Transitioning to Autonomy: Special Challenges for High Reliability Systems

Paul R. Schulman
Department of Government
Mills College
Oakland, CA U.S.A.

Center for Catastrophic Risk Management
University of California, Berkeley

Wednesday, March 11, 2015

Beginnings of HRO Research

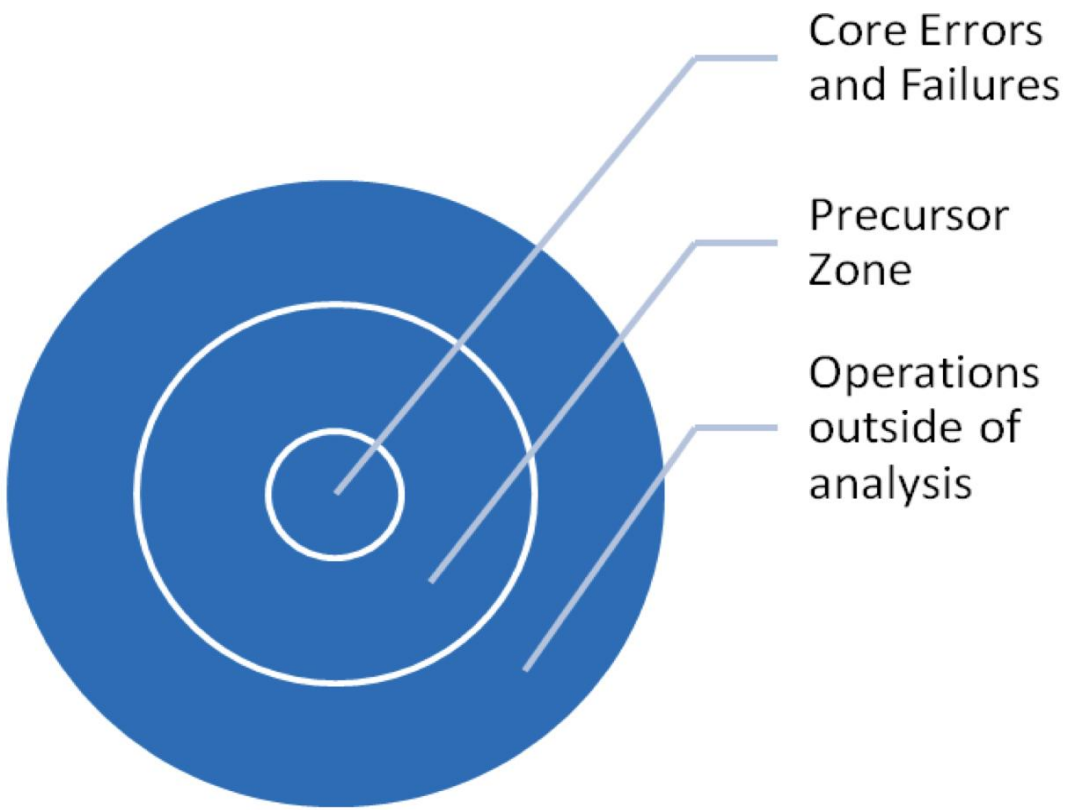
Diablo Canyon Nuclear Power Plant

California High Voltage Electrical Grid

Challenges for HROs

- Unforgiving environments
  - -- public “dread” of catastrophic failure
  - -- low tolerance for failure or mistakes
  - -- limited opportunities for trial and error
- High and continuous demand for service

Core, Precursor and Uncertainty Zones in HROs



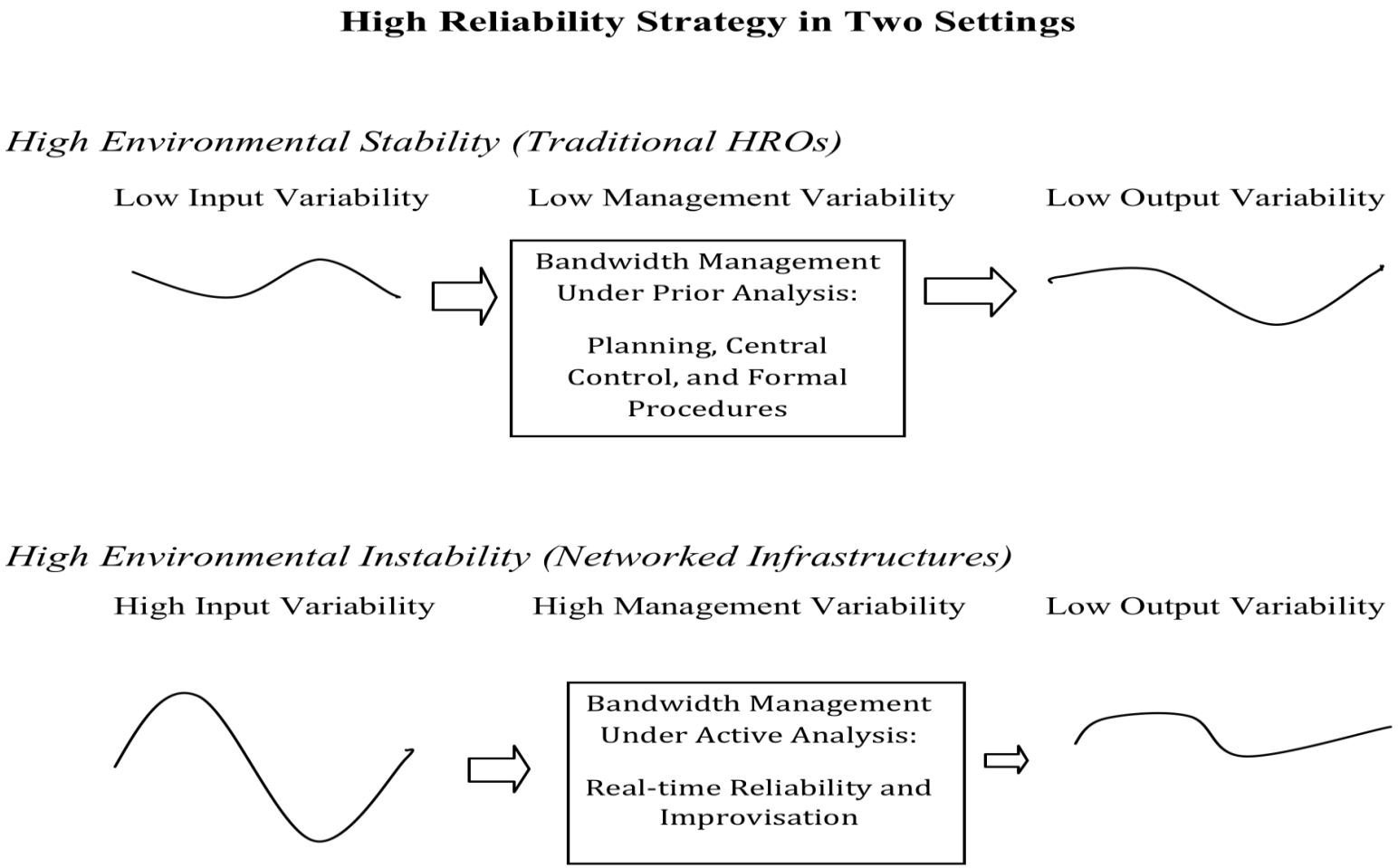
High Reliability: A Conclusion From Observations

High reliability is not invariance but bounded fluctuations in processes and outputs:

- Renewing mindfulness
- Reinforcing credibility
- Restoring trust
- Resolving ambiguity

CAISO: A Special HRO

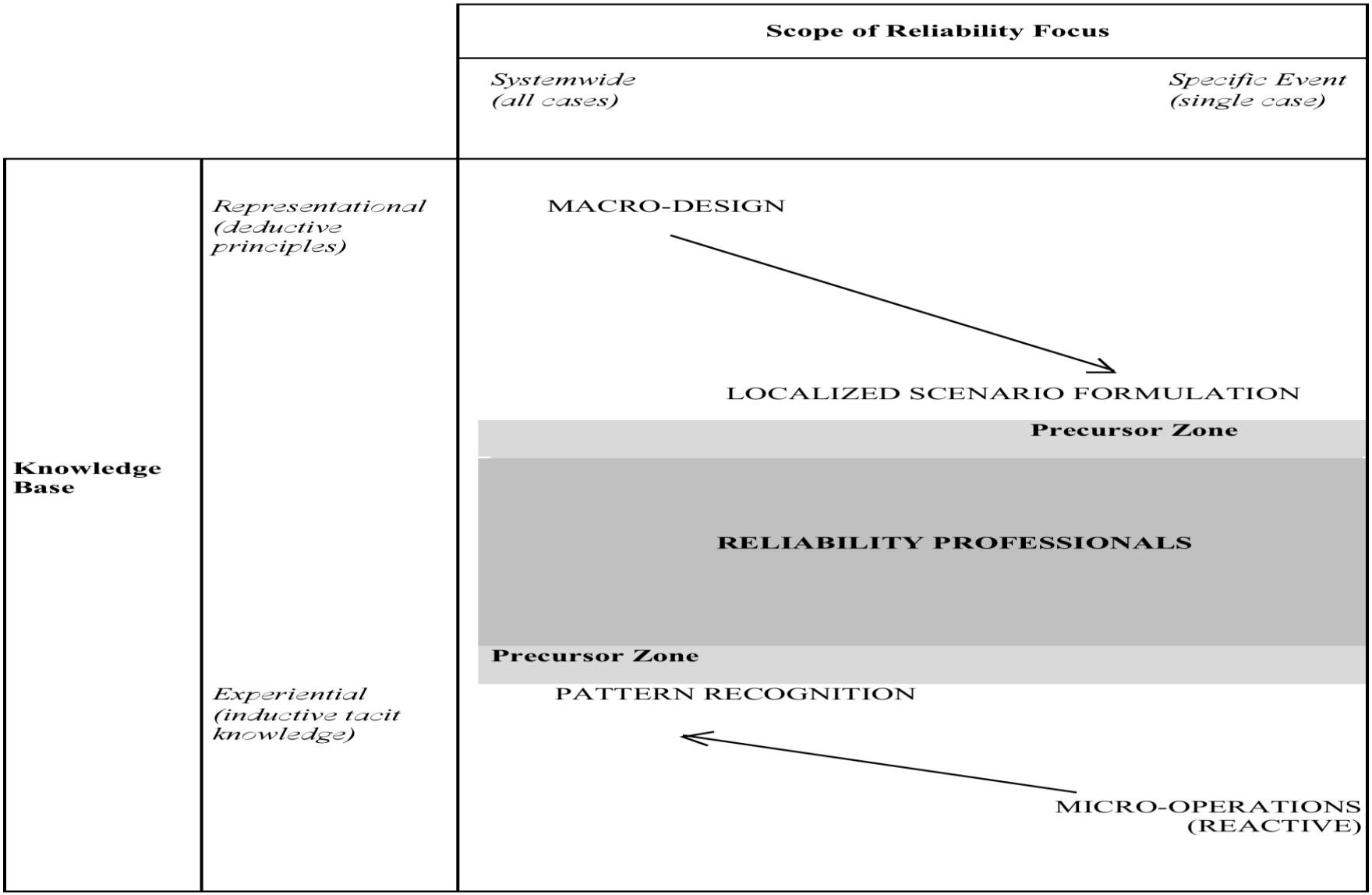
HIGH RELIABILITY STRATEGY IN 2 SETTINGS



Classic HRO vs Resilience Models of High Reliability

Classic HRO	Resilience-Focused
• Standardized raw material; repetitive problems	Unstandardized materials; large problem variety
• Command and control of system inputs and outputs; low input and output variance	High input variance; low output variance; high process variance
• Formal knowledge covers system behavior	Important role for experiential and tacit knowledge
• Action under anticipatory analysis	Important improvisational real- time actions

Reliability Space and its Precursor Zone



Who are Reliability Professionals?

- Individuals, generally part of teams, who have special perspectives on reliability and safety -- cognitively and normatively.
- They mix formal deductive and experiential knowledge in their understanding of the systems they operate and manage.
- Their view of “systems” is larger than their tasks and frequently centered on real-time operations.
- They internalize norms and invest their identity in the reliable and safe operation of their systems.

Performance Modes for the CAISO control room

		System Instability	
		High	*Low*
Network Options Variety	*High*	Just-in-time performance	Just-in-case performance
	Low	Just-for-now performance	Just-this-way performance

Risks in Transitioning to Autonomy

CAISO: A Tale of Two Automation Transitions

- Real-Time Market Application (RTMA) and
- Market Re-Design and Technology Upgrade (MRTU)

RTMA : A software-based system for energy dispatching (adopted in 2004)

- Search for least cost optimization in real-time energy imbalance market dispatching
- Multiple variables optimized in 5 minute grid “solutions” and dispatches
- “The RTMA software implemented in October 2004 was designed to reduce the frequency and degree of dispatcher judgment or intervention required to run the real-time imbalance market.”

CAISO RTMA Assessment Report (2005)

RTMA (Cont'd)

- Early obvious dispatching errors
  (e.g. 5 million megawatts dispatched)
- Later input and output errors harder to detect
- Operators lost the ability to understand the logic of some RTMA dispatches
- Increased volatility of unit dispatches (complaints by numerous unit operators)
- Major operator work around: biasing load forecasts to "adjust" RTMA dispatches
- Software engineers used operator work arounds to "tune" the RTMA software

MRTU: A comprehensive system to automate a day-ahead electricity market to replace real-time markets.

- involved not only CAISO but also other players -- generators and distribution utilities.
- included a "state estimator" – multiple variable model to track state of the grid at all times
- an expert system for energy scheduling and unit dispatching
- imports *information* from operators, but not their real-time *capacities*
- A *substitutional*, not *supplementary* automation

MRTU (Cont'd)

- an attempt to replace real-time cognitive processes of operators, by embedding prior contingencies they've developed into the logic of "if … then" contingencies in the software instructions
- multiple state variables, 3000 market pricing points ("nodes") , fast market solutions and dispatches
- Shorter response times but longer time to diagnose causes of dispatching error
- Implementation all at once and not in pieces

MRTU: Operator Comments

- “MRTU has become finer grained, even a difference of 1 megawatt can make a huge difference now. This is beyond the detectability of the operator.”
- “MRTU squeezes every megawatt out of the system and we have nothing left to help out without cutting into our reserves.”
- “You end up paying attention to precisely that which was promised as making your attention to other matters all the easier.
- Project managers said "the control room would rise to the occasion just as it had in the past, and make sure it worked”. "Yes, that true, we rose to the occasion, but with MRTU it went on too long and took far too much attention than we should have had to give it.

Reliability Risks in *transition* to automated systems

- movement of operators into precursor performance zones
- diversion of operator attention to design details of a new system
- loss of "clawback" options with commitment to comprehensive non-modular implementation
- Use of 30% 60% and 90% design reviews and safety assessments?

Reliability risks in *operation* of automated systems

- As transaction speed and complexity increase, control operators can lose an experiential frame-of-reference for what's happening and why it's happening
- Optimizing strategy associated with many automated systems can reduce margins and slack that buffer error.
- Modelling error or modelling data error may be undetectable or uncorrectable by operators leading to control errors of misrepresentation.

Errors in Matching Time and Scope

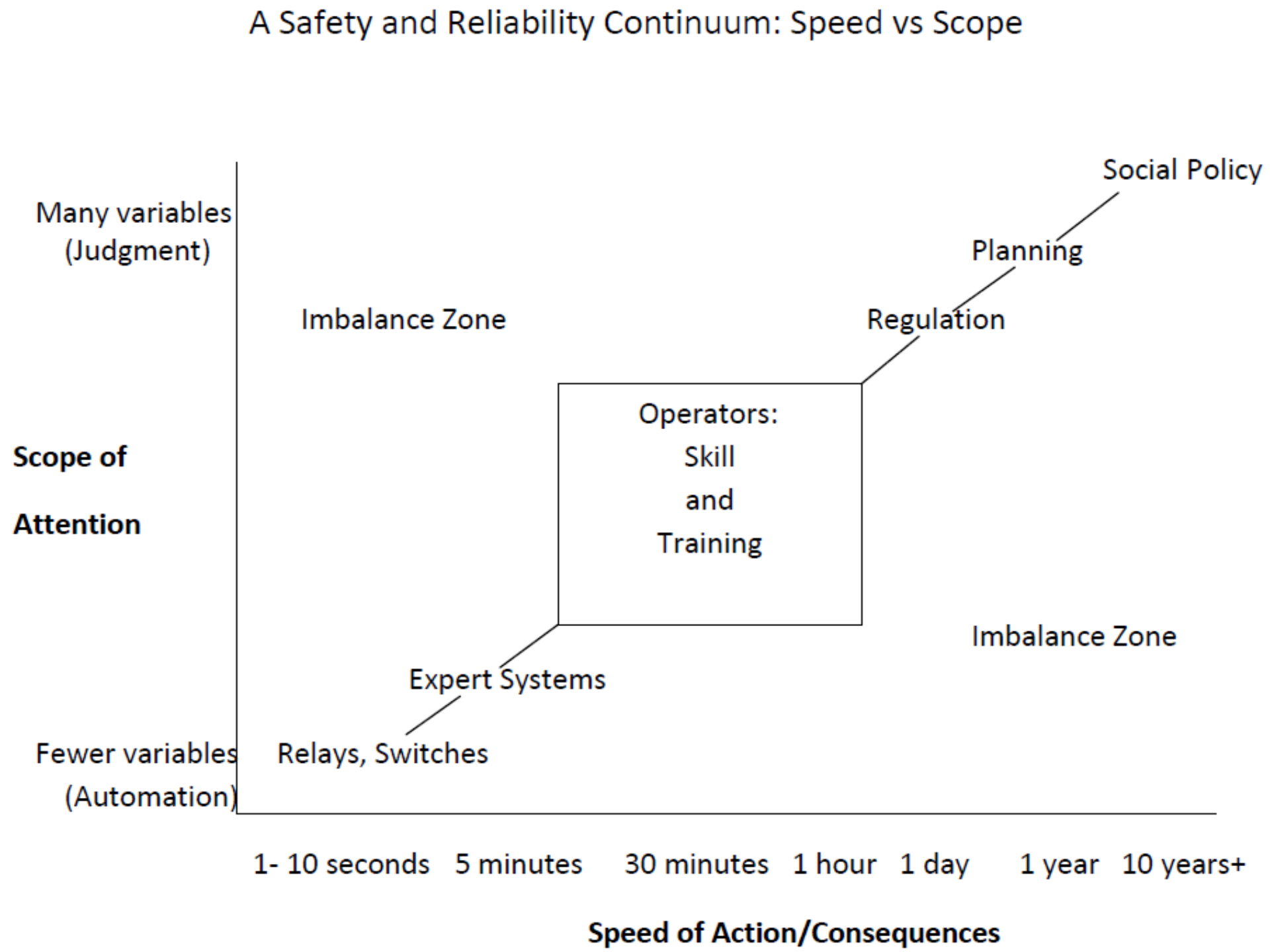
- An important source of reliability in automation is to match appropriately the speed of action to the need and speed of judgment.
- This can mean fast automated action to reach safety in situations where human judgment is too slow.
- It can also mean slowing down specific actions to match the speed of operator judgment.

Control Speed and Reliability

More transactions in a given period of time can mean that the consequences of error from any one are lessened or at least can be corrected more quickly. This is especially the case if faster transactions are accompanied by more accurate feedback of what's actually happening, as feedback gets closer to real-time.

Control Speed and Reliability (Cont'd)

But these benefits are likely only if there is, at the same time, a *protection* against rapidly cascading transaction errors, in which the error of one action rapidly propagates to a succeeding one. Error signals and their interpretation have to *at least match* control transaction speeds to guard against this possibility.


A Safety and Reliability Continuum: Speed vs Scope
Social Policy
Many variables
(Judgment)
Planning
Imbalance Zone
Regulation
Operators:
Skill
and
Training
Scope of
Attention
Imbalance Zone
Expert Systems
Fewer variables
(Automation)
Relays, Switches
1- 10 seconds
5 minutes
30 minutes
1 hour
1 day
1 year
10 years+
Speed of Action/Consequences

Reliability and Automation: Two Propositions

- Reliability *enhancing* automation conditions:
  -- few necessary control variables
  -- fast control speed requirements and fast feedback
  -- low input and system variability
- Reliability *risks* in automation:
  -- many control variables,
  -- high input or state variability
  -- need for experience and judgment in predicting system behavior