Beschreibung sicherheitsrelevanten Verhaltens in der Open Source Softwareentwicklung

Zwischenpräsentation Masterarbeit

Tobias Opel
Institut für Informatik
FU Berlin
19.06.2008

Agenda

- Einleitung/Rückblick
  - Ziel der Arbeit
  - Aufgaben
  - Forschungsmethode
  - Analysemodell
- Kategorien
  - Hauptkategorien
  - Beziehungen
- Hypothesen
- weitere Aufgaben auf meinem Weg
- Diskussion

Ziel der Arbeit

- Entwicklung einer Beschreibung sicherheitsrelevanten Verhaltens in der Open Source Softwareentwicklung
  - Identifikation von Verhaltensweisen und Rollen, welche bei der Behebung von sicherheitsrelevanten Schwachstellen involviert sind
  - durch qualitative Datenanalyse diese Verhaltensweisen, Rollen und deren Beziehungen untereinander beschreiben
  - betrachtet werden dabei Open Source Webanwendungen und Bibliotheken

Aufgaben

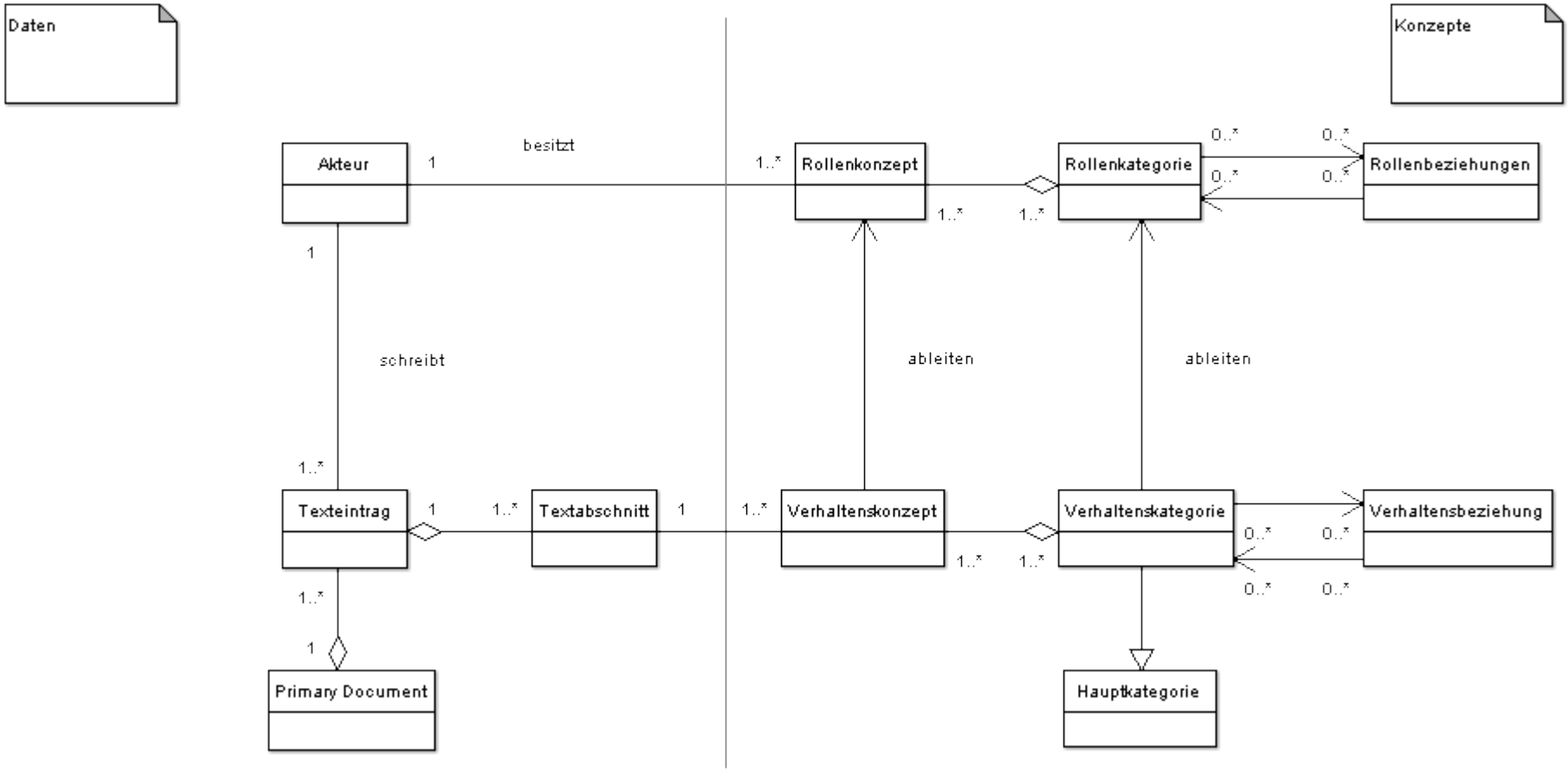
1. Datenbestände zur Behebung sicherheitsrelevanter Schwachstellen finden und auswählen
2. Verhaltenskategorien, Rollen und ihre Beziehungen untereinander aus den Daten ableiten
3. Vergleich von Literatur zur Qualitätssicherung mit den eigenen Erkenntnissen
4. Entwicklung von Erfolgsmaßen und Bewertung unterschiedlicher Formen sicherheitsrelevanten Verhaltens
5. Beschreibung von Verhaltensweisen und Mechanismen zur Vermeidung sicherheitsrelevanter Schwachstellen

Forschungsmethode

Freie Universität Berlin

- Grounded Theory (gegenstandsverankernde Theoriebildung nach Strauss & Corbin):
  - Qualitativer Forschungsansatz
  - Datenerhebung basierend auf dem zu untersuchenden Phänomen
  - Konzeptualisieren der Daten (Kodieren) und Gruppieren der Konzepte zu Kategorien
  - Beziehungen zwischen den Kategorien finden
  - Kernkategorie auswählen und diese in Beziehung zu den anderen Kategorien setzen zur Theoriebildung
  - Datensammlung, Analyse und Theorie stehen in wechselseitiger Beziehung zueinander

Analyse Modell



Hauptkategorien

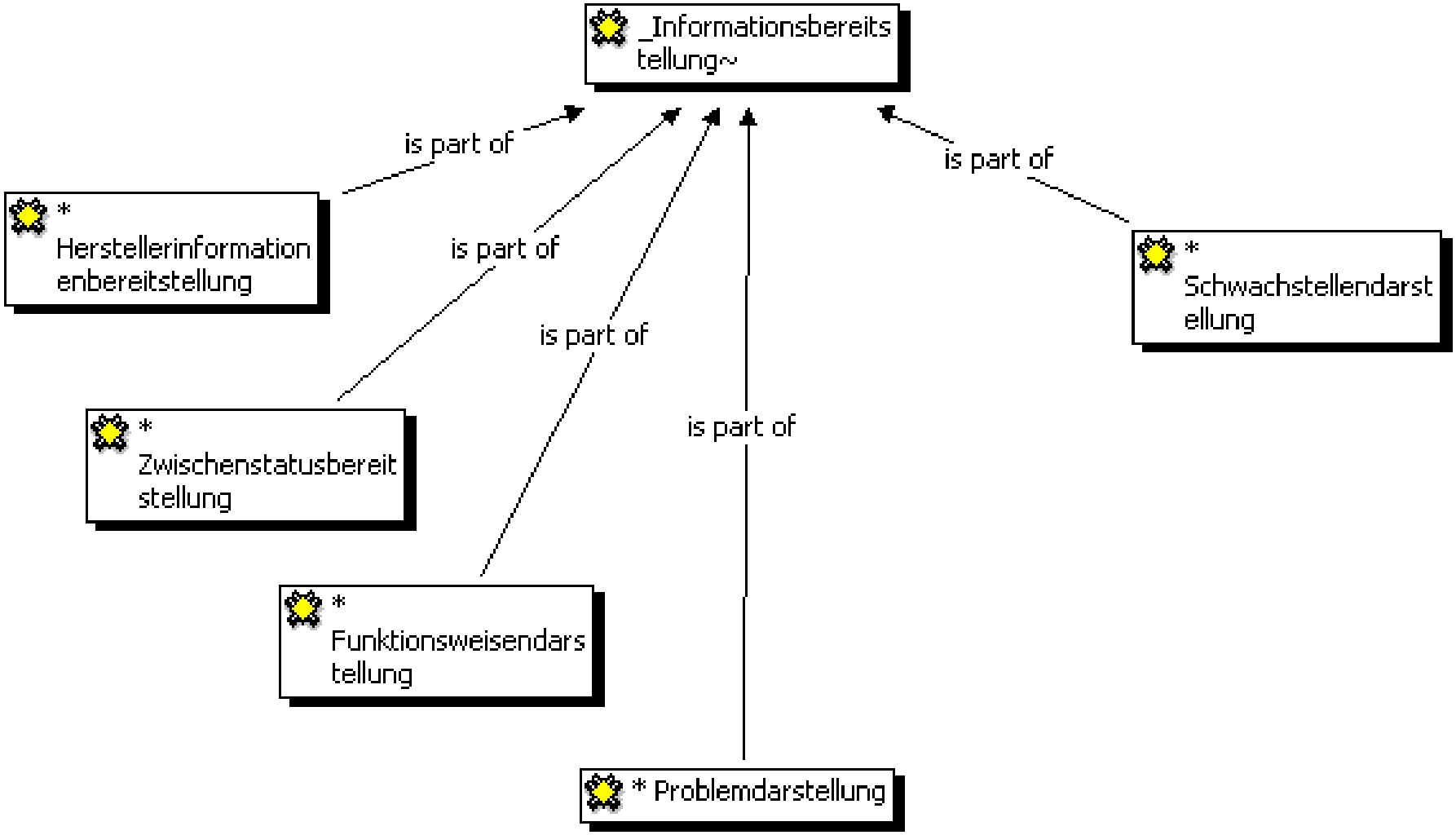
- Informationsbereitstellung
- Informationsverwertung/-verarbeitung
- Einleitung konkreter Maßnahmen
- Umgang mit Konflikten
- Unterstützung
- Einsatz von Werkzeugen

Informationsbereitstellung

- Informationen werden gegeben
  - zu einem konkreten Phänomen (Problem, Schwachstelle etc.)
  - von einer bestimmten Rolle (Hersteller etc.)
  - zu einem bestimmten Zeitpunkt (Zwischenstatus etc.)
- Informationen liegen in verschiedenen Formen vor
  - einzelner Datenstichpunkt (Datum, Versionsnummer etc.)
  - Zusammenfassung verschiedener Datenstichpunkte zu einem Bericht
  - ausführliche Schilderung
    - Begründungen, Beschreibungen aber auch Gedanken, Vermutungen fließen in den Bericht ein

Freie Universität Berlin

Verhaltenskategorien

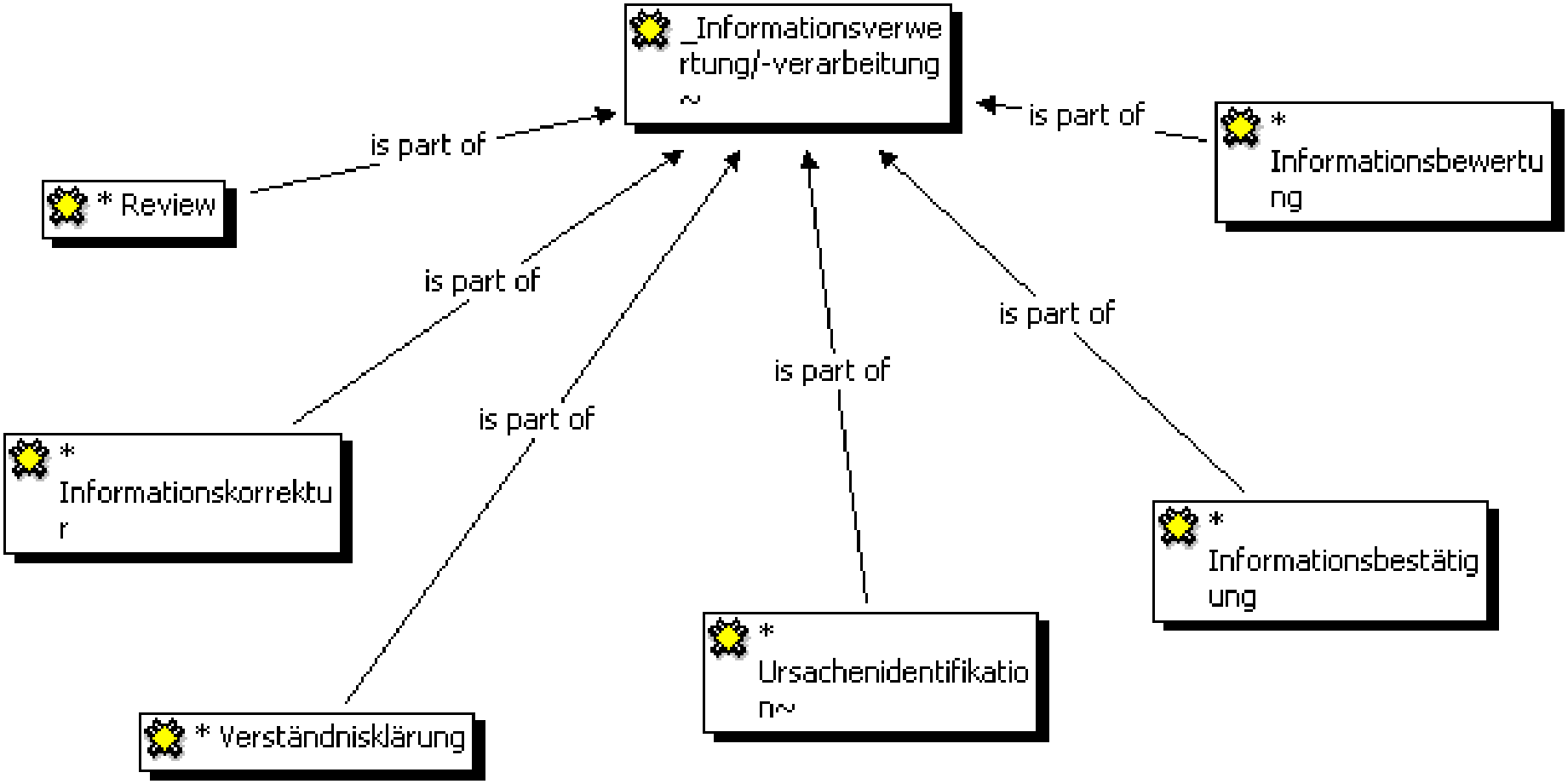


Informationsverwertung/-verarbeitung

Freie Universität Berlin

- bereitgestellte Informationen werden für zugrunde liegende Aufgabe (Schwachstellenbehebung) angenommen und verarbeitet
  - Informationen werden bewertet
  - Informationen werden bestätigt
  - Informationen werden korrigiert
  - Informationen werden erweitert/vervollständigt
  - Informationen werden hinterfragt
- nach der Verarbeitung können durch diese neue Informationen bereitgestellt werden

Verhaltenskategorien



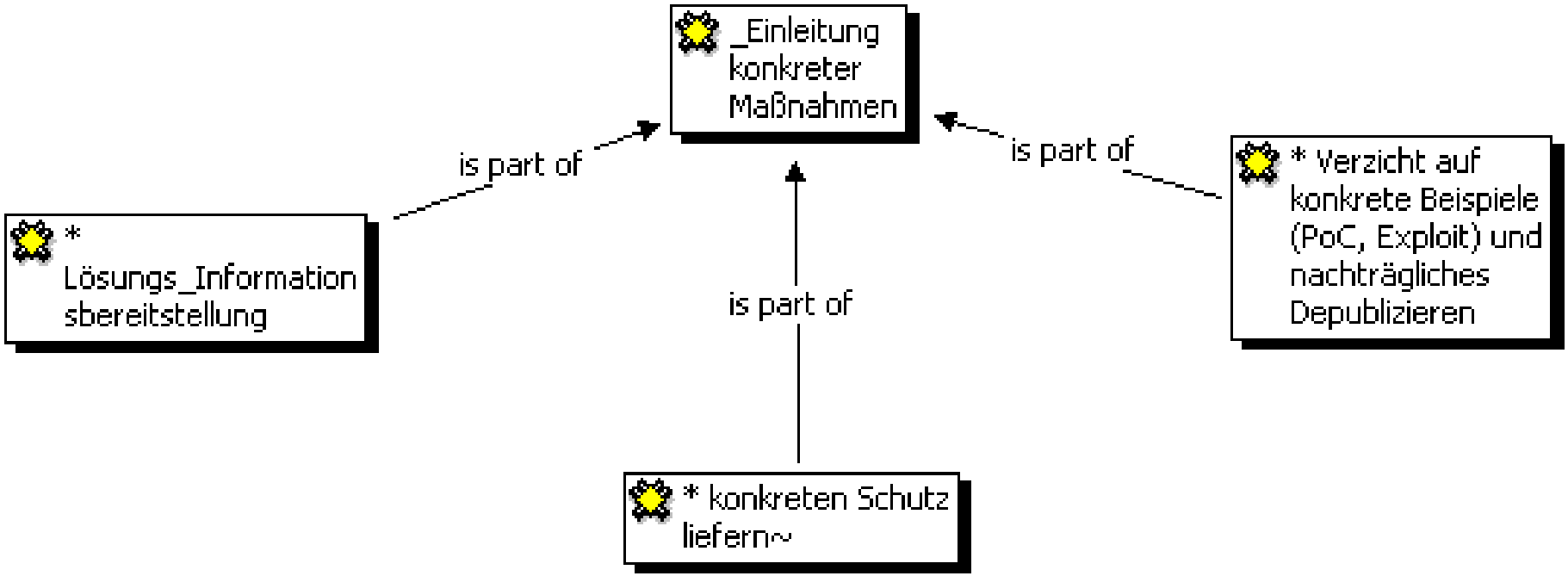
Einleitung konkreter Maßnahmen

Freie Universität Berlin

- für die Lösung der zugrunde liegenden Aufgabe werden Maßnahmen notwendig
- Maßnahmen ergeben sich aus den verarbeiteten Informationen
- unterteilen sich in technische und informative Maßnahmen
- dienen im Endeffekt dazu die Schwachstelle zu beheben
- aber auch Zwischenlösungen werden eingeleitet
  - Symptombekämpfung
  - Workaround
  - Schadensbegrenzung
  - Vermeidungsregeln

Freie Universität Berlin

Verhaltenskategorien

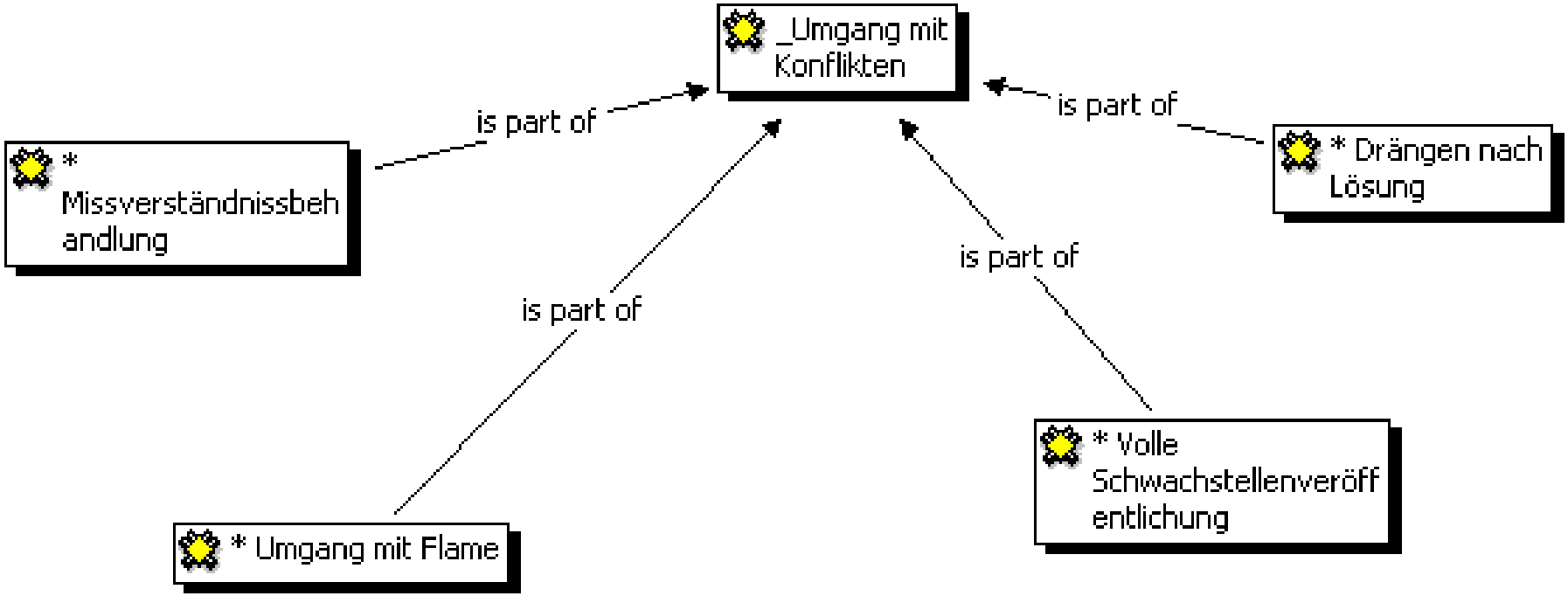


Umgang mit Konflikten

- während des Verlaufs der Behebung können Konflikte auftreten
- Konflikte beruhen meist auf zwischenmenschlicher Kommunikation
- haben (negativen) Einfluss auf die zugrunde liegenden Aufgabe und die anderen Kategorien
- bilden Grundlagen für meine Hypothesen (später)

Freie Universität Berlin

Verhaltenskategorien



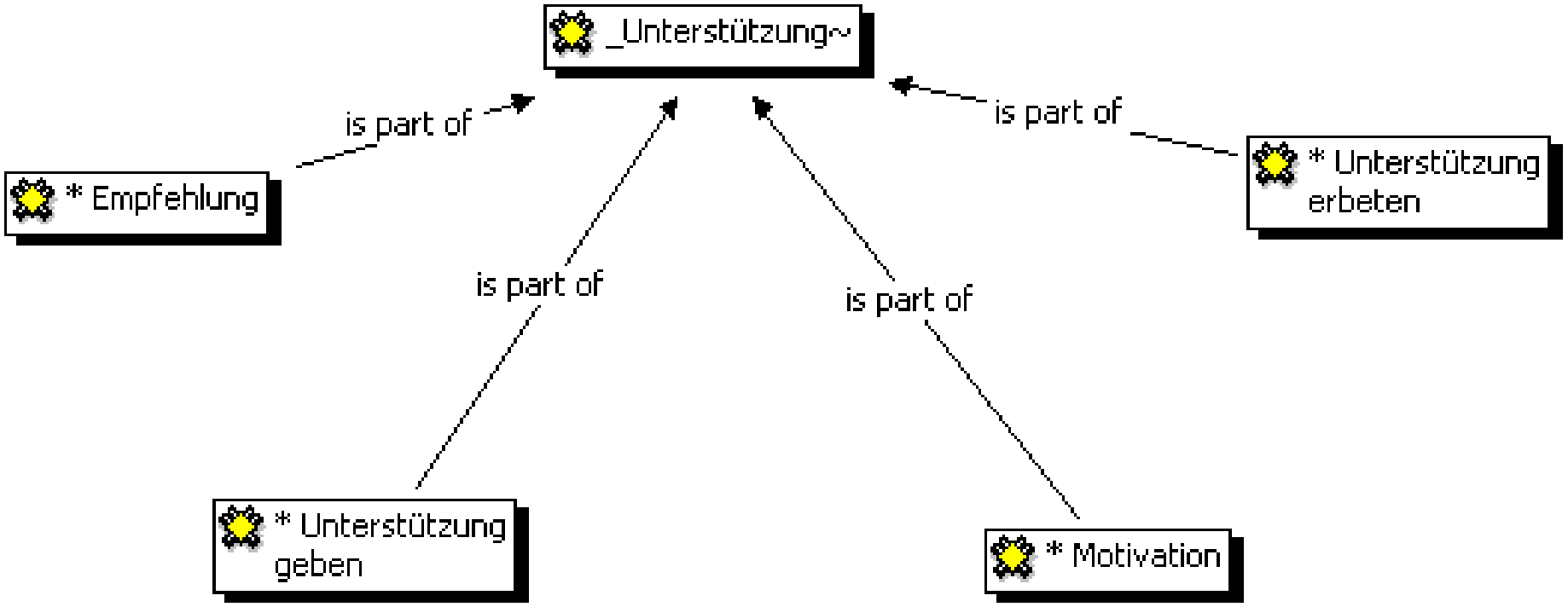
Unterstützung

Freie Universität Berlin

- soziale Aspekte die zur Lösung der zugrunde liegenden Aufgabe beitragen
- das Schema des Geben und Nehmen liegt hier zugrunde
- ebenso Motivation der Akteure
- haben Einfluss auf die zugrunde liegenden Aufgabe und die anderen Kategorien
  - Einfluss hängt von der Intensität der Unterstützung ab

Freie Universität Berlin

Verhaltenskategorien

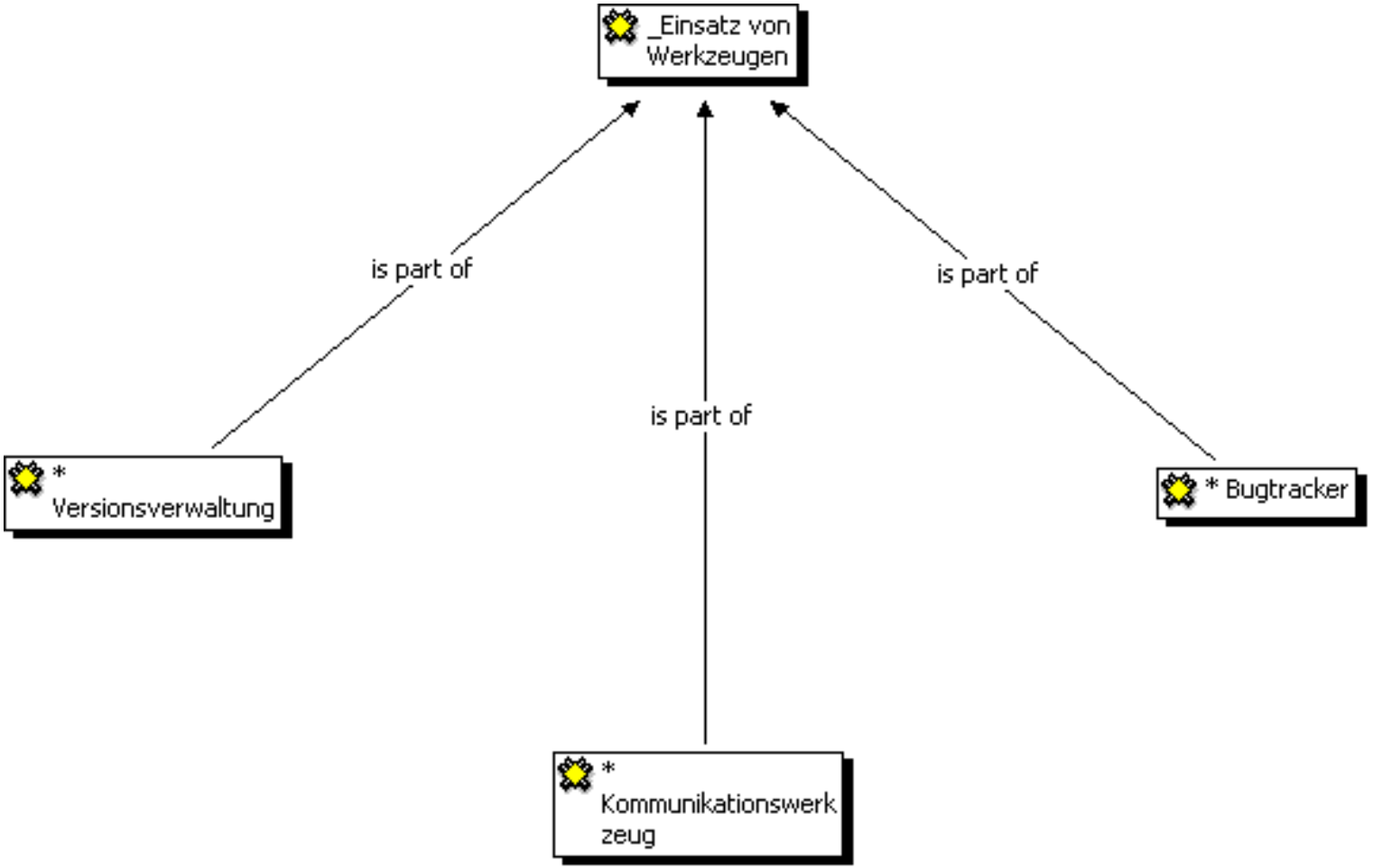


Einsatz von Werkzeugen

- Werkzeuge werden im Verlauf der Behebung eingesetzt
- umfassen z.B. Bugtracker, Foren, Mailinglisten, Chats, Wikis, Versionsverwaltungen
- Kategorie dient dazu, die Konzepte einzusortieren, die übergreifend bei den anderen Kategorien auftreten
- visualisiert den Einsatz von Werkzeugen während der zugrunde liegenden Aufgabe

Freie Universität Berlin

Verhaltenskategorien



Beziehungen zwischen Kategorien

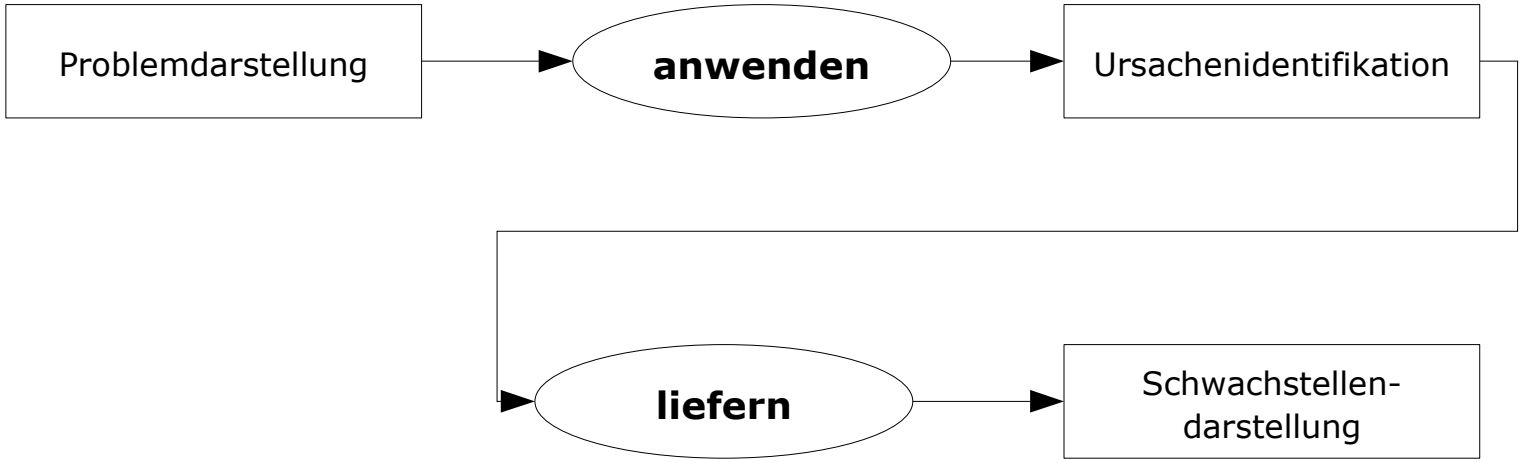
Freie Universität Berlin

- Beziehungen
  - dienen dazu Aussagen über kausale Zusammenhänge zwischen den Kategorien zu treffen
  - beschreiben Phänomene und Abläufe
  - zeigen Einflüsse und Rahmenbedingungen

- es folgen zwei Beispiele aus meiner Arbeit
  - Ursachenfindung von Schwachstellen
    - Problem wird festgestellt und Symptome sind bekannt
    - Ursache wird gesucht
  - Schwachstellenbehebung (vereinfacht)
    - Information zur Schwachstelle liegt vor
    - Weg der Informationen bis zur Behebung

Freie Universität Berlin

Ursachenfindung von Schwachstellen

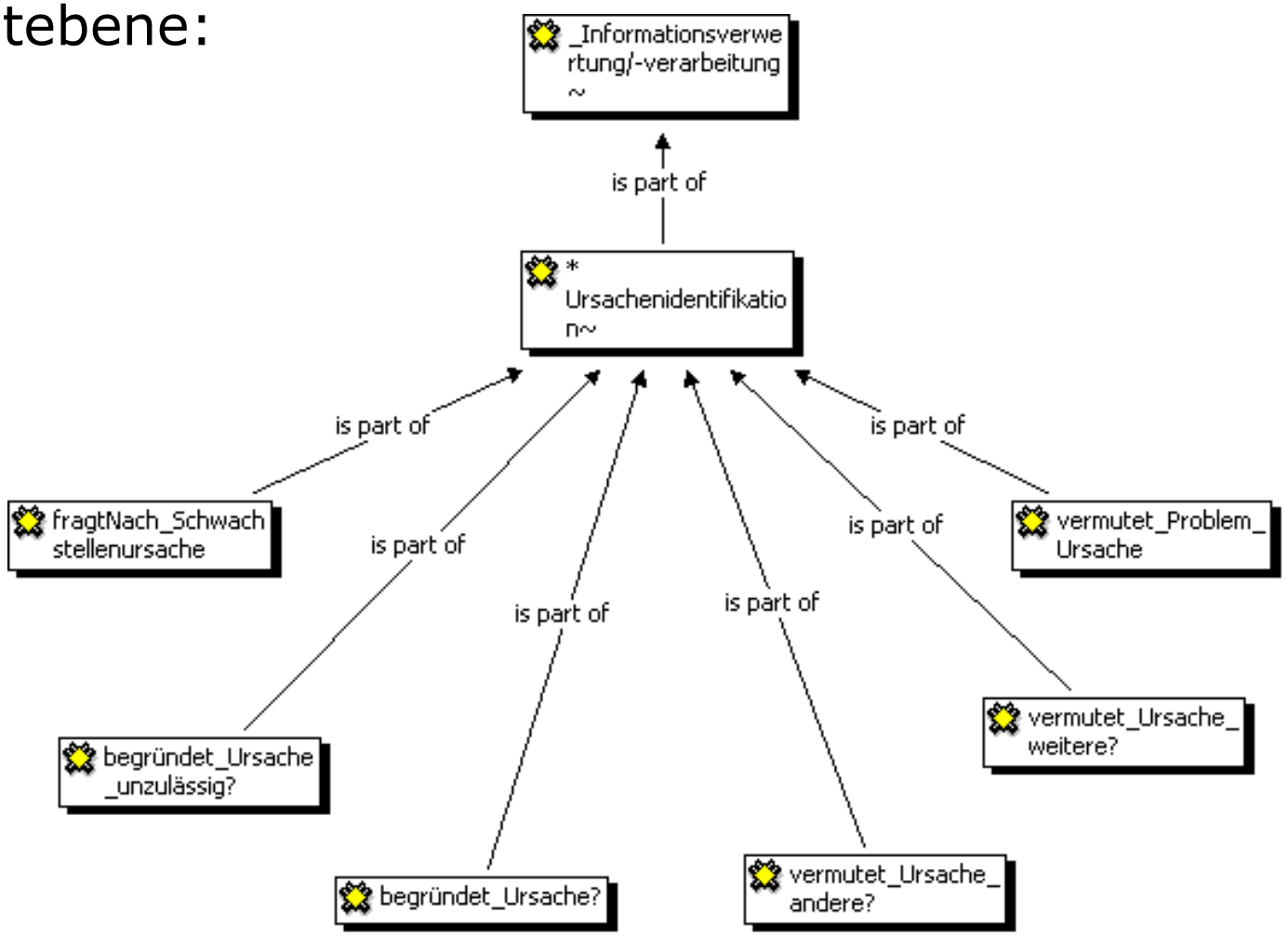


Beziehungen zwischen Kategorien

Freie Universität Berlin

Ursachenfindung von Schwachstellen

Konzeptebene:



Beziehungen zwischen Kategorien

Ursachenfindung von Schwachstellen

Konflikte

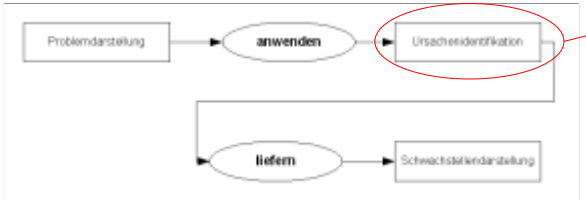
- Missverständniss-behandlung
- Umgang mit Flame

Unterstützung

- Unterstützung erbeten
- Unterstützung geben
- Motivation

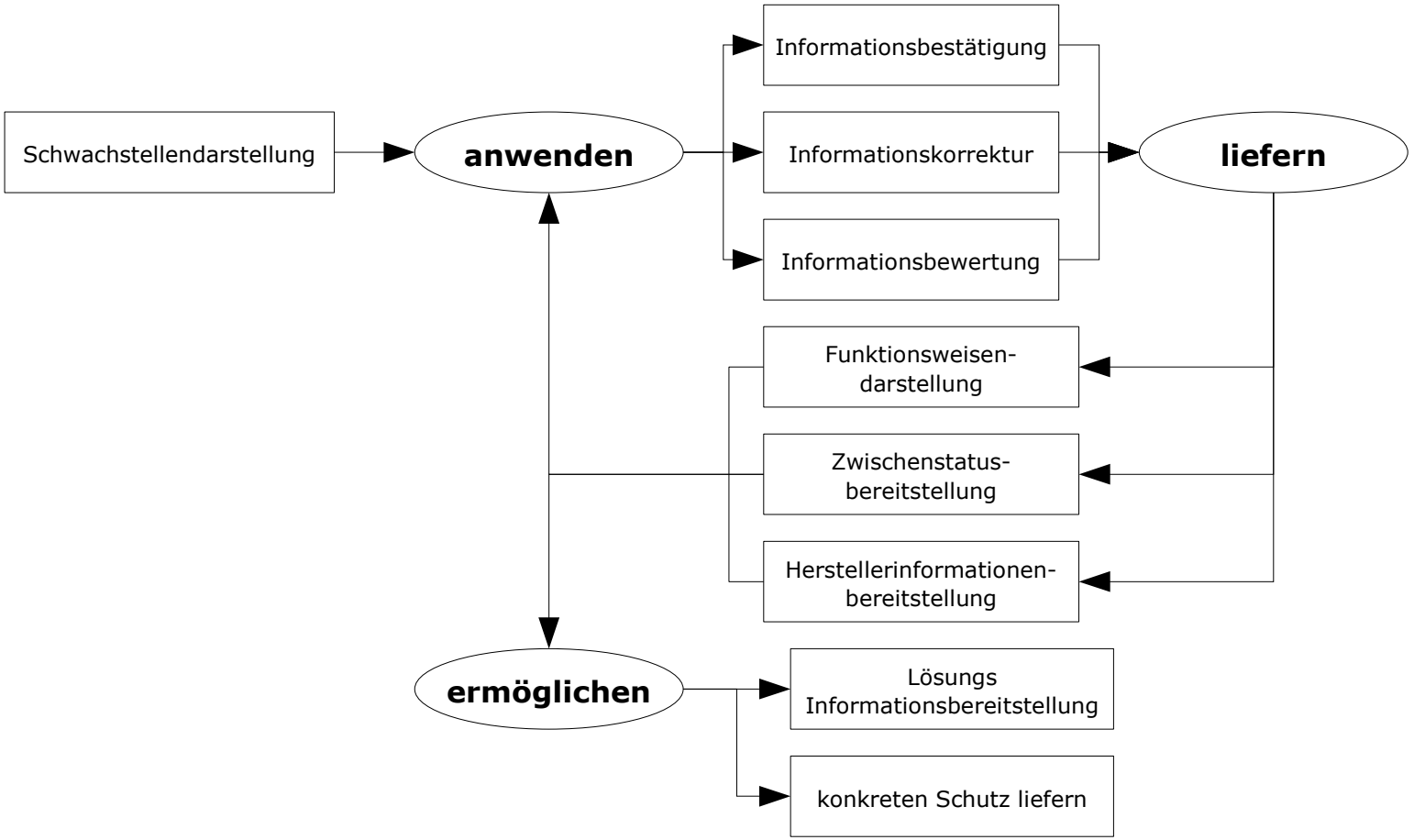
beeinflussen

Ursachenidentifikation



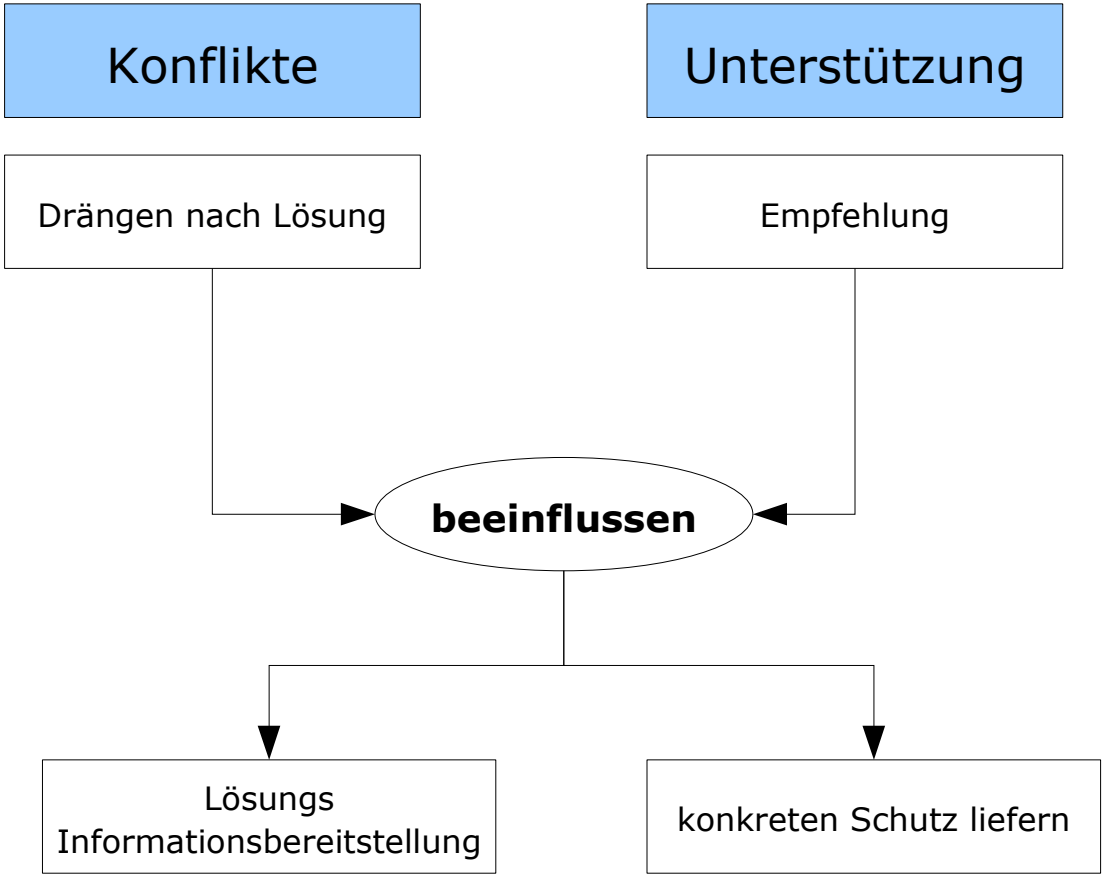
Beziehungen zwischen Kategorien

- Schwachstellenbehebung (vereinfacht)



Beziehungen zwischen Kategorien

- Schwachstellenbehebung (vereinfacht)

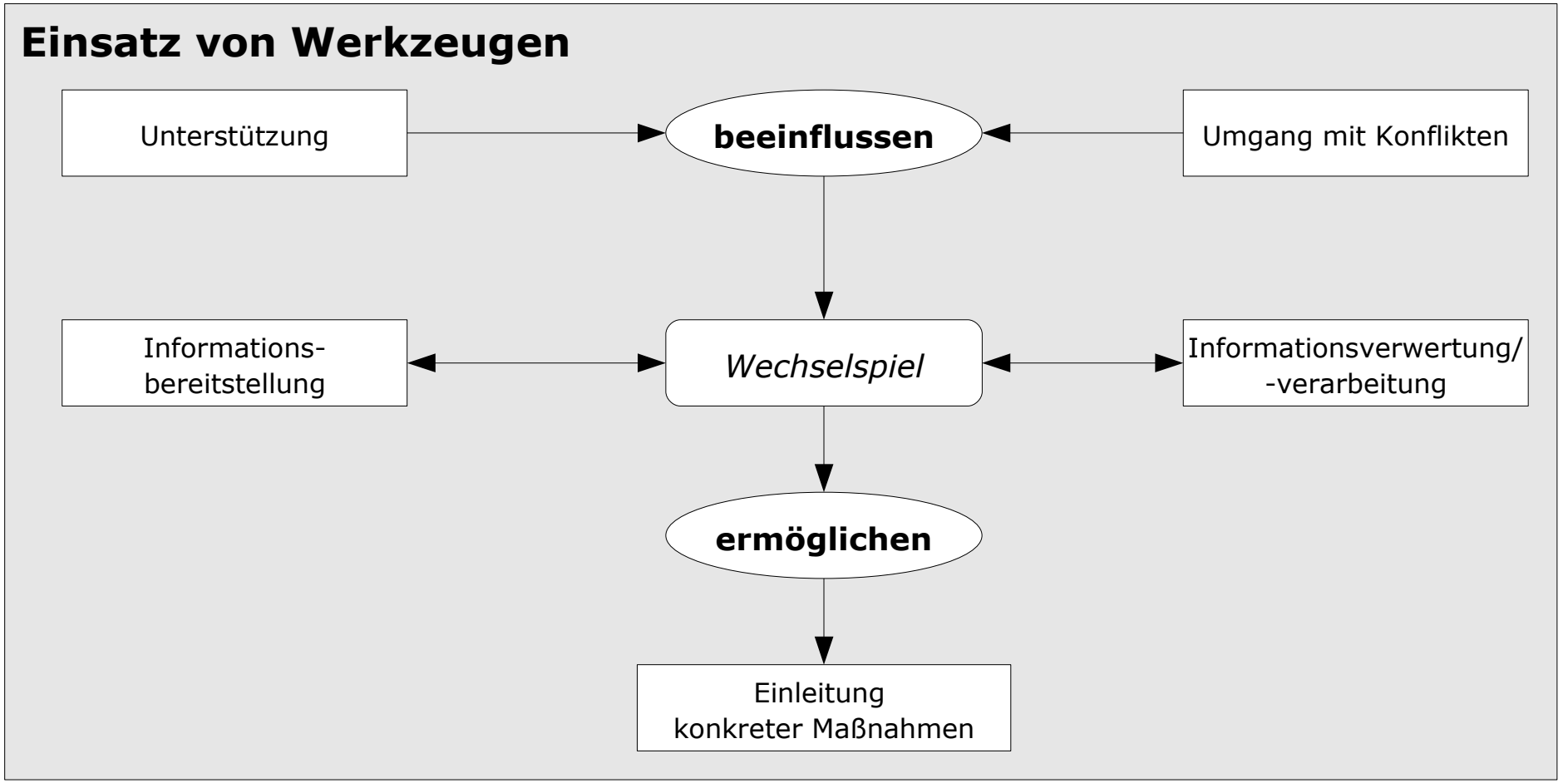


Beziehungen zwischen Kategorien

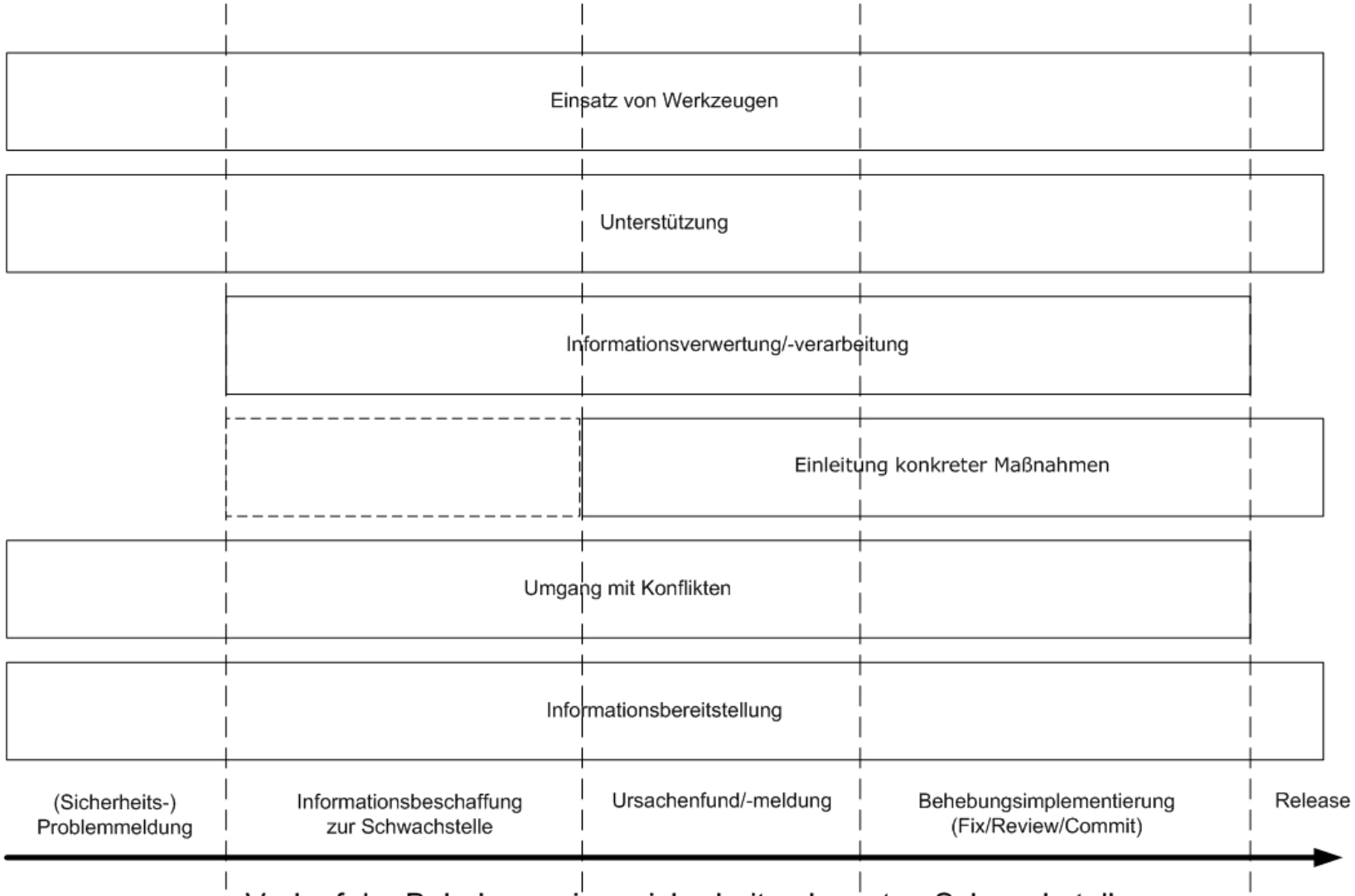
Freie Universität Berlin

- allgemeine Aussagen:
  - Wechselspiel zwischen Informationsbereitstellung und Informationsverwertung/-verarbeitung
  - aus diesem Wechselspiel werden konkrete Maßnahmen eingeleitet
  - Unterstützung und Konflikte haben Einfluss auf das Wechselspiel
  - Werkzeuge ermöglichen und unterstützen Wechselspiel
  - alle anderen Kategorien sind innerhalb der Werkzeuge eingebettet

Beziehungen zwischen Kategorien



Kategorien im Behebungsverlauf



Verlauf der Behebung einer sicherheitsrelevanten Schwachstelle

Hypothese 1

Freie Universität Berlin

Hypothese: Intransparenz im Behebungsverlauf führt zu Drängen durch Community

- Beispiel *Drängen nach Release*
- Nutzer erwarten Zwischenmeldungen und offizielle Lösung zur Schwachstelle
  - *"Oficial solution for SQL injection .. 1.0.10 ? for when?"(20.06.)*
  - *"when will 1.0.10 be released?"(23.06.)*
- Erwartung richtet sich Zeitnah an Bekanntwerden der Schwachstelle
  - *Meldung erschien am 17.06*
- Drängen wird in regelmäßigen Abständen wiederholt
  - wenn offizielle Statusmeldungen ausbleiben oder diese unbegründet sind
- hören auf wenn der offizielle Release erschienen ist

Hypothese 1

- Gründe warum unbedingt offizielle Lösung
  - Misstrauen gegenüber unbestätigten Lösungen [noch zu überprüfen]
  - manuelle Implementierung nicht für jeden Nutzer geeignet
    - *"I wish I could, but I dont even know how to begin using that \'diff\' bit you attached"*
  - Offizielle Lösungen unterliegen Qualitätssicherung
    - *"It has been sent to testing teams for final approval for release."*
  - Offizielle Lösung behebt auch andere Schwachstellen und Probleme gleich mit
    - *"security holes fixed and also fixed many more issues with 1.0.9"*

Hypothese 1

Freie Universität Berlin

- wie kann dem entgegengewirkt werden
  - mehr Transparenz beim Behebungsprozess
    - öfter Zwischenmeldungen geben
      - *"Very thanks ray for fast reply!"*
    - Aufklärungsarbeit zur Schwachstelle leisten
      - *"High level sql injection threat and no mention of it on the NEWS side of the site..."*
  - öfter kleinere offizielle Patches zu schweren Schwachstellen geben und nicht erst sammeln
  - Workarounds, Symptombekämpfung, Schadensbegrenzung liefern
    - Oder die von angesehenen Communitymembern bewerten und bestätigen
    - *"if there a way to fix 1.0 oldest version without updating to a new version please give us the walkthrough"*

Hypothese 2

Hypothese: Schwachstellenveröffentlichung hat Einfluss auf den Behebungsverlauf und das Ausnutzungsverhalten

- 2a: Schwachstellenveröffentlichung sensibilisiert Nutzer gegenüber Gefahr und hilft Entwicklern bei der Behebung
- 2b: Schwachstellenveröffentlichung gibt potentiellen Angreifern mehr Möglichkeiten

Hypothese 2

Freie Universität Berlin

- Ausgangspunkt
  - Externe Akteure veröffentlichen Details zu den Schwachstellen
    - direkt in Foren, Mailinglisten der Open Source Community
    - oder in Sicherheitssites, Vulnerability Datenbanken
  - diese Details reichen von einer einfachen Angabe der Art der Schwachstelle bis hin zu detaillierten Funktionsbeschreibung
    - *"Say the version joomla 1.0.x no have fixed this security bug, somebody know about that"*
    - *"I created an ordinary subscriber with no special permissions and uploaded a special rpcxml file:[..]*
      And was able to edit the post with ID 283, with nothing other than a subscriber account."

Hypothese 2

Freie Universität Berlin

- Welche Folgen hat das?
  - Informationsbereitstellung für Nutzer und Helfer um Schutzmaßnahmen einzuleiten
    - *"I think this bug is being actively exploited, so I may as well, so you can protect yourself."*
  - Informationsbereitstellung für Entwickler zur Behebung
    - *"We have only just become aware of this report and will investigate to see whether this also affects Joomla!"*
  - Informationsbereitstellung für potentielle Angreifer um Schaden anzurichten
    - *"You must now realise that its not just the major people who know the exploit now, but rather, all the script kiddies too."*

Hypothese 2

Freie Universität Berlin

- Einschränkende Möglichkeiten der Veröffentlichung
  - Moderatoren löschen kritische Codeangaben/Verlinkungen
    - *"there is a working proof of concept up here >* ***[removed, please don't post PoCs until there is a fixed release available]****"*
    - *"I know that the* ***[mod note: removed]*** *stuff does work"*
  - Security Team (zukünftige Arbeit)
- Darf Schwachstelle öffentlich bekannt gegeben werden?
  - äußert sich als Grundsatzfrage
    - Nutzer (darunter Veröffentlicher) sagen ja
      - *"HAD you waited, how many more blogs WordPress blogs would have been exploited [..] Now theres a fix."*
    - Entwickler tendieren eher zu nein
      - *"sent to our security address, that way a real fix can be put out before you inform every bad guy [..] about the problem"*

Hypothese 3

Freie Universität Berlin

Hypothese: Informationen zu einer Schwachstelle führen zu Codereview im Bezug auf die Schwachstellenart

- Code wird auf weitere Schwachstellen der gleichen Art hin untersucht
- weitere Schwachstellen werden identifiziert, behoben und gemeldet
  - Beispiel aus Changeset Meldungen:
  - *(In [6709]) Add edit_page cap check.*
  - *(In [6710]) Add edit_page cap check.*
  - *(In [6714]) More cap checks from josephscott.*
  - *(In [6715]) More cap checks from josephscott.*

Weitere Aufgaben

- weitere Projekte heranziehen um meine Kategorien zu bestätigen, erweitern oder anzupassen
- Rollenkategorien ableiten und festigen
- Muster aus Kategorien und deren Beziehungen zur Grundlage der Hypothesen entwickeln
- Hypothesen erweitern

Vielen Dank!

Weitere Aufgaben

- Weitere Arbeit mit den Daten?
  - 1. Auf Konzeptebene weiterarbeiten
    - bestehende Konzepte/Kategorien/Beziehungen anwenden und erweitern
    - neue Konzepte/Kategorien/Beziehungen entwickeln
    - Vorteil: freiere Entwicklung neuer Konzepte/Kategorien
    - Nachteil: mehr Kodierarbeit, vom Weg abkommen
  - 2. Auf Kategorieebene weiterarbeiten
    - Kategorien auf die Daten anwenden
    - wenn Kategorie unpassend in Konzeptebene gehen und wie in 1. für diese Kateorie arbeiten
    - Vorteil: weniger Kodierarbeit wenn Kategorien passen
    - Nachteil: komplett neue Konzepte/Kategorien könnten übersehen werden