Institut für Informatik
Arbeitsgruppe Kommunikationssysteme

Prozessorientierte Biobank-Modellierung

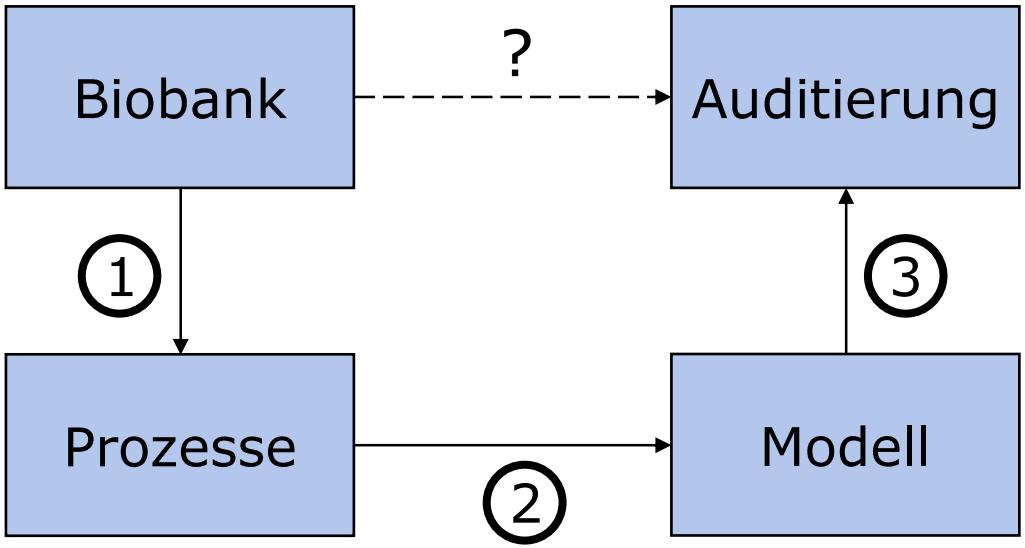
Die Basis für die datenschutzrechtliche Auditierung

Ralph Herkenhöner

Arbeitsgruppe Kommunikationssysteme
Institut für Informatik
Christian-Albrechts-Universität zu Kiel

Übersicht

Institut
für Informatik
Arbeitsgruppe
Kommunikationssysteme



Modellierung von Biobanken

Institut für Informatik
Arbeitsgruppe Kommunikationssysteme

(1) Prozesse, Rollen und ihre Beziehungen erfassen

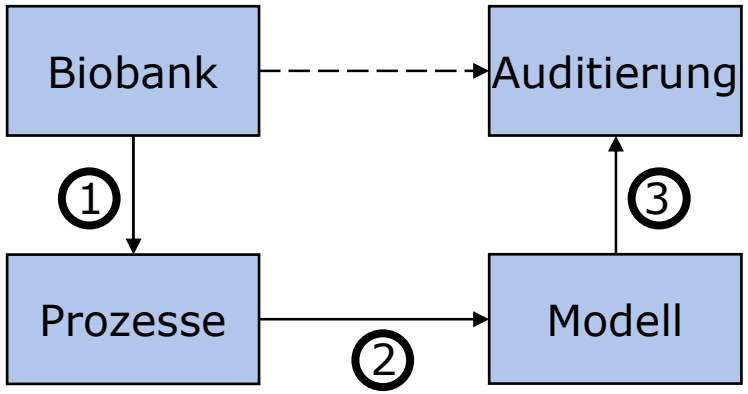
➔ Schaffen von Übersicht

(2) Aktivitäten und Abläufe modellieren

➔ Detaillierter Einblick in Prozesse

(3) Sicherheit und Datenschutz prüfen

➔ Fokus der datenschutzrechtlichen Auditierung



Prozessmodell [1]

Institut
für Informatik
Arbeitsgruppe
Kommunikationssysteme

- Einholung Informed Consent
  1. Erstellung des Formularwerks
  2. Prüfung des Formularwerks
  3. Aufklärung des Spenders
  4. Einwilligungserklärung durch den Spender
  5. Lagerung des Formularwerks

Prozessmodell [2]

Institut
für Informatik
Arbeitsgruppe
Kommunikationssysteme

- Gewinnung und Einlagerung von Proben und Daten
  1. Kontaktaufnahme
  2. Vorbereitung der Erhebung
  3. Erhebung (falls *Einholung Informed Consent* abgeschlossen)
  4. Speicherung der persönlichen Daten (optional)
  5. De-Identifizierung
  6. Einlagerung von Proben und Daten

Prozessmodell [3]

Institut für Informatik
Arbeitsgruppe Kommunikationssysteme

- Erhebung und Eingangsbehandlung
  - Gewinnung und Einlagerung von Proben und Daten
  - Follow-up
  - Daten- und/oder Probenerwerb
- Einhaltung der materiellen Datentreuhänderschaft
  - Einholung Informed Consent
  - Spenderwiderruf/Wegfall des Verwendungszwecks
  - Auskunftsanfragen zur Daten-/Probenverarbeitung
  - Feedback

Prozessmodell [4]

Institut
für Informatik
Arbeitsgruppe
Kommunikationssysteme

- Nutzung und Ausgangsbehandlung
  - Datenaufbereitung
  - Probenaufbereitung
  - Eigenforschung
  - Weitergabe an Dritte
- Management- und Sonderprozesse
  - Prozessmanagement – Zugriffsvergabe, Rollenvergabe
  - Monitoring/Qualitätssicherung
  - Zugriff durch Aufsichtsbehörde/Strafverfolgung

Modellierung von Biobanken

Institut für Informatik
Arbeitsgruppe Kommunikationssysteme

(1) Prozesse, Rollen und ihre Beziehungen erfassen

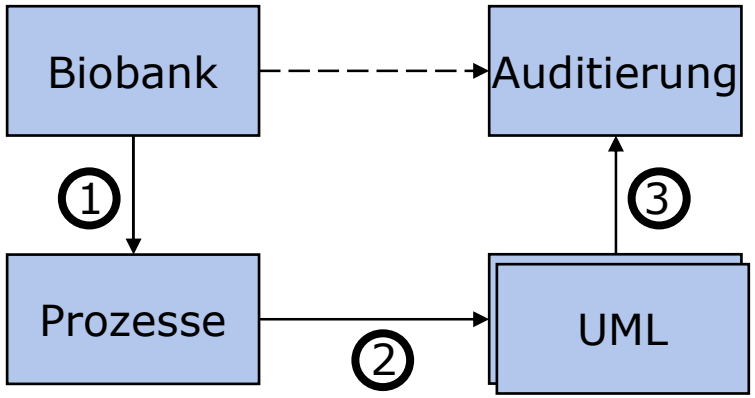
➔ Schaffen von Übersicht

(2) Aktivitäten und Abläufe modellieren

➔ Detaillierter Einblick in Prozesse

(3) Sicherheit und Datenschutz prüfen

➔ Fokus der datenschutzrechtlichen Auditierung



Unified Modeling Language (UML)

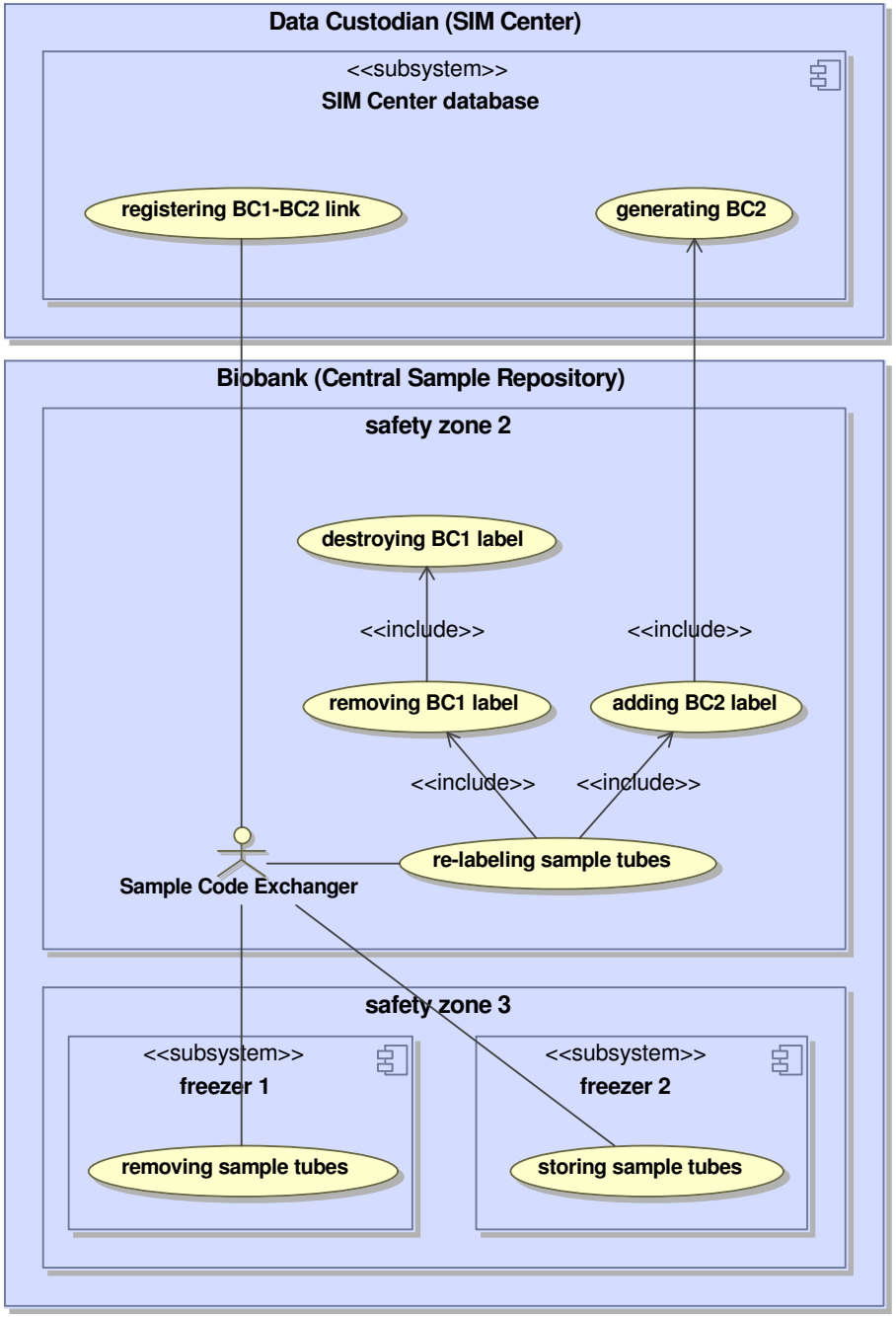
Institut für Informatik
Arbeitsgruppe Kommunikationssysteme

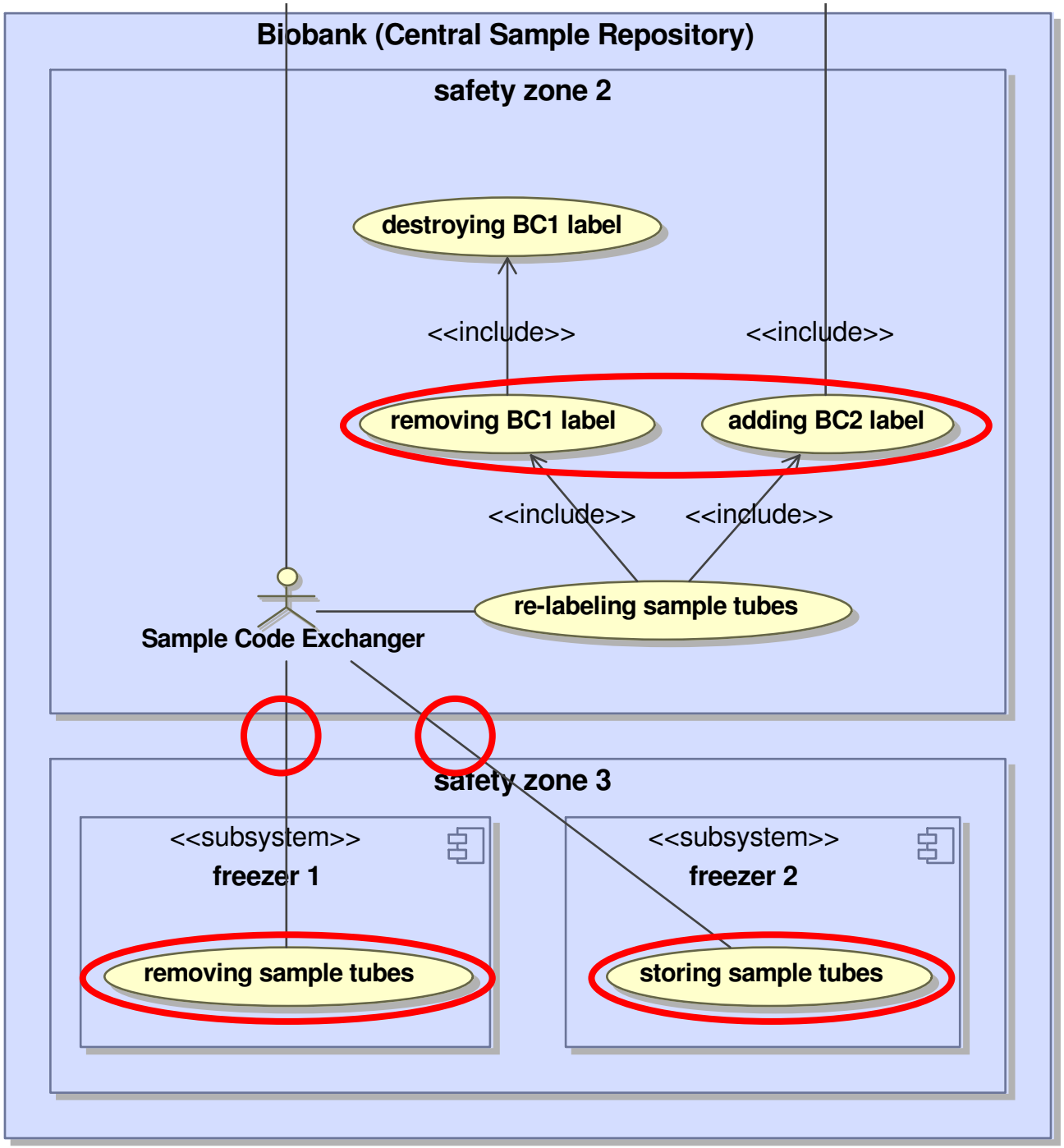
- De-facto-Standard
- *Object Management Group* (OMG)
- Methode für die graphische Systemmodellierung
- abgeschlossene Modellierungssprache
- "Modellierungsbaukasten" mit dreizehn Diagrammtypen
  - Strukturdiagramme
  - Verhaltensdiagramme

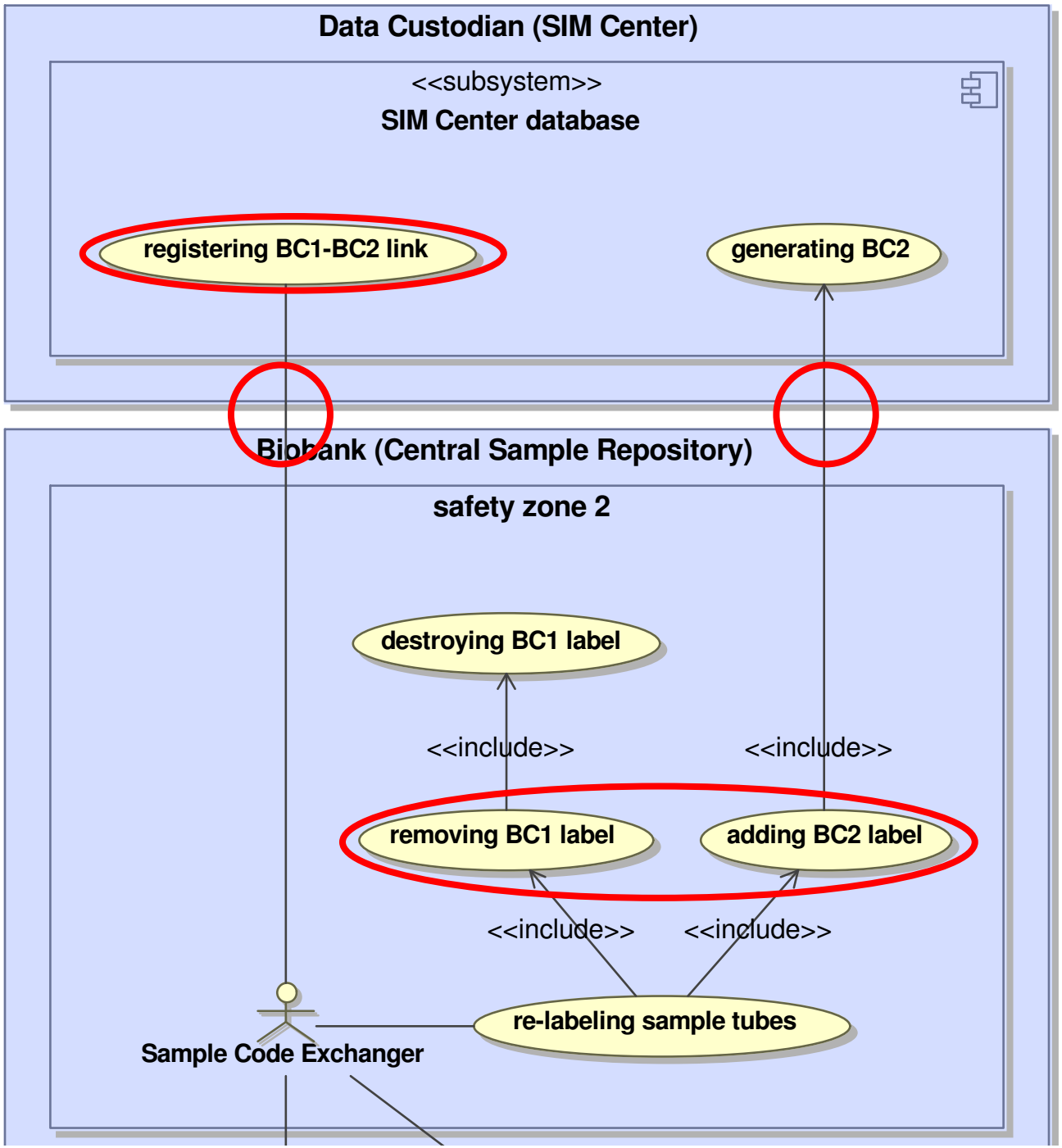
UML-Modellierung von Biobanken

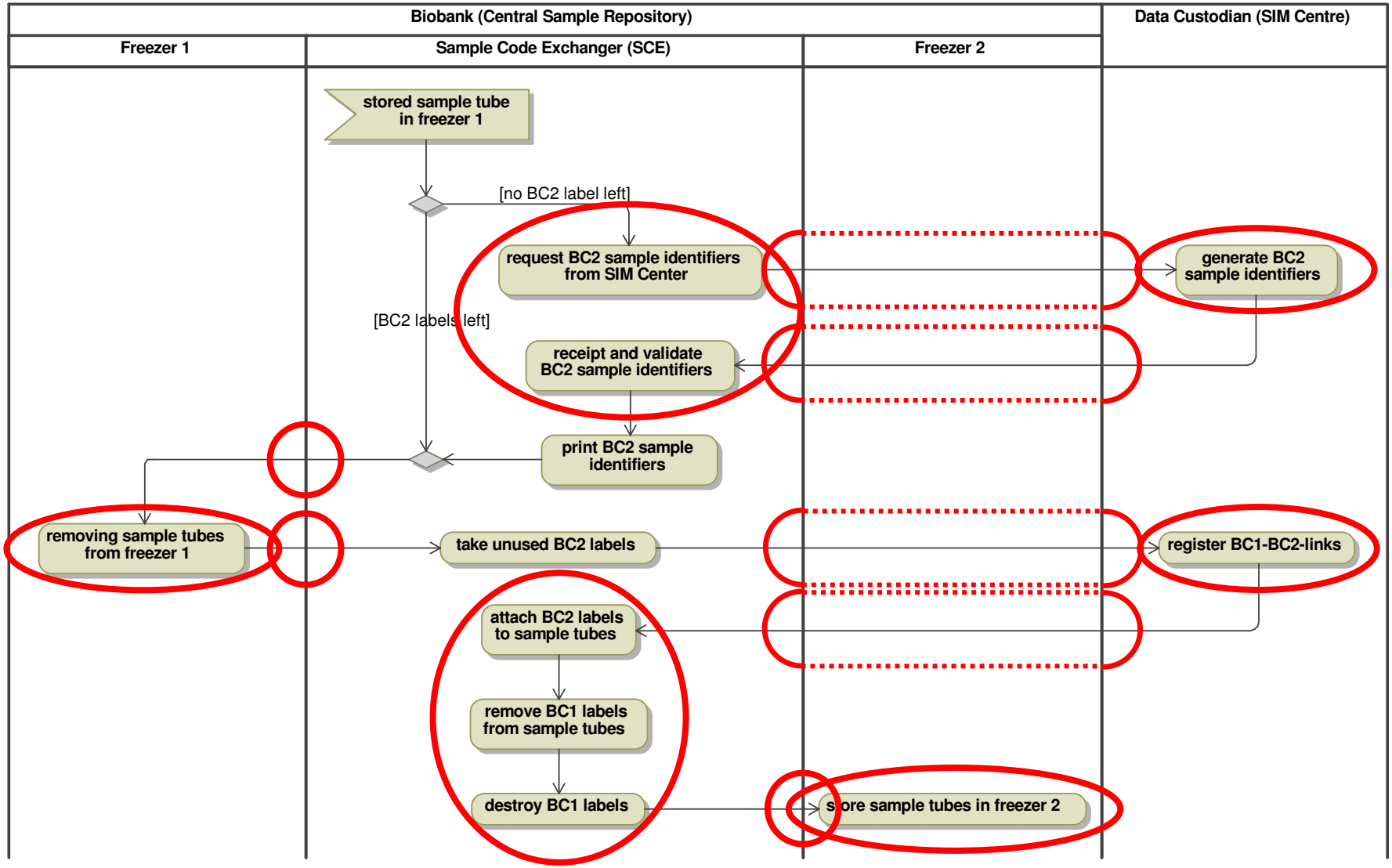
Institut für Informatik
Arbeitsgruppe Kommunikationssysteme

- Prozesse, Rollen und ihre Beziehungen
  - ➔ in UML: Anwendungsfalldiagramme
- Aktivitäten und Abläufe
  - ➔ in UML: Aktivitätsdiagramme
- Sicherheit und Datenschutz
  - ➔ in UML: keine direkte Entsprechung
  - ➔ Erweiterung von UML: z.B. UMLsec


Data Custodian (SIM Center)
<<subsystem>>
SIM Center database
registering BC1-BC2 link
generating BC2
Biobank (Central Sample Repository)
safety zone 2
destroying BC1 label
<<include>>
<<include>>
removing BC1 label
adding BC2 label
<<include>>
<<include>>
re-labeling sample tubes
Sample Code Exchanger
safety zone 3
<<subsystem>>
freezer 1
removing sample tubes
<<subsystem>>
freezer 2
storing sample tubes


Biobank (Central Sample Repository)
safety zone 2
destroying BC1 label
<<include>>
<<include>>
removing BC1 label
adding BC2 label
<<include>>
<<include>>
re-labeling sample tubes
Sample Code Exchanger
safety zone 3
<<subsystem>>
freezer 1
<<subsystem>>
freezer 2
removing sample tubes
storing sample tubes


Data Custodian (SIM Center)
<<subsystem>>
SIM Center database
registering BC1-BC2 link
generating BC2
Biobank (Central Sample Repository)
safety zone 2
destroying BC1 label
<<include>>
<<include>>
removing BC1 label
adding BC2 label
<<include>>
<<include>>
re-labeling sample tubes
Sample Code Exchanger


Biobank (Central Sample Repository)
Data Custodian (SIM Centre)
Freezer 1
Sample Code Exchanger (SCE)
Freezer 2
stored sample tube in freezer 1
[no BC2 label left]
request BC2 sample identifiers from SIM Center
generate BC2 sample identifiers
[BC2 labels left]
receipt and validate BC2 sample identifiers
print BC2 sample identifiers
removing sample tubes from freezer 1
take unused BC2 labels
register BC1-BC2-links
attach BC2 labels to sample tubes
remove BC1 labels from sample tubes
destroy BC1 labels
store sample tubes in freezer 2

Modellierung von Biobanken

Institut für Informatik
Arbeitsgruppe Kommunikationssysteme

(1) Prozesse, Rollen und ihre Beziehungen erfassen

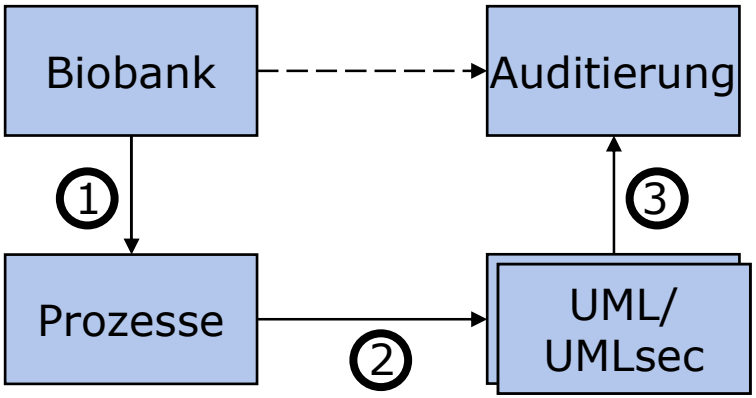
➔ Schaffen von Übersicht

(2) Aktivitäten und Abläufe modellieren

➔ Detaillierter Einblick in Prozesse

(3) Sicherheit und Datenschutz prüfen

➔ Fokus der datenschutzrechtlichen Auditierung



UMLsec

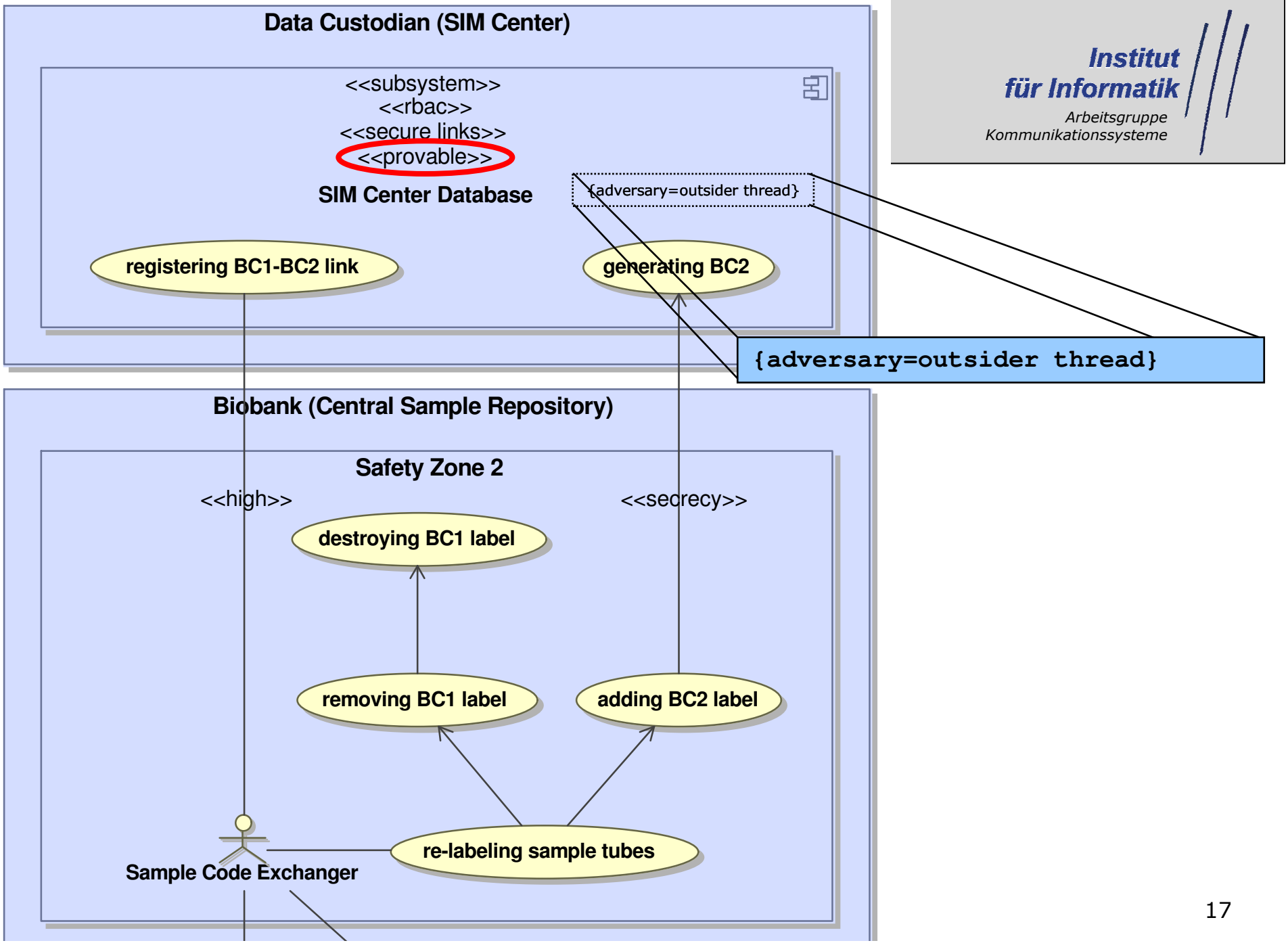
Institut
für Informatik
Arbeitsgruppe
Kommunikationssysteme

- UML-Erweiterung
  - insbesondere für Anwendungsfall-, Aktivitätsdiagramme
  - Einführung neuer sog. *Stereotype* (Eigenschaftsbezeichner) zur Abbildung von Sicherheitseigenschaften, z.B.:
    - offenes Netz: `<<internet>>`
    - Vertraulichkeit: `<<secrecy>>`
    - Nachvollziehbarkeit: `<<provable>>`
  - bietet formale Basis für Sicherheitsanalysen
  - erweiterbar um benutzerdefinierte Stereotype

Gesicherte Kommunikation

Institut für Informatik
Arbeitsgruppe Kommunikationssysteme

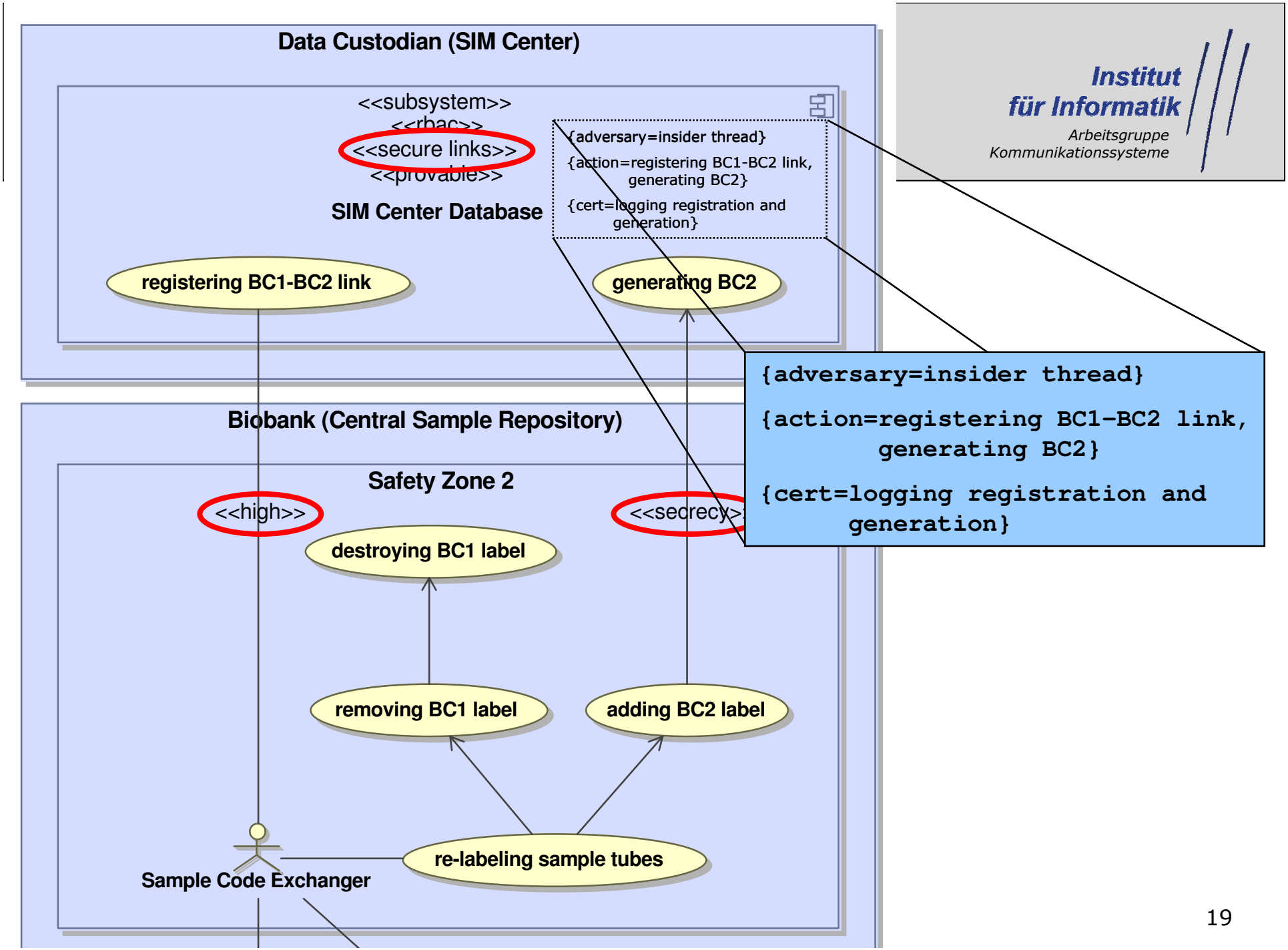
- Bedrohung: unbefugte Verarbeitung oder Kenntnisnahme
- Datenschutz durch: Vertraulichkeit und Integrität
- UMLsec: `<<secure links>>`
  - Angreifermodell: `{adversary=„adversary model“}`
  - Vertraulichkeit: `<<secrecy>>`
  - Integrität: `<<integrity>>`
  - Hochsicherheit: `<<high>>`


Data Custodian (SIM Center)
<<subsystem>>
<<rbac>>
<<secure links>>
<<provable>>
SIM Center Database
{adversary=outsider thread}
registering BC1-BC2 link
generating BC2
{adversary=outsider thread}
Biobank (Central Sample Repository)
Safety Zone 2
<<high>>
<<secrecy>>
destroying BC1 label
removing BC1 label
adding BC2 label
re-labeling sample tubes
Sample Code Exchanger

Protokollierung

Institut für Informatik
Arbeitsgruppe Kommunikationssysteme

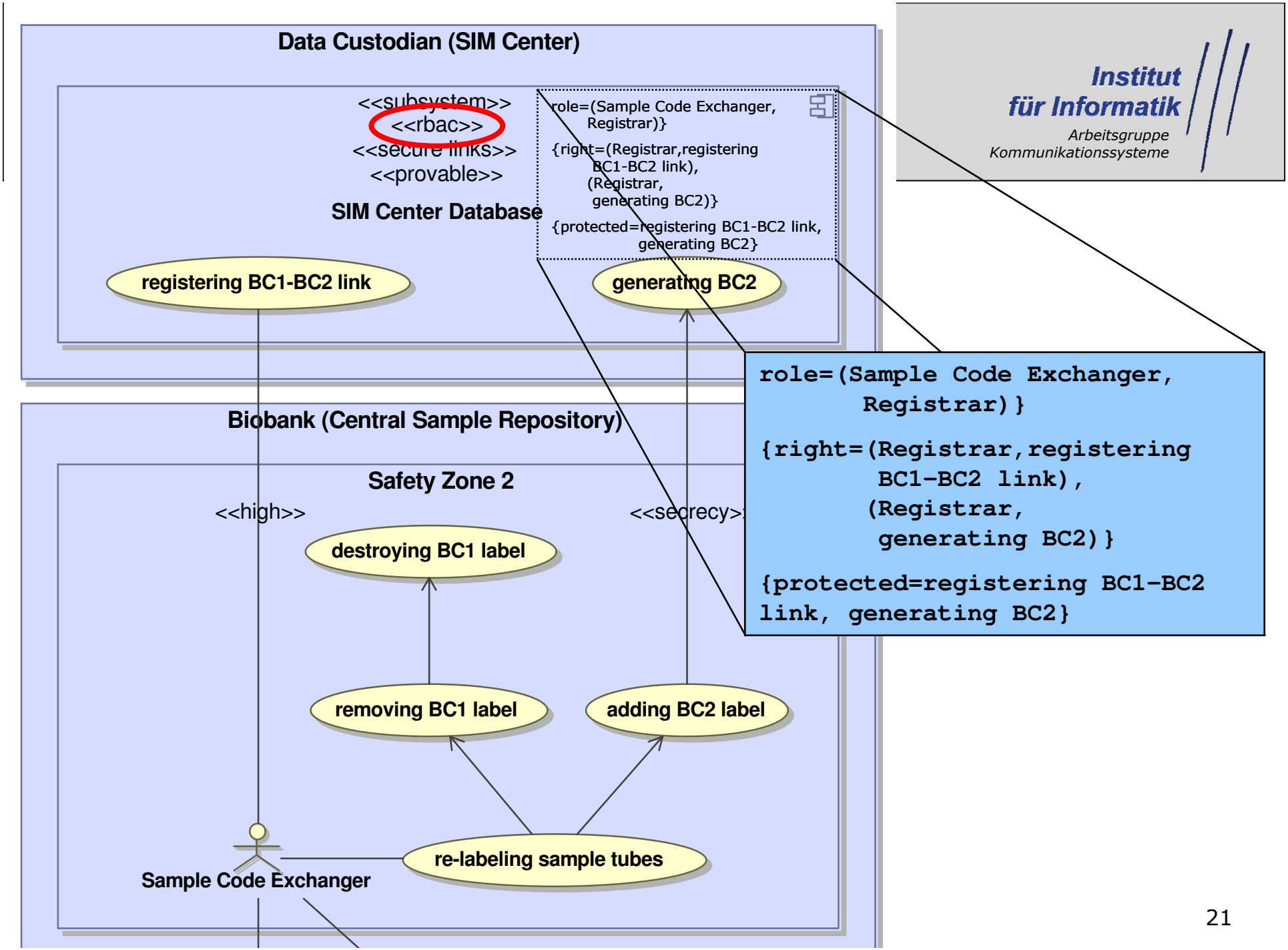
- Bedrohung: abstreitbare oder unbemerkte Verarbeitung
- Datenschutz durch: Transparenz und Nachvollziehbarkeit
- UMLsec: `<<provable>>`
  - Angreifermodell: `{adversary=„adversary model“}`
  - Betroffene Aktivität: `{action=action1,…}`
  - Nachweis: `{cert=„proof“}`


Data Custodian (SIM Center)
<<subsystem>>
<<rbac>>
<<secure links>>
<<provable>>
SIM Center Database
{adversary=insider thread}
{action=registering BC1-BC2 link, generating BC2}
{cert=logging registration and generation}
registering BC1-BC2 link
generating BC2
Biobank (Central Sample Repository)
Safety Zone 2
<<high>>
<<secrecy>>
destroying BC1 label
removing BC1 label
adding BC2 label
Sample Code Exchanger
re-labeling sample tubes
{adversary=insider thread}
{action=registering BC1-BC2 link, generating BC2}
{cert=logging registration and generation}

Rollenbasierter Zugriff

Institut
für Informatik
Arbeitsgruppe
Kommunikationssysteme

- Bedrohung: unerlaubte Zugriffnahme
- Datenschutz durch: Rollen- und Rechtevergabe
- UMLsec: `<<rbac>>`
  - Rollenmodell: `{role=(actor1,role1),…}`
  - Zugriffsrechte: `{right=(role1,action1),…}`
  - Zugriffsgeschütze Aktivitäten: `{protected=action1,…}`


Data Custodian (SIM Center)
<<subsystem>>
<<rbac>>
<<secure links>>
<<provable>>
SIM Center Database
role=(Sample Code Exchanger, Registrar)}
{right=(Registrar,registering BC1-BC2 link), (Registrar, generating BC2)}
{protected=registering BC1-BC2 link, generating BC2}
registering BC1-BC2 link
generating BC2
Biobank (Central Sample Repository)
Safety Zone 2
<<high>>
<<secrecy>>
destroying BC1 label
removing BC1 label
adding BC2 label
re-labeling sample tubes
Sample Code Exchanger
role=(Sample Code Exchanger, Registrar)}
{right=(Registrar,registering BC1-BC2 link), (Registrar, generating BC2)}
{protected=registering BC1-BC2 link, generating BC2}

Modellierung von Sicherheit und Datenschutz in UMLsec

Institut für Informatik
Arbeitsgruppe Kommunikationssysteme

- Gesicherte Kommunikation : `<<secure links>>`
- Protokollierung : `<<provable>>`
- Zugriffskontrolle
  - Rollenbasiert: `<<rbac>>`
  - Geschützt: `<<guarded access>>`
  - Geschützter Datenfluss: `<<no up-flow>>`, `<<no down-flow>>`
- Geschützte Datenvorhaltung: `<<data security>>`
- Geschützte Probenvorhaltung: `<<tissue security>>`
- Prozessverantwortliche Rolle : `<<responsible>>`
- De-Identifizierung: *keine Entsprechung in UMLsec*
  - Gesonderte Betrachtung → *2. Vortrag*

Fazit

- UML anwendbar für die Modellierung von Biobanken
- UMLsec zur Modellierung von Sicherheitsaspekten
- Standardisierte Beschreibung als Basis für die Auditierung
- Vorgehen bei Modellierung:
  - von Prozessen zum Modell
- De-Identifizierung benötigt gesonderte Betrachtung