Normale Katastrophen?

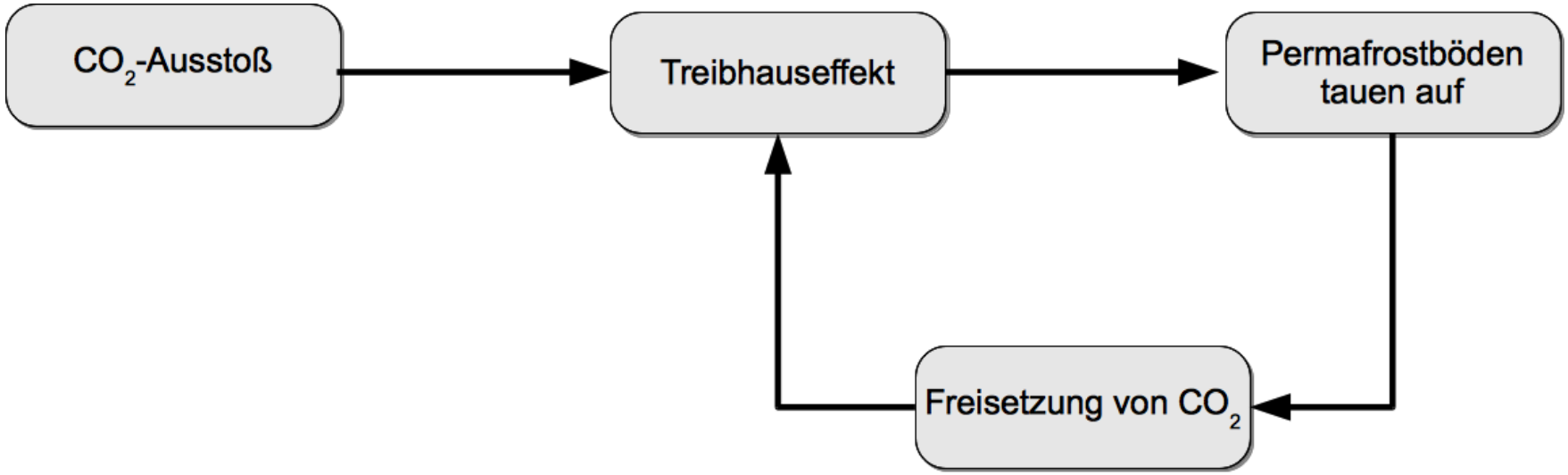
- Charles Perrow (1987)
  - organisationssoziologische Perspektive
  - Unfälle in komplexen Systemen unvermeidlich
- zwei Indikatoren für Risikopotenzial
  - lose/enge Kopplung
  - lineare/komplexe Interaktion

Risiko-Indikator „Komplexität“

Komplexe Systeme	Lineare Systeme
enge Nachbarschaft *(→ Kopplung?)*	räumliche Trennung
Common-Mode-Verknüpfungen (+)	festgelegte Verknüpfungen
verknüpfte Subsysteme (+?)	getrennte Subsysteme *(→ Kopplung)*
Rückkopplungsschleifen (+)	wenig Rückkopplungsschleifen
interagierende Kontrollinstrumente mit Mehrfachfunktionen (+)	unabhängige Kontrollinstrumente mit nur einer Funktion
indirekte Information *(Merkmal von Kompl.?)*	direkte Information
beschränkte Kenntnis *(Merkmal von Kompl.?)*	umfassende Kenntnis

Quelle: Perrow 1987: 129

Nicht-Linearität



- rekursiv
- irreversibel
- eigendynamische Selbstverstärkung

Risiko-Indikator „Kopplung“

Enge Kopplung	Lose Kopplung
keine Verzögerungen des Betriebsablaufs möglich (+)	Verzögerungen des Betriebsablaufs möglich
Unveränderbarkeit des Ablaufs (+)	Ablauf veränderbar
Produktionsziel nur mit einer Methode realisierbar (??)	alternative Methoden möglich
geringer Spielraum bei Betriebsstoffen, Ausrüstung und Personal (+)	mehr oder weniger großer Spielraum verfügbar
Puffer und Redundanzen konstruktiv vorgeplant (!!?)	Puffer und Redundanzen durch zufällige Umstände verfügbar
Substitution von Betriebsstoffen, Ausrüstung und Personal begrenzt und vorgeplant (??)	Substitution je nach Bedarf möglich

Quelle: Perrow 1987: 136

Lineare/komplexe Systeme (eigene Darstellung)

		Lineares System	Komplexes System
SYSTEM	*Topologie*	trassenförmige Pfade ohne Verzweigungen (bzw. mit wenigen Verzweigungen)	vielfach verknüpfte Systeme; netzwerkförmige Architektur mit vielen Verzweigungen
		wenige Kanten, wenige Knoten (?)	viele Kanten, viele Knoten (?)
	Rückkopplungen	nicht möglich	möglich
	Störungstypus	Stau	GAU ("Crash")
	Regeneration	einfach	unterschiedlich (Internet vs. AKW)
NUTZER	*Art der Interaktion*	sequenziell	sequenziell und rekursiv
	Wahlmöglichkeiten	keine Alternativen (bzw. geringe Zahl)	große Zahl an Alternativen
OPERATOR	*Eingriffsmöglichkeiten*	wenige Optionen	alternative Optionen
	Durchschaubarkeit	einfach	schwer
	Lokalisierung von Störungen	einfach	schwer
	Substitution von Komponenten	einfach	schwer
BEISPIELE		Fließband (eng/lose), Schienenverkehr (eng/lose)	Akw, Flugzeug, Chemieanlage, Börse (alle eng), Universität (lose)

Lose/enge Kopplung (eigene Darstellung)

		Lose Kopplung	**Enge Kopplung**
SYSTEM	Puffer (zeitlich, räumlich)	vorhanden	nicht (bzw. nur in geringem Maße) vorhanden → rasche Ausbreitung von Störungen
NUTZER / OPERATOR	Spielräume	vorhanden	kaum vorhanden
	Abläufe	veränderbar	kaum veränderbar
	Verzögerungen	möglich	kaum möglich
BEISPIELE		Post, Handel, Schienenverkehr 1980 (alle linear), Universität (komplex)	eCommerce, Schienenverkehr 2016 (alle linear), Akw, Flugzeug, Börse (alle komplex)

Weitere Dimensionen

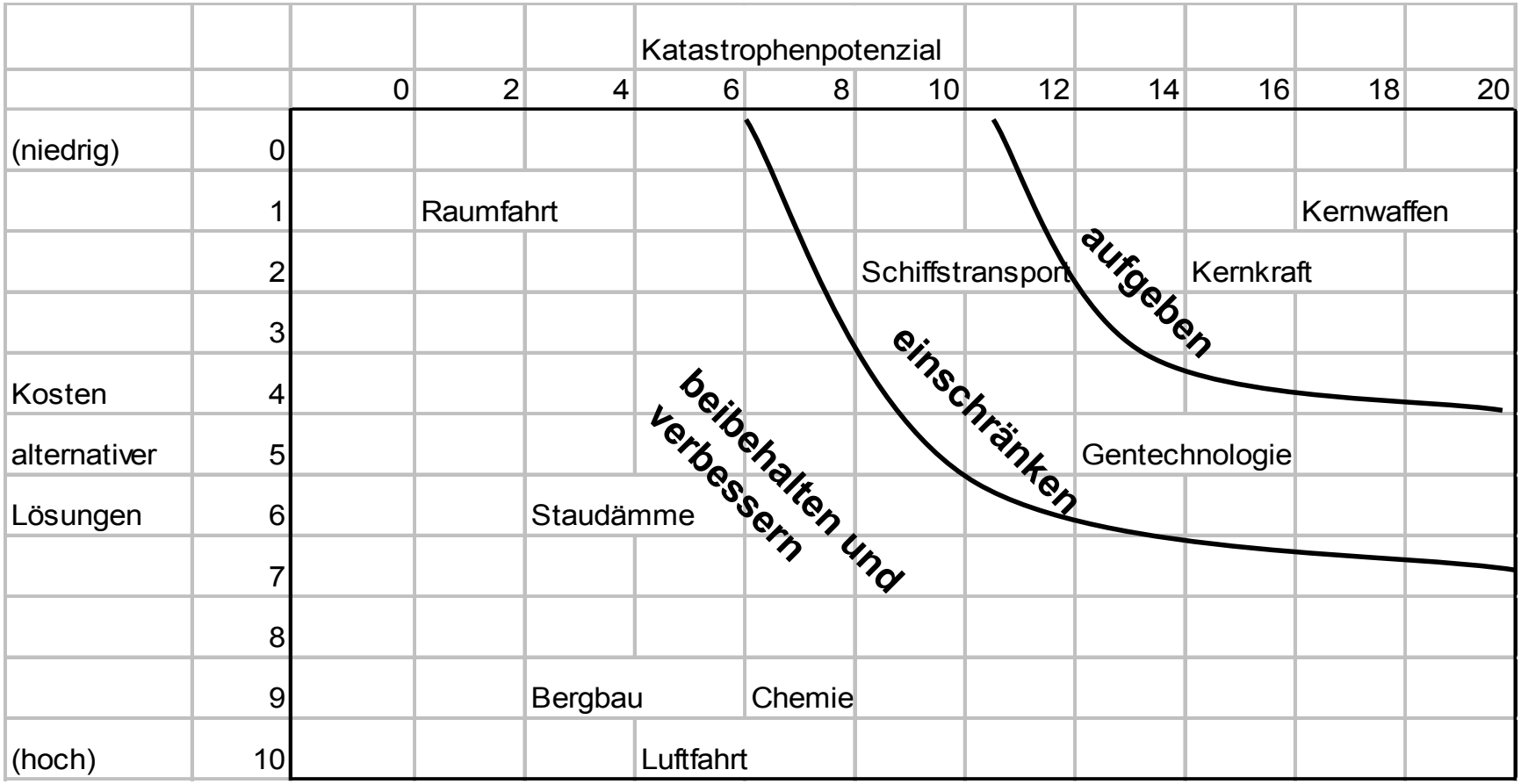
- räumliche Nachbarschaft
- indirekte Anzeigen
- Interaktion mit Umwelt
- Redundanzen durch Sicherheitssysteme

Systemtypologie

		Interaktionen	
		linear	komplex
Kopplung	eng	Staudämme, Kraftwerke, Schienen- und Schiffstransport	Kernkraftwerke, Rüstung, Gentechnologie, großchemische Anlagen, Flugzeuge, Raumflüge
	lose	Verarbeitende Industrie, Handelsschulen, Postamt	Bergwerke, Sozialbehörden, Universitäten

Quelle: Perrow 1987: 387

Politische Empfehlungen



Quelle: Perrow 1987: 408

Kritik an Perrow (1)

- keine objektiven Indikatoren
  - willkürliche Einordnung?
- graduelle Übergänge (linear → komplex)?
- Erfahrung steigert Sicherheit

- Challenger: kein Systemunfall (Hopkins 1999)
- immer komplexe Interaktionen? (Rijpma 2003)

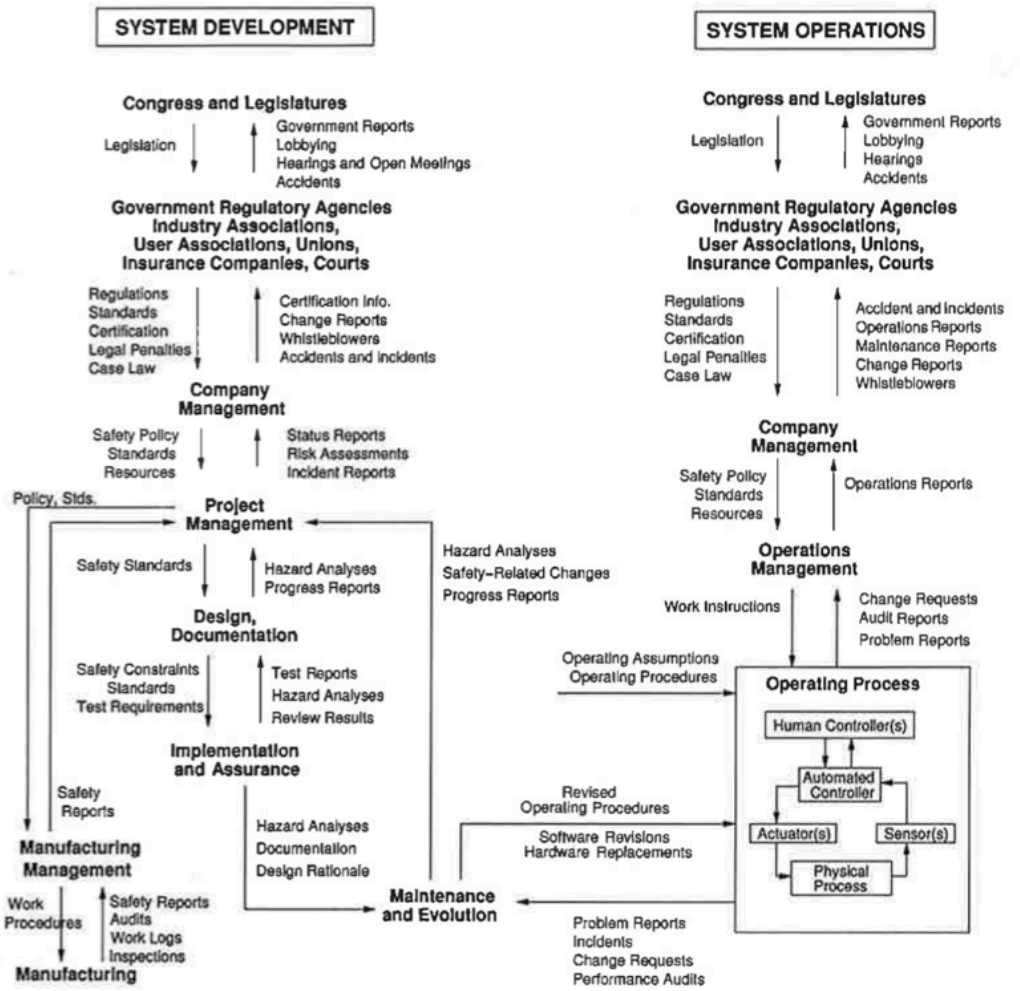
Kritik an Perrow (2)

- Risikodefinition
  - fokussiert auf Eintrittswahrscheinlichkeit
  - ignoriert Schadenshöhe
- Vierfelderschema
  - empirisch nicht haltbar
- pauschale Zuordnung ganzer Branchen
  - konkretes Systemdesign
- Sicherheit ist Systemeigenschaft
  - Komponenten oftmals fehlerfrei (Leveson et al. 2009)

STAMP

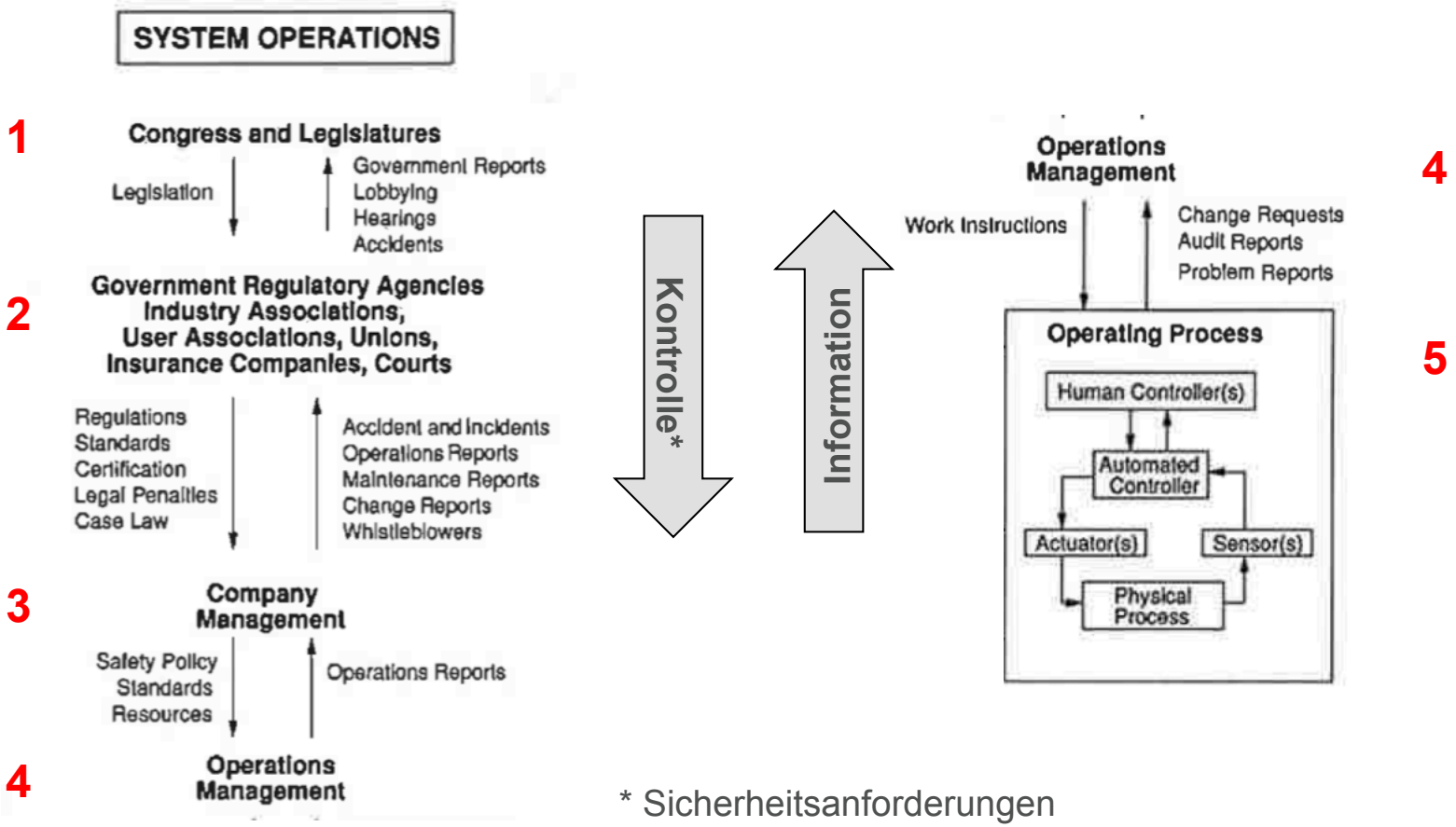
- Systems-Theoretic Accident Modeling and Processes (Leveson et al. 2005, 2009)
  - Sicherheit als emergente Systemeigenschaft
  - integriertes sozio-technische System
  - Modellierung organisationaler Sicherheitsstrukturen
- Hierarchie von Organisations-Ebenen
  - Beziehungen zwischen den Ebenen
  - Sicherheitsanforderung („safety constraints“)
  - branchen- bzw. unternehmensspezifisch

Model of socio-technical control



Leveson et al. 2009: 244

Model of socio-technical control



* Sicherheitsanforderungen

Leveson et al. 2009: 244

Systemunfälle

„Unfälle haben ihre Ursache in Interaktionen zwischen Systemkomponenten, die gegen diese Sicherheitsanforderungen verstoßen.“ (Leveson et al. 2009: 242)

- Sicherheit als Kontrollproblem
  - nicht Komponentenversagen (Perrow?)
  - keine Ereignisketten (Reason?)

„Unfälle geschehen, wenn Ausfälle von Komponenten, externe Störungen und/oder dysfunktionale Interaktionen zwischen Systemkomponenten nicht angemessen verarbeitet (handled) bzw. beherrscht (controlled) werden.“ (ebd.)

Prozess-Modell

- Jeder Controller benötigt ein Modell des kontrollierten Prozesses.
- Unfallursache
  - „mismatch“ zwischen mentalem Modell der beteiligten Manager und aktuellen Systemzustand
  - Beispiele: Columbia, DWH
- verteilte Systeme
  - nicht abgestimmte Entscheidungen
- schleichende Veränderungen (→ Drift)

Modellierung und Simulation

- statisches Modell der Sicherheits-Kontrollstruktur
- dynamisches Prozess-Modell

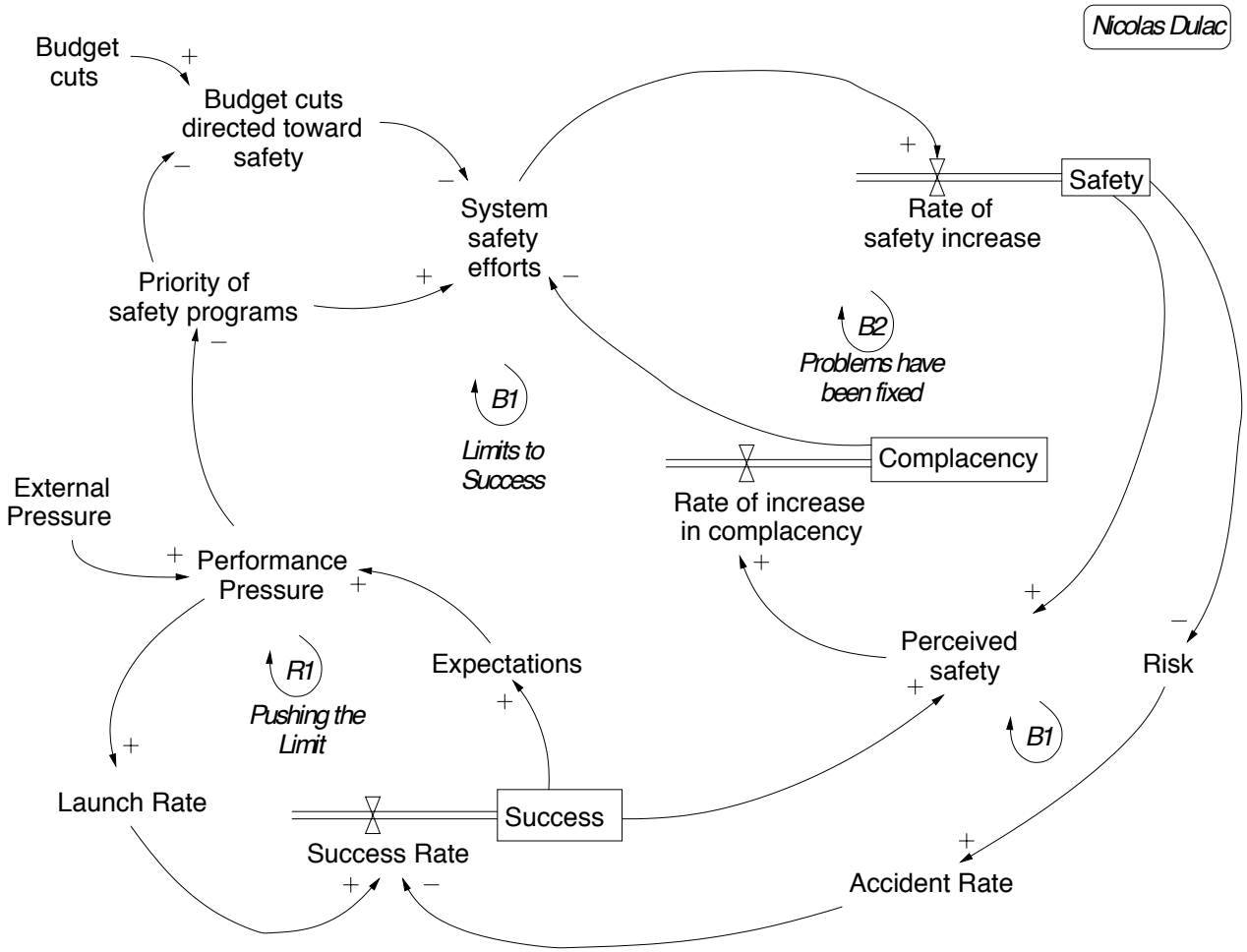
berücksichtigt

- Spezifika der Organisation
- kultureller und politischer Kontext
- Dynamiken und Sachzwänge

ermöglicht

- Identifikation von Schwachstellen
- Auswirkungen von Veränderungen

Model of Columbia loss



Leveson et al. 2005: 11