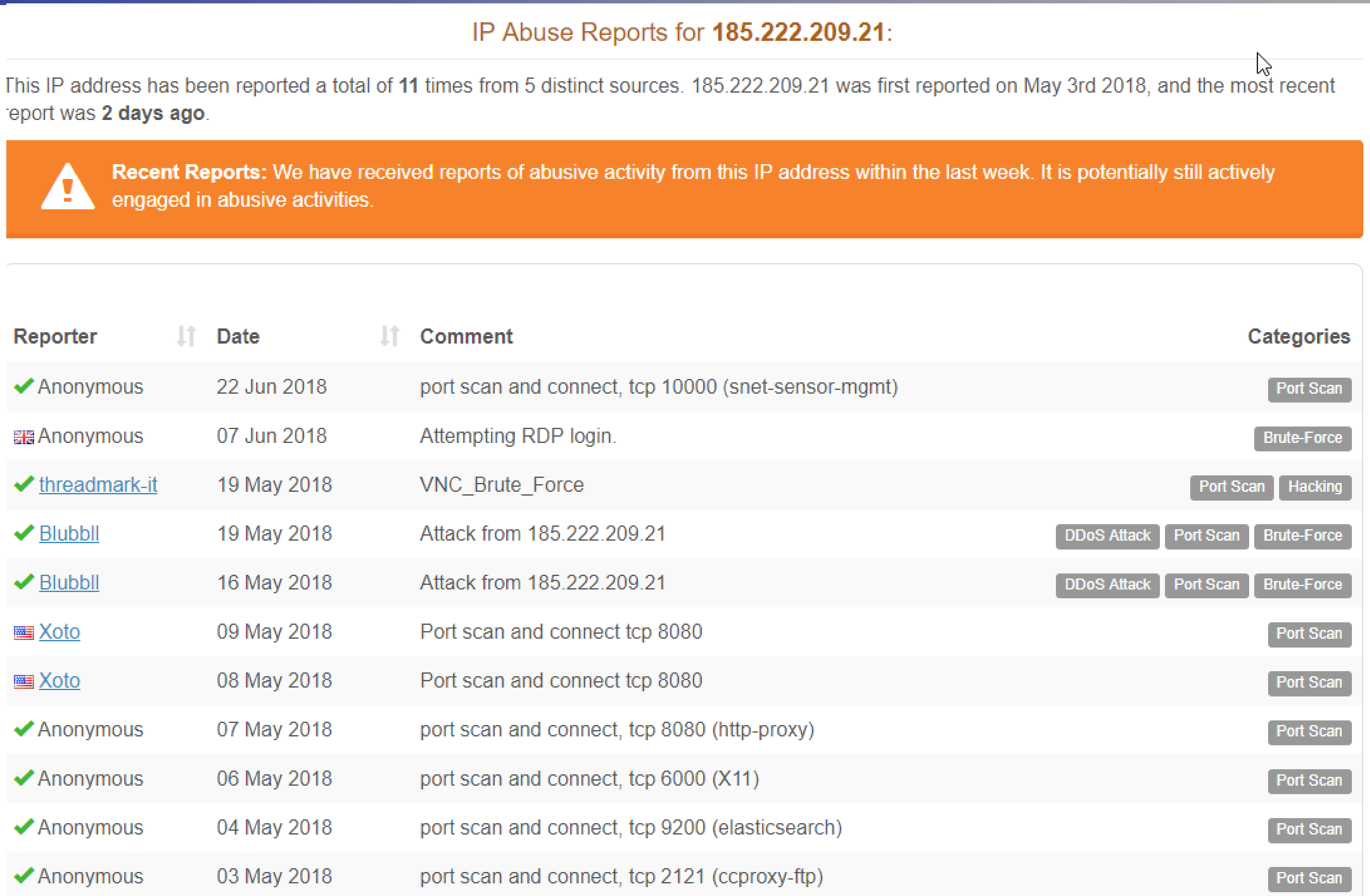
```
[redacted]
HOLDEN,ME. 04429


IN-TANK INVENTORY

TANK PRODUCT             VOLUME TC VOLUME   ULLAGE   HEIGHT    WATER     TEMP
  1  WE_ARE_LEGION         426          0      184    30.96     0.00    40.29
```

- ❑ UNLEADED
- ❑ DIESEL
- ❑ KEROSENE
- ❑ JET FUEL
- ❑ UNLEADED PREMIUM
- ❑ TOLUENE
- ❑ AV GAS
- ❑ #2 HEATING OIL
- ❑ WASTE OIL
- ❑ WATER
- ❑ PRODUCT
- ❑ GASOLINE

GasPot 2



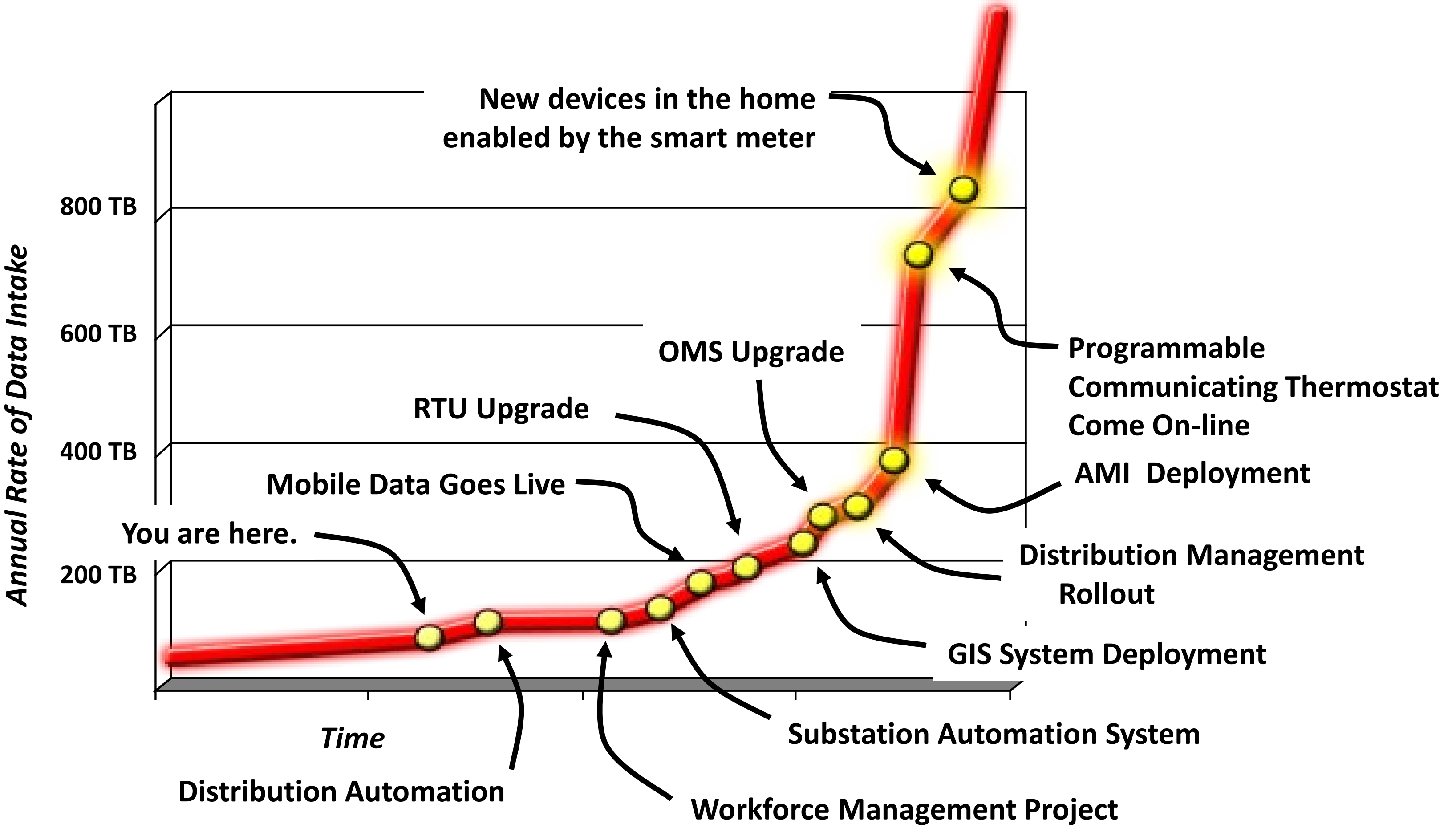
IP Abuse Reports for **185.222.209.21**:

This IP address has been reported a total of **11** times from 5 distinct sources. 185.222.209.21 was first reported on May 3rd 2018, and the most recent eport was **2 days ago**.

Recent Reports: We have received reports of abusive activity from this IP address within the last week. It is potentially still actively engaged in abusive activities.

Reporter	Date	Comment	Categories
✓ Anonymous	22 Jun 2018	port scan and connect, tcp 10000 (snet-sensor-mgmt)	Port Scan
Anonymous	07 Jun 2018	Attempting RDP login.	Brute-Force
✓ threadmark-it	19 May 2018	VNC_Brute_Force	Port Scan Hacking
✓ Blubbll	19 May 2018	Attack from 185.222.209.21	DDoS Attack Port Scan Brute-Force
✓ Blubbll	16 May 2018	Attack from 185.222.209.21	DDoS Attack Port Scan Brute-Force
Xoto	09 May 2018	Port scan and connect tcp 8080	Port Scan
Xoto	08 May 2018	Port scan and connect tcp 8080	Port Scan
✓ Anonymous	07 May 2018	port scan and connect, tcp 8080 (http-proxy)	Port Scan
✓ Anonymous	06 May 2018	port scan and connect, tcp 6000 (X11)	Port Scan
✓ Anonymous	04 May 2018	port scan and connect, tcp 9200 (elasticsearch)	Port Scan
✓ Anonymous	03 May 2018	port scan and connect, tcp 2121 (ccproxy-ftp)	Port Scan

Smart Grid: Tsunami of Data Developing

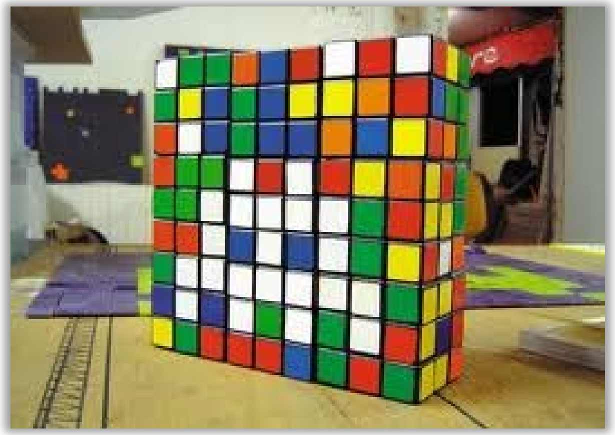


Tremendous amount of data coming from the field in the near future - paradigm shift for how utilities operate and maintain the grid

SWS SMART WATER SUMMIT

Paradigm Shift – Data at MN Valley Coop

- **Before smart meters**
  - Monthly read
  - 480,000 data points per year
- **After smart meters**
  - 15-60 minute kWh
  - Peak demand
  - Voltage
  - Power interruptions
  - 480,000,000 data points per year



SMART WATER SUMMIT

Industry Needs to Connect 50 Billion Devices by 2020

An unsolved problem costing billions per year in wasted resources requires radically improved wireless performance and lower cost

Battery Powered
1B Water Meters
1B Gas Meters

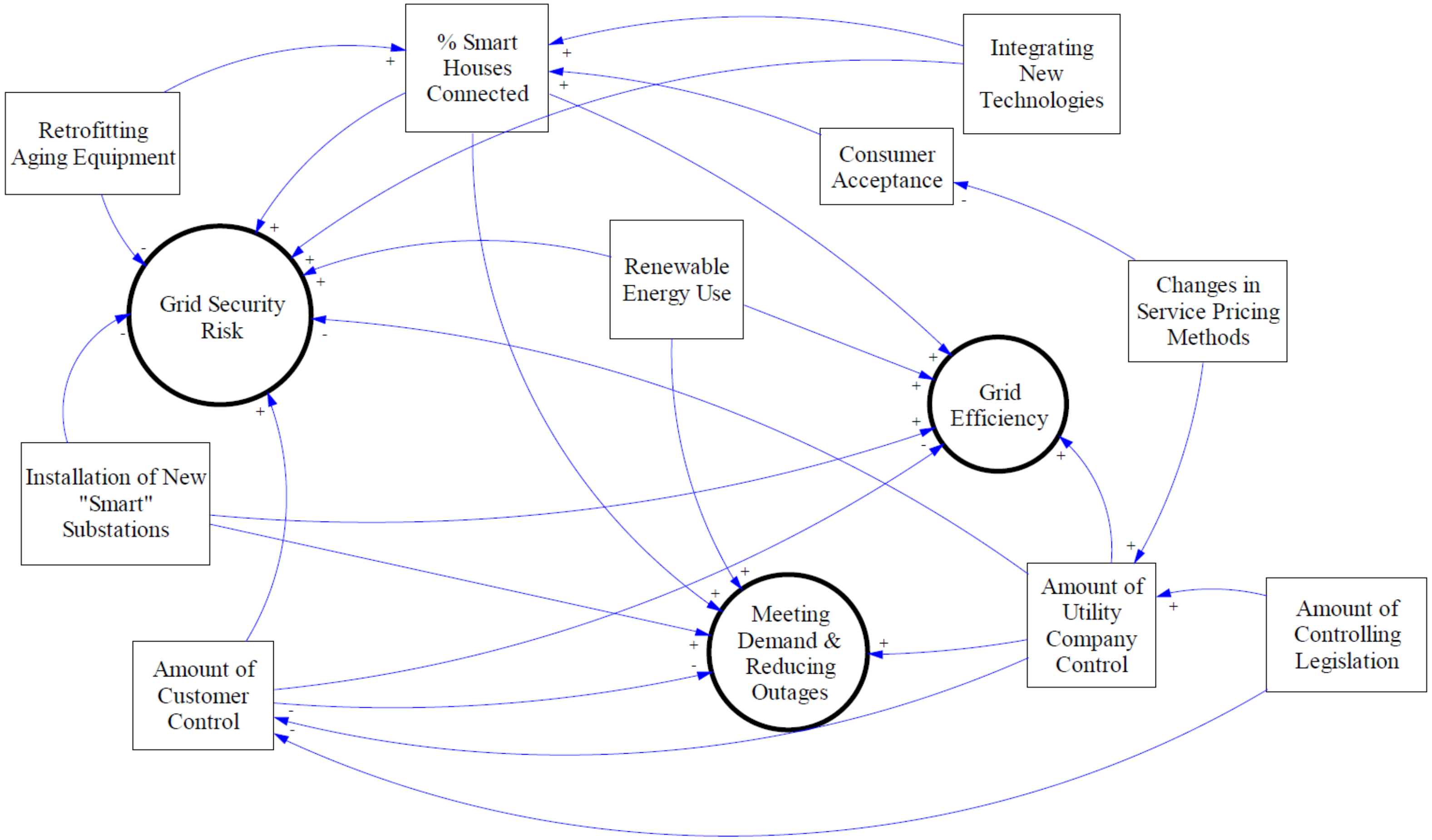
In Vaults
100M meters

Indoors
1B sensors

Underground
Millions of miles of Pipelines & Circuits

Smart Grid Interdependencies

Security, Efficiency, and Resilience


% Smart Houses Connected
Integrating New Technologies
Retrofitting Aging Equipment
Consumer Acceptance
Renewable Energy Use
Grid Security Risk
Changes in Service Pricing Methods
Grid Efficiency
Installation of New "Smart" Substations
Amount of Utility Company Control
Amount of Controlling Legislation
Meeting Demand & Reducing Outages
Amount of Customer Control

SMART WATER SUMMIT

… Thus There are Multiple Scenarios to Plan For…

	Inadvertent	*Deliberate*
External Threat	Power failures Natural disasters Economic upheaval	Malware Denial of service Sophisticated, organized attacks
Insider Threat	Unpatched systems Code vulnerability Lack of change control Human error or carelessness	Developer-created back door Information theft Insider fraud

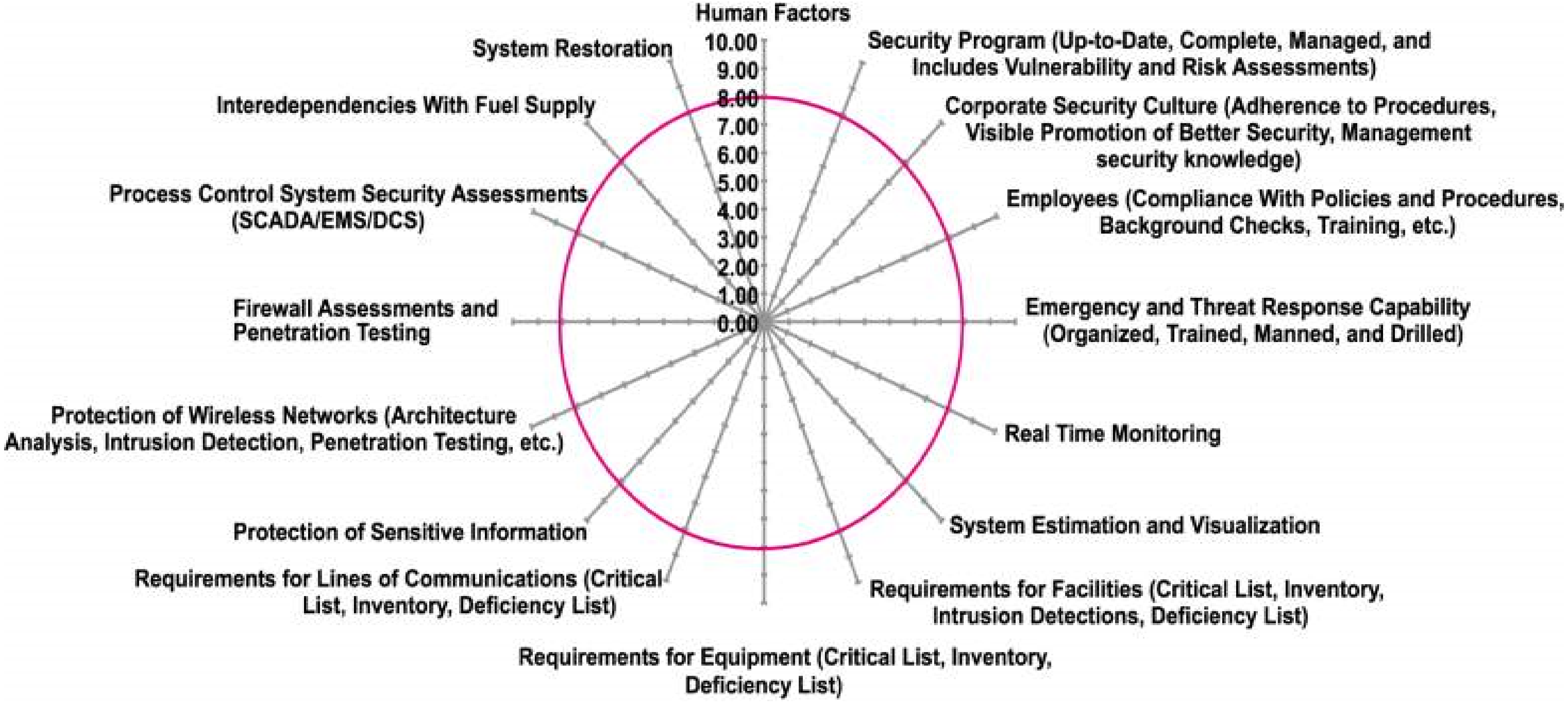
Prioritization: Security Index

General	Corporate culture
	Security Program
	Employees
	Emergency and threat response capability
Physical	Requirements for facilities, equipment and lines of communication
	Protection of sensitive information
Cyber and IT	Protection of wired and wireless networks
	Firewall assessments
	Process control system security assessments

Courtesy of: Prof. Massoud Amin, TLI

Assessment & Prioritization:

A Composite Spider Diagram to Display Security Indices



SWS
SMART WATER SUMMIT

Courtesy of: Prof. Massoud Amin, TLI

Approach

- Vulnerability mapping

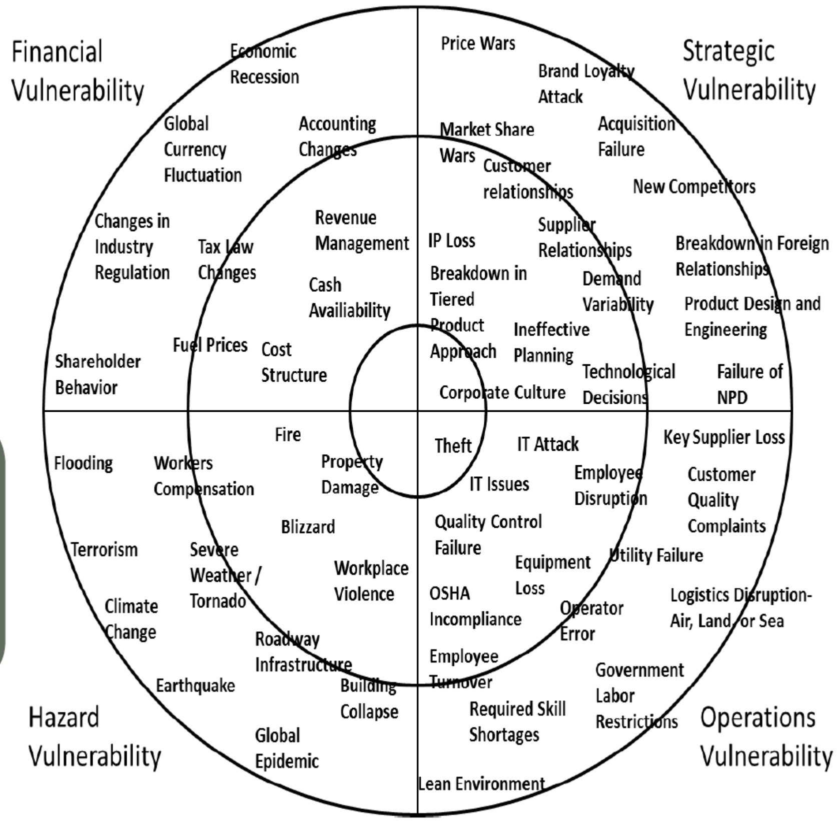


Figure 2

This illustration provides a target-and-crosshairs model for vulnerability mapping to prioritize risk factors across four sectors, including operational, hazard, financial and strategic vulnerabilities

- Scenario analysis
  - The green movement
    - Resilience requirement for new suppliers
  - Middle East embargo
    - New projects require improved delivery
  - Non-renewable energy abundance
    - Supplier and product distribution will provide snapshot of product portfolio health

SWS
SMART WATER SUMMIT

Key Challenges

- Technology
- Cost
- Policy
- Business Continuity
- Training
- Audits
- Culture and Human Factors

Quantitative Metrics

- Shodan scan - 251 exposed systems
- Honeypot - 11 attacks/3 weeks
- ~191 attacks/year
- Yields ~2 breaches/year

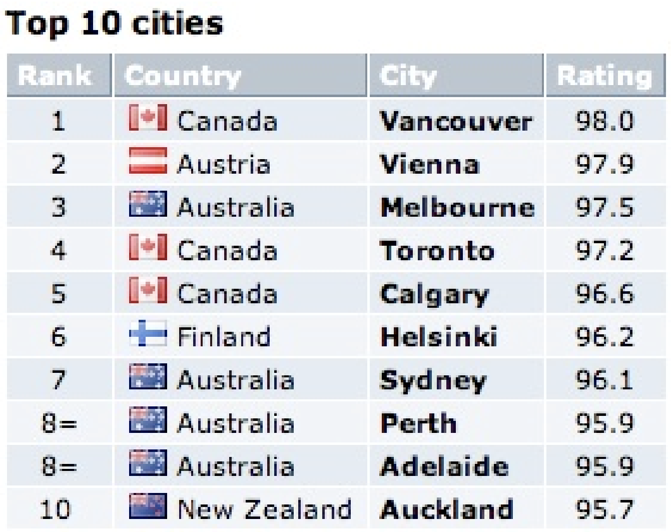
Smarter about education, safety, energy, water, food, transp., e-gov… Innovative Cities:

- **Smarter transportation**
  Stockholm, Dublin, Singapore and Brisbane are working with IBM to develop smart systems ranging from predictive tools to smart cards to congestion charging in order to reduce traffic and pollution.
- **Smarter policing and emergency response**
  New York, Syracuse, Santa Barbara and St. Louis are using data analytics, wireless and video surveillance capabilities to strengthen crime fighting and the coordination of emergency response units.
- **Smarter power and water management**
  Local government agencies, farmers and ranchers in the Paraguay-Paraná River basin to understand the factors that can help to safeguard the quality and availability of the water system. Malta is building a smart grid that links the power and water systems, and will detect leakages, allow for variable pricing and provide more control to consumers. Ultimately, it will enable this island country to replace fossil fuels with sustainable energy sources.
- **Smarter governance**
  Albuquerque is using a business intelligence solution to automate data sharing among its 7,000 employees in more than 20 departments, so every employee gets a single version of the truth. It has realized cost savings of almost 2,000%.

By 2050, 70 percent of people will be living in cities.

'Cities are perfect for promoting change and renewable energies. Cities can serve as innovation platforms, creating clusters of business around green energy."

Claude Turmes
Member of the European Parlament,
Reuters, February 10, 2009



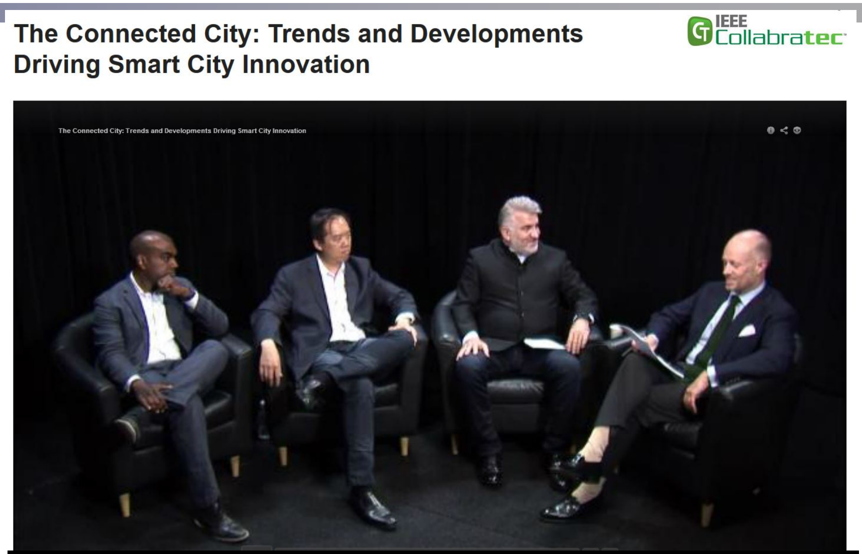
Top 10 cities

Rank	Country	City	Rating
1	Canada	**Vancouver**	98.0
2	Austria	**Vienna**	97.9
3	Australia	**Melbourne**	97.5
4	Canada	**Toronto**	97.2
5	Canada	**Calgary**	96.6
6	Finland	**Helsinki**	96.2
7	Australia	**Sydney**	96.1
8=	Australia	**Perth**	95.9
8=	Australia	**Adelaide**	95.9
10	New Zealand	**Auckland**	95.7

The Connected City: Trends and Developments Driving Smart City Innovation

- A "Smart City" is more than just high-tech infrastructure - it's about advancing our society.

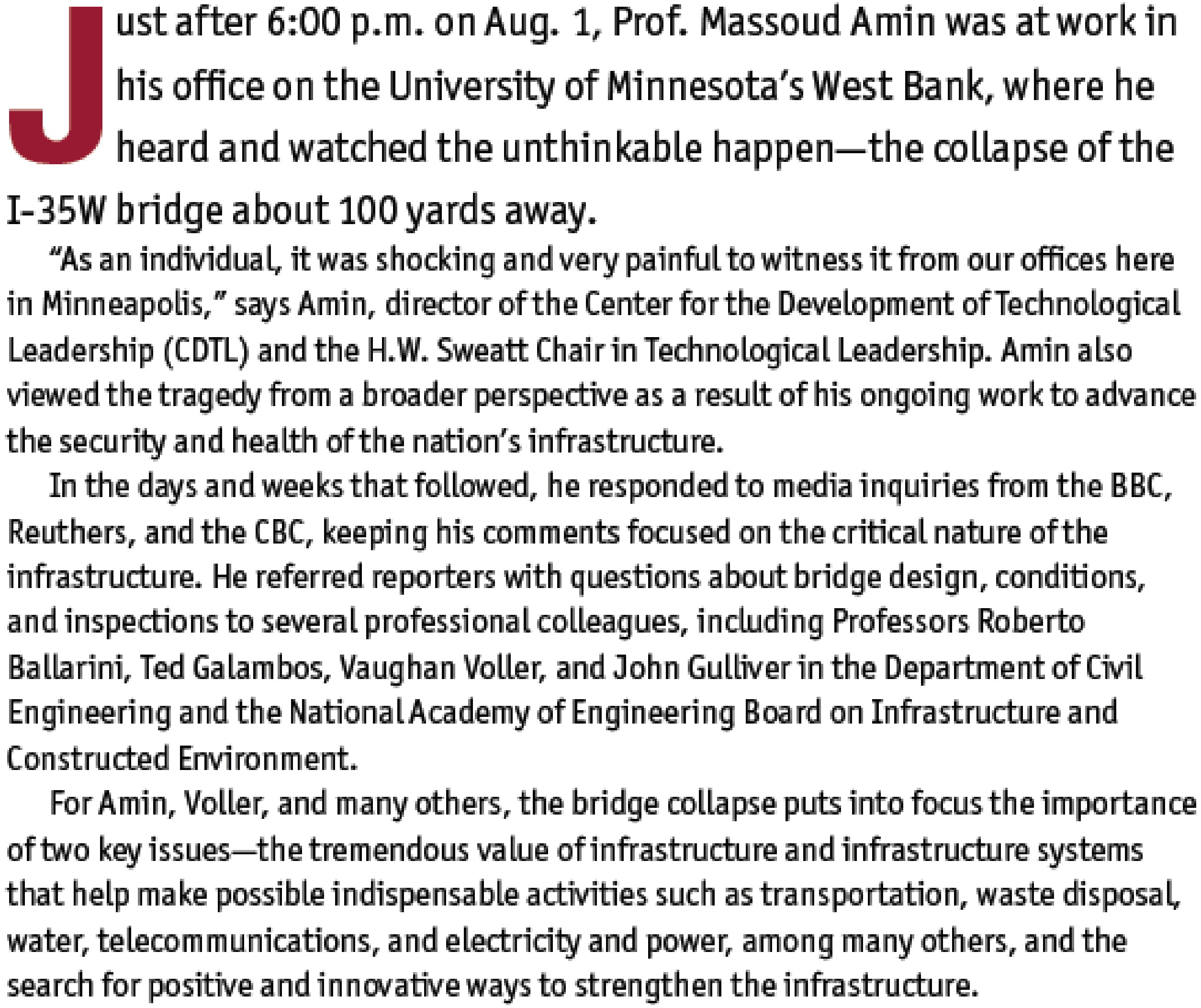
- Improving human condition and advancing the civilization that we often take for granted … As engineers, we enable better quality of life for people
- The whole idea of a smart city is not just about power or buildings. It’s about the whole ecosystem--how you educate people, how you empower people, the economic growth it can bring and what opportunities it can bring.



The Connected City: Trends and Developments Driving Smart City Innovation

“The Connected City: Trends and Developments Driving Smart City Innovation,” produced by MIT Technology Review and IEEE Collabratec.… vision, efficient use of technology, an environment that attracts a talented workforce, and an enabling infrastructure. Everything we do is geared towards that vision.

I-35W bridge



Just after 6:00 p.m. on Aug. 1, Prof. Massoud Amin was at work in his office on the University of Minnesota's West Bank, where he heard and watched the unthinkable happen—the collapse of the I-35W bridge about 100 yards away.

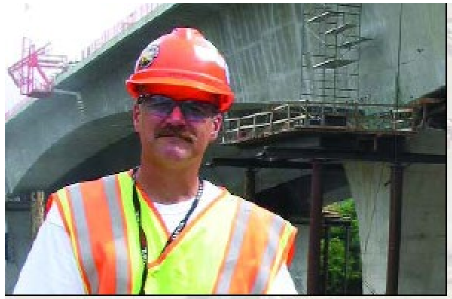
"As an individual, it was shocking and very painful to witness it from our offices here in Minneapolis," says Amin, director of the Center for the Development of Technological Leadership (CDTL) and the H.W. Sweatt Chair in Technological Leadership. Amin also viewed the tragedy from a broader perspective as a result of his ongoing work to advance the security and health of the nation's infrastructure.

In the days and weeks that followed, he responded to media inquiries from the BBC, Reuthers, and the CBC, keeping his comments focused on the critical nature of the infrastructure. He referred reporters with questions about bridge design, conditions, and inspections to several professional colleagues, including Professors Roberto Ballarini, Ted Galambos, Vaughan Voller, and John Gulliver in the Department of Civil Engineering and the National Academy of Engineering Board on Infrastructure and Constructed Environment.

For Amin, Voller, and many others, the bridge collapse puts into focus the importance of two key issues—the tremendous value of infrastructure and infrastructure systems that help make possible indispensable activities such as transportation, waste disposal, water, telecommunications, and electricity and power, among many others, and the search for positive and innovative ways to strengthen the infrastructure.

To improve the future and avoid a repetition of the past:

Sensors built in to the I-35W bridge at less than 0.5% total cost by TLI alumni



Terry Ward

Heidi Hamilton

Val Svensson

Joe Nietfeld

SWS
SMART WATER SUMMIT

Not Just Utilities … Our Role in Minnesota:
2015 MN2050 Survey

MN 2050
Infrastructure planning, long term success

			2015 Values		
	Small City	Large City	County	State	Total
Roads	$4,174,022,424	$10,517,476,430	$27,647,815,260	$29,338,312,840	$71,677,626,954
Bridges	$1,151,894,172	$807,350,570	$1,456,009,206	$6,592,940,562	$10,008,194,510
Transit	$0	$0	$0	$0	$0
Traffic	$14,168,440	$138,820,460	$59,985,398	$0	$212,974,298
Buildings	$7,583,657,510	$13,724,959,690	$4,869,723,674	$501,696,056	$26,680,036,930
Water	$1,499,020,952	$6,279,799,230	$0	$0	$7,778,820,182
Waste Water	$1,704,463,332	$4,244,983,540	$0	$6,494,782,638	$12,444,229,510
Storm sewer	$0	$2,085,960,070	$0	$0	$2,085,960,070
Storm ponds	$150,185,464	$65,757,060	$5,453,218	$0	$221,395,742
Airports	$1,240,446,922	$1,344,366,560	$0	$0	$2,584,813,482
Ports	$0	$0	$0	$0	$0
Rail	$0	$0	$3,173,772,876	$0	$3,173,772,876
Electrical	$0	$10,564,967,640	$0	$0	$10,564,967,640
Solid Waste	$0	$94,982,420	$796,169,828	$0	$891,152,248
Natural Gas	$2,056,549,066	$2,747,183,840	$0	$0	$4,803,732,906
Total	**$19.5B**	**$52.6B**	**$38.0B**	**$42.9B**	**$153B**

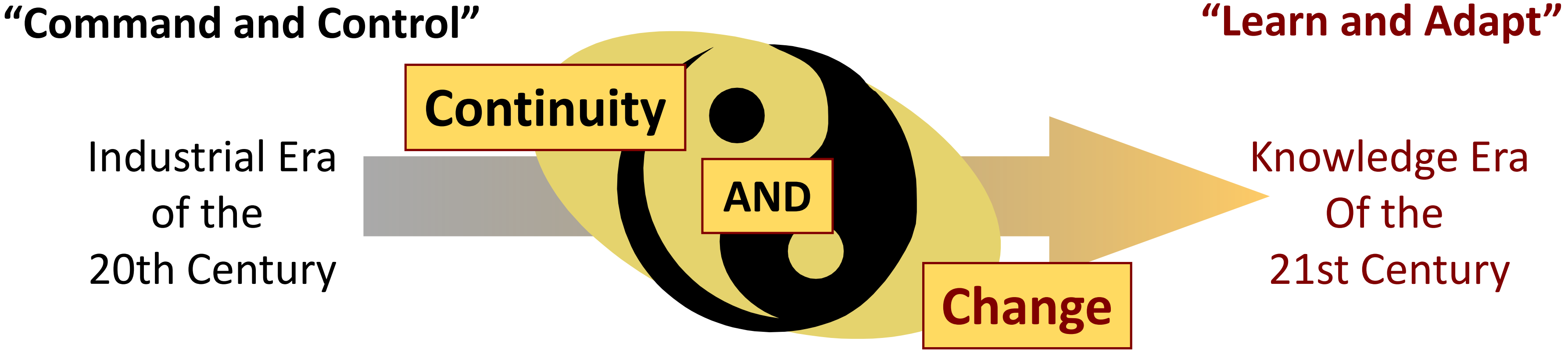
SWS
SMART WATER SUMMIT

Dynamic Adaptation Requires Chaordic Leadership

Chaord [kay'-ord]: any self-governing adaptive, non-linear complex organism, organization, community or system which harmoniously blends characteristics of both order and chaos.

Chaordic: harmoniously blending characteristics of both order and chaos in a pattern dominated by neither.

From Dee Hock: The Chaordic Organization, 1999.


"Command and Control"
Industrial Era of the 20th Century
Continuity
AND
Change
"Learn and Adapt"
Knowledge Era Of the 21st Century

Best Examples: Change & Continuity

Think about someone you have experienced as a great leader during transitions.

1. What made him or her great versus good?
2. *What specifically did this leader do that made him/her stand out?*

3. What worked well, and what didn't during these transitions?
4. Any back-stepping/rewinding needed? Any wisdom gained?
5. *How did your team perform in terms of results?*

6. *What is/are the road(s) ahead look like?*
7. *What does continuity and change mean to you, your team and your organization, and industry?*

In pairs, please spend 5 minutes discussing these and any other questions.

Insight to Action

What **insights** did you gain from this discussion and what **action** can you take to be a more effective team member / leader as a result of this insight?

Polite
"Wait and See"

Frustrated
"Get me out!"

Engaged
"Let's rock"

Producing
"Confident, Capable & Adaptive"

BASIS OF FUTURE COMPETITION

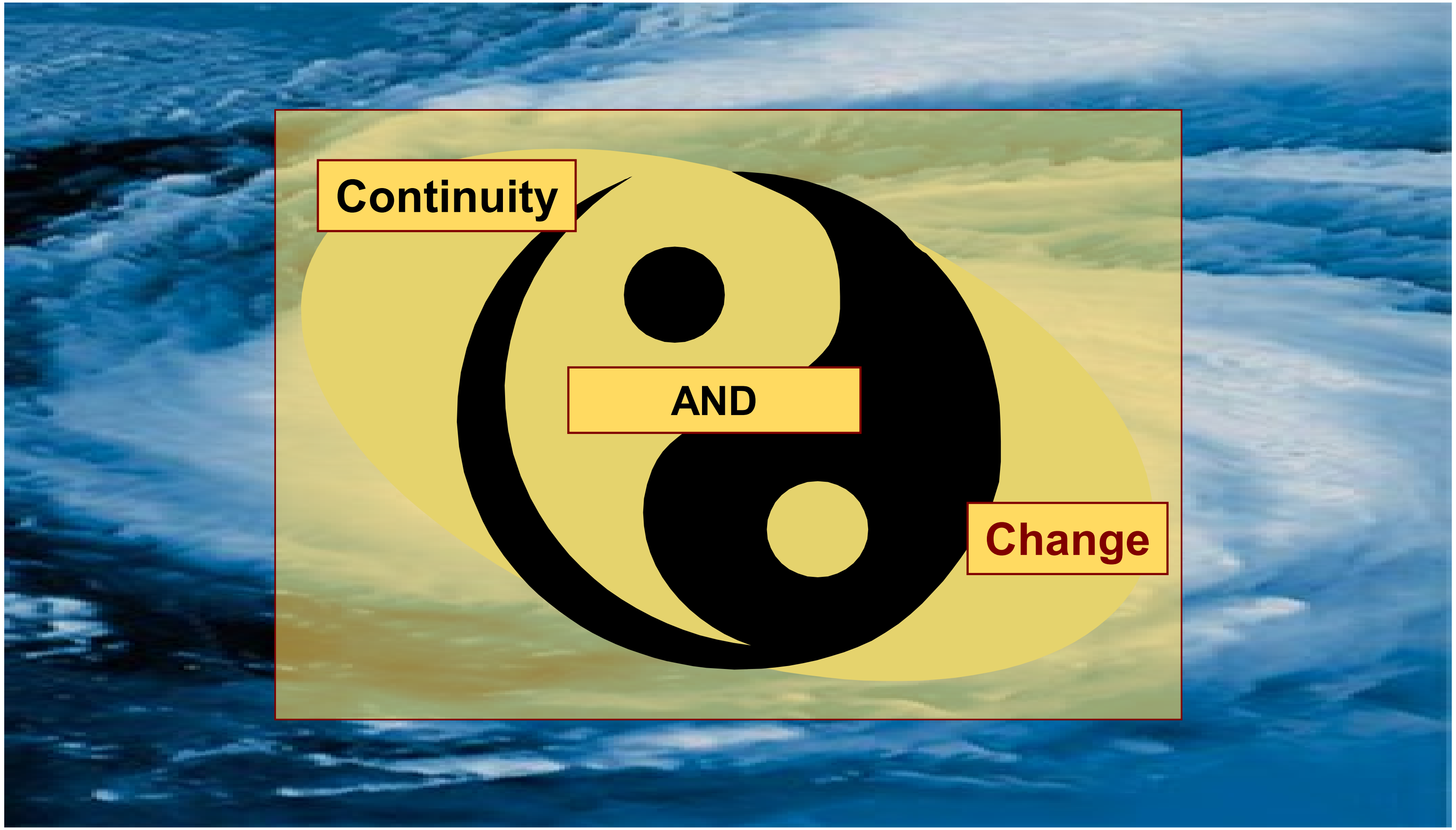
The speed at which an Enterprise can

- **Gather**
- **Collate**
- **Analyze**
- **Apply information**

SMART WATER SUMMIT

LEADERSHIP

Questions?



SMART WATER SUMMIT

SWS
SMART WATER SUMMIT