An Introduction to System Dynamics

George P. Richardson
Rockefeller College of Public Affairs and Policy
University at Albany, State University of New York
A Systems Perspective

Events and Decisions
Patterns of Behavior
System Structure

Reactive
Adaptive
Generative

Increasing leverage
“Distancing...”

A systems view stands back just far enough to...

• Deliberately blur discrete events into patterns of behavior

• Deliberately move from a focus on individual decisions to a focus on policy structure
Four Key Patterns of Thought

• Dynamic thinking (graphs over time)
• Causal thinking (feedback loops)
• Stock-and-flow thinking (accumulations)
• Thinking endogenously (system as cause)
Prejudice and Minority Achievement (Myrdal, Merton)

Prejudice

Discrimination

(R)

Prejudice

Opportunities for the minority

Achievements of the minority

Minority perceptions of the gap

Minority efforts to achieve

(B)

Striving

(R)

Hope or despair

Aspirations of the minority

+ + + + +
Stocks, Flows, and Feedback Loops
Here: a gasoline shortage crisis
Dynamics

• Define problems in terms of graphs over time.
  • Graph important variables
  • Graph historical data
  • Graph anticipated dynamics
  • Graph preferred dynamics
• Use these to focus systems thinking and modeling
U.S. Unemployment 1948-2012
(annual average %)
Carbon Emissions 1800-2000

Global Fossil Carbon Emissions

- Total
- Petroleum
- Coal
- Natural Gas
- Cement Production

Million Metric Tons of Carbon / Year

1800 1850 1900 1950 2000

Rockefeller College of Public Affairs and Policy
University at Albany
Systems Structure

- Accumulations (populations, resources…)
- Causal structure: “feedback” loops
- Delays
- Perceptions (a kind of accumulation)
- Pressures
- Affects, emotions, (ir)rationalities
- Policies governing decisions
Causal Diagrams

- Causal mapping is a powerful tool for representing structure in complex systems.
- Arrows indicate *causal* influence.
Polarities of Causal Links

• Positive and negative signs show the direction of causality:
  + ... “direct” relation
  – …“inverse” relation
Feedback Loops

A feedback loop exists when decisions change the state of the system, changing the conditions and information that influence future decisions.
Two kinds of feedback loops

- **Reinforcing loops**
  - Growth producing
  - Destabilizing
  - Accelerating
  - Positive: an even number of –’s

- **Symbolized by**

- **Balancing loops**
  - Counteracting
  - Goal seeking
  - Stabilizing
  - Negative: an odd number of –’s

- **Symbolized by**
Examples of Reinforcing Loops

- Births per year → Population
- Attractiveness for business → Number of private businesses
- Expected profitability of business → Tax base
- Tax rate
- Performance
- Motivation
Typical Reinforcing Loop Behaviors

Population and Births Loop

Businesses and Taxes Loop
Examples of Balancing or Counteracting Loops

- Water in glass
  - Desired amount of water in glass
  - Fraction filled
  - Pouring rate

- Population
  - Outmigration

- Gypsie moth net growth
  - Wasps
  - Wasp net growth
  - Gypsie moths
Typical Counteracting Loop Behaviors

Filling a Glass

Population and emigration

Predator-prey interactions
But There are Subtleties: Not all Word-and-Arrow Diagrams are Alike!
These arrows mean ‘and then’

- We start with some understandings of the problem and its systemic context, **and then** we conceptualize (map) the system.
- **Then** we build the beginnings of a model, which we **then** test to understand it.
- **Then** we reformulate, or reconceptualize, or revise our understandings, or do some of all three, **and then** continue…
Arrows here are *flows* of material

The words here represent accumulations of carbon – *stocks* -- and the arrows represent *flows*.

This is not a *causal* diagram.

This is a view of the “carbon cycle.”
Only this one is a *causal* loop

This causal loop tells a very compelling and important self-reinforcing story.
Stocks and Flows

Stocks are accumulations.

- Stocks are increased by **inflows** and decreased by **outflows**.
- When a link means “add” or “subtract” we have a stock-and-flow structure.
- Example: Inventory
Human Activity, CO2, and Global Temperature

Thought experiment:

- Capital stock
- Economic activity
- CO2 annual production
- Global heat energy
- Uptake of atmospheric CO2
- Incoming solar heat energy
- Outgoing global heat energy

Rockefeller College of Public Affairs and Policy
University at Albany
The system dynamics modeling process

Adapted from Saeed 1992

Rockefeller College of Public Affairs and Policy
University at Albany
Processes focusing on system structure

Mental Models, Experience, Literature

Perceptions of System Structure

Empirical Evidence

System Conceptualization

Comparison and Reconciliation

Model Formulation

Representation of Model Structure

Diagramming and Description Tools
Processes focusing on system behavior

1. Empirical Evidence
2. System Conceptualization
3. Model Formulation
   - Empirical and Inferred Time Series
   - Comparison and Reconciliation
   - Deduction Of Model Behavior
   - Literature, Experience
   - Computing Aids
Two kinds of validating processes

Mental Models, Experience, Literature

Perceptions of System Structure

Comparison and Reconciliation

Structure Validating Processes

Representation of Model Structure

Diagramming and Description Tools

Empirical Evidence

System Conceptualization

Model Formulation

Deduction Of Model Behavior

Behavior Validating Processes

Computing Aids

Empirical and Inferred Time Series

Comparison and Reconciliation

Literature, Experience
Pictures Can Get Really Complicated!

[Diagram of complex relationships involving tobacco policies, health risks, and economic factors.]

Rockefeller College of Public Affairs and Policy
University at Albany
The Endogenous Point of View

The “X/N” Matrix

Predominant Mode of Analysis

Exogenous  Endogenous

Exogenous

Endogenous

True (Predominant) State of Affairs
A Lightening-Fast Example

- Security on off-shore oil platforms during a technology transition
- Mixed consulting / theory building intervention
- Two group model building workshops, May and September with various high-level management people from Norsk Hydro and related professional groups
Hopes and fears

**Hopes**
- Establish a Platform for Communicating SD for Hydro.
- Consensus about 3 yr agenda
- come up with a useful case/model
- Hope Hydro becomes very involved
- We do not catch Hydro’s interest
- Clear Picture of Workshops down the road
- Norsk Hydro may not be the right case
- Establish a SD Model giving new insight
- Focus on security
- Getting lost in detail
- Establishing a SD Model that gives no new insights
- too much focus on safety
- This SD-Modell does not improve security (& safety) in e-Operation
- Some managers think we should never open the platforms
- We don’t understand the situations
- More safe & secure e-operations
- Process will help Hydro understand what may happen

**Fears**
- HYDRO is new to group modelling
- Find a common case for all (AUC, SINTEF, HYDRO)
- Centrifugal Forces blow AMBASEC, IRMA, HYDRO apart
- Getting lost in detail
- Establishing a SD Model that gives no new insights
- focus on security
- Identify valuable insights for all
- Some managers think we should never open the platforms
- We don’t understand the situations
- Someone on-shore will inadvertently intervene off-shore

**Get a firm understanding system dynamic mapping**
- How to simulate Risk/Stress
- Too little time to be successful

**Rockefeller College of Public Affairs and Policy**
University at Albany
Stakeholders

- Chief Executive Officer
- Managers of unsecured external networks
- National Politicians
- HSE responsible
- Local Politicians
- Government
- Developers of COTS
- IT EXPERT (Support)
- SYSTEM ADMIN
- The one detecting the incident
- Incident Response Team Member
- CRO Control Room Operator
- OIL COMPANY (System Owner)
- PLATFORM CHIEF
- Control Room Manager
- Work planner / administrator
- Contractors doing drilling & modification fixed platforms
- Operators doing drilling & modification fixed platforms
- Incident Response Team Manager
- Suppliers (maintenance of PCs/ESD)
- Service Supplier (handling within their organization)
- CSIRT in a virtual organisation
- Local Communities/Generel, Public
- MALICIOUS OUTSIDER
- Interval Intruder Attacker
- Terrorists
- COMPETING OIL COMPANY
- ECOLOGICAL ACTIVISTS
- WORKERS
- Nature
- People responsible for e-Op Change processes
- CISO (Chief InfoSeq. Officer)
- OIL COMPANY (System Owner)
- Government
- Incidents Response Team Manager
- CIO
- MALICIOUS OUTSIDER
- Interval Intruder Attacker
- Nature
- People responsible for e-Op Change processes
- CISO (Chief InfoSeq. Officer)
- OIL COMPANY (System Owner)
- Government
- Incidents Response Team Manager
- CIO
- MALICIOUS OUTSIDER
- Interval Intruder Attacker
- Nature
- People responsible for e-Op Change processes
- CISO (Chief InfoSeq. Officer)
- OIL COMPANY (System Owner)
- Government
- Incidents Response Team Manager
- CIO
- MALICIOUS OUTSIDER
- Interval Intruder Attacker
- Nature
- People responsible for e-Op Change processes
- CISO (Chief InfoSeq. Officer)
- OIL COMPANY (System Owner)
- Government
- Incidents Response Team Manager
- CIO
- MALICIOUS OUTSIDER
- Interval Intruder Attacker
- Nature
- People responsible for e-Op Change processes
- CISO (Chief InfoSeq. Officer)
- OIL COMPANY (System Owner)
- Government
- Incidents Response Team Manager
- CIO
- MALICIOUS OUTSIDER
- Interval Intruder Attacker
- Nature
- People responsible for e-Op Change processes
- CISO (Chief InfoSeq. Officer)
- OIL COMPANY (System Owner)
- Government
- Incidents Response Team Manager
- CIO
- MALICIOUS OUTSIDER
- Interval Intruder Attacker
- Nature
- People responsible for e-Op Change processes
- CISO (Chief InfoSeq. Officer)
- OIL COMPANY (System Owner)
- Government
- Incidents Response Team Manager
- CIO
- MALICIOUS OUTSIDER
- Interval Intruder Attacker
- Nature
- People responsible for e-Op Change processes
- CISO (Chief InfoSeq. Officer)
- OIL COMPANY (System Owner)
- Government
- Incidents Response Team Manager
- CIO
- MALICIOUS OUTSIDER
- Interval Intruder Attacker
- Nature
- People responsible for e-Op Change processes
- CISO (Chief InfoSeq. Officer)
- OIL COMPANY (System Owner)
- Government
- Incidents Response Team Manager
- CIO
- MALICIOUS OUTSIDER
- Interval Intruder Attacker
- Nature
- People responsible for e-Op Change processes
- CISO (Chief InfoSeq. Officer)
- OIL COMPANY (System Owner)
- Government
- Incidents Response Team Manager
- CIO
- MALICIOUS OUTSIDER
- Interval Intruder Attacker
- Nature
- People responsible for e-Op Change processes
- CISO (Chief InfoSeq. Officer)
- OIL COMPANY (System Owner)
- Government
- Incidents Response Team Manager
- CIO
- MALICIOUS OUTSIDER
- Interval Intruder Attacker
- Nature
- People responsible for e-Op Change processes
- CISO (Chief InfoSeq. Officer)
- OIL COMPANY (System Owner)
- Government
- Incidents Response Team Manager
- CIO
- MALICIOUS OUTSIDER
- Interval Intruder Attacker
- Nature
- People responsible for e-Op Change processes
- CISO (Chief InfoSeq. Officer)
- OIL COMPANY (System Owner)
- Government
- Incidents Response Team Manager
- CIO
- MALICIOUS OUTSIDER
- Interval Intruder Attacker
- Nature
- People responsible for e-Op Change processes
- CISO (Chief InfoSeq. Officer)
- OIL COMPANY (System Owner)
- Government
- Incidents Response Team Manager
- CIO
- MALICIOUS OUTSIDER
- Interval Intruder Attacker
- Nature
- People responsible for e-Op Change processes
- CISO (Chief InfoSeq. Officer)
- OIL COMPANY (System Owner)
- Government
- Incidents Response Team Manager
- CIO
- MALICIOUS OUTSIDER
- Interval Intruder Attacker
- Nature
- People responsible for e-Op Change processes
- CISO (Chief InfoSeq. Officer)
- OIL COMPANY (System Owner)
- Government
- Incidents Response Team Manager
- CIO
- MALICIOUS OUTSIDER
- Interval Intruder Attacker
- Nature
- People responsible for e-Op Change processes
- CISO (Chief InfoSeq. Officer)
- OIL COMPANY (System Owner)
- Government
- Incidents Response Team Manager
- CIO
- MALICIOUS OUTSIDER
- Interval Intruder Attacker
- Nature
- People responsible for e-Op Change processes
- CISO (Chief InfoSeq. Officer)
- OIL COMPANY (System Owner)
- Government
- Incidents Response Team Manager
- CIO
- MALICIOUS OUTSIDER
- Interval Intruder Attacker
- Nature
- People responsible for e-Op Change processes
- CISO (Chief InfoSeq. Officer)
- OIL COMPANY (System Owner)
- Government
- Incidents Response Team Manager
- CIO
- MALICIOUS OUTSIDER
- Interval Intruder Attacker
- Nature
- People responsible for e-Op Change processes
- CISO (Chief InfoSeq. Officer)
- OIL COMPANY (System Owner)
- Government
- Incidents Response Team Manager
- CIO
- MALICIOUS OUTSIDER
- Interval Intruder Attacker
- Nature
- People responsible for e-Op Change processes
- CISO (Chief InfoSeq. Officer)
- OIL COMPANY (System Owner)
- Government
- Incidents Response Team Manager
- CIO
- MALICIOUS OUTSIDER
- Interval Intruder Attacker
- Nature
- People responsible for e-Op Change processes
- CISO (Chief InfoSeq. Officer)
- OIL COMPANY (System Owner)
- Government
- Incidents Response Team Manager
- CIO
- MALICIOUS OUTSIDER
- Interval Intruder Attacker
- Nature
- People responsible for e-Op Change processes
- CISO (Chief InfoSeq. Officer)
- OIL COMPANY (System Owner)
- Government
- Incidents Response Team Manager
- CIO
- MALICIOUS OUTSIDER
- Interval Intruder Attacker
- Nature
- People responsible for e-Op Change processes
- CISO (Chief InfoSeq. Officer)
- OIL COMPANY (System Owner)
- Government
- Incidents Response Team Manager
- CIO
- MALICIOUS OUTSIDER
- Interval Intruder Attacker
- Nature
- People responsible for e-Op Change processes
- CISO (Chief InfoSeq. Officer)
- OIL COMPANY (System Owner)
- Government
- Incidents Response Team Manager
- CIO
- MALICIOUS OUTSIDER
- Interval Intruder Attacker
- Nature
- People responsible for e-Op Change processes
- CISO (Chief InfoSeq. Officer)
- OIL COMPANY (System Owner)
- Government
- Incidents Response Team Manager
- CIO
- MALICIOUS OUTSIDER
- Interval Intruder Attacker
- Nature
- People responsible for e-Op Change processes
- CISO (Chief InfoSeq. Officer)
- OIL COMPANY (System Owner)
- Government
- Incidents Response Team Manager
- CIO
- MALICIOUS OUTSIDER
- Interval Intruder Attacker
- Nature
- People responsible for e-Op Change processes
- CISO (Chief InfoSeq. Officer)
- OIL COMPANY (System Owner)
- Government
- Incidents Response Team Manager
- CIO
- MALICIOUS OUTSIDER
- Interval Intruder Attacker
- Nature
- People responsible for e-Op Change processes
- CISO (Chief InfoSeq. Officer)
- OIL COMPANY (System Owner)
- Government
- Incidents Response Team Manager
- CIO
- MALICIOUS OUTSIDER
- Interval Intruder Attacker
- Nature
- People responsible for e-Op Change processes
- CISO (Chief InfoSeq. Officer)
- OIL COMPANY (System Owner)
- Government
- Incidents Response Team Manager
- CIO
- MALICIOUS OUTSIDER
- Interval Intruder Attacker
- Nature
- People responsible for e-Op Change processes
- CISO (Chief InfoSeq. Officer)
- OIL COMPANY (System Owner)
- Government
- Incidents Response Team Manager
- CIO
- MALICIOUS OUTSIDER
- Interval Intruder Attacker
- Nature
- People responsible for e-Op Change processes
- CISO (Chief InfoSeq. Officer)
- OIL COMPANY (System Owner)
- Government
- Incidents Response Team Manager
- CIO
- MALICIOUS OUTSIDER
- Interval Intruder Attacker
- Nature
- People responsible for e-Op Change processes
- CISO (Chief InfoSeq. Officer)
- OIL COMPANY (System Owner)
- Government
- Incidents Response Team Manager
- CIO
- MALICIOUS OUTSIDER
- Interval Intruder Attacker
- Nature
- People responsible for e-Op Change processes
- CISO (Chief InfoSeq. Officer)
- OIL COMPANY (System Owner)
- Government
- Incidents Response Team Manager
- CIO
- MALICIOUS OUTSIDER
- Interval Intruder Attacker
- Nature
- People responsible for e-Op Change processes
- CISO (Chief InfoSeq. Officer)
- OIL COMPANY (System Owner)
- Government
- Incidents Response Team Manager
- CIO
- MALICIOUS OUTSIDER
- Interval Intruder Attacker
- Nature
- People responsible for e-Op Change processes
- CISO (Chief InfoSeq. Officer)
- OIL COMPANY (System Owner)
- Government
- Incidents Response Team Manager
- CIO
- MALICIOUS OUTSIDER
- Interval Intruder Attacker
- Nature
- People responsible for e-Op Change processes
- CISO (Chief InfoSeq. Officer)
- OIL COMPANY (System Owner)
- Government
- Incidents Response Team Manager
- CIO
- MALICIOUS OUTSIDER
- Interval Intruder Attacker
- Nature
- People responsible for e-Op Change processes
- CISO (Chief InfoSeq. Officer)
- OIL COMPANY (System Owner)
- Government
- Incidents Response Team Manager
- CIO
- MALICIOUS OUTSIDER
- Interval Intruder Attacker
- Nature
- People responsible for e-Op Change processes
- CISO (Chief InfoSeq. Officer)
- OIL COMPANY (System Owner)
- Government
- Incidents Response Team Manager
- CIO
- MALICIOUS OUTSIDER
- Interval Intruder Attacker
- Nature
- People responsible for e-Op Change processes
- CISO (Chief InfoSeq. Officer)
- OIL COMPANY (System Owner)
- Government
- Incidents Response Team Manager
- CIO
- MALICIOUS OUTSIDER
- Interval Intruder Attacker
- Nature
- People responsible for e-Op Change processes
- CISO (Chief InfoSeq. Officer)
- OIL COMPANY (System Owner)
- Government
- Incidents Response Team Manager
- CIO
- MALICIOUS OUTSIDER
- Interval Intruder Attacker
- Nature
- People responsible for e-Op Change processes
- CISO (Chief InfoSeq. Office
Behaviour over time

Overview
| Policies |
|-------------------|-------------------|-------------------|-------------------|-------------------|-------------------|-------------------|
| Improve the safety and security culture | Prevent out of sight out of mind mentality | Annual awareness campaigns for measures in security culture | Increase the amount of incident reports from IRT & CEO | Be open about security incidents | Increase knowledge information sharing across industry |
| Establish common risk perception | Common security requirement on products and services | Higher level of security | Improve incident reporting | Establish CSRS | Cooperation between IRTs in different organisations |
| Balance work & RD of CSIRT | Understand the erosion of compliance | Increase CSIRTS authority | Create formal CSIRTS | Establish common system incident report management -common report in –publish incidents in industry | Build IDS to systematically gather information |
| Invest in survivability Solutions | Identify ‘Best practice’ other countries other industries | Establish Best /Good Practice Against Insider Threat | Training to close knowledge gap | a warning system for the communication network | Share and learn from incident B/W Orgs. & W/n Orgs |
| Perform HazOp of the e-operation solution of 2010 | Investigate in Vulnerability Detection | Perform Pilots do intrusion tests and spread success stories | Risk assessment in change processes (continuously) | Monitor/Measure Risk Change (Auditing) | Establish a security Quality process improvement |

- Prioritization by group members
- Added day two

---

Rockefeller College of Public Affairs and Policy
University at Albany
A Tiny Model Capturing the Problem Dynamics
A Tiny Model Capturing the Problem Dynamics
A Tiny Model Capturing the Problem Dynamics

- Potential capacity to transition
- Synergies between potential and experience
- Speed of transition
- Experience with transition
- Time to fully integrate ops
- Risk
- Cost per bbl

- Capacity in Traditional ops
- Transition to Integrated ops
- New capacity in Integrated ops
- Maturing Integrated ops
- Mature capacity in Integrated ops
Behavior of this Tiny Beginning Model

- Traditional capacity (blue) phasing out
- New capacity (red) rising, peaking and declining
- Mature capacity (green) slowly rising
- Cost per barrel (black) declining to a new low
- Risk (grey) rising, peaking, and declining
- …all just what the problem description called for

But vastly oversimplified.

Serious group modeling was needed.
Group Modeling Work in Process
Policy Simulations with Hydro1
When It Works, Why?

- Engagement
- Mental models
- Complexity
- Alignment
- Refutability
- Empowerment