Session 2
Giving the floor to the younger members: Grand Challenges for our community

Speakers: Saman Zonouz, Catello Di Martino, Marcus Völp, Jiangshan Yu

Chair: Karthik Pattabiraman

Rapporteur: **Andrea Ceccarelli**

Different talks with (hidden?) commonalities

SAMAN - Cyber-Physical Intrusion Resilience

LELIO - Challenges for dependable 6G technology

MARCUS - Complexity, an old forgotten enemy

JIANGSHAN - The Future of Trust: Research and Community Challenges - A viewpoint

Saman - Cyber-Physical Intrusion Resilience

Short summary:

For cyber-physical systems intrusion resilience, relying on AI alone may not provide all the required answers.

- Physical dynamics should be better considered also at a software level, to connect the physical rules with the software and the application
  - plus the human in the loop!
  - plus the possibility to simplify unnecessary complex systems!

More in detail (next slides)

Saman - Cyber-Physical Intrusion Resilience

1. predictive situational awareness (with online monitoring)
   - Consideration of physical dynamics to be "ahead-of-time", which is more than just reactive monitoring to detected situations
2. physics-aware software analysis
   - semantic gap between the software concepts and the physics processes
3. Human Assisted Intrusion Response
   - Fully automated response and recovery in cyber-physical systems is too complex
   - can learn from an operator how to perform response and recovery

Saman - Cyber-Physical Intrusion Resilience

4. Domain-Specific AI for security
   - Most AI models are developed for Computer Vision and not made specific to other domains
   - From tuning to «physics-informed» neural networks (e.g., mimicry of power signal)
5. Resilience vs (supply chain) complexity
   - simplify (unnecessarily) bloated systems
   - how to remove the unnecessary part robustly?
6. Trustworthy w/Untrusted (edge) AI
   - We already know the security and safety problem of AI → edge AI is an additional step

different talks with (hidden?) commonalities

SAMAN - Cyber-Physical Intrusion Resilience

- **not just AI-only approaches: introduce physical laws, involve humans**
- **strive to simplify!**

LELIO - Challenges for dependable 6G technology

MARCUS - Complexity, an old forgotten enemy

- Strive to simplify!

JIANGSHAN - The Future of Trust: Research and Community Challenges - A viewpoint

Lelio - Challenges for dependable 6G technology

Short summary.

Future industrial applications need a network able to allocate and guarantee SLAs on demand. 6G will offer the network performance to make this new generation of network-based applications possible. But:

- Complexity will be very difficult to manage! (thousands of configurations alternative, to be decided rapidly)

- More in detail (next slides)

Reconfigurable Factory Floor Example

Challenge

- Frequent reconfiguration of the factory floor
  - Average of 900 changeovers / SMT line / month
  - 200-600 Eur for each new cable connection
  - Production batch: 2-3 hours
  - Quantities: 100s – 3 million pieces

Open problems (selected)

- Use case specific SLA.
- SLAs require coordination with software layers (e.g., edge containers and orchestration) and network.
- Lack of deterministic behavior
- Mix of Low-latency traffic vs. high-bandwidth traffic
- Data-shower and uplink bandwidth

Lelio - Challenges for dependable 6G technology

Challenge: guarantee SLA in a network with frequent reconfigurations

How to realize this (not short term!):

- Continuos control loop for continuous network SLA validation
- The configuration must be done automatically, based on some complex AI
- Possible thanks to network digital twins, that contain the AI to avoid "untested configuration" (a major source of telco outages)

different talks with (hidden?) commonalities

SAMAN - Cyber-Physical Intrusion Resilience

- not just AI-only approaches: introduce physical laws, involve humans
- strive to simplify!

LELIO - Challenges for dependable 6G technology

- **Need to push on AI and automation (limit humans)**
- **Complexity will be unavoidable**

MARCUS - Complexity, an old forgotten enemy

JIANGSHAN - The Future of Trust: Research and Community Challenges - A viewpoint

Marcus: Complexity, an old forgotten enemy

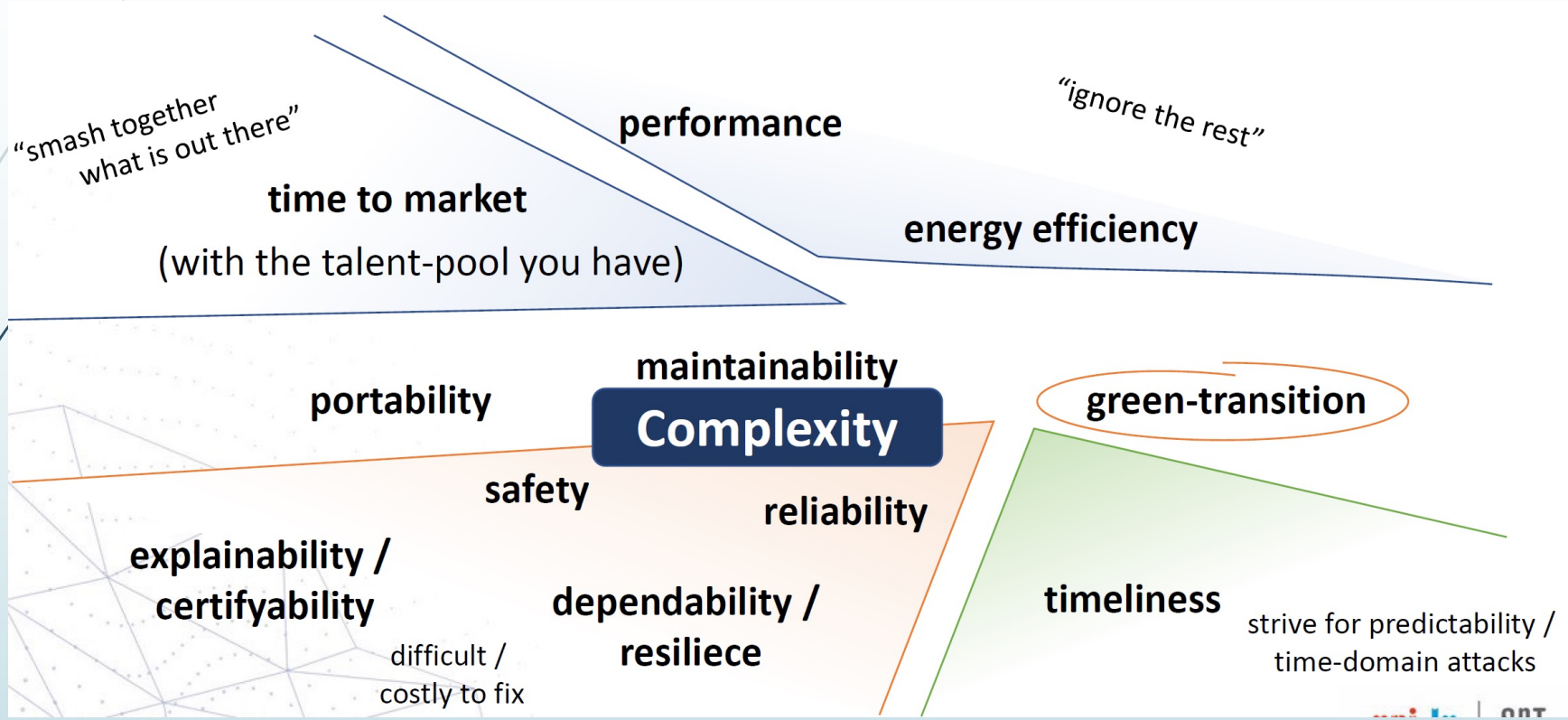
Short Summary.

We can optimize for many things (time-to-market, performance, energy efficiency, …) but

we may underestimate complexity issues, if we keep adding things (also AI is in this direction)

The talk reviews complexity drivers (with examples) from the past to the future, concluding that efforts should be done to avoid or filter out complexity

What we can optimize (conflicting properties)



Marcus: Complexity, an old forgotten enemy

Examples reported of some discontinued research line:

- Performance of dependable/fault-tolerant systems from PBFT to TEE-BFT, from covert channels to side channels to multi-level secure systems
  - All characterized by some raise in complexity somewhere.

A look into the future:

- Rather than adding new layers/functionalities/secure components, research how to avoid or filter out complexity - at least not having to trust the overly complex components
  - incrementally eliminate complexity killers in existing systems(HW / OS / SW / AI / …)
  - tools to enforce human understanding of tech. interplay
  - privacy through data minimality

different talks with (hidden?) commonalities

SAMAN - Cyber-Physical Intrusion Resilience

- not just AI-only approaches: introduce physical laws, involve humans
- strive to simplify!

LELIO - Challenges for dependable 6G technology

- Need to push on AI and automation (limit humans)
- Complexity will be unavoidable

MARCUS - Complexity, an old forgotten enemy

- **Operate to reduce complexity!**

JIANGSHAN - The Future of Trust: Research and Community Challenges - A viewpoint

Jiangshan - The Future of Trust

Brief summary:

- Research vision: establish trust by using technology alone, for a **trustworthy digital economy**
  - This is a socio-technical challenge (trust in the technology)
- The digital economy will be successful only if this trust is achieved

Jiangshan - The Future of Trust

3 main socio-technical challenges

1. **Meaningful guarantees** of large-scale systems
   - Diversity does not scale well (limits to guarantees in very large-scale BFT protocols)
   - Uncertainty: who are we trusting? How to measure uncertainty? what is the correct method if we want to deploy an e-government blockchain?

     2 mining pools control >50%;
     14 mining pools control 99.5% mining power

2. **Adapting blockchain-** replacing/advancing existing infrastructure is very challenging
   - Example: digital health & diversity of medical machines
3. **Community**: gaps between communities (dependability, security, database, AI, ...)

Very different talks with (hidden?) commonalities

COMPLEXITY

SAMAN - Cyber-Physical Intrusion Resilience

- not just AI-only approaches: introduce physical laws, involve humans
- strive to simplify!

LELIO - Challenges for dependable 6G technology

- Need to push on AI and automation (limit humans)
- Complexity will be unavoidable

MARCUS - Complexity, an old forgotten enemy

- Operate to reduce complexity!

JIANGSHAN - The Future of Trust: Research and Community Challenges - A viewpoint

- **Socio-technical challenges in heterogeneous, large, complex systems!**