Agenda

May 6, 2024: “Leverson on Systems"

- **Introduction:**
  - Code of Conduct
  - Communication -- Miro and Zoom Chat
  - Continuing the discussion: Discord server (ask Ruth for invite)
  - Introduce Adrian Cockburn. (Follow Adrian on Mastodon: @adrianco@mastodon.social)

- **Discussion led by Adrian Cockcroft**
  Paper: How to Perform Hazard Analysis on a "System-of-Systems" by Nancy Leveson
  - Introductions in chat or miro sticky - where are you (location/work) and something about why you are here
  - Why is this paper interesting?
  - What is the definition of a system
  - Emergence
  - Systems of systems and increasing complexity
  - System Theoretic Process Analysis (STPA) http://psas.scripts.mit.edu/home/
  - Ballistic Missile Defense System example
  - STPA based top down hazard analysis
  - Failing over without falling over - applying STPA to IT infrastructure
  - https://github.com/adrianco/slides/blob/master/FailingWithoutFalling-9.29.pdf

Paper (http, pdf): http://sunnyday.mit.edu/SOS-hazard-analysis.pdf

- **Wrap**
  - Thank you Adrian! And everyone participating.
  - Next session: June 3: Mel Conway, "Ubiquitous wideband peer-to-peer nudging is taking us to an unfamiliar place" https://checkout.tito.io/bredemeyer/conway

Main ideas covered in the paper

Acronyms:
STPA - Systems Theoretic Process Analysis

UCA - Unsafe Control Action

SC - Safety Constraint

This systems analysis focuses on man-made systems.

Social systems are man-made.

"While the components may exist in reality, the system itself only exists in the minds of the viewers."

1

Systems have states.

A state is a set of relevant properties describing the system at a point in time.

interactions between components have their own state spaces beyond the component states

Events cause state changes.

A hazard is a system state that results in loss.

"System of systems" - Dunbar's number and phase transition points at different levels of "system" - Kim

Summary of paper:
- Systems of systems isn't really a thing; it's just a system
- Basic definition of a system (hasn't changed in decades, but not well known)
- Examples how STPA works on something previously called "system of systems"

System Theoretic Process Analysis (STPA) http://psas.scripts.mit.edu/home/

Failing over without falling over - applying STPA to IT infrastructure
https://github.com/adrianco/slides/blob/master/FailingWithoutFalling-9.29.pdf

Comparison between FMEA and STPA:
https://link.springer.com/content/pdf/10.1007/s11219-017-9396-0.pdf?pdf=button

STPA and STAMP tutorial: https://psas.scripts.mit.edu/home/wp-content/uploads/2014/03/Systems-Theoretic-Process-Analysis-STPA-v9-v2-san.pdf

STPA at google: http://psas.scripts.mit.edu/home/wp-content/uploads/2021/06/2021-06-23-1210__Falzone_Thomas.pdf

"Dev

STPA Handbook https://psas.scripts.mit.edu/home/get_file.php?name=STPA_handbook.pdf

Engineering a safer world: https://mitpress.mit.edu/9780262533690/engineering-a-safer-world/

"Make illegal states unrepresentable" principle from Jaron Minsky

Related theories

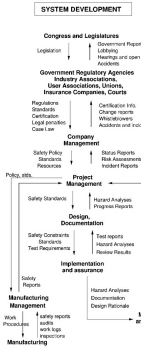

Figure 3.2: A

Residuality theory:
https://www.cutter.com/sites/default/files/APM/2020/baseeu2005.pdf

https://www.uptime.eu/building-sustainable-software-architectures-using-residuality-theory/

Stressor analysis in RT: https://weave-it.org/blog/designing-resilient-bounded-contexts-residuality-theory-ddd/

HAZOP: https://en.wikipedia.org/wiki/Hazard_and_operability_study

Common ground and coordination in joint activity:
https://jeffreymbradshaw.net/publications/Common_Ground_Single.pdf

A CLASSIFICATION OF UNCERTAINTY FOR EARLY PRODUCT AND SYSTEM DESIGN :
https://web.mit.edu/deweck/Public/Alstom/deWeck_Eckert_Uncertainty_2007.pdf

We'll add notes from Zoom chat
http://sunnyday.mit.edu/SOS-hazard-analysis.pdf

Thank you for this topic Adrian!

STPA - Systems Theoretic Process Analysis

You could describe Rube Goldberg machines as being systems made out of components nobody expected to go together.

I've been mentally comparing this definition to what I've been reading about complex systems recently.
It's ok to have competing definitions, the paper is nice because it defines *its* use then uses it.
This paper reminded me of Chunglin Kea's baroque vs romantic complexity, which I know of through John Law's work:
https://www.lancaster.ac.uk/fass/resources/sociology-online-papers/papers/law-and-if-the-global-were-small.pdf

The difference by observer recalls Susan Leigh Star's idea of infrastructure as a relation (dependent on point of view of the observer) in The Ethnography of Infrastructure and Got Infrastructure?

One of the distinctions here is that she limits her focus to designed/engineered systems, where some of the other discussions have dealt with biological/ecological systems that don't necessarily have a specific intended purpose.

I loved the explicit point that social systems are man-made systems.
That was a point that I found interesting, too - especially since our social systems are often *not* designed with an intentional purpose, but they *are* still human-constructed.
Which again contrasts strongly with notions of social in other disciplines 🙂

I think it's not a strict binary. For large enough systems that last for a long time (like a city), the emergent properties probably affect as much any purpose/design.

This work accords strongly with "stock and flows" Systems Dynamics, which makes sense to me as both come out of MIT

Clarifying the terms states and events is really crucial point to sort out in the real world where the difference might be more ambiguous.

If the environment can affect the system is it part of the system?

In this paper, and most systems work, no. The notion of system boundaries is pretty central
Depends on perspective in some cases. If the system is conceived of as *open*, there's necessarily an environment outside "the system".
Subsystems seem like a useful abstraction here too. A will have different boundaries from AB and from A2.

Code of Conduct

Our participation here reflects our mutual agreement and commitment to each other to follow this code of conduct during our discussion today. It applies equally to all of us (including facilitators).

- We share a commitment to providing a friendly, safe and welcoming meeting experience for all, regardless of level of experience, gender identity and expression, sexual orientation, disability, personal appearance, body size, race, ethnicity, age, religion, nationality, or other similar characteristic.
- Please be kind and courteous. Please avoid using terms that might detract from a friendly, safe and welcoming environment for all.
- Respect that people have differences of opinion and that our discussions will reflect different perspectives, trade-offs and impacts. There is seldom a right answer.
- Should anyone insult, demean or harass others in this setting, they will be excluded from interaction (contact the facilitators, if this happens). That is not welcome behavior.
- Likewise any spamming, trolling, flaming, baiting or other attention-stealing behavior is not welcome.

Note: We have adapted this code of conduct from the Ruby Code of Conduct.

Adrian Cockcroft
Monterey, California
Semi-retired technologist and advisor
@adrianco@mastodon.social

Dave van Stein
Netherlands

Organisation anthropologist & archeologist (ie I try to make sense of organisational processes) aka agile compliance/risk/security person

@dave_von_s@infosec.exchange

Michael McCliment
Toronto

Leading an automation/build & release team at Ubisoft

Essentially doing architecture for sociotechnical systems these days

Bruno Felix
Madrid, Spain

Software engineer - currently acting as architect for the anti-money laundering business unit at Klarna

junosuarez.com
software engineer in core infrastructure @ Slack
Portland, Oregon

Kim Wallmark
Boston area, USA

Primarily a software developer, with a lot of experience in legacy code and other complex systems / problems / situations.

Ruben Mezas

Head of IT - Software Engineer, Architecture, Security

Hi! Ben Braithwaite, I'm a doctor in East London, UK, with an interest in patient safety. Stretching the very limits of my comfort zone here...

Nathan Schimke
Practicing systems engineer, SRE, etc. Building platforms for production infrastructure, presently at a cloud security provider. Interested in system legibility and safety.

Andra Sonea, London
University of Warwick
Researcher, Solutions architect

Claudius Link
from Kassel/Germany
Software Developer turned Cybersecurity Consultant
Securing Sustainable Energy Production
@realn2s@infosec.exchange

Ruth Malan
I work in systems design, architecture, tech leadersip etc areas

I'm Shaun Greene (he/him). I help build digital systems for enterprises, largely in robotics and manufacturing, often called "digital twins". I'm here as part of this community of systems thinkers inspecting and attempting to understand how things work beyond individual choices as a way to think more of one human brain
shaungreene@mastodon.social
ductape312@twitter

'm Yvonne Lam (she/her), in Seattle, WA USA. Currently not working; when I am I work on non-product software areas: reliability, quality, release engineering/deployment, data analysis.

Tiani Jones
I working organizational effectiveness for socio-technical systems and coincidentally mostly in aerospace recently

Subsystems seem like a useful abstraction here too. A will have different boundaries from AB and from A2.

shrieks in externalities

It's useful to conceive of "degree of openness/closedness" on a spectrum, rather than a binary

I like the hazard part and compare it to exception handling in code and how a robust system deals with the errors it knows will happen all the way up to how it involves/affects a human eventually.
You can generically handle many exceptional things, but some have greater impact than others.

Healthcare, automotive, etc. also

Teams are systems too. I've seen what happens when someone assumes that team 1 + team 2 = double-powered team goodness with no additional work needed.

Adding to this... each of us participates in multiple teams at the same time. This causes the teams to be integrated into a wider system.

Yeah. The paper's point that an airport is different overlapping systems from different perspectives seemed really relevant to human interactions.
I appreciated the description of emergent properties in this paper, it made the concept more clear for me than in the past. The comparison of the *weight* of all the components as a decomposable, non-emergent property when combined was really useful to understand it.
Bear in mind technically those are not hazards, those are causal factors that you find as part of step 4 of STPA (finding loss scenarios). Hazards are defined at the system-level, in step 1 of STPA

At the end of the day, in a control structure you're modeling decision, either by automated software or by humans.

This footnote on page 6 was my favorite gem of this whole paper

Probably a good topic for a whole session, but I would guess it's related to Wardley's concept of hierarchy in organizations resistance to openness. It was really important for those in power of these organizations to not allow systems analysis of the organization or it would be discovered how broken it is to achieve objectives, but to preserve power.

even STPA was not new; HAZOP sort of tries to accomplish the same thing and was developed in the 60s (although it was only named HAZOP in the 80s)

Wardley is presenting at Complexity Lounge soon, perhaps we could get him for Papers in Systems 🙂

*decisions
FMEA is based on component reliability -- you will miss *a lot* of scenarios that lead to bad outcomes. Reliability != safety
Ruben, it sounds like you've worked with STPA? I'd love to hear if you have any experiences to share

The STPA handbook is great - just read the 2 first chapters, about 50-60 pages

Interesting. Including operators are in system analysis, could lead to more dependencies (experience level, training, permissions/authority, etc.)

This ties in with research in expertise and expert performance.

Yes! I liked the example in this paper about the "top" command level being responsible for the training of the lower level operator s

And readiness

Wrong order in the boundaries of large systems is so hard. You can track it in your own system, but it's hard to hold the complexit y of both together to understand it well.

Ruben

1. Yes :) I'm presenting this year at the STAMP Workshop (I'm a Site Reliability Engineer at Google)

   To system complexity, we see a system as the pieces working together towards a purposeful whole. But when we have syste ms where the parts don't see their local purpose as part of the broader whole there are tricky properties and interactions that are hard to control at the larger system level.
   Much more so when it's a bunch of individual people.

   The point of the paper appeared, at least in part, to be an explanation of why there doesn't need to be a separate STPA/STAM P variation for "systems of systems".,

   If she's being asked when her team will be producing something that satisfies that terminology, this is a relevant response.

   I have to go; thanks again for this great session and see you all next time!

   Thank you Adrian! And everyone participating.
2. Next session: June 3: Mel Conway, "Ubiquitous wideband peer-to-peer nudging is taking us to an unfamiliar place" https://checkout.tito.io/bredemeyer/conway

Michael, IMO your tool is a control structure at the right level of abstraction.

You're getting at the core of STAMP, which is the accident causality model underlying STPA: accidents happen not because of com ponents failing, but because interactions between components are not controlled. Interactions are controlled by enforcing constra ints on the behavior of the components (incl. humans) -- those constraints are defined top down.

I liked the distinction between Accident and Hazard - here, Hazard is by definition controllable in principle

ah, interesting

see slide 60 of https://psas.scripts.mit.edu/home/wp-content/uploads/2014/03/Systems-Theoretic-Process-Analysis-STPA-v9-v2-san.pdf

I suspect it's easier for people to decide to put in the effort to do something like this after a big embarrassing incident happens.

“Political will for investing in systems understanding”

I'm beginning to understand why trying to use eg FMEA for even a simple healthcare example gets rapidly bogged down: far too many components and failure mode s ever to get a proper grasp of the system

I can't even imagine how many components are part of these systems, let alone the interactions.

this is what I love about systems methods: you can start "in the middle" rather than traditional engineering processes which try to get to an imagined "foundational l evel" and go bottom-up

DDD takes a lot from this, as well

Gotta leave, thanks everyone & Adrian for driving -- great discussion!

One of the consequences of emergent behavior can be that you rely on behavior that you don't know about. (this is the "we unplugged Sam's desktop and payroll sto pped working" problem) Analyzing that is harder and riskier.

As we hit time boundary: Thank you everyone, and thank you Adrian!

We continue for 30 minutes of "hallway track" for those who can stay
A CLASSIFICATION OF UNCERTAINTY FOR EARLY
PRODUCT AND SYSTEM DESIGN, DeWeck
https://web.mit.edu/deweck/Public/Alstom/deWeck_Eckert_Uncertainty_2007.pdf
You 2:01 PM

1. Next session: June 3: Mel Conway, "Ubiquitous wideband peer-to-peer nudging is taking us to an unfamiliar place" https://checkout.tito.io/bredemeyer/conway

Wish I could stay! See you next time

NEXT TIME:
https://melconway.com/Home/pdf/UbiquitousConnectivity.pdf

"lumpy inequitable states"! That's great

We read this paper last year, I think; dropping it here for those who came in later: https://asletaiwan.org/wp-content/uploads/2021/10/On-nonscalability.pdf

The scale of connections creates a level of uncertainty that becomes too difficult to understand or model.

Need to run momentarily. Thanks all! 👋

"lumpy inequitable observers"

All observers are inaccurate, some observers are useful.

An expensive and imprecise but flexible observer is complaints / swearing on social media

"The more reliable a system becomes the more catastrophic the failures become" is the thesis of Careful by Steve Casner. https://www.goodreads.com/book/show/3 2765270-careful

We pay attention to the chance of failures less, so they get worse when we don't think about them as possible.

Listening to customer support's information is so important! Both volume and "it seems like a lot of people are having trouble with [x] this week" anecdotal informati on.

Drift into Failure by Dekker is also an excellent book on this

Love Barbara´s point about weak signals being super important

Sometimes it's the scale of those small failures that causes the larger failure because the system isn't use to dealing with that much of such a formerly-infrequent event.

Bugs in error-handling paths, too.

haha, complex locking failures sounds very scary.

I

I wonder if there is correlation/research on near misses/weak signals, and the network effec ts Mel will be talking about next month...

Great discussion as usual everyone, I have to go! Looking forward to the next session

Second this suggestion for July/August
https://web.mit.edu/deweck/Public/Alstom/deWeck_Eckert_Uncertainty_2007.pdf

I'm sure Mel is writing it just for us!

Peter Naur's programming as theory building could be interesting to discuss https://pages.c s.wisc.edu/~remzi/Naur.pdf

Vi is great imho

We need the paper "A classification of uncertainty for individual operators in an emergent s ystem"

Thank you all! This was yet another wonderful discussion. So many new thoughts to conside r.

Thanks
I enjoyed it tremendously :-)