Management Analytics

Cyber Risks to Nuclear Safety

Fred Cohen 2021

- Looking Ahead
  - Model-based situation anticipation and constraint
- Nuclear Safety
  - Safety
  - Nuclear (and fused)
- Cyber
  - Sensors, Actuators, Communications, Decisions
- Risks
  - Anticipated futures
- What to do about it
  - Anticipate and constrain

Background and Overview

- Everything I will say **should be obvious** to all of you
- I am **not** providing / saying anything **classified** as far as I am aware
- Hopefully this will be a "**nothing new**" talk and you are already prepared for everything I will talk about
- If this is NOT true, I am available on a consulting basis...

- BS-EE, MS-IS, PhD-EE
- Computer Viruses
- Info Superhighway
- Management Analytics
- **All.Net** and related sites
- Deception for protection
- Digital forensics
- Sandia National Labs
- Industry Analyst
- Cal Sci
- Angel to Exit

Management Analytics

Before we start

- How to defeat any system:
  - Identify the assumptions
  - Violate them
- Example:
  - What's the precision?
    - 1 microgram at 30 ft?
    - Pass 0.1 microgram every 60 feet as many times as required
- Problem:
  - Identify assumptions how?
- Solution:
  - Experiment
- There is a cost to all sides
  - Leverage to make it economically infeasible and detectable

Management Analytics

Cyber Risks to Nuclear Safety

Fred Cohen 2021

- Looking Ahead
  - Model-based situation anticipation and constraint
- Nuclear Safety
  - Safety
  - Nuclear (and fused)
- Cyber
  - Sensors, Actuators, Communications, Decisions
- Risks
  - Anticipated futures
- What to do about it
  - Anticipate and constrain

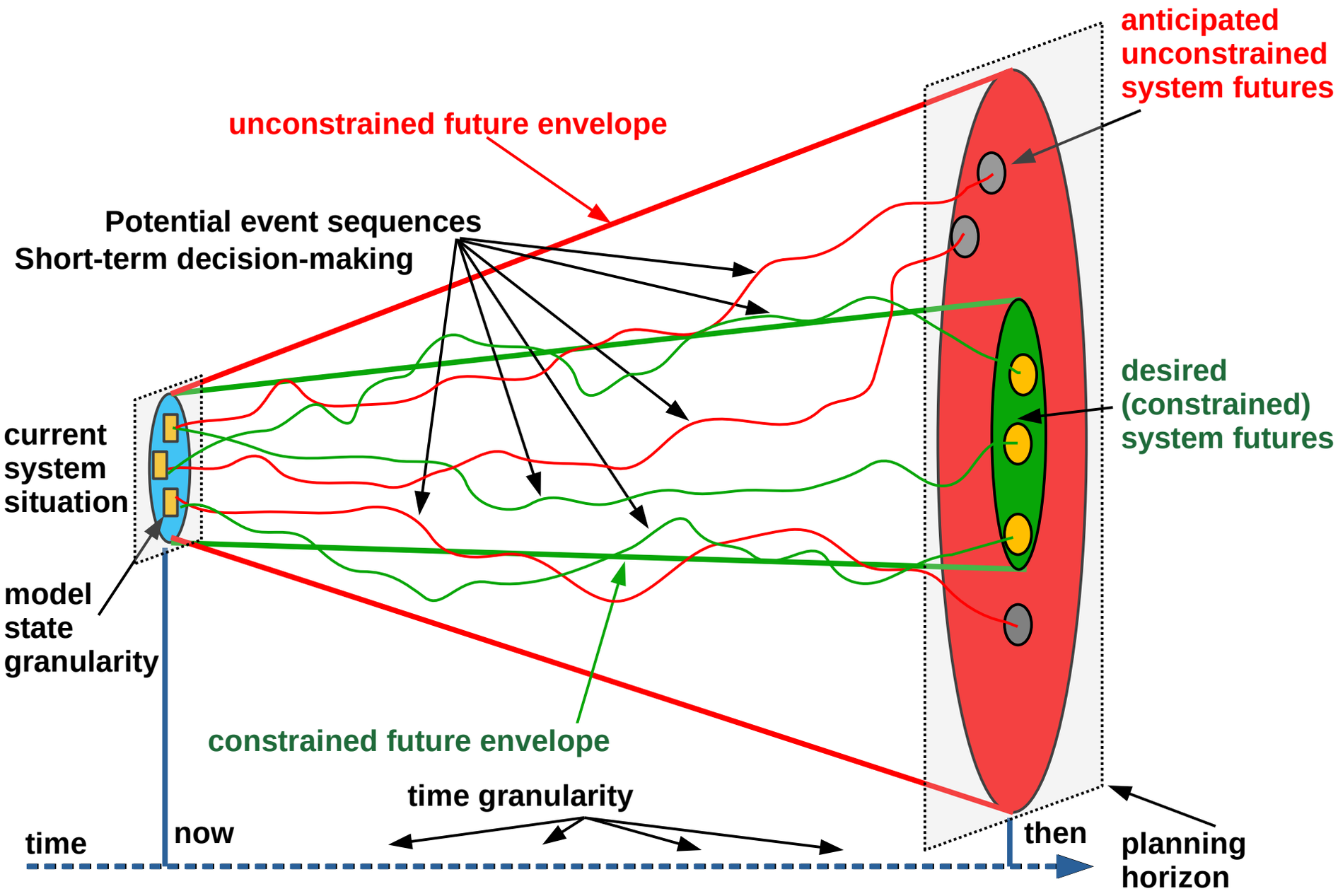
Management Analytics

Anticipated consequences drive decisions

- Unanticipated consequences are ignored
  - Since they are unanticipated… they are ignored
  - But nothing new in cybersecurity since… early 1990s?
  - Unanticipated because we don’t bother to notice it
- Better decision-making comes from what?
  - Better anticipation?
  - More feasible options?
  - Better linkage of options to consequences?
  - More skilled decision-makers?
  - Better tools?
- Likely, all of these…

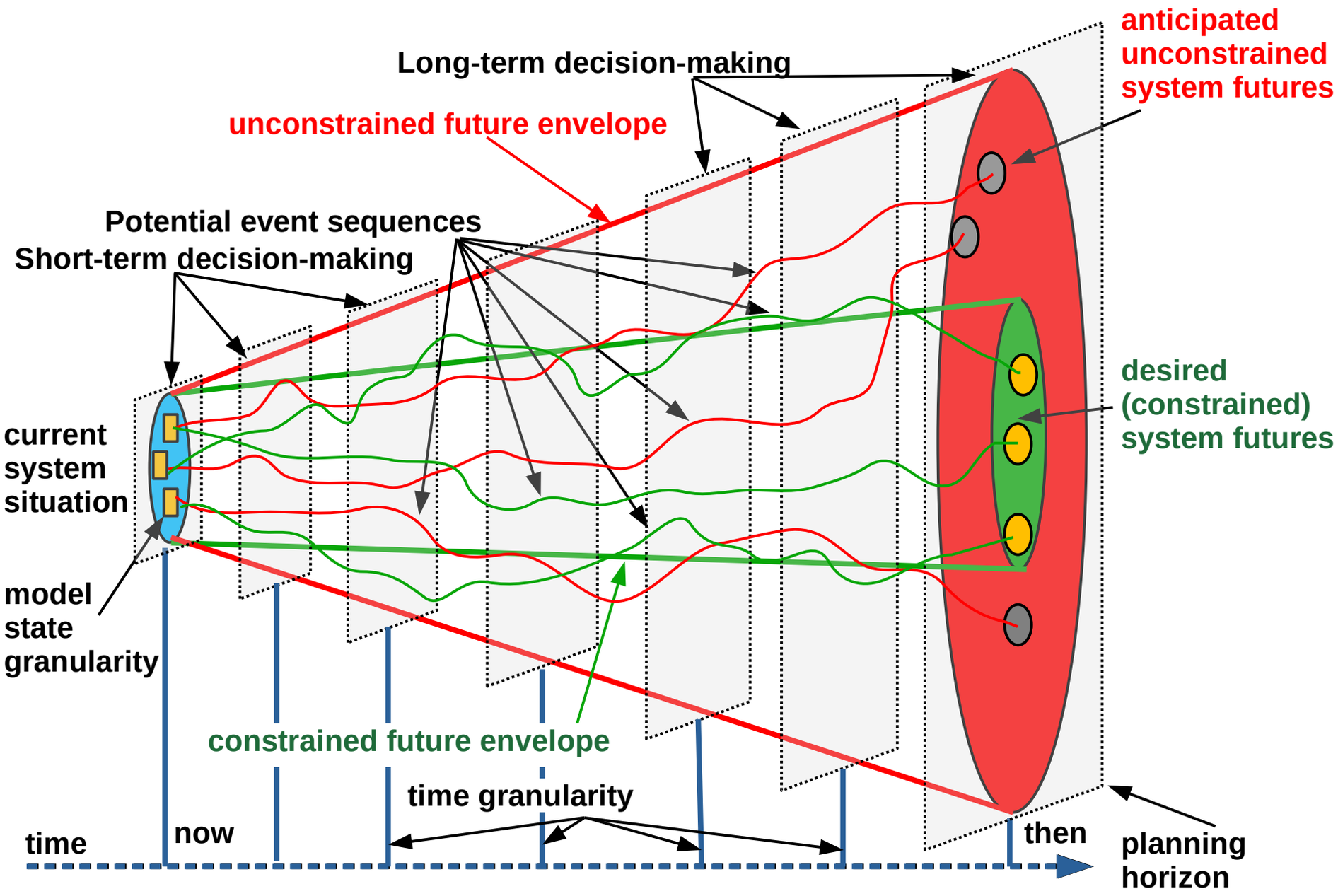
Management Analytics

Model-based situation anticipation and constraint



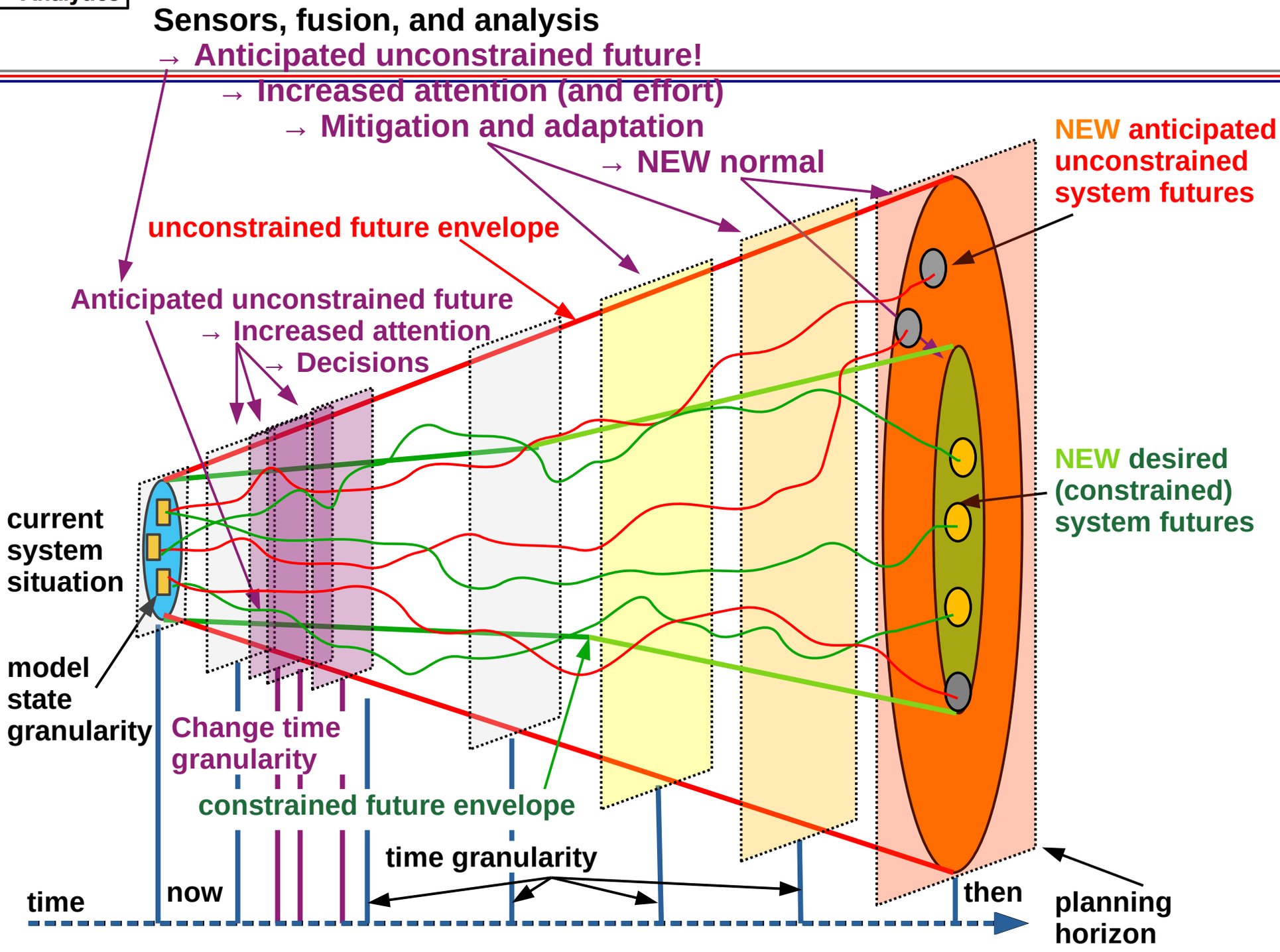
Management Analytics

Model-based situation anticipation and constraint



Management Analytics

Model-based situation anticipation and constraint



Management Analytics

Cyber Risks to Nuclear Safety

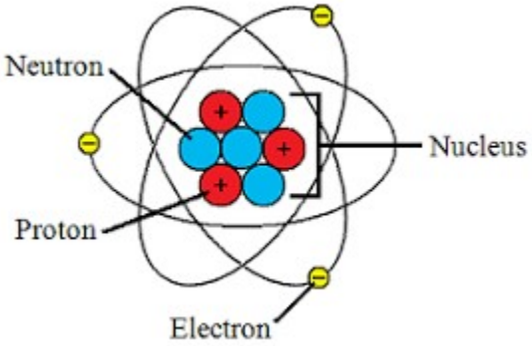
Fred Cohen 2021

- Looking Ahead
  - Model-based situation anticipation and constraint
- Nuclear Safety
  - Safety
  - Nuclear (and fused)
- Cyber
  - Sensors, Actuators, Communications, Decisions
- Risks
  - Anticipated futures
- What to do about it
  - Anticipate and constrain

Management Analytics

Nuclear Safety

- Safety• Nuclear
  - relating to the nucleus of an atom.



    - denoting, relating to, or powered by the energy released in nuclear fission or fusion.
    - denoting, possessing, or involving weapons using nuclear energy.
  - relating to the nucleus of a cell.

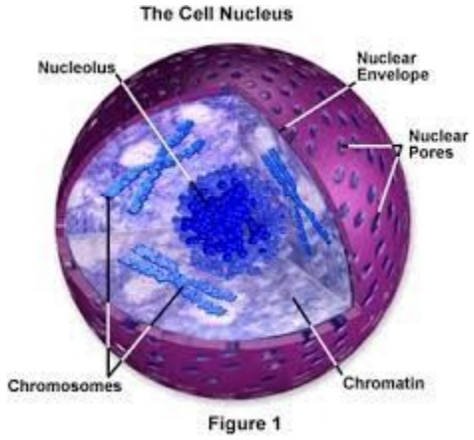


Figure 1

    - "nuclear DNA" – I think this is not at issue here today.
    - However, most of what I will discuss applies to this as well.

Management Analytics

Nuclear Safety

- Nuclear • Safety
  - the condition of being protected from or unlikely to cause danger, risk, or injury.
    - "they should leave for their own safety"
  - a defensive back who normally is positioned well behind the line of scrimmage.
    - I think you were talking about the other one...

- Nuclear Safety (pick the one that applies)
  - A defensive back positioned well behind the line of scrimmage to protect the nucleus of a cell
  - The condition of being protected from the energy released in nuclear fission or fusion and weapons using nuclear energy.

Management Analytics

It’s not just the direct harm

- Direct harm:
  - Protect from the energy released in nuclear fission or fusion and weapons using nuclear energy. (big boom)
- Indirect harm:
  - The cost of protection → Not spending on other things
  - The fear of harm → Disruption of national psyche
  - False positives → Response impacts on national psyche
  - Actual event →
    - Cleanup costs, Economic loss (direct and indirect)
    - Supply chain effects (direct and indirect)
    - Short and long term medical (death → illness → genetic)
    - Potentials for exploitation and escalation at all levels
    - And plenty of other things you could come up with
      - PLEASE DO!!! - Make the more complete list

Management Analytics

It’s not just the direct cause

- Causality: $C \rightarrow^{m} E$
  - Causes work through mechanisms to produce effects
  - Causal chains are transitive $C \rightarrow^{m} E \rightarrow^{m} E \rightarrow^{m} E \rightarrow^{m} E \rightarrow^{m} E \rightarrow^{m} E$
  - Anticipating effects → transitive causal analysis
  - Constraining effects → transitive causal analysis
  - These grow rapidly (exponentially or worse) with
    - Model fidelity (granularity):
      - All the causes, mechanisms, effects?
      - Time granularity and span (planning horizon)
    - Reducing this implies finding (minimal) causality cuts
  - Example terminologies:
    - Supply chain / Interdependency analysis
    - Matching surety to consequence

Management Analytics

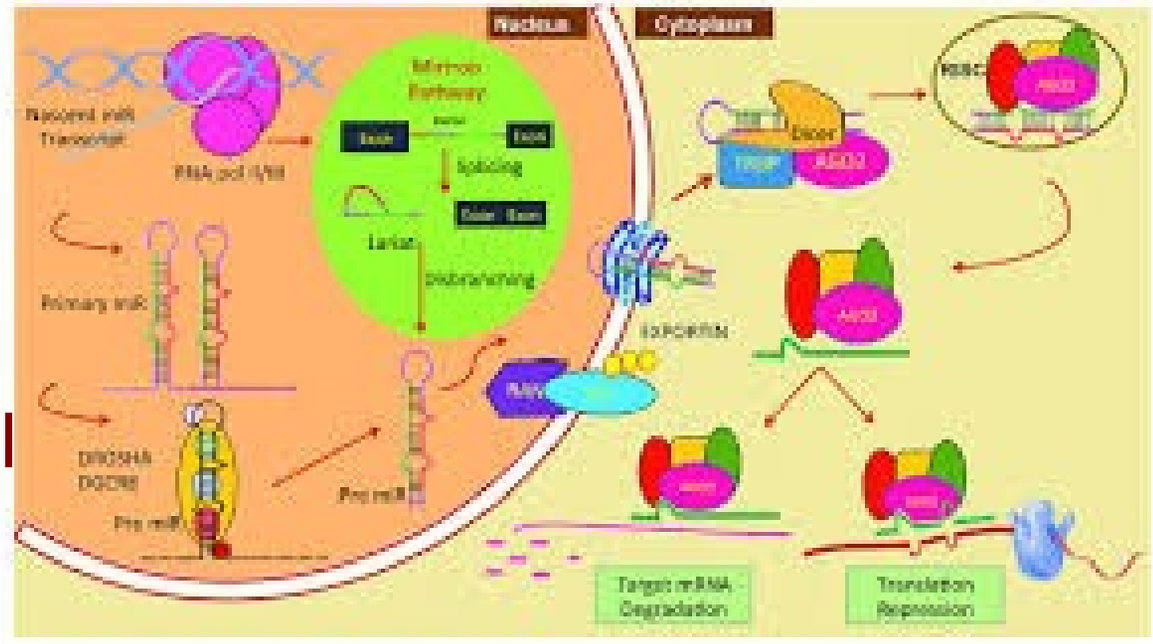
Note: This is not that!

- Incident → Accident
  - NOT INTENTIONAL
  - Does intent matter?
- Big boomer
  - NOT A CONTAMINATION
- Direct consequence focus
  - Indirect consequences may be far higher
- Nuclear → Nuclear
  - Atomic nuclear events also produce biological nuclear events...

Outline of the Accident

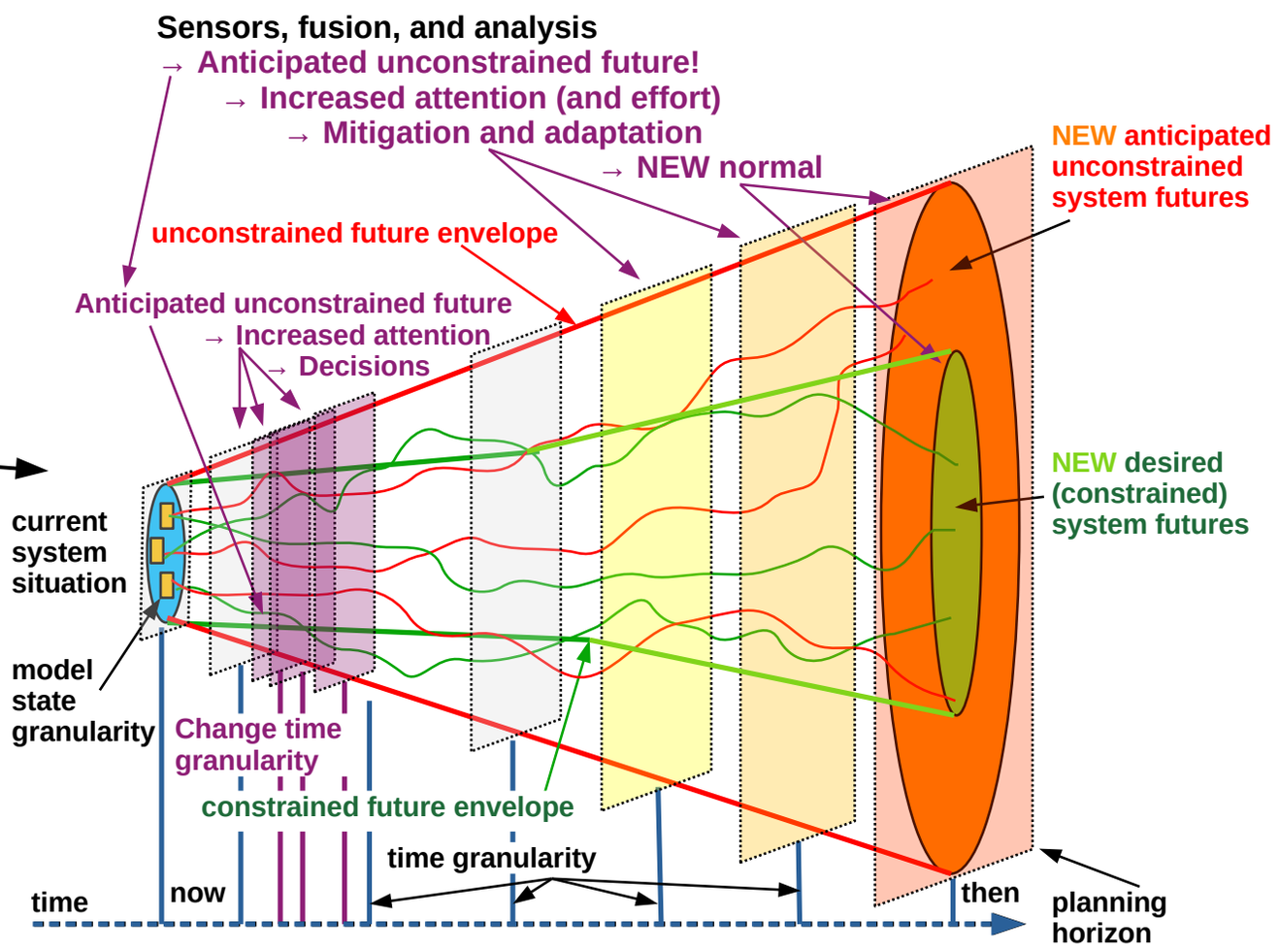
International Nuclear Event Scale (INES)

	Level	Accident examples
Accident	7 Major accident	Former Soviet Union: Chernobyl Nuclear Power Plant accident (1986) Japan: Tokyo Electric Power Company (TEPCO)'s Fukushima Daiichi Nuclear Power Station (NPS) accident (2011)
	6 Serious accident	Provisionally evaluated as Level 7 on April 12, 2011
	5 Accident with wider consequences	UK: Windscale Nuclear Power Plant fire accident (1957) US: Three Mile Island Nuclear Power Plant accident (1979)
	4 Accident with local consequences	Japan: JCO criticality accident (1999) France: Saint-Laurent Nuclear Power Plant accident (1980)
Abnormal incident	3 Serious incident	Spain: Fire at Vandellos Nuclear Power Plant (1989)
	2 Incident	Japan: Damage to steam generator heat exchanger tube at Unit 2, Mihama NPS (1991)
	1 Anomaly	Japan: Sodium leak accident at Monju (1995) Japan: Primary coolant leak at Unit 2, Tsuruga NPS (1999) Japan: Pipe rupture in the residual heat removal system at Unit 1, Hamaoka NPS (2001) Japan: Pipe failure in the secondary system at Unit 3, Mihama NPS (2004)



Nuclear Safety in Context

- Nuclear Safety (pick the one that applies)
  - Protect from the energy released in nuclear fission or fusion and weapons using nuclear energy.
- How do we do this?
- By using this?



Management Analytics

- **Uncle Bill's Truck Full of Smoke Detectors**

Cyber Risks to Nuclear Safety

Fred Cohen 2021

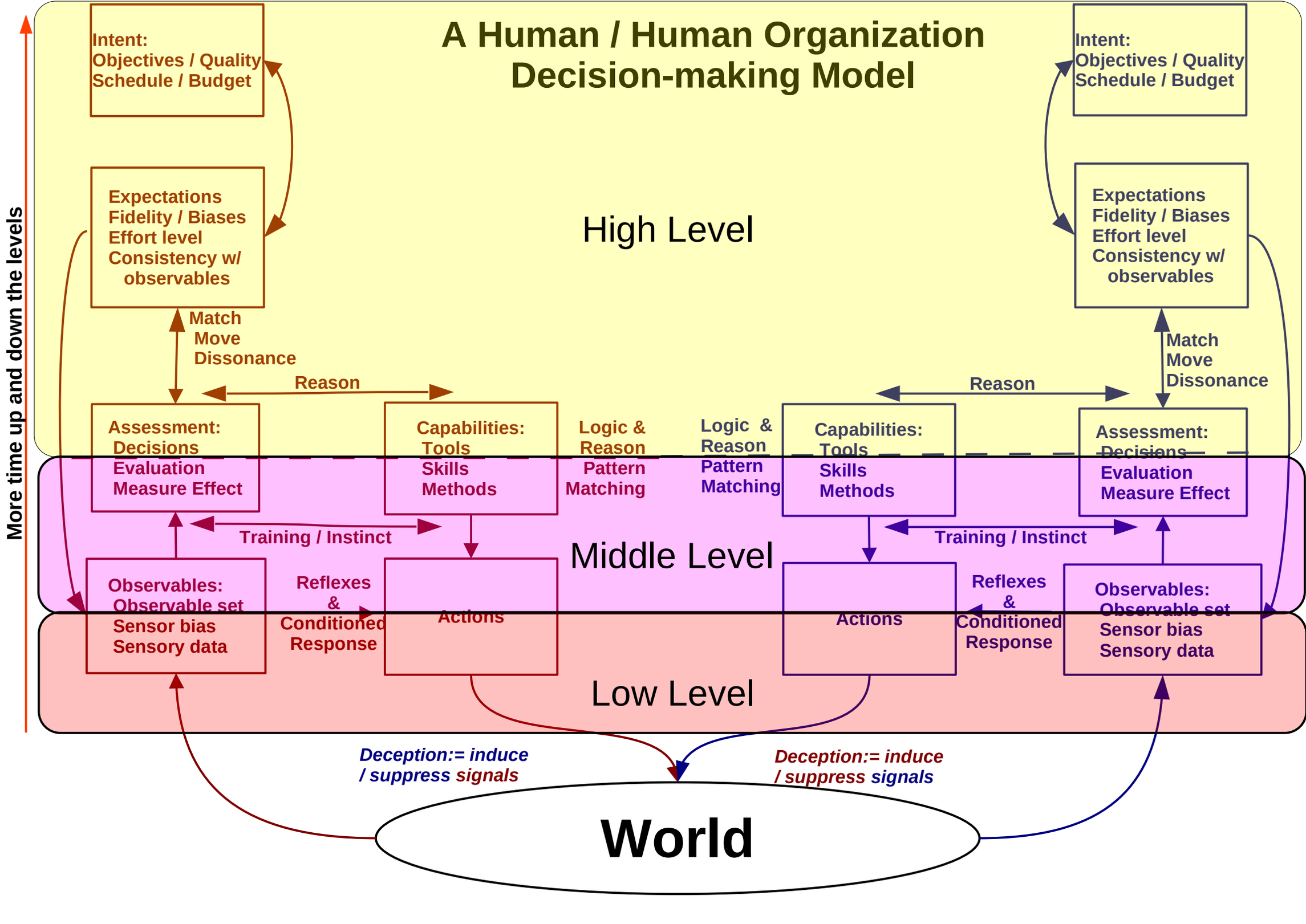
- Looking Ahead
  - Model-based situation anticipation and constraint
- Nuclear Safety
  - Safety
  - Nuclear (and fused)
- Cyber
  - Sensors, Actuators, Communications, Decisions
- Risks
  - Anticipated futures
- What to do about it
  - Anticipate and constrain

Management Analytics

Cybernetic systems

- Cyber:=
  - Sensors
  - Actuators
  - Communication
  - Control (decisions)
- In all dimensions
  - Physical
  - Psychological
  - Financial
  - Sociological
  - Others?
- Offense (make it unsafe)
  - Apply cybernetic systems to cause harm
- Defense (make it safe)
  - Deter, Prevent, Interdict, Detect, React, Adapt
- Using cyber against anything
  - Anything used against cyber
- Across the spectrum of conflict
  - Peace to war and back

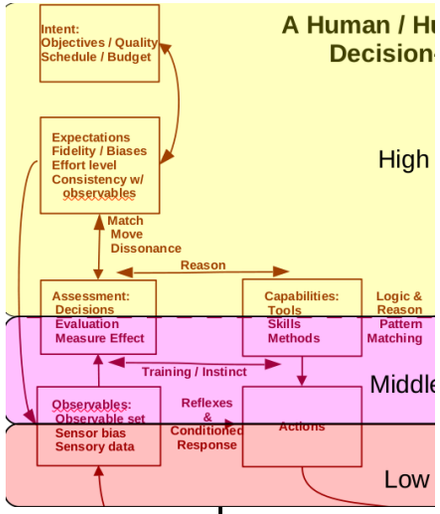
A many-player, finite but unbounded memory, real-time, simultaneous, non-zero-sum game with partially shared memory and uncommon objectives – in an infinite dimensional Hilbert space

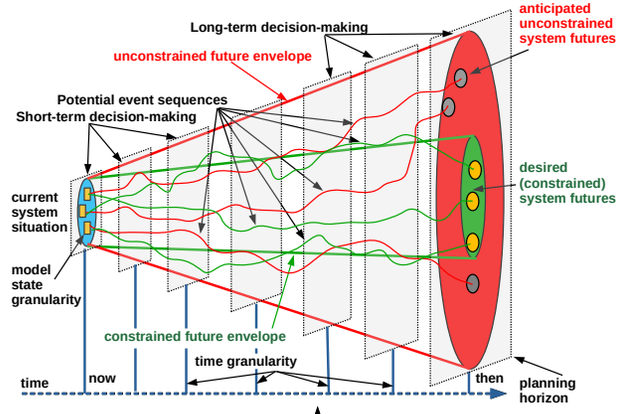

A Human / Human Organization
Decision-making Model
More time up and down the levels
Intent:
Objectives / Quality
Schedule / Budget
Expectations
Fidelity / Biases
Effort level
Consistency w/
observables
Match
Move
Dissonance
Reason
Assessment:
Decisions
Evaluation
Measure Effect
Capabilities:
Tools
Skills
Methods
Logic &
Reason
Pattern
Matching
High Level
Middle Level
Low Level
Training / Instinct
Observables:
Observable set
Sensor bias
Sensory data
Reflexes
&
Conditioned
Response
Actions
Deception:= induce
/ suppress signals
World

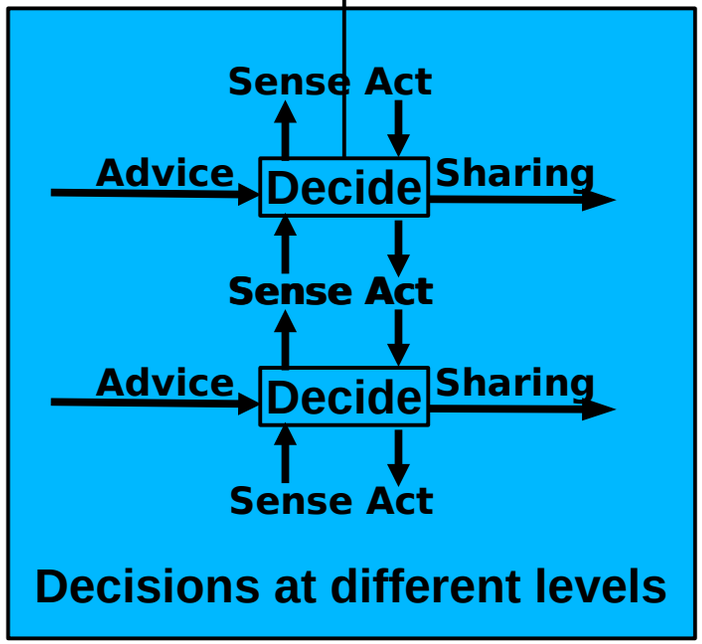
Management Analytics

How decisions get made

- Decision-makers
  - Have a model
    - In their minds / Formalized?
  - Get additional information
    - From advice and sensors
    - From “above” and “below”
  - Update their model
    - Internally and structurally
  - Make decisions
    - Internal decision and justification
  - Act on them
    - By sending information
  - Loop







Management Analytics

Cyber Risks to Nuclear Safety

Fred Cohen 2021

John's nuclear car

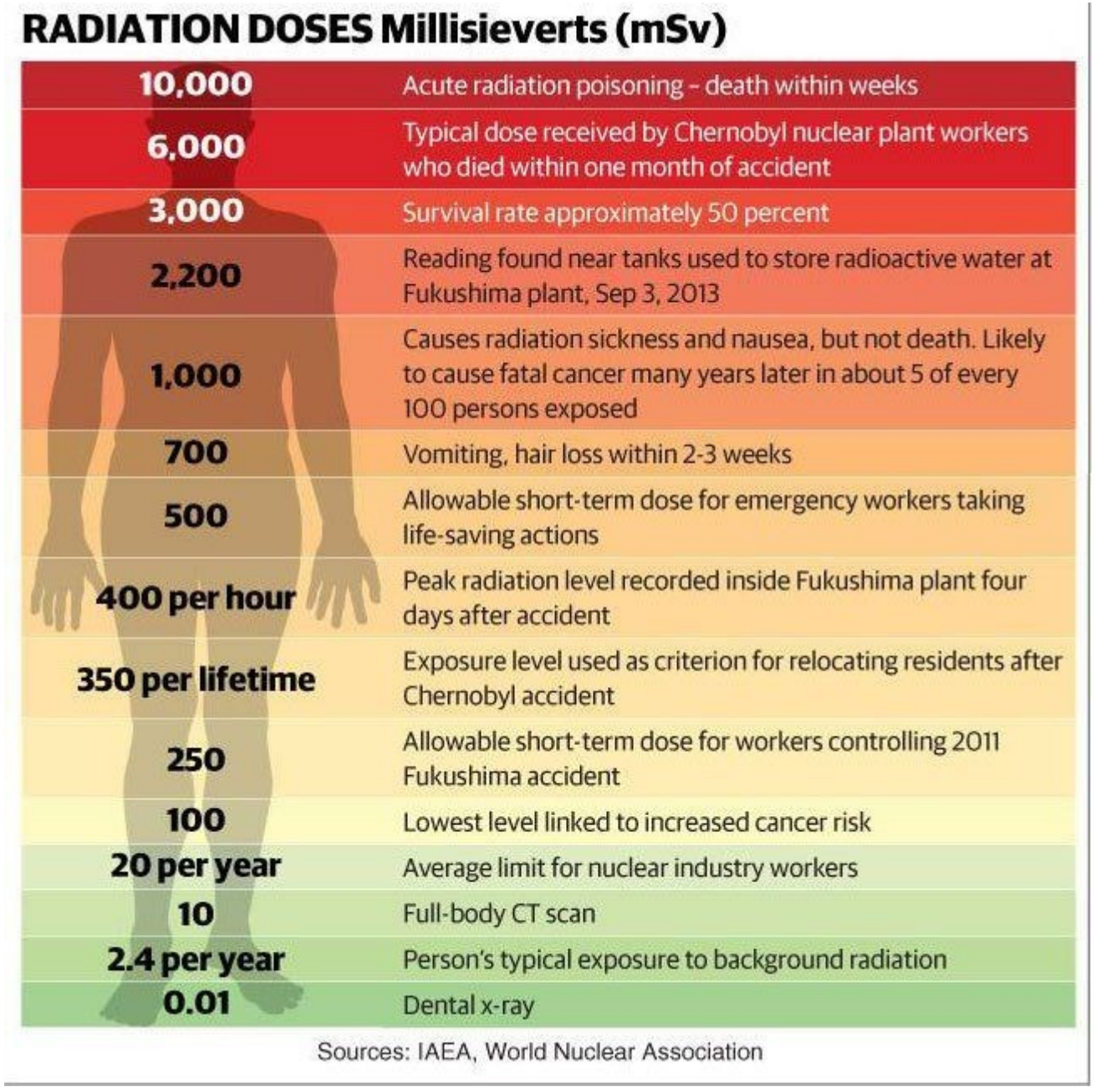
- Looking Ahead
  - Model-based situation anticipation and constraint
- Nuclear Safety
  - Safety
  - Nuclear (and fused)
- Cyber
  - Sensors, Actuators, Communications, Decisions
- Risks
  - Anticipated futures
- What to do about it
  - Anticipate and constrain

Management Analytics

My Father's microgram → milligram

Yes – human doses are important

- What is the dosage effect on cybernetic systems?
  - Cyber systems have radiation-related damage as well
  - What doses have what effects on cybernetic systems?
  - Where is the dosage chart and what are the consequences and indirect effects on everything else?



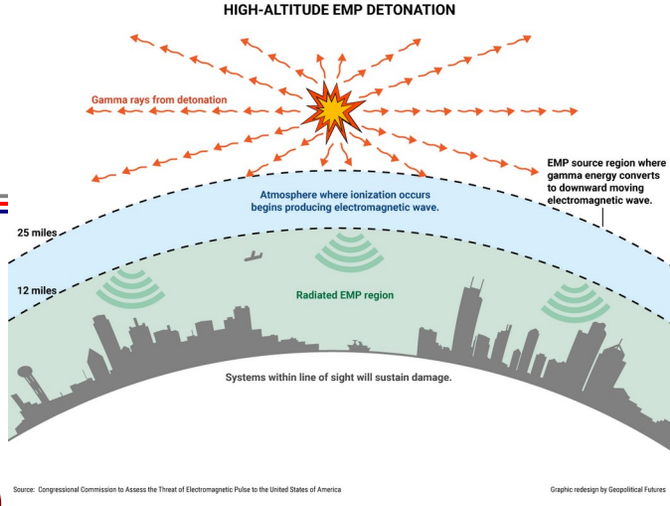
Management Analytics

What could go wrong?

- Physical events:
  - Nuclear stuff has to get there (where?)
  - It has to come from somewhere (else?)
  - It can get there at any speed over any route in any parts
  - It may have to do something to be worth worrying
- Stuff:
  - All forms including precursors
  - Conservation of matter (pre-boom)
    - It has to come from somewhere to get somewhere
    - Where is it **all** now? How sure are we?
  - All paths from sources to targets (ST graphs)
    - How much has to get there and how much shrinkage?

Management Analytics

What could go wrong?



- Physical events:
  - Nuclear stuff has to get there (where?)
  - It has to come from somewhere (else?)
  - It can get there at any speed over any route in any parts
- Routes:
  - Under ground / Under water
  - On ground/ On water
  - In the air
  - Outer space
  - Sequences of all of these
  - In as many parts as desired
  - Hand grenades & horse shoes

1,000,000 UxVs
- **S**ubmersibles
- **A**erial
- **G**round crawlers
- **A**ir/**S**pace dropped
- Combos (**SAGAS**)
- Independently operating
- Aimed at 1000 or more targets
- Launched at different times
- From different places
- Each a unique look and feel
- Different size/shape/color

They don't need to combine

Management Analytics

What could go wrong?

- Physical events:
  - Nuclear stuff has to get there (where?)
  - It has to come from somewhere (else?)
  - It can get there at any speed over any route in any parts
- Concealment:
  - In what quantity in what packaging?
    - How sensitive is detection?
    - At what radius from detector?
    - Against what signal reduction methods?
    - In the presence of what noise levels?
    - How many false positives/negatives can we stand?
  - The boiling frog attack

Management Analytics

What could go wrong?

- Physical events:
  - Nuclear stuff has to get there (where?)
  - It has to come from somewhere (else?)
  - It can get there at any speed over any route in any parts
- Detection:
  - How sure are we of the detectors?
    - The supply chain and operational protections
    - The cybernetic system that applies them
    - Are they detecting the right things? Can we false+
    - Can they detect them in time? Can we slow them?
    - How many do we need to cover what?
    - e.g., 1,000,000 SAGAS disbursed could drive insanity
      - Even the credible threat of it could have serious effects

Management Analytics

Exploring the space

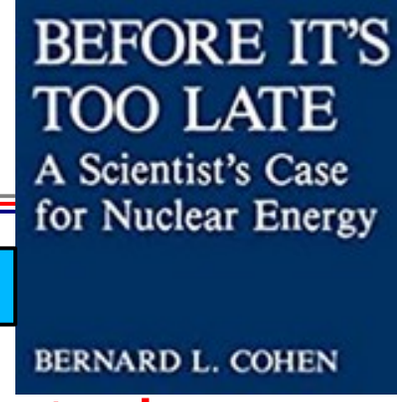
- That was just one small part of the larger puzzle
  - Physical attack getting nuclear material there to here
- Expanding on this:
  - What about the stuff that is already here?
    - Cyber systems protect and account for it
      - Attack those systems to cause desired effects
    - People end up being a possible weak link
      - Use cyber as part of elicitation and turning
  - What about getting the stuff to somewhere else?
    - Hit the supply chain of the West not in the most protected place in the world
  - What about using our own mechanisms against us
    - Get into our systems and cause them to act for them

Exploring the space

- What about getting stuff already there to go wrong?
  - Cause a plant to go critical?
    - Not connected to the world?
      - How do I control it when there is a Fukashima?
      - There are people there who can do it…
  - Cause a bomb to go boom? (They are made to do that)
    - Bombs are meant to go boom (or splat or in between)
      - Is a one in a million chance good enough? What is?
      - Every once in a while we accidentally … can you make it intentionally happen? Can we put the toothpaste back?
  - Cause a therapy machine to radiate people?
    - It has already happened
      - But what about all/lots of them?
  - Cause a process to create/do the wrong stuff?
    - Cause a centrifuge to …

Management Analytics

Exploring the space



1983

- And examples from other dimensions?
  - Psychological

Anti-nuclear power movement → Global climate change

    - Creating the perception that this is happening
      - Or could be happening
    - Create a minor event to demonstrate capability
      - Even if that's all you have, you can still threaten
  - Financial
    - Get the right people afraid enough to support defense
      - We use unlimited funds forever against the possibilities
        - I am available on a consulting basis – spend all you like
        - I can give this talk to congress for added budget
  - Sociological
    - Create fear in the society to sway elections
      - Oops – that is being done all the time anyway
  - Others?

Management Analytics

Cyber Risks to Nuclear Safety

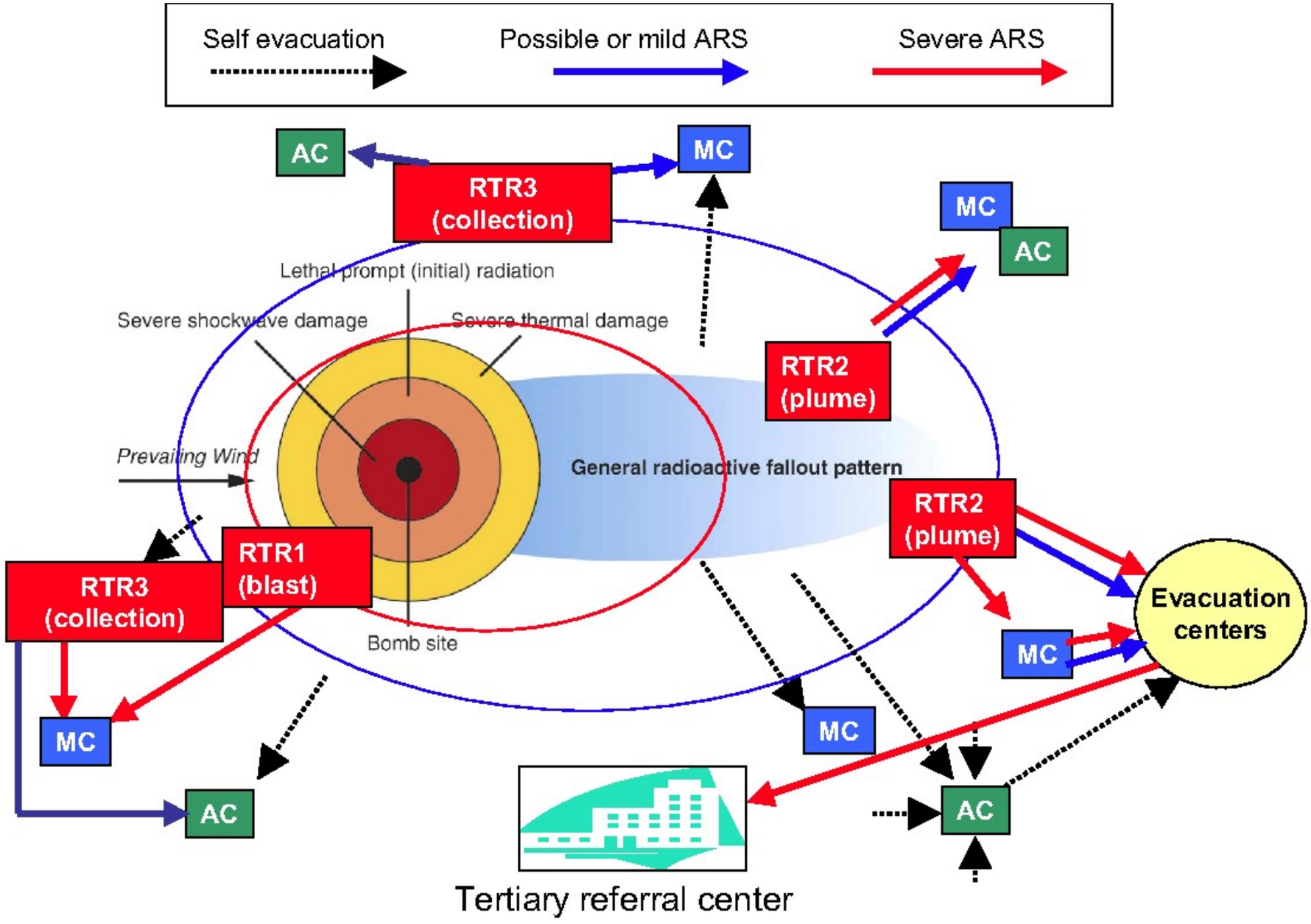
Fred Cohen 2021

- Looking Ahead
  - Model-based situation anticipation and constraint
- Nuclear Safety
  - Safety
  - Nuclear (and fused)
- Cyber
  - Sensors, Actuators, Communications, Decisions
- Risks
  - Anticipated futures
- What to do about it
  - Anticipate and constrain

Management Analytics

Run Away!!!

- Reacting to a nuclear event

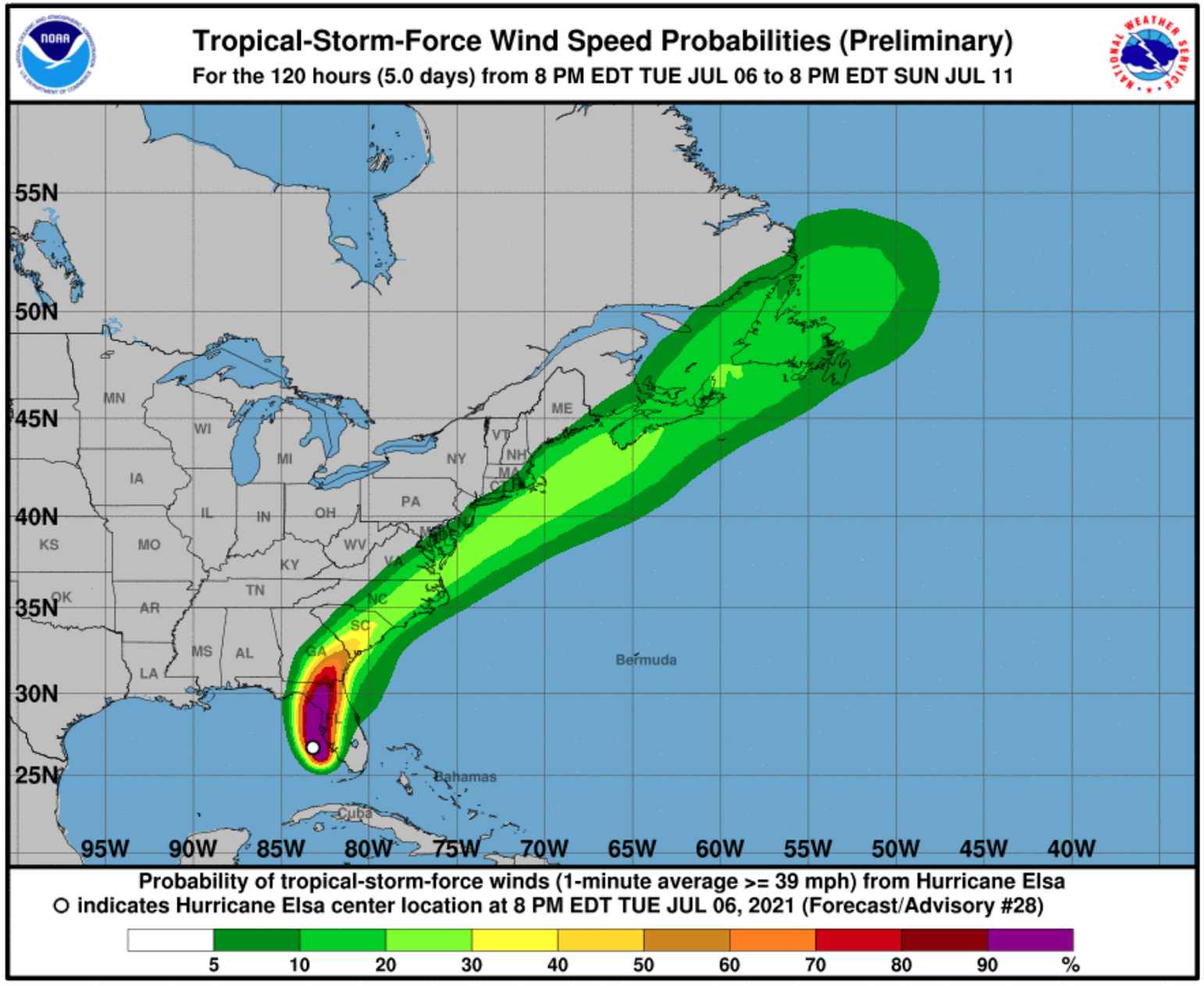


hematic for triage and response to a large-scale radiation event developed by the Office of the Assistant Secretary for Preparedness and

Management Analytics

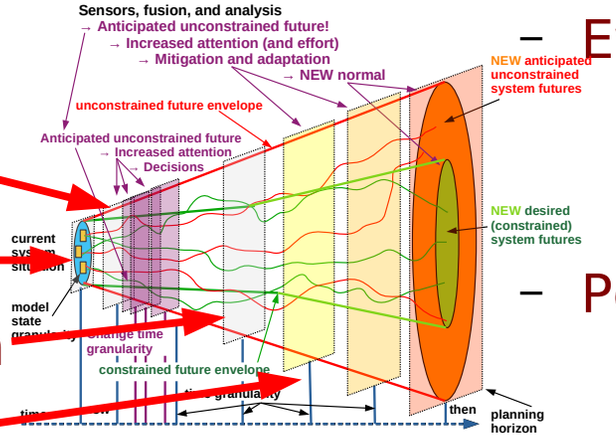
We do this for weather

- Model-based situation anticipation
  - And run away

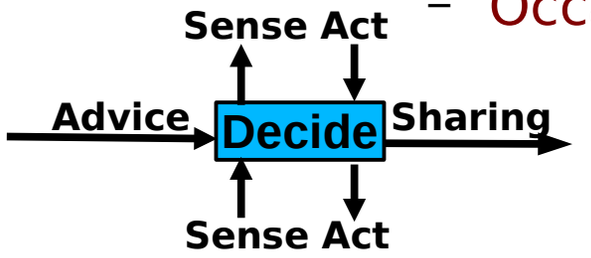


Parameters of the decision-maker

- At a low level:
  - Available observations (sense)
  - Available effects (acts)
  - Available advice
  - Decision capacity
  - Available time
- Decision modes:
  - Emergency
  - Day-to-day
  - Event-driven
  - Periodic
  - Occasional



- Decision modes:
  - Emergency
    - Consequence (t) → tempo
    - High load
  - Day-to-day
    - Standard time/load/consequence
  - Event-driven
    - Standard time/load/consequence
      - Drives new modes
  - Periodic
    - Designated time/load/consequence
      - Consequence-based times
  - Occasional
    - Ad-hoc time/load/consequence



Management Analytics

Organizational Decision-Making Design

Ownership and Board Cognitive System

Intent: Self image and World image / Knowledge, theories, models of people, systems, and the World

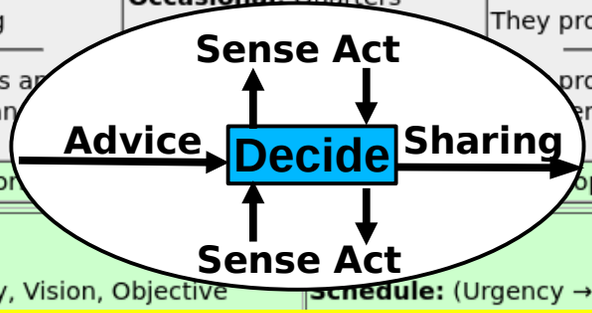
Objectives: (Assessment → Defined problems) Board sets quarterly and annual performance and growth goals and identifies overall strategic objectives.	**Quality:** (Personality, Vision, Objective Driven) Board sets values and vision.	**Schedule:** (Urgency → Timing) Board identifies strategic time frames for identified objectives.	**Budget:** (Importance → Spending) Board reviews and opines on budgets and uses internal audit to verify that expenditures are properly allocated.

Outside Sources Personal and Professional and Platforms and Groups and Legal and Regulators and Auditors	Information is received by the Chairman and Board and CEO → → They get external Advice and Intelligence ↑ They get internal Advice and Intelligence and Feedback and Notifications and Conditions and Analysis and Audits	***Decision Time Frames*** **Emergency:** Hours **Urgent:** Days **Timely:** Weeks **Day-to-day:** Quarters **Periodic:** Quarters **Occasional:** Years	→ Decisions are made and executed by the Voting Members They provide outbound Influence and Sharing → They provide internal Advice and Influence and Requirements and Directives ↓	**Ownership Control** Understand Business and Define Duties

NOTE: Matching I/O and [timing → consequence] are critical

Top Management Cognitive System

Outside Sources Personal and Professional and Groups and Legal and Advisors and Auditors	↑ They provide internal Advice and Intelligence and Feedback and Notifications and Conditions and Analysis and Audits Information is received by the CEO and Executive Team → → They get external Advice and Sharing ↑ They get internal Feedback and Alerts ar… Notifications and Conditions and Data an… Analysis and Responses and Audits	***Decision Time Frames*** **Emergency:** Minutes **Urgent:** Hours **Timely:** Days **Day-to-day:** Weeks **Periodic:** Quarters **Occasional:** Quarters	↓ They receive internal Advice and Influence and Requirements and Directives → Decisions are made and executed by the CEO and Executive Team They provide outbound Influence and Sharing → …provide internal Advice and Influence and …ements and Directives and Policy ↓	**Executive Control** Understand Business and Define Duties and Manage Risk and Specify Operations and Verify Operations



Intent: Self image and Wor… …ople, systems, and the World

Objectives: (Assessment → Defined problems) CEO works with board to define and assess performance and growth goals and for… manage… roll-ups … paths forwa… completing…	**Quality:** (Personality, Vision, Objective	**Schedule:** (Urgency → Timing) Based on	**Budget:** (Importance → Spending) CEO works with top executive team to identify… …ch

All of this introduces ways to get in your OODA loop

Russians have a name for it … "Reflexive Control"

Management Analytics

Some high level options

- Deter
  - Can we attribute material and actions to actors?
    - Forensics and tagents are feasible against holders
    - Strong intelligence and treaty terms support this
  - If so, we can threaten retaliation
    - And we can certainly retaliate

- Prevent
  - Limiting who has it and protecting it well
    - A well worn path always in need of improvement
- Interdict, Detect, React, Adapt
  - Figure it out en route from there to here (or here to here)
  - Indications and Warnings with actions in time frames

Management Analytics

Some high level options

- Deter, Prevent, Interdict, Detect
  - After “GO” before “GONE”
    - The NEST team(s) → Next Generation Version
  - At boom (or during slow boom)
    - The NEST team(s) → Next Generation Version
  - After boom – how soon?
- React
  - Evacuation / Shelter in place / Medical / Economic / Psychological / Sociological / Geopolitical / Supply chain
- Adapt
  - Try doing it in anticipation to constrain if possible
    - And keep adapting as the world keeps changing

Management Analytics

To summarize

- This is a hard set of issues
  - "Problems worthy of attack, prove their worth by fighting back"
    Alan Perlis – Turing Award Winner
- Too bad... we have to deal with them
  - Model-based situation anticipation and constraint
    - Or we could just try to guess right
- The real battle is the battle of wills and wits
  - The ability to model and constrain
    - Modeling is actually the hard part of this
      - Including the intelligence that has to go with it
      - Attack graph generation and analysis
        - Generate alternative moves for all parties – seek cuts
        - Computational limits on fidelity and planning horizon
    - Assume they are doing this as well… A battle of wits

Management Analytics

The battle of wits and wills

- The world is full of these mechanisms
  - 7.8B of them and growing
  - PLUS the artificial ones
- Who can out-think whom?
  - How do we augment our thinking?
- As you think, you need to build
  - Advanced real-time manufacturing
- As you build you need to deploy
  - Custom real-time cybernetic systems
- As you deploy, they deploy
  - The new (better/faster/cheaper) arms race!