

SoK: Policy and Governance for Sociotechnical Systems

Discussion Points

Munindar P. Singh

To be joint work with SoS colleagues:

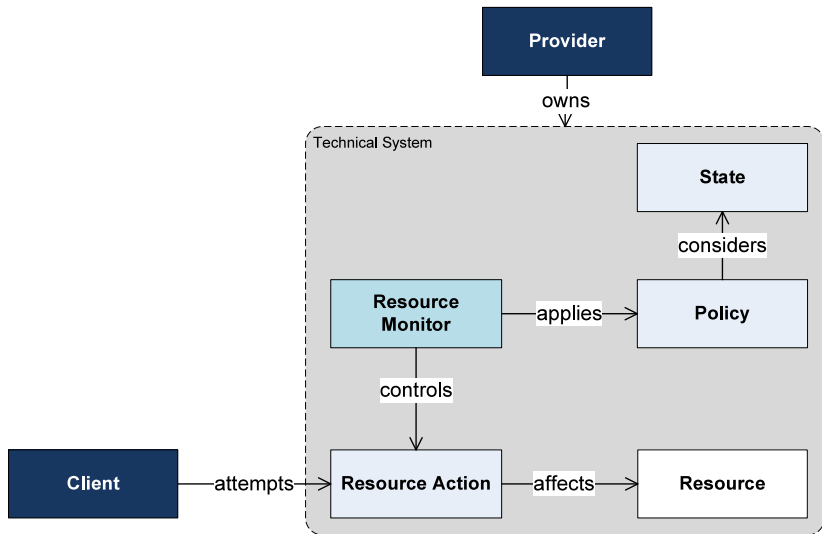
David Nicol, John Baras, Ninghui Li, Travis Breaux (?)

Department of Computer Science
North Carolina State University

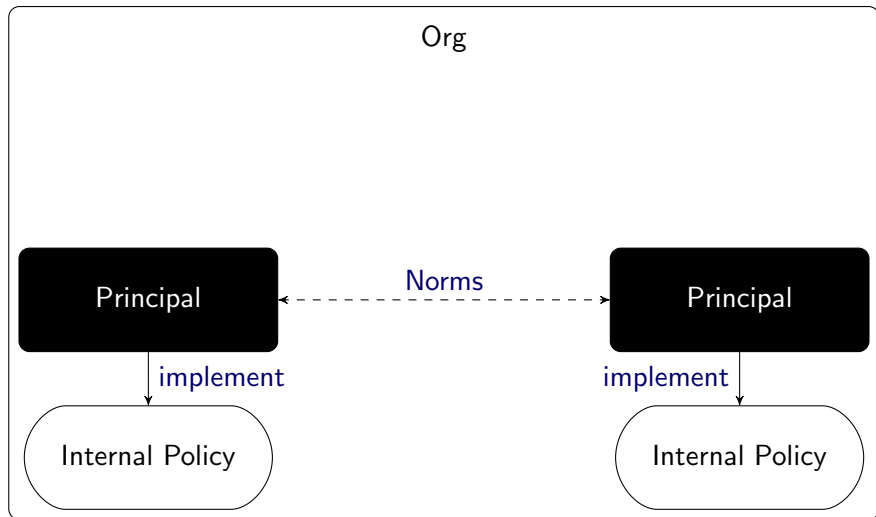
Governance and Security

- ▶ Governance is about administering sociotechnical systems to meet stakeholder objectives
 - ▶ Security is about ensuring we can meet stakeholder objectives
- ▶ Norms specify what governance should achieve despite autonomy of participants
 - ▶ Provide the standards of correctness
- ▶ Policies specify how participants interact
 - ▶ May not individually or collectively comply with norms
 - ▶ May thus violate security expectations

Traditional View: Systems as Artifacts



Simple Normative Framework: Systems as Societies



Principles of Governance: What Policies Give Us

Administration that is intelligent and intelligible

- ▶ Vividness of modeling
 - ▶ Grounded in applications; modeled entities are real
- ▶ Minimality of operational specifications
 - ▶ Leaving restrictions unstated except where essential to correctness
- ▶ Reification of representations
 - ▶ Explicit: hence, inspectable, sharable, and manipulable

Principles of Governance: What Norms Give Us

Administration that is intelligent and intelligible

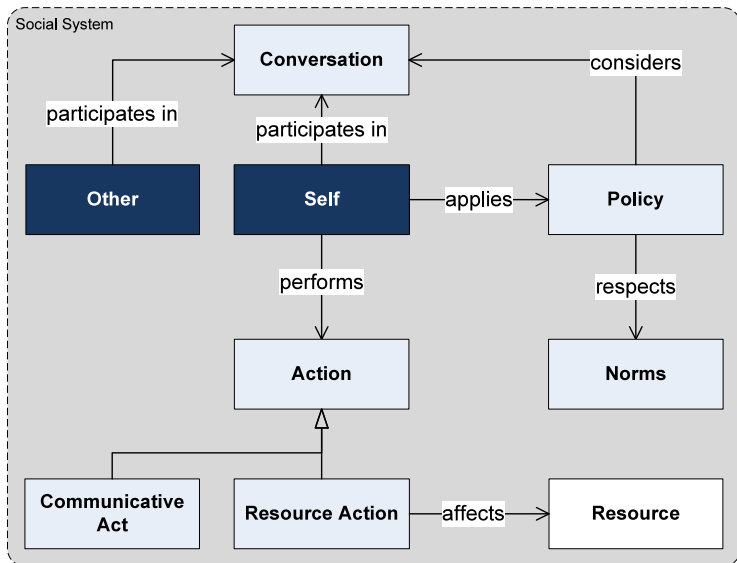
- ▶ Autonomy and interdependence of participants
 - ▶ Stating rules of encounter; omitting policies from specifications
- ▶ Centrality of organizations
 - ▶ Modeling businesses, communities of practice; specifying rules of encounter; monitoring contracts; sanctioning violators
- ▶ Institutional actions
 - ▶ Creation and manipulation of commitments; granting or denying powers, authorizations; effecting sanctions
 - ▶ Separation of concerns from those of operational interactions

Regulation versus Regimentation

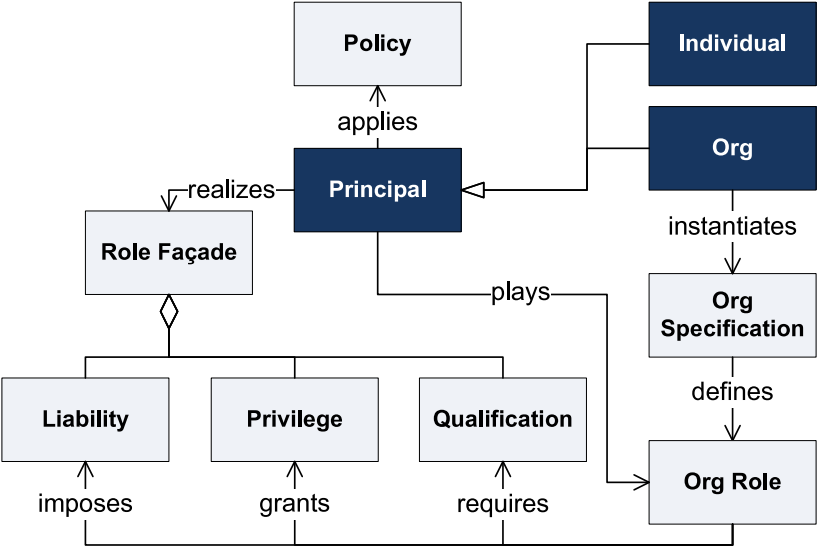
- ▶ Regimentation: preventing bad behavior
 - ▶ Fits a closed system
 - ▶ Reflects a pessimistic stance
 - ▶ Presumes a regimenting infrastructure
- ▶ Regulation: discouraging and correcting—though *allowing*—bad behavior
 - ▶ Fits an open system
 - ▶ Reflects an optimistic stance
 - ▶ Presumes a regulating social system

Proposed View: Systems as Societies

Conversations with autonomous parties; control over resources

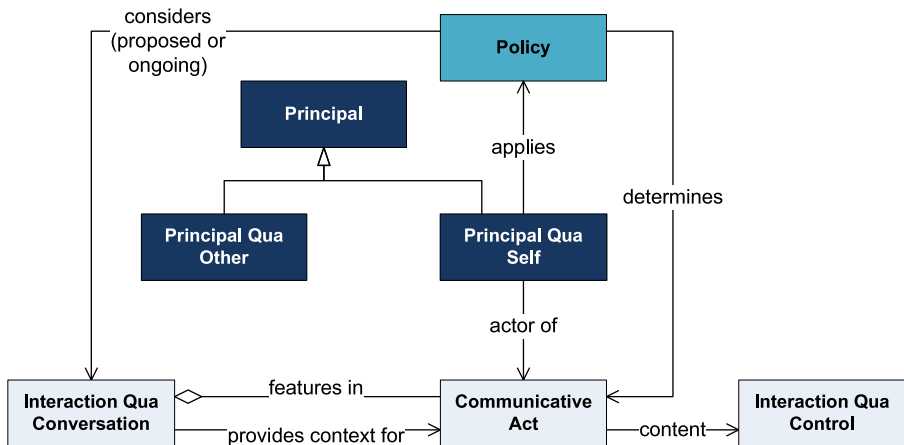


Governance Overview



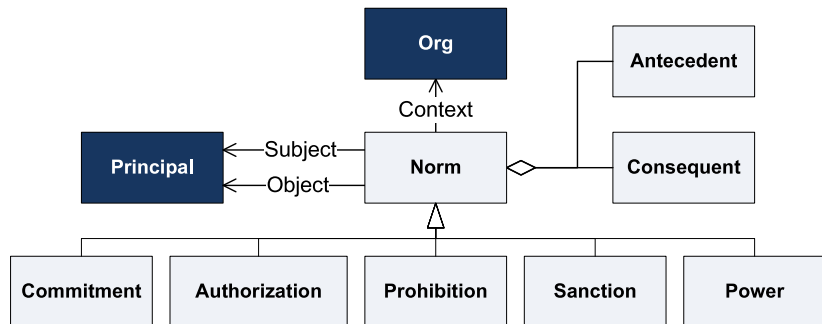
Governance and Policies

Conversations with autonomous parties; control over resources



Types of Norms

Unified logical form: Norm(subject, object, context, antecedent, consequent)

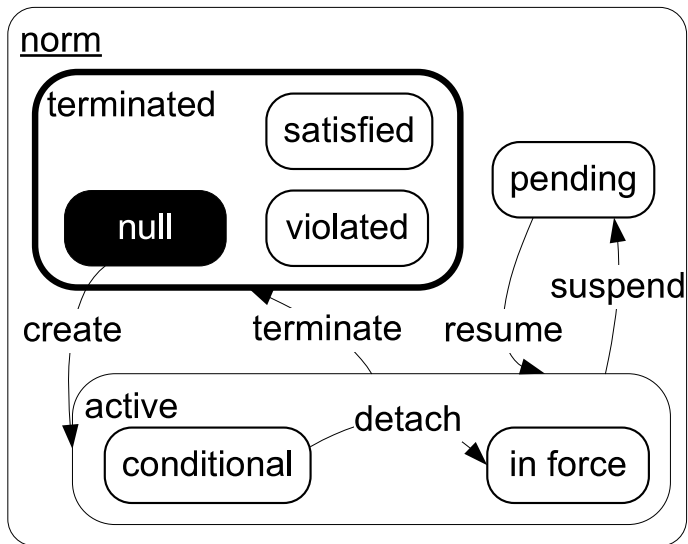


- ▶ Directed
- ▶ Declarative
- ▶ Composable
- ▶ Manipulable

Norms as Façades

Norm	Subject's Façade	Object's Façade
<i>Commitment</i>	Liability	Privilege
<i>Authorization</i>	Privilege	Liability
<i>Power</i>	Privilege	Liability
<i>Prohibition</i>	Liability	Privilege
<i>Sanction</i>	Liability	Privilege

Norm Life Cycle: 1



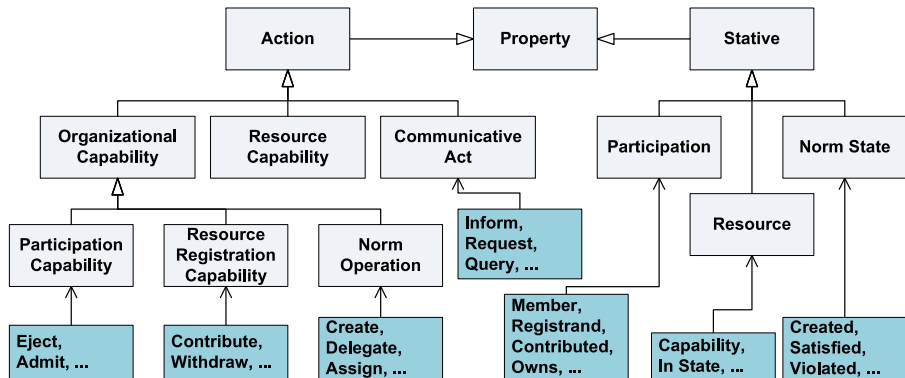
Norm Life Cycle: 2

Substate of a terminated norm

If terminated in		Then				
ant	con	Com	Aut	Pro	San	Pow
false	false	null	null	null	null	null
false	true	sat	vio	null	null	null
true	false	vio	null	sat	null	vio
true	true	sat	sat	vio	sat	sat

Vocabulary for Governance

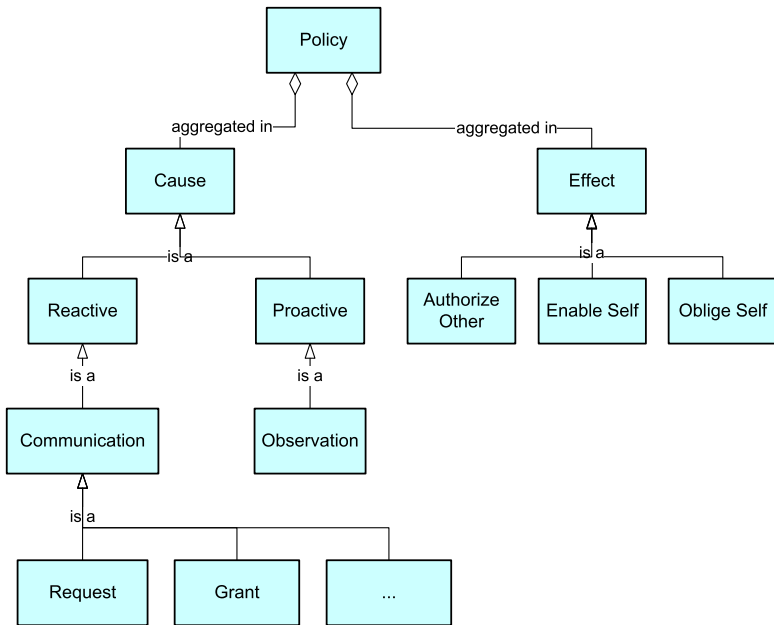
Norms, Orgs, and Policies



Policy Model: Types

The policy interactions need to go beyond traditional access control

- ▶ Each policy can be understood in terms of its cause and its effect
- ▶ Cause
 - ▶ *Reactive*: triggered by a request from another stakeholder
 - ▶ *Proactive*: triggered by local observations
- ▶ Effect
 - ▶ *Authorization* of action to be taken on behalf of requester
 - ▶ *Enablement* of action, which would otherwise not be taken
 - ▶ *Obligation* of action, which would now be performed



Dimensions for Systemization

- ▶ Kinds of interaction and support for autonomy
- ▶ Reactive versus proactive
- ▶ Achitecture
- ▶ Representation for policies
 - ▶ Information model
 - ▶ Discrete to continuous
 - ▶ Utilities
- ▶ Support for verifying system-level properties
 - ▶ Liveness with respect to an objective
 - ▶ Safety with respect to a threat
- ▶ Composability of
 - ▶ Validating norms
 - ▶ Verifying policies with respect to norms
 - ▶ Realizability in architecture

Thanks!

<http://www.csc.ncsu.edu/faculty/mpsingh/>