NexComm 2018

Panel on Networking and Systems

Theme: Developing Reliable and Resilient Systems

Topic: Autonomy, Robustness and Safety Triangle

Introduction

Eugen Borcoci

Developing Reliable and Resilient Systems
Autonomy, Robustness and Safety Triangle

- **Moderator: Eugen Borcoci, University POLITEHNICA of Bucharest, Romania**
- **Panelists:**
  - **Catherine Menon, University of Hertfordshire, Great Britain**
    - **"Assuring safety for autonomous systems"**
  - **Ilias Iliadis, IBM Research - Zurich, Switzerland**
    - **"Cloud Storage Reliability Aspects"**
  - **Tomasz Hyla, Marine Technology sp. z o.o., Poland**
    - **"Automatic over-the-air updates in life critical systems; cybers security threats impact on systems design"**
  - **Eugen Borcoci, University POLITEHNICA of Bucharest, Romania**
    - **"Increasing autonomy in network management; 5G case"**

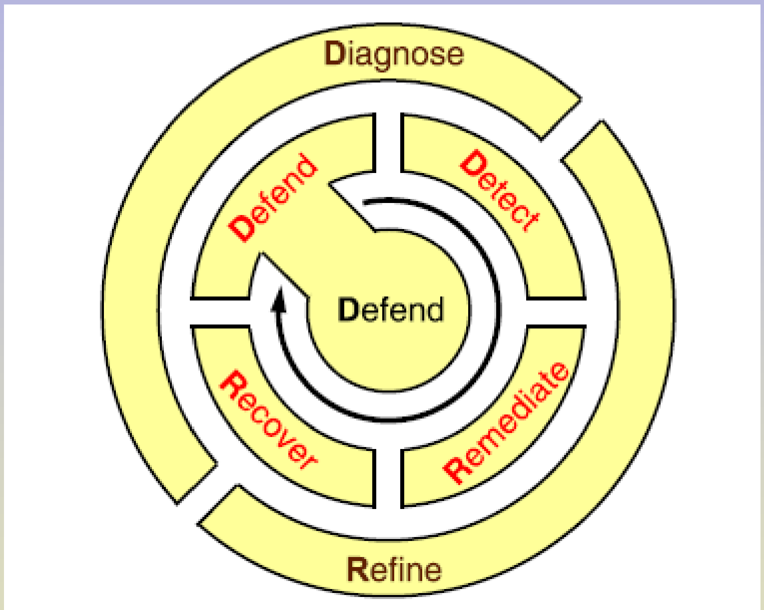
NexComm 2019, Valencia, 24-28 March 2019

Developing Reliable and Resilient Systems
Autonomy, Robustness and Safety Triangle

- **Many definitions exist….**
- **Examples**
- **Resilience**
  - **Ability of a system (e,g. network)** to **provide and maintain an acceptable level of service** while facing various faults and challenges to normal operation
  - system's **ability to recover or regenerate** its performance after an unexpected impact produces a degradation of its performance
  - **Computer networking community:** combination of trustworthiness (dependability, security, performance) and tolerance (survivability, disruption tolerance and traffic tolerance)
  - **Dependable computing community**: persistence of service delivery that can justifiably be trusted, when facing changes
    - (i.e., unexpected failures, attacks or accidents (e.g., disasters), increased loads, ..)

Developing Reliable and Resilient Systems
Autonomy, Robustness and Safety Triangle

- **Resilience** (loop): **D2 R2 + DR**
  - defend, detect, remediate, recover and
  - diagnose, refine



Source: J. P.G. Sterbenz, D. Hutchison, E. K. Çetinkaya, A. Jabbar, J. P. Rohrer, M. Schöller, Paul Smith, "Resilience and survivability in communication networks: strate-gies, principles, and survey of disciplines," Comput. Networks, vol. 54 iss.June (8), (2010), pp.1245–1265.

Developing Reliable and Resilient Systems
Autonomy, Robustness and Safety Triangle

- **Robustness**
  - the degree to which a **system is able to withstand** an **unexpected internal or external event** or change, **without degradation** in system's performance
    - E.g.: two systems A and B—of equal performance
      - the A-robustness > B robustness
      - if the same unexpected impact on both systems leaves system A with greater performance than B
  - Resilience and robustness are partially overlapping…
  - **Design problem trade-off:**
    - **Resources, complexity, performance, cost – vs. acceptable resiliency and robustness ??**

Developing Reliable and Resilient Systems
Autonomy, Robustness and Safety Triangle

- **Autonomous/adaptive/autonomic..**
  - **Autonomous: a** system (e.g**.,** network) that runs with minimal to no human intervention - able to configure, monitor, and maintain itself independently
    - This is the highest level of independence
  - **Adaptive System** (e.g., network): a system that is ***self-aware*** and can ***self-configure, self-monitor, self-heal and self-optimize***
    - by constantly assessing system pressures and automatically reallocating resources
    - but is bound by the rules and policies set by the system operator and is under constant human supervision
  - **Artificial Intelligence (e.g. Machine learning) –** recently recognized to bring significant contribution in creation of novel systems, having better autonomy and adaptability properties

Developing Reliable and Resilient Systems
Autonomy, Robustness and Safety Triangle

- **Autonomous/adaptive/autonomic**..(cont'd)
  - **IBM definitions of autonomy levels (>2001)**
  - ***..***
  - **Level 4 or Adaptive Level**
    - The system gathers monitored information and predicts situations but also **reacts automatically** in many situations **with no human intervention**
      - based on a **better understanding of system behavior and control**. Once knowledge is specified, of **what** to perform, in **which situation,** then the system can carry out lower level decisions and actions
  - **Level 5 Autonomic Level**
    - **Highest level :** the interactions between the humans and the systems are only **based on high-level goals.**
    - **Human operators** only specify **business policies and objectives** to govern systems, while the **system interprets these high-level policies** and responds accordingly
      - **Human operators will trust the system** in managing themselves and will concentrate solely on **higher level business**

Developing Reliable and Resilient Systems
Autonomy, Robustness and Safety Triangle

- **Reliability** is the probability that a system will perform its intended function satisfactorily
- **Safety**
  - **Safety properties** informally specify some "**bad actions**" that **must never happen** in a centralized/distributed system or algorithm
  - The system safety concept calls for a **risk management strategy** based on identification, analysis of hazards and application of remedial controls using a systems-based approach
  - **Safety**
    - means **freedom from accidents or losses**
    - **is not identical with reliability** (they partially overlap)
    - **is not identical with security** (they partially overlap)
      - security means protection or defense against attacks, interferences, or espionage

Developing Reliable and Resilient Systems
Autonomy, Robustness and Safety Triangle

- **Safety**
  - **Process:** Eight steps to follow towards the safety of a system
    - 1 Identify the hazards
    - 2 Determine the risks
    - 3 Define the safety measures
    - 4 Create safety requirements
    - 5 Create safe designs
    - 6 Implement safety
    - 7 Assure the safety process
    - 8 Test

Source: B. P.Douglass, "Designing Mission and Safety-Critical Systems", Doing Hard Time: Developing Real-Time Systems with UML, Objects, Frameworks, and Patterns, Addison-Wesley Publishing, 1999.

- Switch to the speakers' presentations…

NexComm 2018

Panel on Networking and Systems

Theme: Developing Reliable and Resilient Systems

Topic: Autonomy, Robustness and Safety Triangle

Increasing autonomy in network management - 5G case

Eugen Borcoci
University POLITEHNICA of Bucharest, Romania
Eugen.Borcoci@elcom.pub.ro

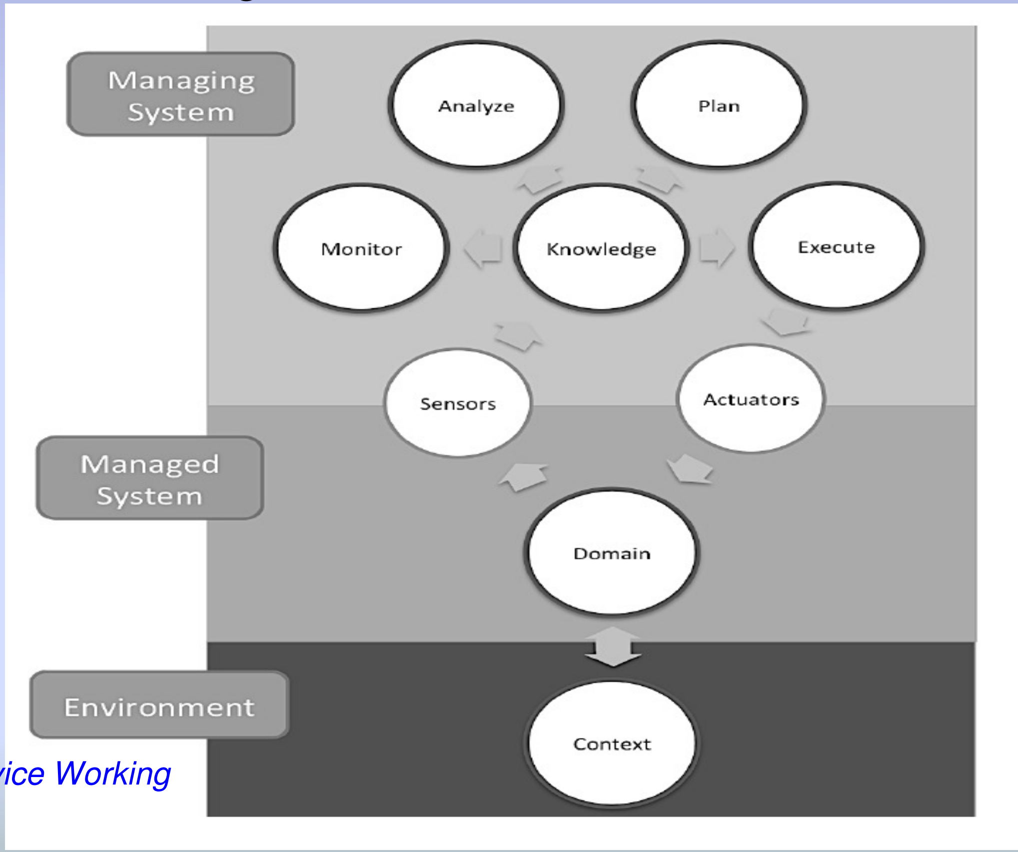
1. Autonomic and Cognitive Management

5G networks –complex management requirements (multi –tenant/ domain/ operator character and softwarization of network resources)

- Need of **management** based on a **hierarchy of complex decision making techniques** based on analysis of *historical, temporal* and *frequency network data*
- **Cognitive network management** – recent trend using **Artificial Intelligence (AI)** and in particular **Machine Learning (ML)**
  - to develop **self-x, (x= -aware, -configuring, -optimization, -healing and -protecting systems)**
- Cognitive management– extension of **Autonomic Management (AM)** (coined by IBM ~ 2001)
  - **AM + Machine learning = Cognitive Management (CogM)**
- **Challenge:** to deploy the CogM and its orchestration across multiple heterogeneous networks: Radio & Other Access Networks, Core & Aggregation, Edge Networks, Edge and Computing Clouds and Satellite Networks

1. Autonomic and Cognitive Management (cont'd)

- **Autonomous Network Management (ANM) :** introduce self-governed networks for pursuing business and network goals while maintaining performance
- IBM original AM - later extended in networking domain → **ANM**
  - **Loop: Monitor-Analyse-Plan-Execute** over a shared **Knowledge**
  - (**MAPE-K**) is a control theory-based feedback model for self-adaptive systems
  - **AM –** hierarchical and recursive approach



Source: 5GPPP Network Management & Quality of Service Working Group, "Cognitive Network Management for 5G", 2017

Increasing autonomy in network management - 5G case

1. Autonomic and Cognitive Management (cont'd)

- **Autonomic Network Management functions**
  - **Monitoring**: active/passive, centralized/distributed, granularity/time-based, and programmable
  - **Analysis:** many approaches exist – relying, e.g., on probability and Bayesian models for anticipation on knowledge, timing, mechanism, network, user, applicvations
    - Challenge: to define a concentrated data set that captures information across all anticipation points
    - **Recent solutions – use learning and reasoning** to achieve such specific ends
  - **Planning and Execution**
    - Dimensions of the network adaptation plan are: knowledge, strategy, purposefulness, degree of adaptation autonomy, stimuli, adaptation rate, temporal/spatial scope, open/closed adaptation and security
    - Current status: no unanimity in defining proper planning and execution guidelines

Increasing autonomy in network management - 5G case

1. Autonomic and Cognitive Management (cont'd)

- **Autonomic Network Management functions** (cont'd)
  - **Knowledge base**
    - The network information is shared across the MAPE-K architecture
    - Many approaches exist - to build knowledge on network/topology, including models from learning and reasoning, ontology and DEN-ng models.
    - Integrated solution- able to capture knowledge on: structure , control and behaviour
  - **Typically:**
    - a knowledge-based framework processes input data from multiple sources
    - and extracts relevant knowledge, through **learning-based classification, prediction and clustering models**
    - to drive the decisions of **Self Organizing Network (SON)-type**, e.g., self-planning, self-optimization and self-healing

2. Automation of 5G network slicing management with Machine Learning

- **Network functions requiring automation**
  - **Planning and design**: Requirements and environment analysis, topology determination; it provide inputs to :
  - **Construction and deployment**: Static resource allocation, VNF placement, orchestration actions; it provide inputs to :
    - **Operation, control and management**: Dynamic resource allocation, adjustment; policy adaptation; it interact bi-directionally with :
      - **Fault detection**: Syslog analysis, behavior analysis, fault localization
      - **Monitoring**: Workload, performance, resource utilization
      - **Security:** Traffic analysis, DPI, threat identification, infection isolation

Adapted from source: V. P. Kafle, et. al., "Consideration on Automation of 5G Network slicing with Machine Learning" , ITU Caleidoscope Santafe 2018

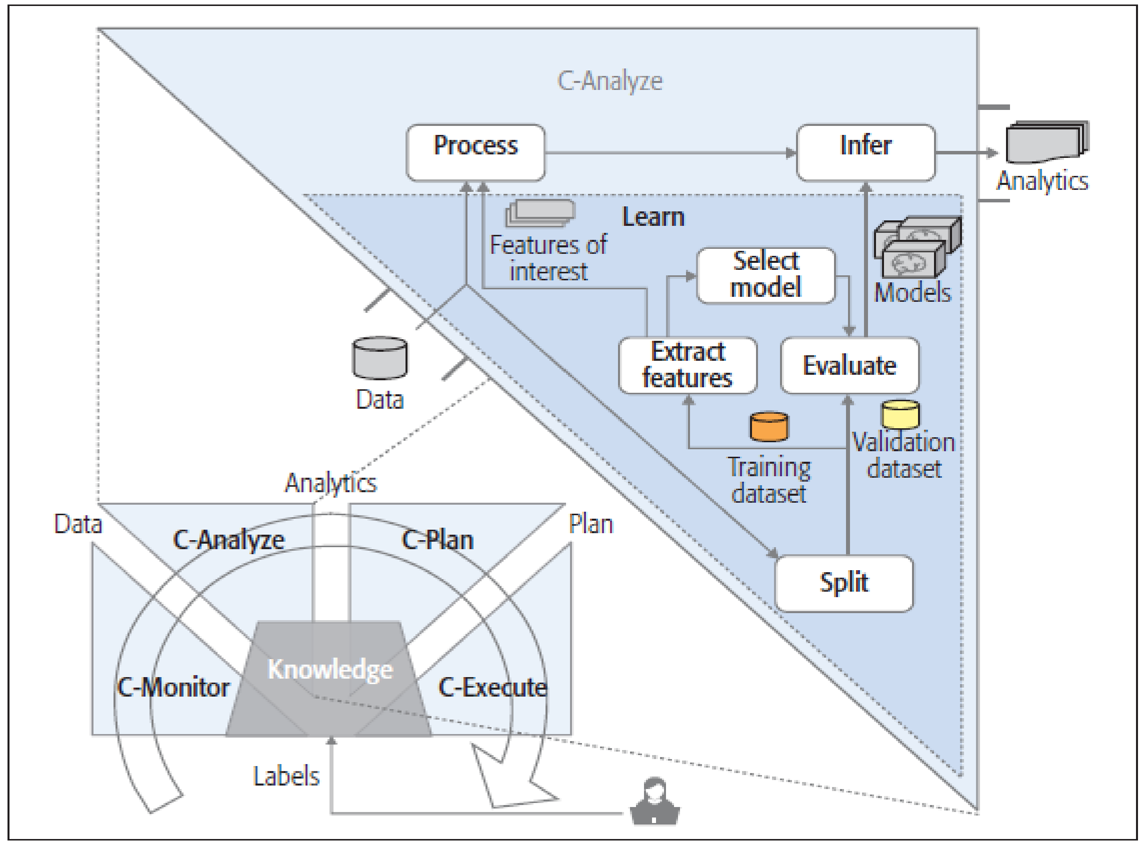
Increasing autonomy in network management - 5G case

3. Example of an architecture embedding cognitive management

- **MAPE- full cognitive loop**

Source: Sara Ayoubi, et.al., Machine Learning for Cognitive Network Management, IEEE Comm.Magazine , January 2018, pp.158-165

- Traditional – MAPE: only Analyze Phase included cognitive properties
- **Novel proposal : to introduce ML in all phases**
- ML: introducing **learning** and **inference** in every function.



3. Example of an architecture embedding cognitive management

- **MAPE- full cognitive loop** (cont'd)
  - **C-Monitor: intelligent probing –**adapted to network conditions
  - **C-Analyze**: **detects or predicts changes** in the network environment (e.g., faults, policy violations, frauds, low performance, attacks)
  - **C-Plan:** can leverage **ML** to develop an **intelligent automated planning** (AP) engine that reacts to changes in the network by selecting or composing a change plan
  - **C-Execute: schedules the generated plans** and determine the course of action should the execution of a plan fail
    - **Reinforcement Learning** is –naturally- applied: C-Execute agent could exploit past successful experiences to generate optimal execution policies, and explore new actions in case the execution plan fails

Source: Sara Ayoubi, et.al., Machine Learning for Cognitive Network Management, IEEE Comm.Magazine , January 2018, pp.158-165

- Thank you !

Zurich Research Laboratory

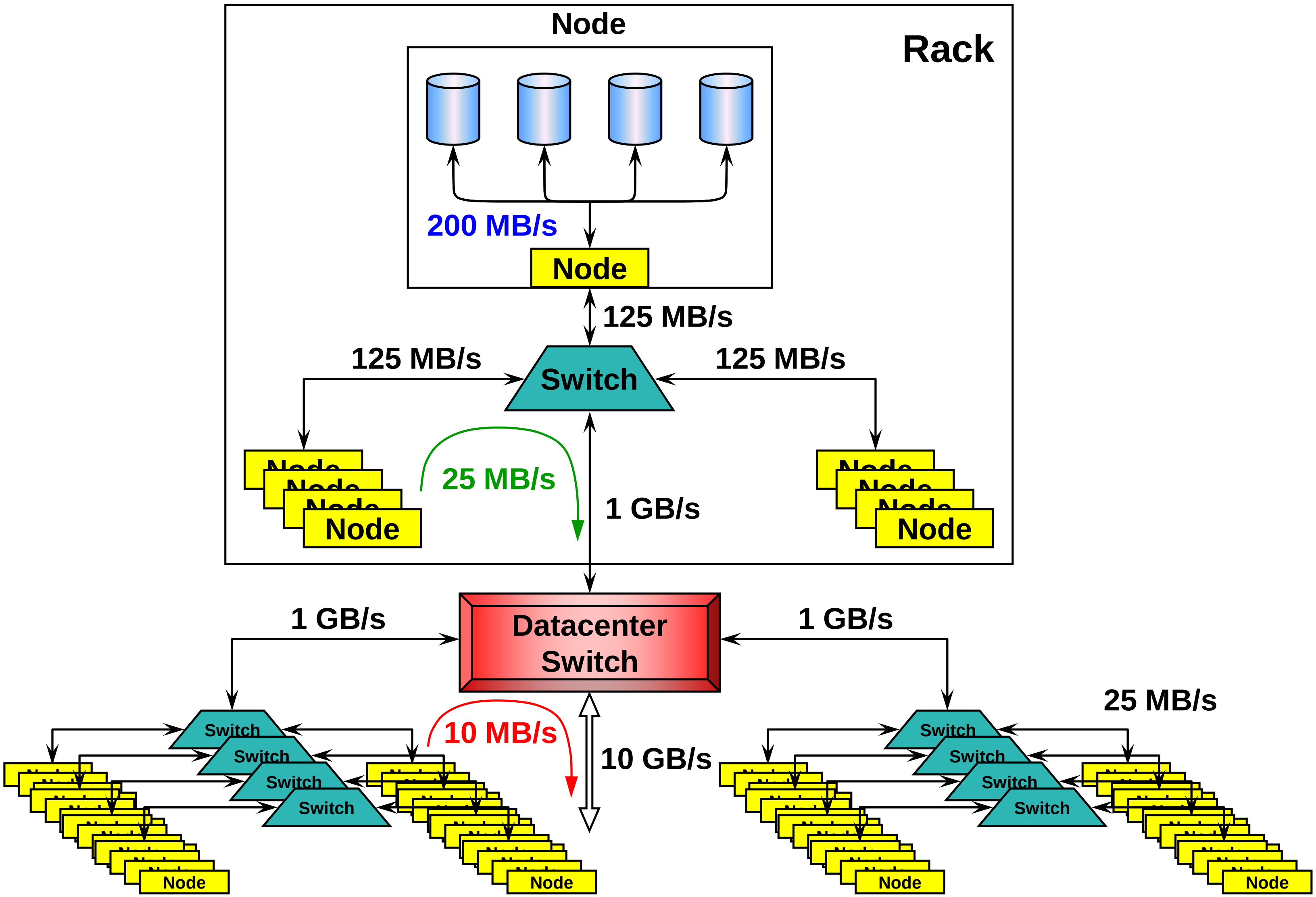
Panel on Networks and Systems

Theme: Developing Reliable and Resilient Systems

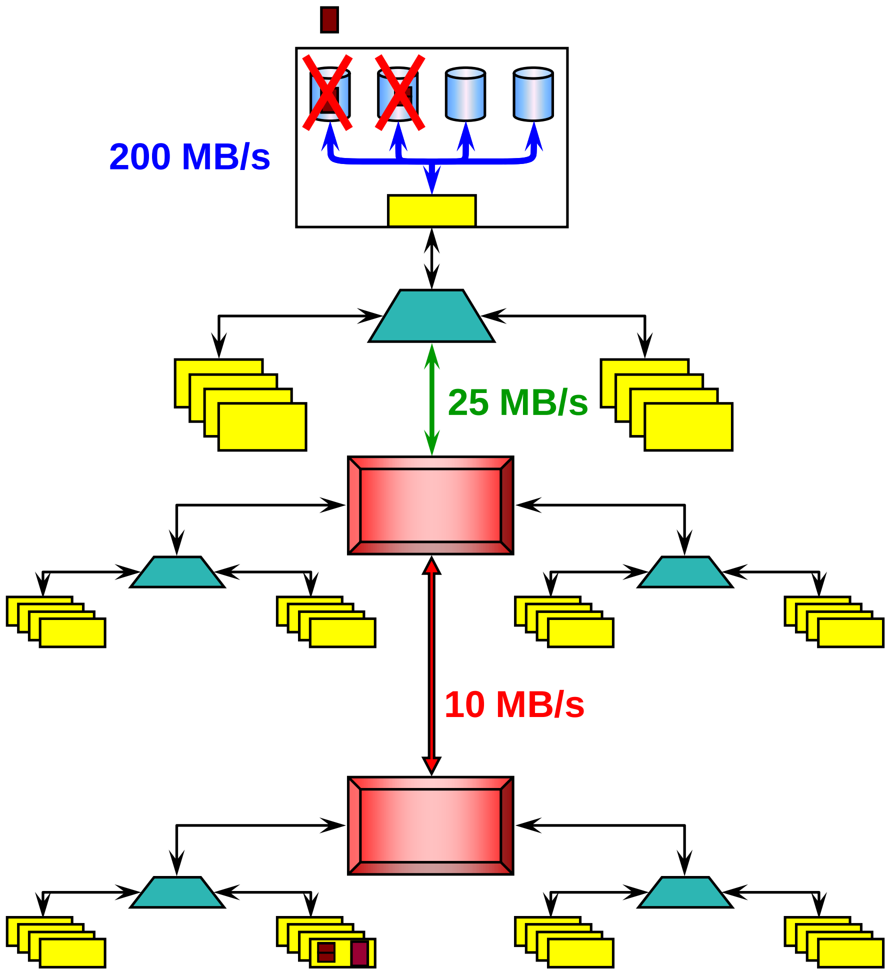
Cloud Storage Reliability Aspects

Ilias Iliadis
March 27, 2019

Storage Hierarchy of a Datacenter



Reliability Issues



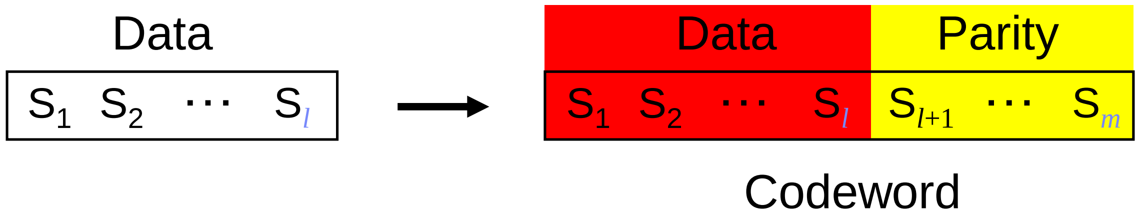
Reliability improvement through data replication

- Replica placement
  - Within the same node
    - ➢ Fast rebuild at 200 MB/s **(+)**
    - ➢ Exposure due to disk failure correlation **(-)**
  - Across datacenters
    - ➢ No exposure due to correlated failures **(+)**
- Rebuild process
  - Direct rebuild to the affected node
    - ➢ Slow rebuild at 10 MB/s
      - Long vulnerability window **(-)**
  - Staged rebuild
    - ➢ First local rebuild
      - Fast rebuild at 200 MB/s
        - ✓ Short vulnerability window **(+)**
      - Same location
        - ✓ Exposure due to correlated failures **(0)**
    - ➢ Replica then migrated to the affected node
- Replication factor
  - How many replicas are required?

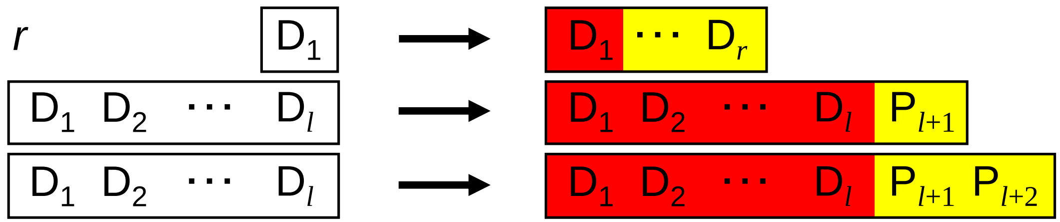
Tradeoffs of various placement and rebuild schemes

Erasure Coded Schemes

- User data divided into blocks (symbols) of fixed size
  - Complemented with parity symbols
    - ➢ codewords



- (m,l) maximum distance separable (MDS) erasure codes
- Any subset of l symbols can be used to reconstruct the codeword
  - Replication : $l = 1$ and $m = r$
  - RAID-5 : $m = l + 1$
  - RAID-6 : $m = l + 2$



- Storage efficiency : $s_{\mathrm{eff}} = l/m$ (Code rate)

- Google : Three-way replication (3,1) → s_{eff} = 33% to Reed-Solomon (9,6) → s_{eff} = 66 %
- Facebook : Three-way replication (3,1) → s_{eff} = 33% to Reed-Solomon (14,10) → s_{eff} = 71 %
- Microsoft Azure : Three-way replication (3,1) → s_{eff} = 33% to LRC (16,12) → s_{eff} = 75 %

University of Hertfordshire

Does a Loss of Social Credibility Impact Robot Safety?

Catherine Menon

University of Hertfordshire

The Institution of Engineering and Technology

Assistive robots

- Robots designed to support independent living
  - Elderly, vulnerable users

Care-O-Bot

Assistive robots

- Robots designed to support independent living
  - Elderly, vulnerable users
- Customisable functionality includes:
  - Reminding a user to take medication
  - Alerting the user to hazards (e.g. oven left on)
  - Providing companionship and conversation

User acceptance and social behaviour

- User acceptance is imperative for assistive robots
  - Functionality of robot
  - Behaviour appropriate to the social role the robot plays
- Many factors affect social interaction with robots
  - Appearance

User acceptance and social behaviour

- User acceptance is imperative
  - Functionality of robot
  - Behaviour appropriate to the social role the robot plays
- Many factors affect social interaction with robots
  - Appearance

User acceptance and social behaviour

- User acceptance is imperative
  - Functionality of robot
  - Behaviour appropriate to the social role the robot plays
- Many factors affect social interaction with robots
  - Appearance (gait, voice)
  - Greeting behaviour
  - Personal space
  - Timing and turn-taking
- Much existing research!

SocCred project: Social credibility

- Funded IET and Lloyds Registry Foundation Assuring Autonomy International Program
- SocCred: identifying the link between social behaviours and safety behaviours
- Fundamental concept: **social credibility**
- Social credibility relates to socially appropriate behaviour
  - "Is the robot acting as a functional social being?"
  - Not the same as being polite!
  - People are functional social beings, but not always polite

Social credibility

- 1. Does this robot obey environmental social norms for people?
  - E.g. appropriate physical movement, responsiveness to verbal and non-verbal feedback, following behaviour
- 2. Understanding communicated as to robot capabilities
  - The user must understand what the robot is capable of to consider it a functional social being
  - What sensors does it have, and how does it process information?

Social credibility

- Emotional engagement and trust are not necessarily good predictors of social credibility
  - E.g. "pet" robots are emotionally engaging
  - Automated (vs autonomous) systems can be trusted

- Social credibility is dynamic – socially questionable actions can temporarily diminish it

SocCred: Safety of assistive robots

- Physical hazards: slips, trips falls
- **Functional hazards: failure to alert**
  - In its monitoring role the robot acts as partial mitigation for many risks
  - Human action is essential for complete mitigation
    - Take action after being alerted (e.g. switch off the oven)
- **Requires end-user cooperation with the robot**

Safety and social credibility

- End-users of assistive robots are not engineers
  - Elderly, vulnerable users, in their own home
- Safety-critical behaviour involves interruptions
  - Robot in a monitoring role, alerts human to take action
- Interruptions can harm social credibility

“You’ve interrupted several times for something routine”

“You came too close”

“You interrupted me urgently but then didn’t sound worried”

SocCred: safety and social credibility

- Loss of social credibility can lead to user disengagement
- Why?

1. **Robots breaking social norms may trigger irritation**
    - Users may be less willing to "listen to" the robot
    - E.g. drivers switching off an "irritating" speed warning system despite acknowledging its utility
2. **Social credibility has a protective aspect**
    - Users regard robot no longer as just a machine – don't want to switch it off!

SocCred: safety and social credibility

- User disengagement is a significant safety problem!
- Results in interruptions being ignored or the robot switched off
  - In both these cases, the robot cannot effectively perform its safety critical functions

SocCred: social credibility and safety

Inappropriate interruptions

SocCred: social credibility and safety

Inappropriate interruptions

Loss of social credibility

SocCred: social credibility and safety

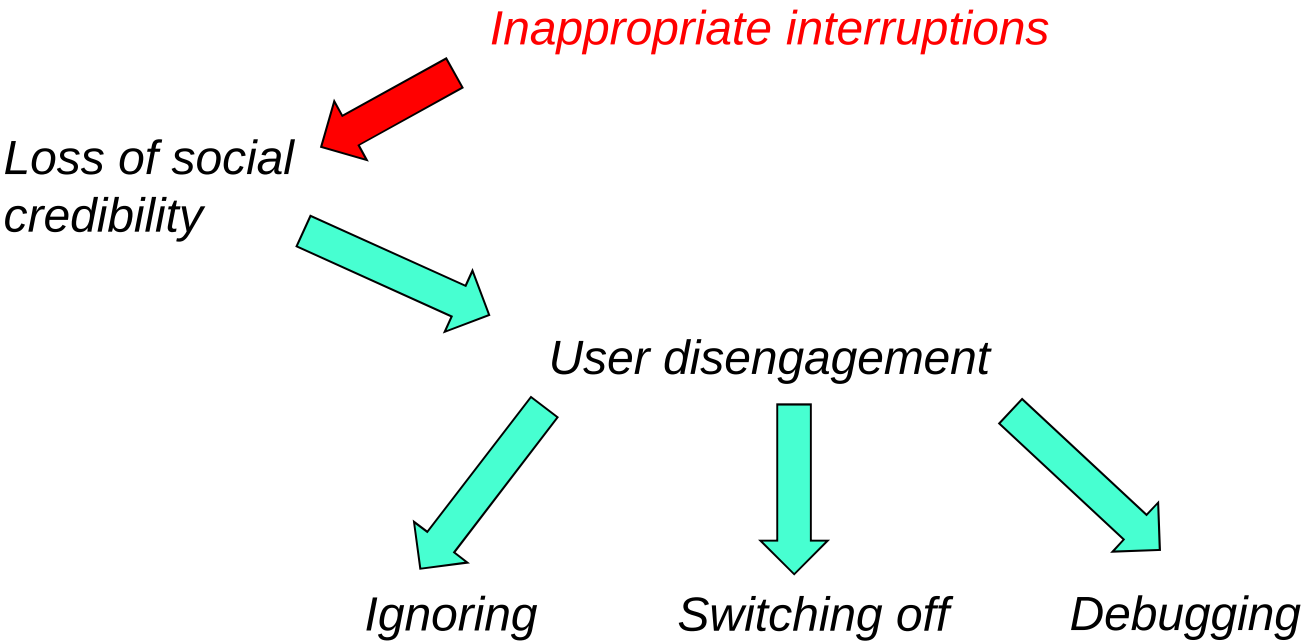
Inappropriate interruptions

Loss of social credibility

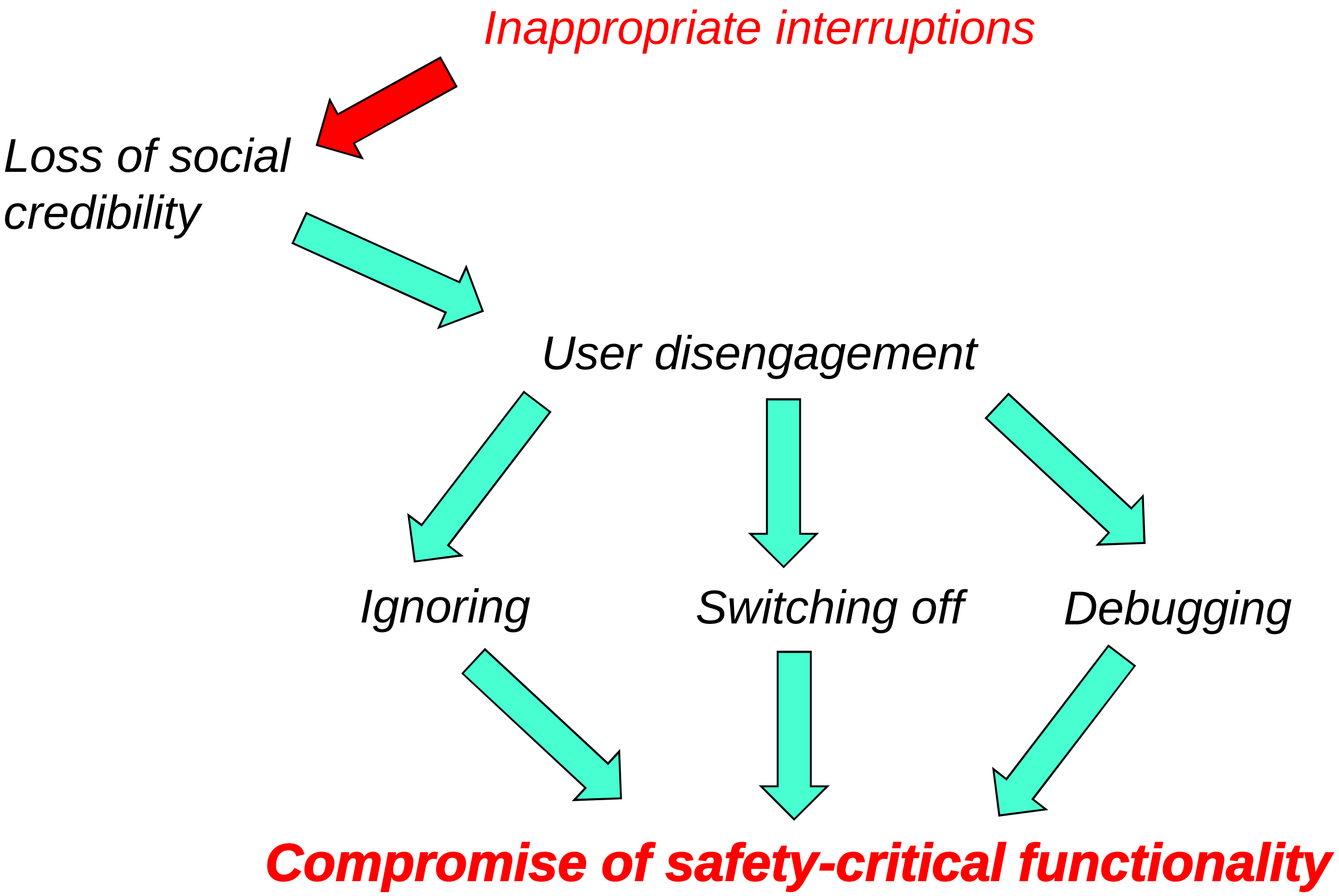
User disengagement

University *of* Hertfordshire

SocCred: social credibility and safety



SocCred: social credibility and safety



SocCred: behaviour trade-offs

- To be effective in its safety critical role, a robot must display social credibility
- Balancing the social and safety needs
  - When to prioritise a social behaviour?
  - When to prioritise a safety behaviour?
- A minimum threshold of social credibility is needed for both user acceptance and safety performance
- Simultaneously, risks must be shown to be ALARP
  - (UK requirement only)

SocCred: experimental aims

- Experiment to identify safety performance when social behaviour is varied
- Create models of behaviour prioritisation based on dynamic social credibility
- Can be viewed as a scheduling problem
  - I want to maintain social credibility threshold, and ALARP risks
  - Which behaviour (social? safety?) should I execute at any given time?
  - Which behaviours can I drop when resources are limited?

SocCred: behaviour trade-offs

- Intended to characterise link between social credibility and safety
- Both user acceptance and safety performance depend on social credibility of the robot
- Interruptions can affect social credibility, but are necessary for safety
- Duty of care – end-users cannot be expected to be familiar with this!

Panel on Networks and Systems
Theme: Developing Reliable and Resilient Systems
Topic: Autonomy, Robustness and Safety Triangle

Automatic over-the-air updates in life critical systems (e.g., car' auto-steering system).
How cybersecurity threats impact systems design and what are safety consequences?

Tomasz Hyla

1. West Pomeranian University of Technology, Szczecin, Poland – Assistant Professor, head of Information Security Research Team
2. Marine Technology Ltd.

Over-the-air (OTA) updates

- Popular in smartphones
- OTA in life critical systems can impact safety significantly:
  - the possibility to upload software update with undetected errors lack of control or certification from third parties
  - cyberattack can potentially take control over device
- In Europe, starting from 2019 every new car has a connection to a mobile network – obligatory only for after accident emergency calls
- In cars two types of systems are present:
  - Non-life-critical – entertainment, navigation
  - Life-critical – auto-steering, breaking

OTA updates – Tesla case

Posted by u/beastpilot Model P3D, X100, Investor 1 day ago 2

It's BACK! After 6 months of working fine, 2019.5.15 drives at barriers again

Software/Hardware

763 Comments Share Save 98% Upvoted

WIRED SUBSCRIBE

AARIAN MARSHALL TRANSPORTATION 05.30.18 07:46 PM

TESLA'S QUICK FIX FOR ITS BRAKING SYSTEM CAME FROM THE ETHER

Consumer Reports also criticized the Model 3 for its control panel, which consolidates all knobs and adjusters and infotainment options onto an iPad-like screen on the central control. Some of its concerns could be resolved with over-the-air updates, too. TESLA

https://www.reddit.com/r/teslamotors/comments/b36x27/its_back_after_6_months_of_working_fine_2019515/
https://www.wired.com/story/tesla-model3-braking-software-update-consumer-reports/

Technical solution and threats

- Security implemented using a mechanism similar to online banking
- Are security mechanisms free of implementation errors?
- What about long-term validity of crypto-algorithms?
- What about social engineering attack?
- What about state-sponsored, large scale attacks on manufacturer?
- In future, it is real that someone will take control over all cars of given manufacturer and create a mega-accident?
- Is the risk level acceptable?
- How OTA systems should be designed, tested, audited, and secured?