Assuring Safe Interoperability of Medical Systems through Conformance Profiles

Jens H. Weber
University of Victoria and University of B. C.

University of Victoria

2023

University of B. C.

About the lab

We acknowledge and respect the lək̓ʷəŋən peoples on whose traditional territory the university stands and the Songhees, Esquimalt and W̱SÁNEĆ peoples whose historical relationships with the land continue to this day.

Medicine

Primary Care

Infor-matics

Quality

Software & Data

Engineering

Prof. Jens Weber, PhD, PEng

Prof. Morgan Price, PhD, MD

Acknowledgement: Oscar Costa, Aakash Tyagi

Medical device interoperability

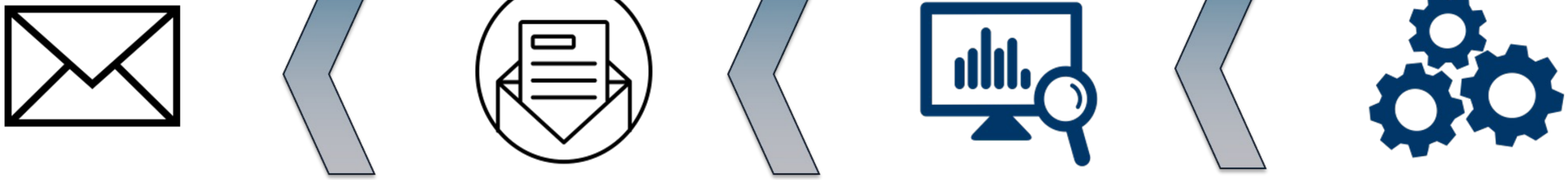
The ability to safely, securely, and effectively exchange and use information among one or more devices, products, technologies, or systems. [FDA] https://www.fda.gov/medical-devices/digital-health-center-excellence/medical-device-interoperability

Photo by National Cancer Institute on Unsplash

- heterogeneity
- complexity & scale
- no central control
- evolution

Levels of interoperability

Foundational → **Structural** → **Semantic** → **Organizational**



Connectivity *Format* *Meaning* *Use*

[HIMSS] https://www.himss.org/resources/interoperability-healthcare

Medical Interoperability & Safety

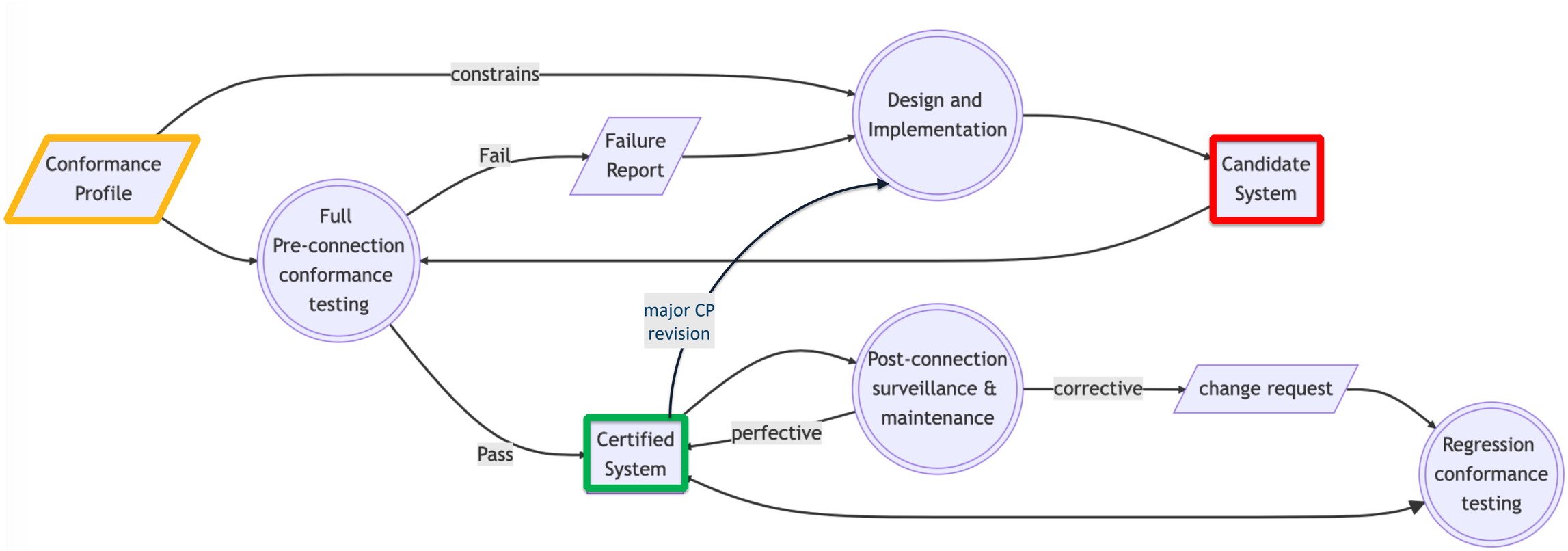
A significant percentage of patient safety events (PSEs) have been attributed to interoperability issues:

- How et al. (2018) 18.1% (Pennsylvania Patient Safety Authority)
- Leading categories: medication, laboratory, radiology

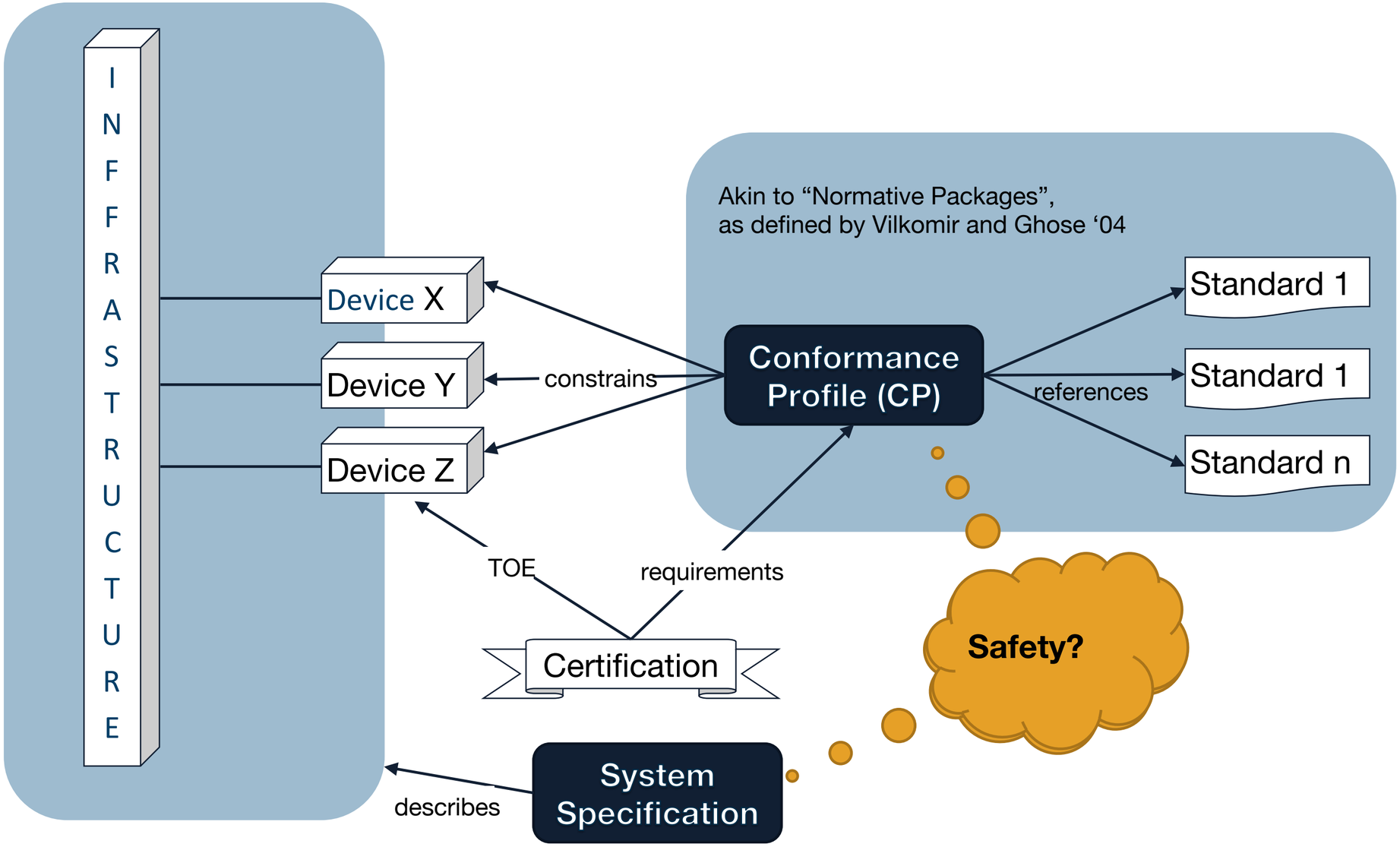
Li E, Clarke J, Ashrafian H, Darzi A, Neves AL. The Impact of Electronic Health Record Interoperability on Safety and Quality of Care in High-Income Countries: Systematic Review. J Med Internet Res. 2022 Sep 15;24(9):e38144. doi: 10.2196/38144. PMID: 36107486; PMCID: PMC9523524.

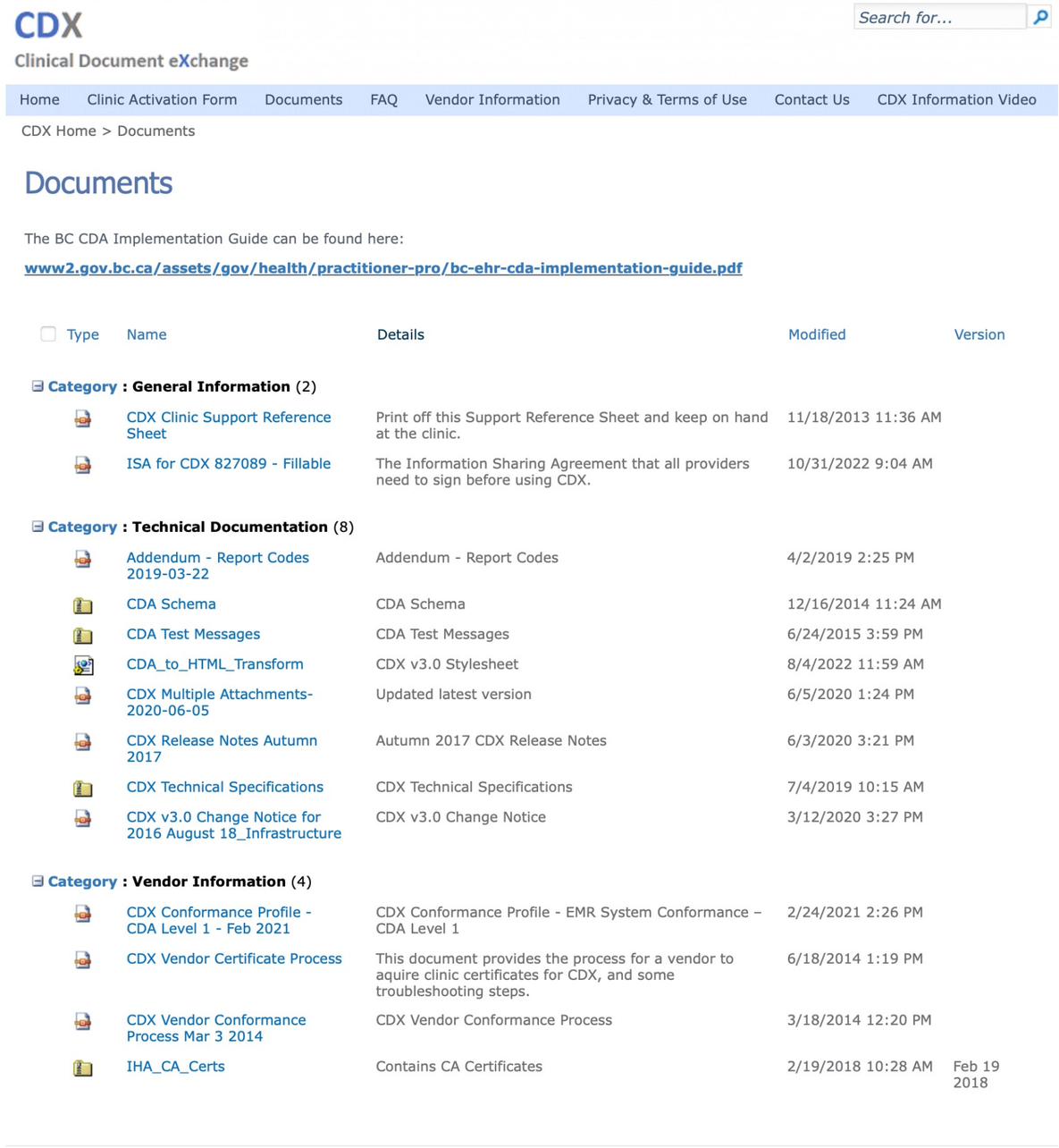
Conformance Profiles

A pivotal component in the conformance process



Challenge: Assurance of CPs





Case Study: British Columbia Clinical Document eXchange (CDX)

Conformance Profile and supporting documents at bccdx.ca

LEADLAB R&D project with PHSA and OSCAR EMR

R: Safe interoperability by Design

D: Develop CDX for OSCAR

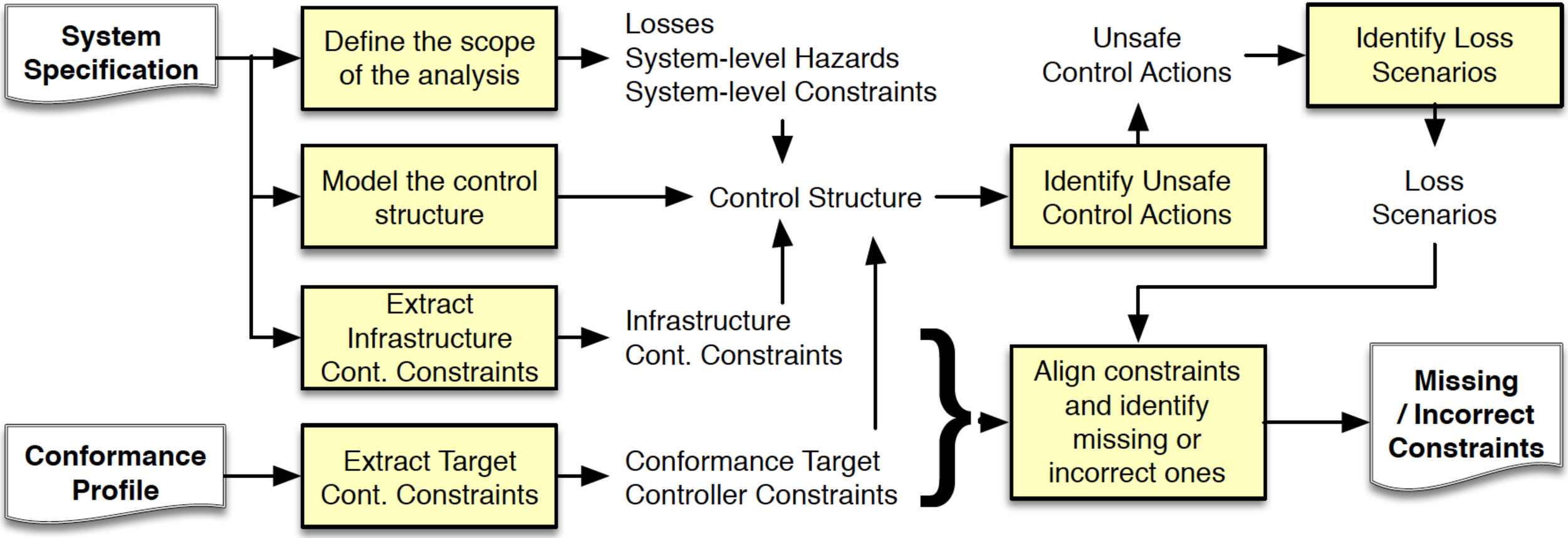
Research Question

Is hazard analysis at the level of Conformance Profiles possible and effective?

(i.e., without assumption about the design of a particular medical device)

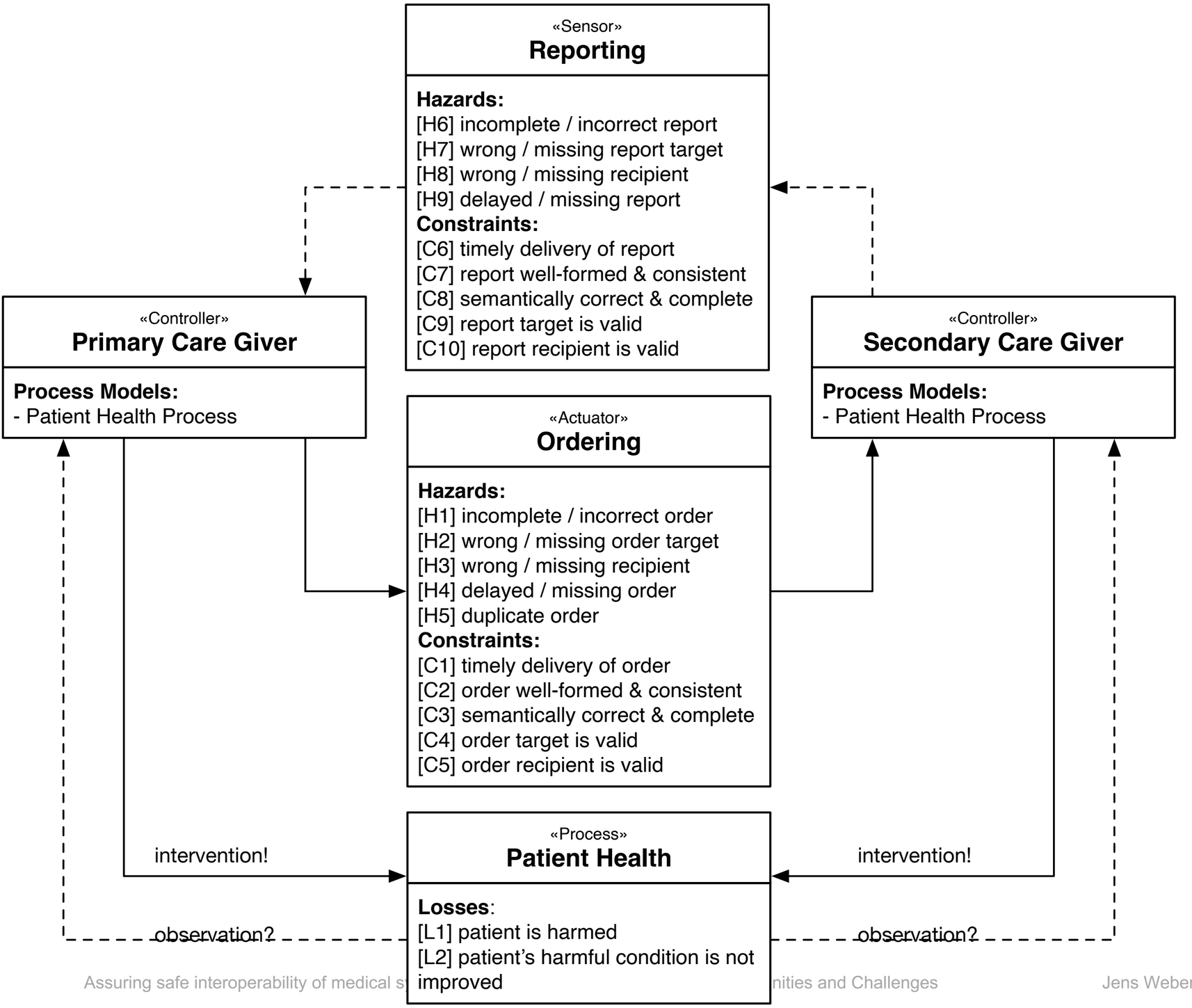
- Selected STPA for suitability to early lifecycle analysis
  - N. G. Leveson, Safety Analysis in Early Concept Development and Requirements Generation, INCOSE Int. Symp., vol. 28, no. 1, pp. 441–455, 2018
- Tailored method to evaluate interoperability conformance profiles (STPA-ICPA)

STPA-ICPA Method Overview



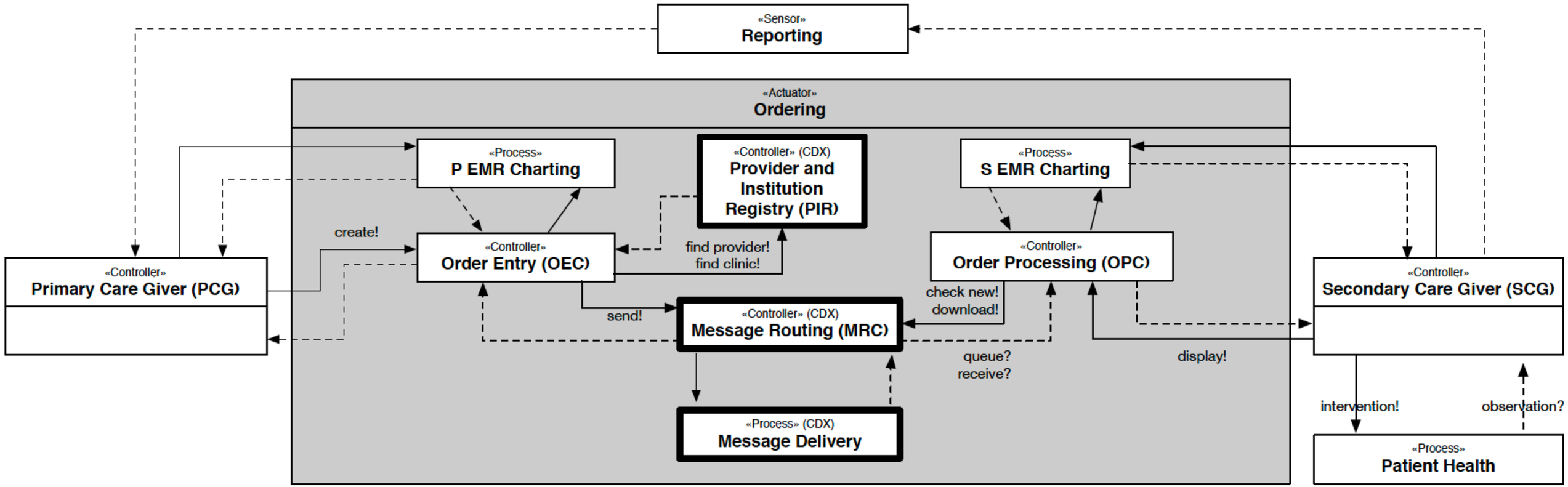
System-Level Control Structure

Example: e-Referral



Decomposition of *Order* Actuator

*** bold frames are elements of the interoperability infrastructure**



Extraction of Target Controller Constraints

- 42 safety-relevant constraints in 62 conformance statements
- Statements may be *mandatory* (SHALL), *recommended* (SHOULD), or *optional* (MAY)
- Assign to **controller** and control **action / feedback**

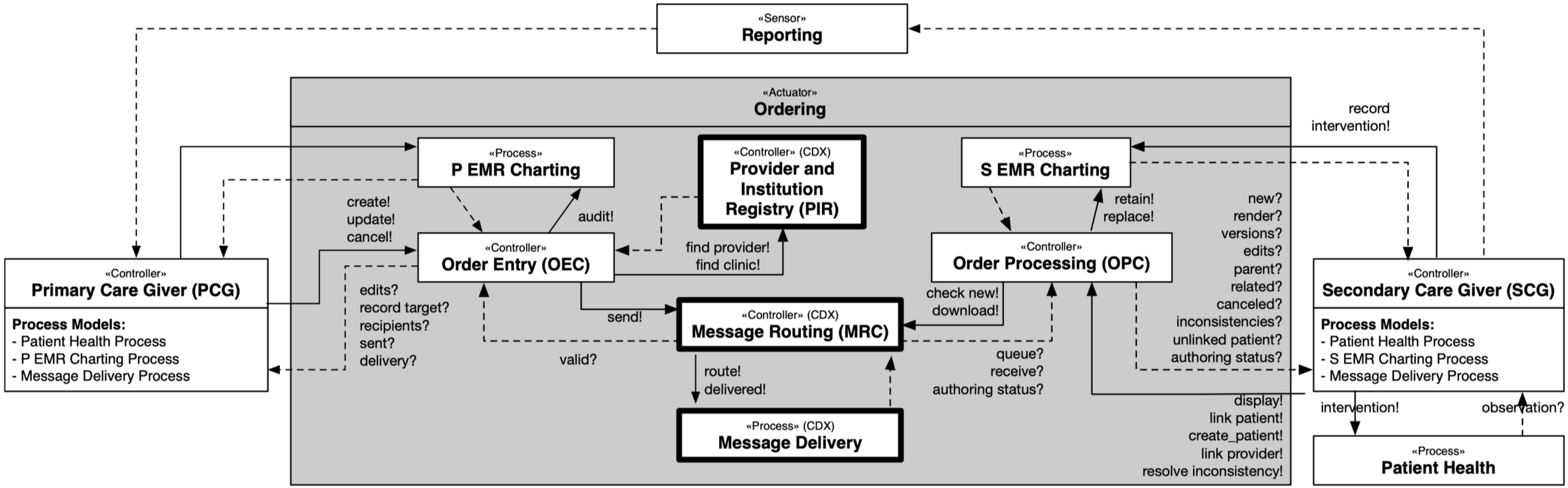
Controller Constraint	Reference	Controller(s)	Action / Feedback
CC1: sent messages are standards conform	R39	OEC	*send!*
CC2: receiver can link orders to patients manually if automatic linking is not possible	R16	OPC	***link patient!***
CC3: receiver can create a new patient chart created with the demographic information provided	R16	OPC	***create patient!***
CC4: receiver alerts users of cancelled orders (MAY)	R23	OPC	***cancelled?***
CC5: standards-conform messages can be received	R1,2,3,4	OPC	*download! receive?*
CC6: standards-conform documents can be rendered	R1,2,3,4	OPC	***render?***
CC7: message linked to at least one provider at clinic	R12,13	OPC	
CC8: no automatic deletion of messages	R12,13	OPC	
CC9: automatic patient linking requires at least 4-point match	R14	OPC	
CC10: users are alerted of inconsistencies between order and EMR data (patient demographics)	R15	OPC	***inconsistencies?***
CC11: inconsistencies between EMR data and order data can manually be resolved (SHOULD)	R15	OPC	***resolve inconsistency!***

Extraction of Infrastructure Controller Constraints

- More difficult, since infrastructure spec is less structured
- Extracted 11 safety-relevant constraints
  - 2 of them *cannot* be enforced by the infrastructure (!)

Controller Constraint	Reference	Controller(s)	Action / Feedback
CC43: Participating parties periodically check in with CDX for new documents	p. 11	OPC or SCG	*check new!*
CC44: if message specifies recipient provider but no clinic, then it is routed to all locations associated with provider	p. 11	MRC	***route!***
CC45: if message specifies recipient provider with specific clinic → route only to specified clinic	p. 11	MRC	*route!*
CC46: if recipient clinic is specified but no provider → route to clinic	p. 12	MRC	*route!*
CC47: if message specifies recipient provider as well as a clinic, but (according to CDX) the provider is not associated with the specified clinic, route to clinic	p. 12	MRC	*route!*
CC48: providers and clinics have unique identifiers	p. 12	PIR	
CC49: send messages must be valid in order to be routed. validation result returned to sender.	p. 14	MRC	***valid?***
CC50: message cannot be received by a party who is not a recipient	p. 14	MRC	*receive?*
CC51: a message is considered "new" (i.e., undelivered) for a location if and only if that location has not attempted to download it (*download!*)	p. 15	MRC	***delivered!***
CC52: receiver ensures that all messages indicated as new (i.e., undelivered) are eventually successfully downloaded	p 15	OPC	*queued?* *download!*
CC53: messages are re-downloadable for a finite period of time	p. 17	MRC	*download!*

Control Structure after adding extracted control actions & feedback signals



Identification of Unsafe Control Actions (UCAs)

Identified 74 UCAs

Control Action	Not providing causes hazard	Providing causes hazard	Too early, too late, out of sequence	Stopped too soon, applied too long
CA4: *send!*	**UCA4.1**: OEC does not provide *send!* when a PCG has provided *create!*, *update!* or *cancel!* [H4]	**UCA4.2**: OEC provides *send!* with record target/recipients/content different from what PCG has entered when providing *create!*, *update!* or *cancel!* [H1-H4]	**UCA4.3**: OEC provides *send!* too early, when the PCG is not ready to finish providing *create!*, *update!* or *cancel!* [H1-3] **UCA4.4**: OEC provides *send!* too late, when the PCG has already finished providing *create!*, *update!* or *cancel!*[H1-3]	
CA6: *route!*	**UCA6.1**: MRC does not provide *route!* because of inconsistency in recipient information [H4] **UCA6.2**: MRC does not provide *route!* because of a malfunction [H4].		**UCA6.3**: MRC provides *route!* on subsequently *sent!* messages in an order differently from the order the messages were *sent!* [H1]	**UCA6.4**: MRC stops providing *route!* too soon, before *sent!* message has been delivered to all recipients [H5] **UCA6.5**: MRC continues providing *route!* too long, routing duplicate messages delivered to recipients [H5]

Identify Loss Scenarios & align constraints

-> identify missing / incorrect constraints

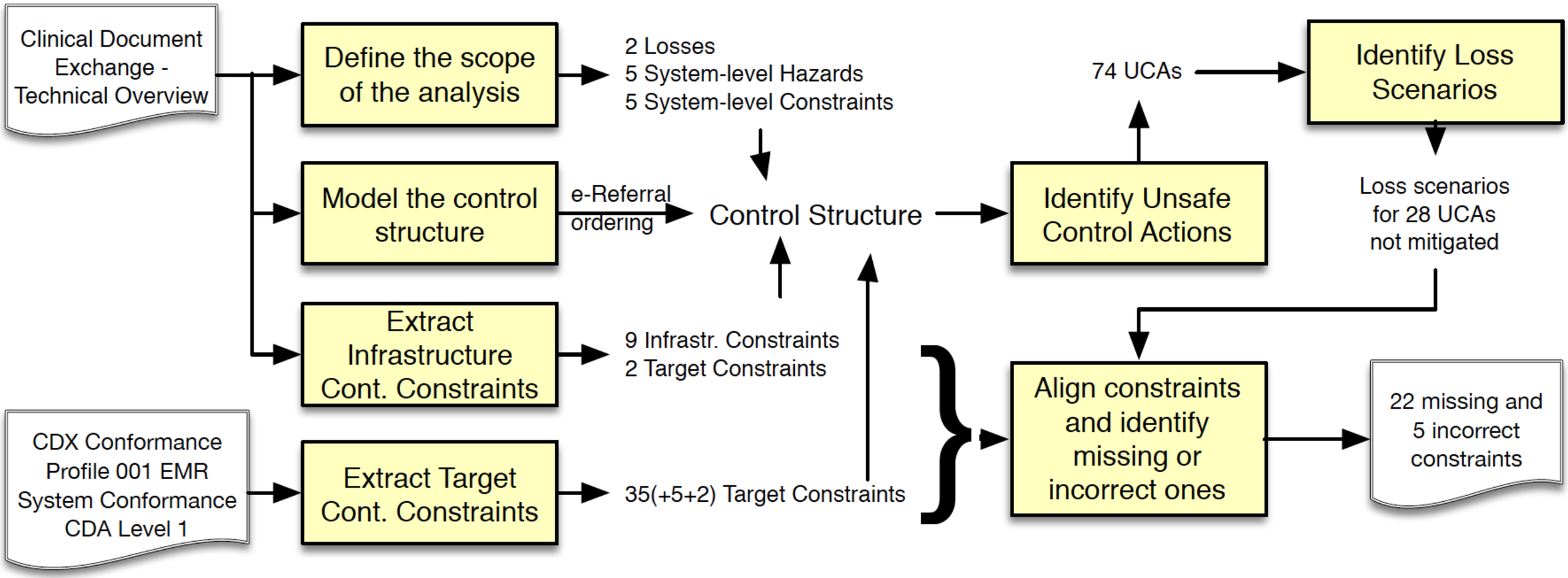
UCA	Loss Scenarios	Aligned Controller Constraints	Additional Feedback
UCA1.1: PCG provides *create!* with mis-identified / ambiguous / missing record target [H2]	• PCG picks wrong patient with similar name / ID • PCG has multiple patient charts open and creates order for wrong chart • PCG enters patient data incorrectly • PCG forgets to specify patient	• CC1: sent messages are standards conform (implies record target present) • CC24: record target shown clearly in user's view (while creating order) • CC25: record target identified with 4-point info in order	
UCA1.3: PCG provides *create!* with incomplete/ incorrect order content [H1]	• PCG creates order that incorporates data directly from the EMR; PCGs mental model of the incorporated data is not consistent with the actual incorporated data; • the data incorporated into the order is incorrectly/incompletely transformed into the interoperability standard	(**new**) Compiled order content is rendered completely in user view (OEC) (**new association with OEC**) CC17: order is rendered with approved viewer (OEC)	***render?***

UCA6.3: MRC provides *route!* on subsequently *sent!* messages in an order differently from the order the messages were *sent!* [H1]	a first message is sent by the OEC, followed by an update, correction or cancellation message; the two messages are routed (and queued) in reverse order; the receiving OPC accepts replaces the first received message by the later received message, leading to an incorrect /superseded order.	(**new**) The order by which messages are queued is not significant (OPC) **(modified)** CC14: a document with "final" authoring status that ~~**is received**~~ was authored after a version of the same document with "preliminary" status replaces the latter; they are not concatenated **(modified)** CC15: if document with "cancelled" authoring status ~~**is received**~~ that was authored after previous document version, cancelled document replaces previous one; history is maintained **(modified)** CC16: if document with "updated/corrected" authoring status is received, previously authored version of document is replaced; history is maintained	
UCA7.3: MRC provides *delivered!* too early, before OPC has completed providing *download!* [H4]	The OPC begins downloading a message at which time the MRC marks it as "delivered", but the download is interrupted due to either a failure of the MRC or the OPC. The MRC now considers the message delivered, while it has not been downloaded.	(**new**) CC52: receiver ensures that all messages indicated as new (i.e., undelivered) are eventually successfully downloaded (mentioned in implementation guide but not enforced in conformance profile)	
UCA12.3: SCG provides *display!* on the wrong document associated with the right patient [H1]	There are several active orders for a patient. The SCG opens an order that was already acted on rather than opening the order that has not yet been executed.	**(new)** the order fulfillment status is indicated in the user view (OPC)	***fufilled?***

Hazard analysis identified 22 missing constraints and 5 incorrect ones

Constraint	Controller	Status
NC1: Compiled order content is rendered completely in user view	OEC	new
NC2: Dismissing the order entry view requires confirmation if order not sent; unsent orders can be saved	OEC	new
NC3: The existence of unsent orders is indicated in PCGs regular work view	OEC	new
NC4: Validation errors are displayed and can be resolved	OEC	new
NC5: Active orders for the same record target are in the user view	OEC	new
NC6: the record target of a sent order cannot be updated. (an order created for the wrong record target must be cancelled)	OEC	new
NC7: when an order is updated or cancelled, recipients can only be added but not removed	OEC	new
NC8: only the latest version of an order can be updated or cancelled	OEC	new
NC9: Only active orders (not fulfilled ones) can be updated or cancelled	OEC	new
NC10: order carries cryptographic checksum	OEC	new
NC11: message integrity checked	MRC	assumed
NC12: order send action requires user confirmation	OEC	new
NC13: user alerted of undelivered orders after timeout	OEC	new
NC14: The order by which messages are queued is not significant	OPC	new
CC14: a document with “final” authoring status that ~~**is received**~~ was authored after a version of the same document with “preliminary” status replaces the latter; they are not concatenated	OPC	corrected

Summary of Analysis Results



Work Experience and Effort

e-referrals are just *one* of seven bidirectional clinical workflows supported by CDX

Other workflows are similar (as they use the same infrastructure and foundational interoperability mechanisms) but also have semantic and organizational differences.

- reuse models

Concrete medical devices (like OSCAR) further refine the analysis models

- Tool support beyond spreadsheets and text documents greatly facilitates reuse and traceability

Candidate STPA Tools

Open Source:

- XSTAMPP (U Stuttgart, Germany)
- STAMP Workbench (IPA, Japan)
- CAIRIS (Bournemouth U, England)
- WebSTAMP (ITA, Brazil)
- FASTEN (Siemens, Germany)

Selected FASTEN (active project, projectional editor based on JetBrains MPS)

Extensions to FASTEN to support STPA-ICPA

- Traceability between constraints, UCAs, controller actions and feedback.
- All four element types (**controllers, actuators, sensors, and processes**)
- Consistency verification
- Linked loss scenarios
- Full document exports/reports

Oscar Costa's thesis on FASTEN web site

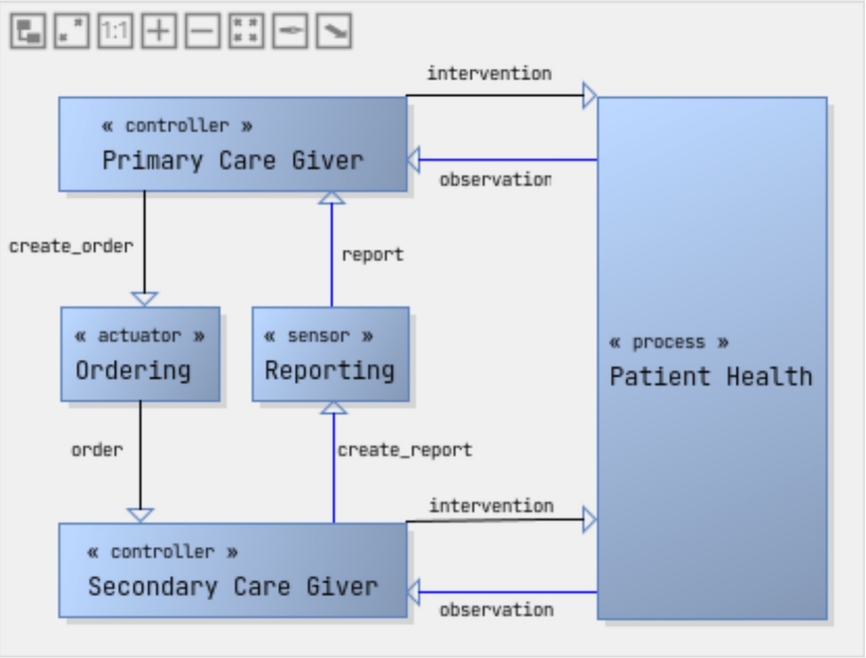
Source code on Github:
https://github.com/oscarcosta/stpa.icpa.

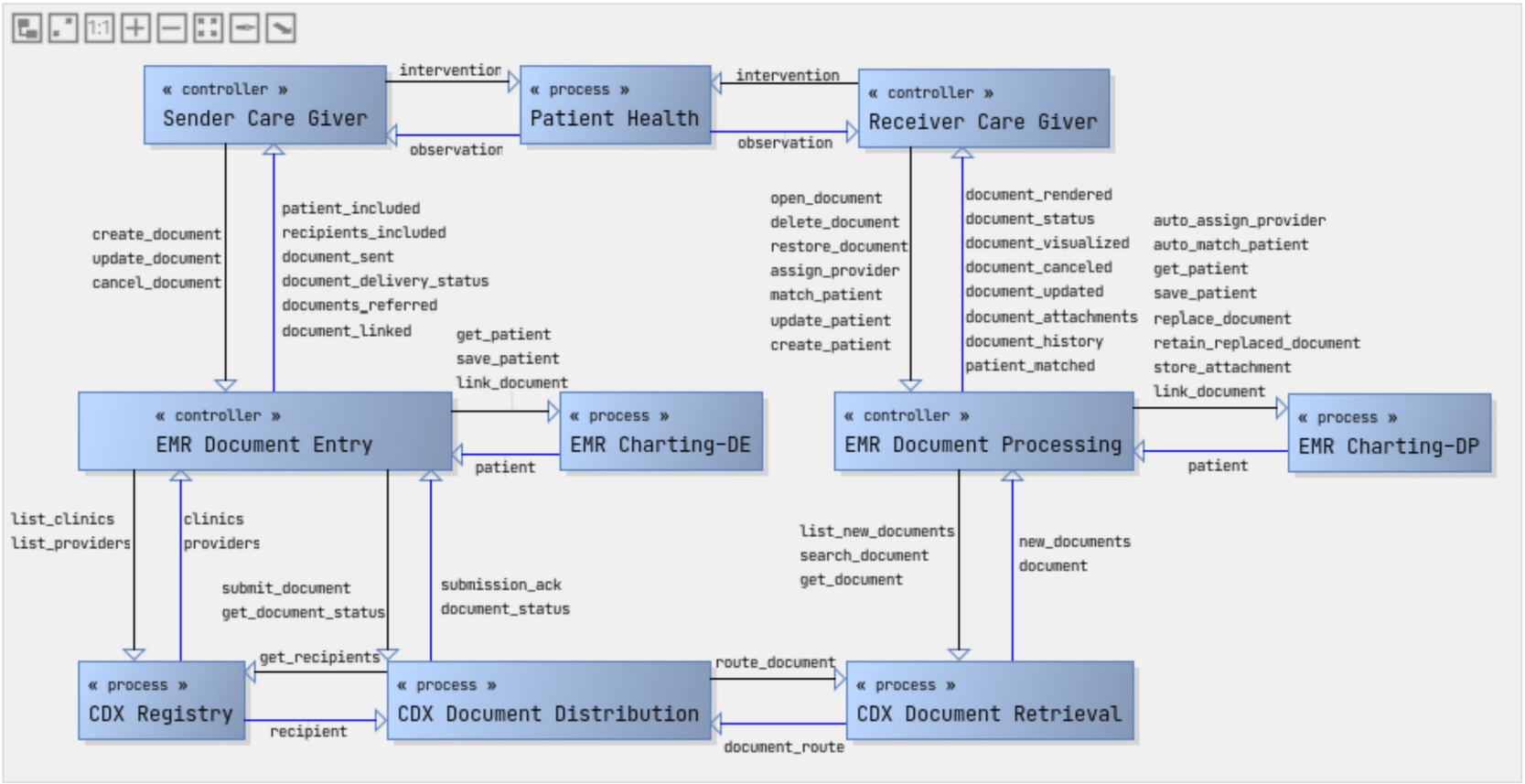
Req CC-002 : Standardized documents are rendered.
kind: controller constraint - associated control actions:
controller: Receiver Care Giver - **action/feedback:** open_document
controller: EMR Document Processing - **action/feedback:** document_rendered

Reference: CDX Conformance Profile - CDA Level 1,
Conformance Sessions IDs 1, 2, 3, 4, 28, 38

Req CC-003 : Received documents are automatically assigned to at least one provider.
kind: controller constraint - associated control actions:
controller: EMR Document Processing - **action/feedback:** auto_assign_provider

Reference: CDX Conformance Profile - CDA Level 1,
Conformance Sessions IDs 12, 13





Tool greatly facilitates analysis

Conclusions

- System-theoretic hazard analysis on Conformance Profiles is an effective way to ensure safer interoperability
  - ➢ Identified several high-profile problems
- Tool support is highly recommended
  - ➢ Model reuse, traceability, and consistency checks
- Results of the HA communicated back to PHSA
- Separate HA for OSCAR EMR
- OSCAR has been certified and is in clinical use
- All results of the project available in open source

Thanks

jens@acm.org

University of Victoria

2023

University of B. C.

References

1. N. G. Leveson, **Safety Analysis in Early Concept Development and Requirements Generation**, INCOSE Int. Symp., vol. 28, no. 1, pp. 441–455, 2018
2. J. Weber and O. Costa (2020**). Adapting a System-Theoretic Hazard Analysis Method for the Analysis of an eHealth Interoperability Conformance Profile**. Proc. of AMIA 2020 Informatics Summit, March 23-26, Houston, USA
3. J. Weber and J. Ho. (2019). **Applying Bidirectional Transformations to the Design of Interoperable EMR Systems**. J Healthc Inform Res. Springer, DOI 10.1007/s41666-019-00065-0
4. J. Weber and O. Costa (2019). **Hazard Analysis of Interoperability Conformance Profiles – An Industrial Case Study in Healthcare**. Proc. of CASCON 2019, Nov. 4-6, Toronto, IBM Corp
5. **Adapting a System-Theoretic Hazard Analysis Method for Interoperability of Information Systems in Health Care**, by O. Costa Rocha, Master Thesis, University of Victoria, 2022
6. A. Scarinci, A. Quilici, D. Ribeiro, F. Oliveira, D. Patrick, and N. G. Leveson, “Requirement Generation for Highly Integrated Aircraft Systems Through STPA: An Application,” J. Aerosp. Inf. Syst., vol. 16, no. 1, pp. 9– 21, Nov. 2018.