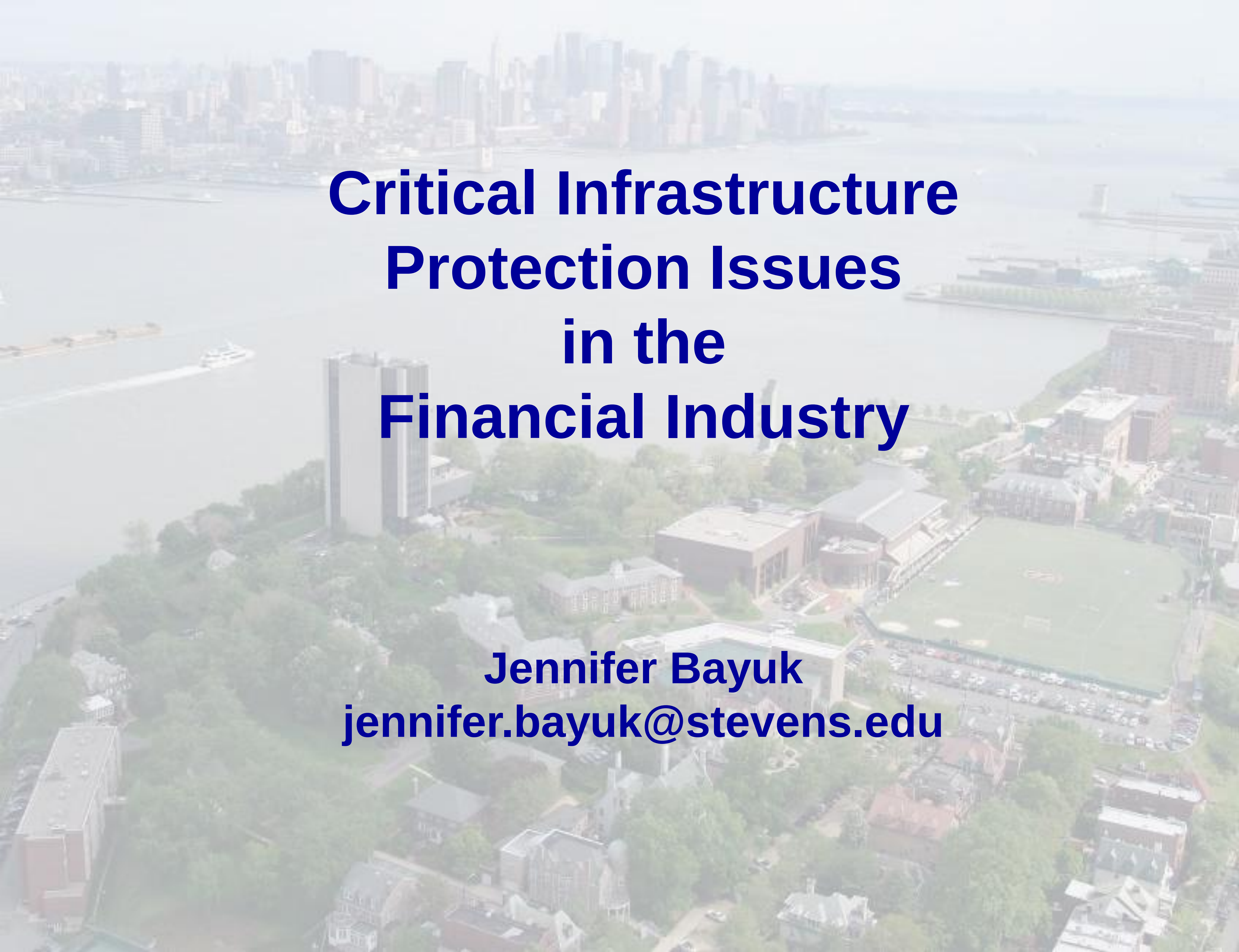
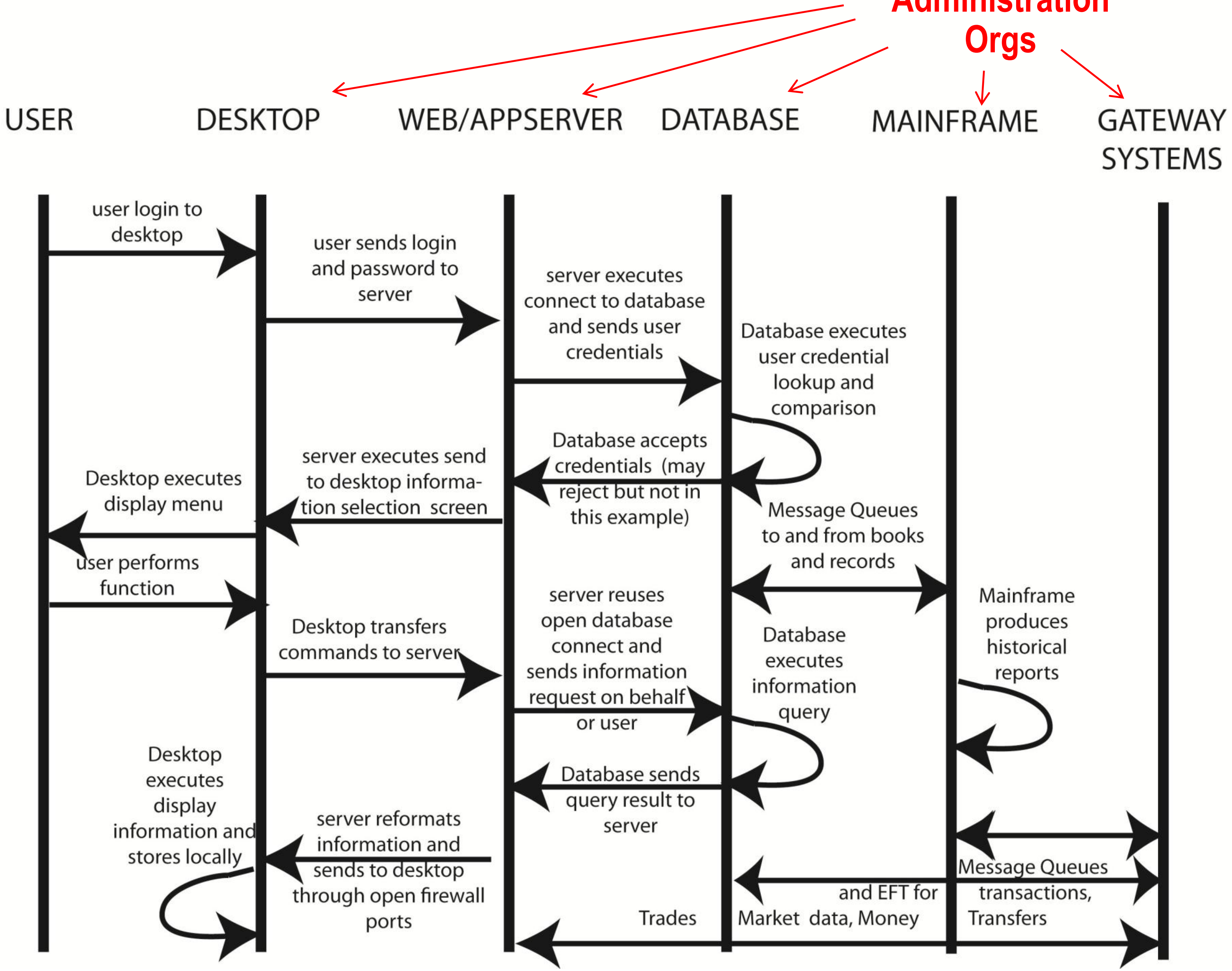


Critical Infrastructure Protection Issues in the Financial Industry

Jennifer Bayuk
jennifer.bayuk@stevens.edu

Example Financial Services System



Separate Administration Orgs

USER

DESKTOP

WEB/APPSERVER

DATABASE

MAINFRAME

GATEWAY SYSTEMS

user login to desktop

user sends login and password to server

server executes connect to database and sends user credentials

Database executes user credential lookup and comparison

Database accepts credentials (may reject but not in this example)

server executes send to desktop information selection screen

Desktop executes display menu

Message Queues to and from books and records

user performs function

Desktop transfers commands to server

server reuses open database connect and sends information request on behalf or user

Database executes information query

Mainframe produces historical reports

Database sends query result to server

Desktop executes display information and stores locally

server reformats information and sends to desktop through open firewall ports

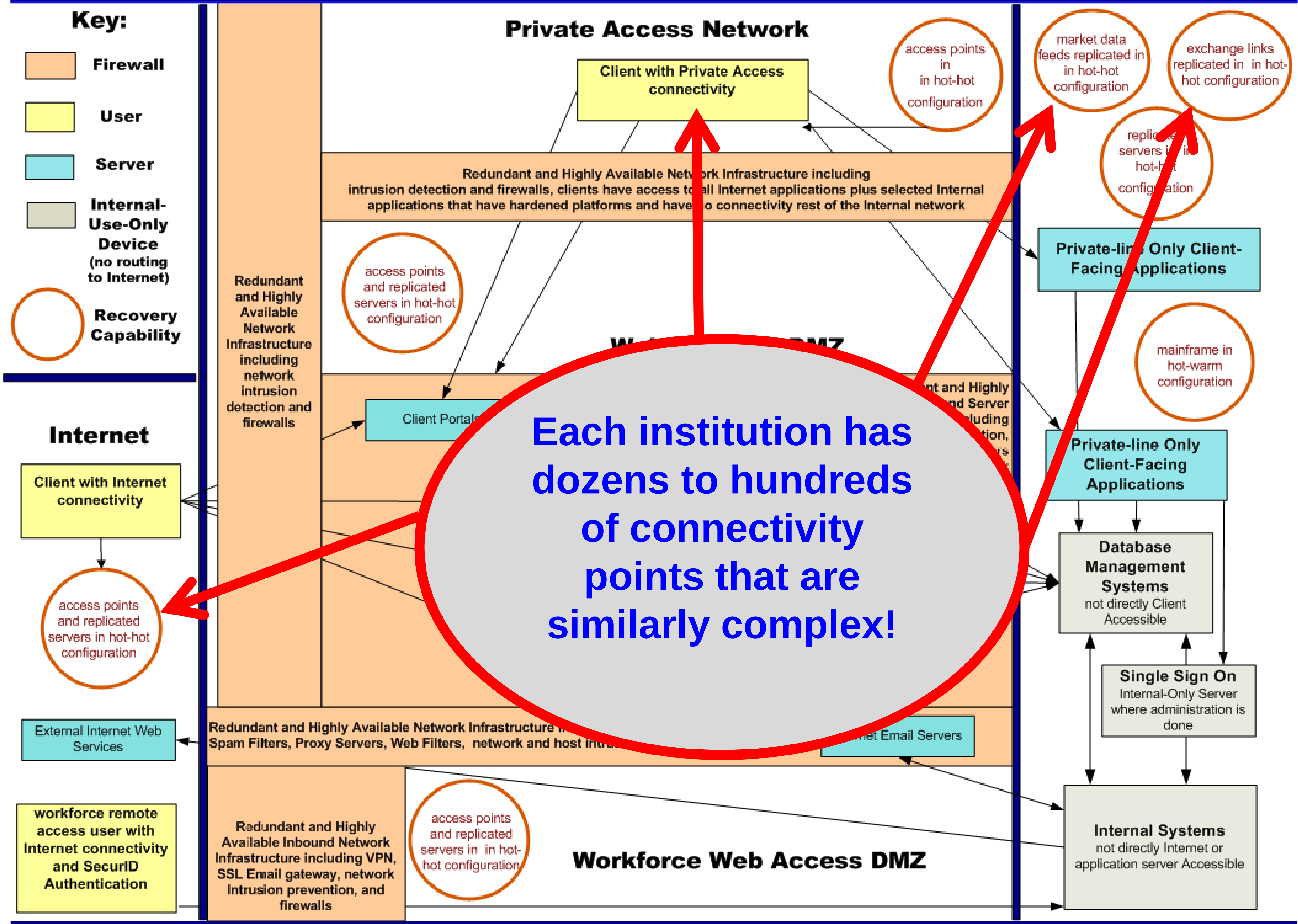
Message Queues transactions, Transfers

and EFT for

Market data, Money

Trades

Example Financial Services Production Environment



Key:

🟧 Firewall

🟨 User

🟦 Server

⬜ Internal-Use-Only Device (no routing to Internet)

○ Recovery Capability

Private Access Network

Client with Private Access connectivity

access points in in hot-hot configuration

market data feeds replicated in in hot-hot configuration

exchange links replicated in in hot-hot configuration

replicated servers in in hot-hot configuration

Redundant and Highly Available Network Infrastructure including intrusion detection and firewalls, clients have access to all Internet applications plus selected Internal applications that have hardened platforms and have no connectivity rest of the Internal network

Redundant and Highly Available Network Infrastructure including network intrusion detection and firewalls

access points and replicated servers in hot-hot configuration

Private-line Only Client-Facing Applications

mainframe in hot-warm configuration

W DMZ

Client Portal

nt and Highly
nd Server
luding
tion,
rs

Internet

Client with Internet connectivity

access points and replicated servers in hot-hot configuration

Private-line Only Client-Facing Applications

Database Management Systems
not directly Client Accessible

Single Sign On
Internal-Only Server where administration is done

External Internet Web Services

Redundant and Highly Available Network Infrastructure
Spam Filters, Proxy Servers, Web Filters, network and host intru

net Email Servers

workforce remote access user with Internet connectivity and SecurID Authentication

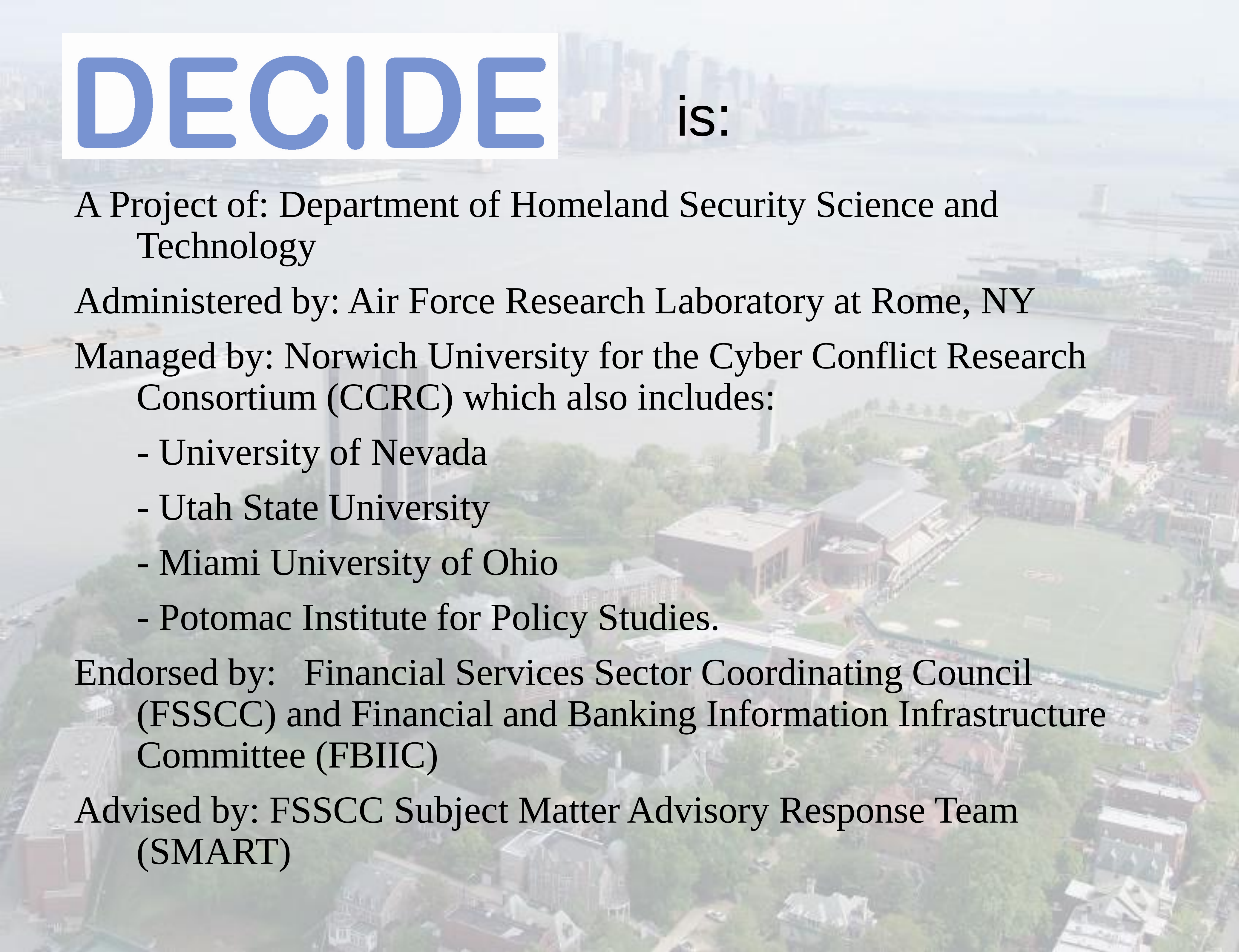
Redundant and Highly Available Inbound Network Infrastructure including VPN, SSL Email gateway, network Intrusion prevention, and firewalls

access points and replicated servers in in hot-hot configuration

Workforce Web Access DMZ

Internal Systems
not directly Internet or application server Accessible

Each institution has dozens to hundreds of connectivity points that are similarly complex!



DECIDE is:

A Project of: Department of Homeland Security Science and Technology

Administered by: Air Force Research Laboratory at Rome, NY

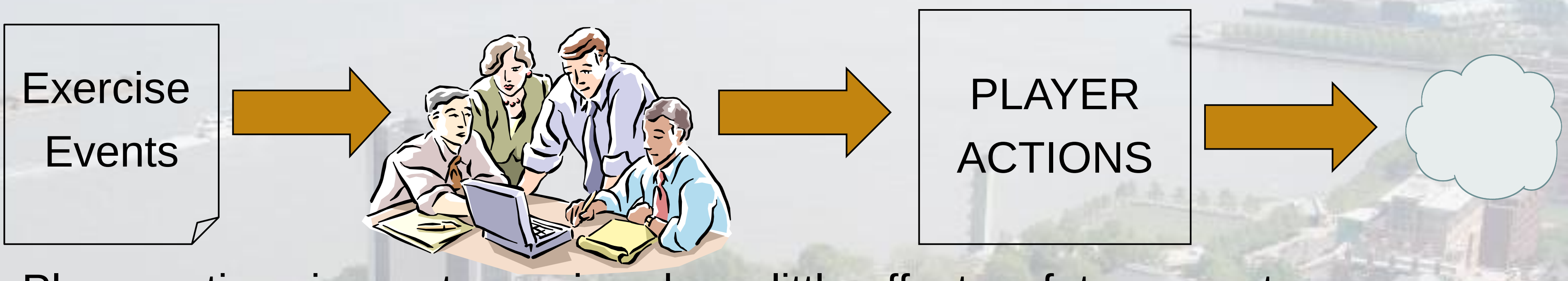
Managed by: Norwich University for the Cyber Conflict Research Consortium (CCRC) which also includes:

- University of Nevada
- Utah State University
- Miami University of Ohio
- Potomac Institute for Policy Studies.

Endorsed by: Financial Services Sector Coordinating Council (FSSCC) and Financial and Banking Information Infrastructure Committee (FBIIC)

Advised by: FSSCC Subject Matter Advisory Response Team (SMART)

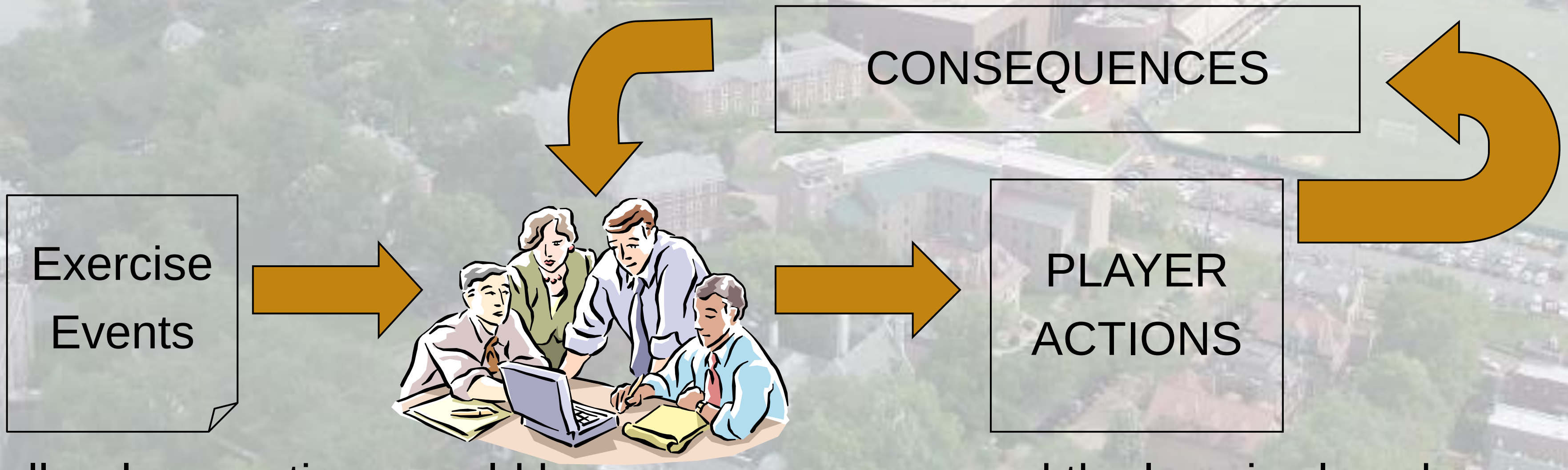
Open and Closed Loop Exercises



Exercise Events

PLAYER ACTIONS

Player actions in most exercises have little effect on future events



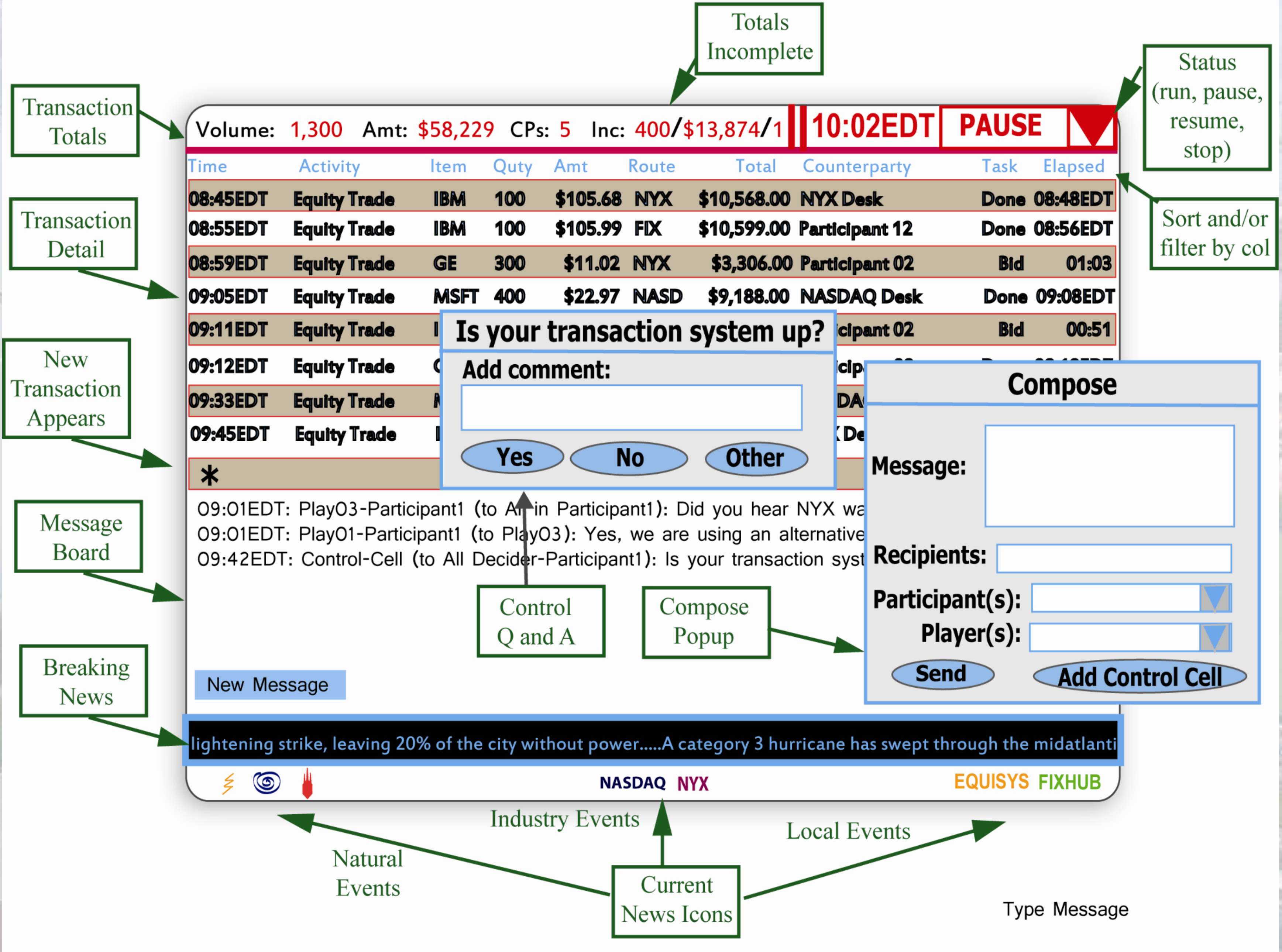
CONSEQUENCES

Exercise Events

PLAYER ACTIONS

Ideally, player actions would have consequences and the loop is closed

PLAYER VIEW OF TRANSACTIONS DURING EXERCISE



Volume: 1,300 Amt: $58,229 CPs: 5 Inc: 400/$13,874/1 10:02EDT PAUSE

Time	Activity	Item	Quty	Amt	Route	Total	Counterparty	Task	Elapsed
08:45EDT	Equity Trade	IBM	100	$105.68	NYX	$10,568.00	NYX Desk	Done	08:48EDT
08:55EDT	Equity Trade	IBM	100	$105.99	FIX	$10,599.00	Participant 12	Done	08:56EDT
08:59EDT	Equity Trade	GE	300	$11.02	NYX	$3,306.00	Participant 02	Bid	01:03
09:05EDT	Equity Trade	MSFT	400	$22.97	NASD	$9,188.00	NASDAQ Desk	Done	09:08EDT
09:11EDT	Equity Trade	I					icipant 02	Bid	00:51
09:12EDT	Equity Trade	C					icip		
09:33EDT	Equity Trade	M					DA		
09:45EDT	Equity Trade	I					De		
*									

Is your transaction system up?

Add comment:

Yes No Other

09:01EDT: Play03-Participant1 (to All in Participant1): Did you hear NYX wa
09:01EDT: Play01-Participant1 (to Play03): Yes, we are using an alternative
09:42EDT: Control-Cell (to All Decider-Participant1): Is your transaction syst

New Message

Compose

Message:

Recipients:

Participant(s):

Player(s):

Send Add Control Cell

lightening strike, leaving 20% of the city without power.....A category 3 hurricane has swept through the midatlanti

DATA FLOW SCREEN
DISPLAY ONLY

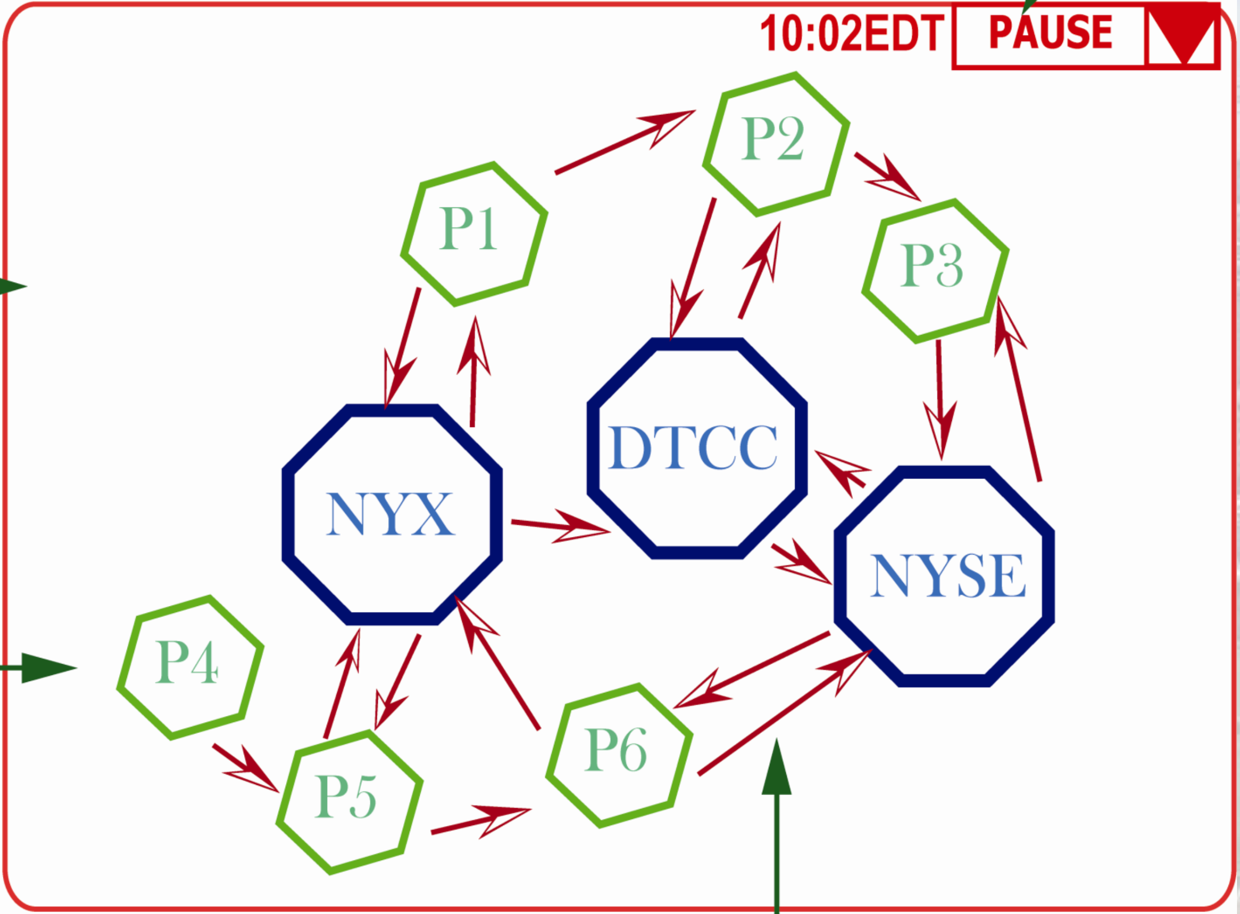
Time and Status

Graphic Builds During Set-up.

Data Flow between Participants

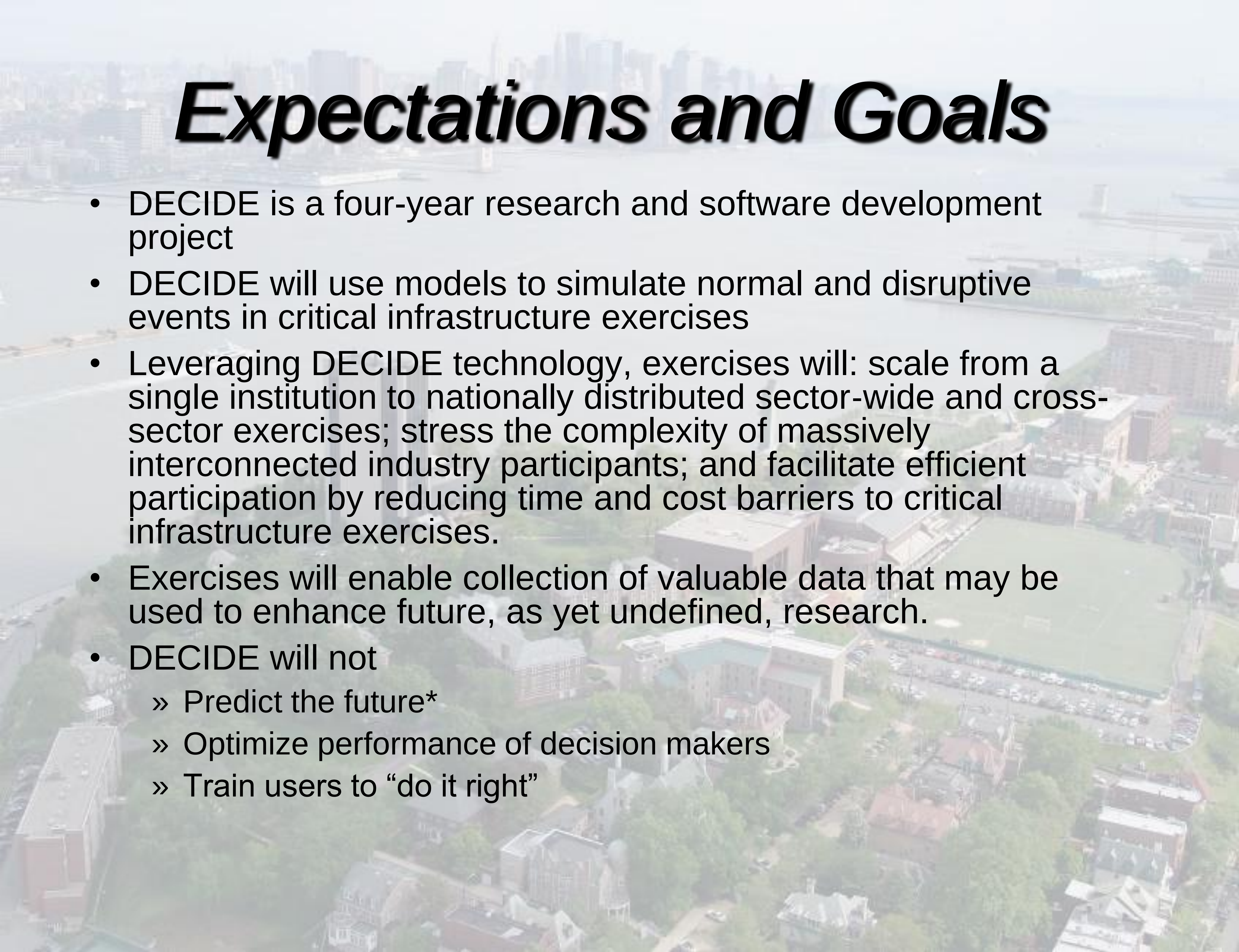
Becomes Visible During Play:

Participant Isolation May Indicate Issues:



Transactions are represented by lines within time intervals and change dynamically with play.

Potentially may be displayed at internal resource level.



Expectations and Goals

- DECIDE is a four-year research and software development project
- DECIDE will use models to simulate normal and disruptive events in critical infrastructure exercises
- Leveraging DECIDE technology, exercises will: scale from a single institution to nationally distributed sector-wide and cross-sector exercises; stress the complexity of massively interconnected industry participants; and facilitate efficient participation by reducing time and cost barriers to critical infrastructure exercises.
- Exercises will enable collection of valuable data that may be used to enhance future, as yet undefined, research.
- DECIDE will not
  - » Predict the future*
  - » Optimize performance of decision makers
  - » Train users to “do it right”

“All models are wrong. Some models are useful.”

- George Box