Modelling Security of Critical Infrastructures: A Survivability Assessment

Ricardo J. Rodríguez†, José Merseguer†, Simona Bernardi§
{rjrodriguez, jmerse, simonab}@unizar.es

†Dpto. de Informática e Ingeniería de Sistemas
Universidad de Zaragoza, Zaragoza, Spain

§Centro Universitario de la Defensa
Academia General Militar, Zaragoza, Spain

15 de Junio, 2016

II Jornadas Nacionales de Investigación en Ciberseguridad

Granada, España

Accepted in *The Computer Journal*. doi: 10.1093/comjnl/BXU096

Introduction (I)

Critical Infrastructures

- Provide essential services to the society
  - Power distribution, water treatment, telco, financial services...
- Discontinuity of service may lead to fatalities or injuries
  - Different nature, from unintended acts of nature to intentional attacks (e.g., sabotage, terrorism)





Universidad Zaragoza

Introduction (II)

Recent examples

2003 Northeast (U.S.) blackout

- Attributed to downed power line
- 11 deaths and an estimated $6B in economic damages, plus disrupted power over a wide area for two days

2013 Bowman Avenue Dam in NY was compromised, and control of the floodgates was gained

- Attributed to Iranian hackers

2015 Prykarpattyaoblenergo Control Center (PCC) in the Ivano-Frankivsk region of Western Ukraine

- Leaving 230K residents without power for up to 6 hours
- Presumed Russian cyberattacker

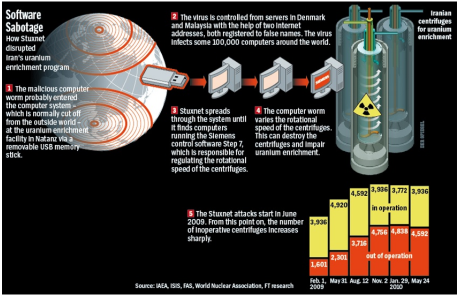
Not only safe, but also secure

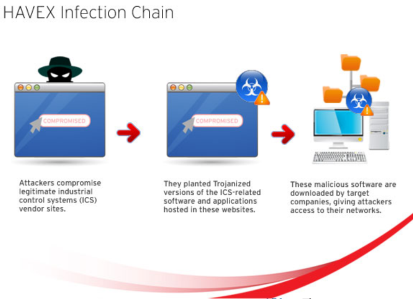
Universidad Zaragoza

Introduction (III)

The *game* just begun...

- Cyberattacks against SCADA systems doubled in 2014: more than 160K (Dell's 2015 Annual Security Report)
- Malware targeting SCADA systems identified:
  - Examples: Stuxnet, Havex, and BlackEnergy3





Zaragoza

Introduction (IV)

Survivability

- *Capability of a system to fulfill its mission, in a timely manner, in the presence of attacks, failures, or accidents*
- Usually qualitative in nature; and not precise or detailed enough to facilitate measurable survivability requirements and evaluations
- Survivability strategies phases:
  1. Resistance
  2. Recognition
  3. Recovery

Introduction (IV)

Survivability

- *Capability of a system to fulfill its mission, in a timely manner, in the presence of attacks, failures, or accidents*
- Usually qualitative in nature; and not precise or detailed enough to facilitate measurable survivability requirements and evaluations
- Survivability strategies phases:
  1. Resistance
  2. Recognition
  3. Recovery

Our proposal

- `SecAM` (Security Analysis and Modelling) UML profile
  - Enables survivability analysis for critical infrastructures to provide capabilities for assessing defence plans

Universidad Zaragoza 1542

Introduction (V)

Advantages

- Specification, in a quantitatively and quantitatively manner, of security and survivability in early stages of development
- Specific models for infrastructures and attack patterns
- Survivability analysis through formal models (in particular, Generalized Stochastic Petri nets)
  - Model-checking techniques
  - Allows steady-state analysis
  - Efficient techniques, as linear algebra and linear programming-based techniques

Introduction (V)

Advantages

- Specification, in a quantitatively and quantitatively manner, of security and survivability in early stages of development
- Specific models for infrastructures and attack patterns
- Survivability analysis through formal models (in particular, Generalized Stochastic Petri nets)
  - Model-checking techniques
  - Allows steady-state analysis
  - Efficient techniques, as linear algebra and linear programming-based techniques

Disadvantages

- Model complexity increased
- Lack of CASE tools with automated translation

Universidad Zaragoza 1542

Background (I): UML profile

UML profile

- UML tailored for specific purposes: profiling
- Stereotypes and tagged values
  - Extend model semantics
  - Allow to express non-functional properties (e.g., performance, reliability, security) within the model

Universidad Zaragoza

Background (I): UML profile

UML profile

- UML tailored for specific purposes: profiling
- Stereotypes and tagged values
  - Extend model semantics
  - Allow to express non-functional properties (e.g., performance, reliability, security) within the model

OMG example

- *Modelling and Analysis of RT Embedded systems* (MARTE)
  - Provides support for performance and schedulability analysis
  - Well-defined language to express NFPs (VSL, *Value Specification Language*)

Universidad Zaragoza 1542

Background (II): GSPNs

UML profiling sounds cool, but. . .

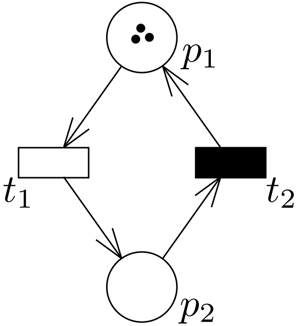
- Express quantitative properties for analysis
  - Transformation to formal models (in particular, Generalized Stochastic Petri nets)
  - Good (and mature) analysis framework

Universidad Zaragoza

Background (II): GSPNs

UML profiling sounds cool, but...

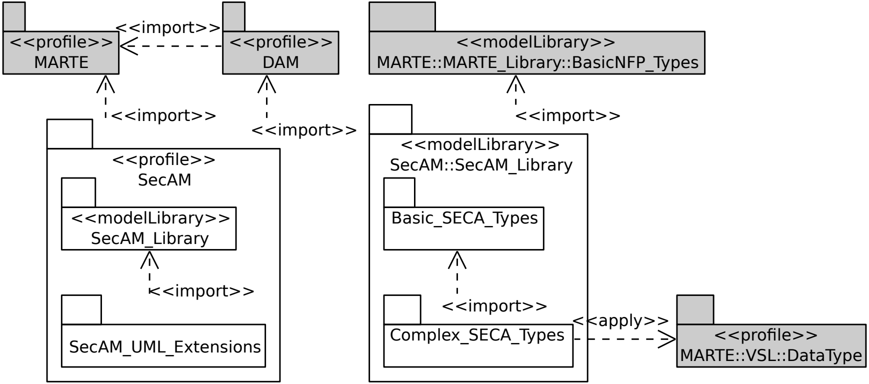
- Express quantitative properties for analysis
  - Transformation to formal models (in particular, Generalized Stochastic Petri nets)
  - Good (and mature) analysis framework



GSPN – explanation simplified

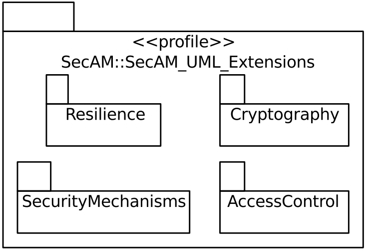
- Underlying Markov-chain
- Places (circles, p_X)
- Transitions (white/black bars, t_X)
- Time interpretation
  - Immediate transitions ($t = 0$)
  - Timed (allows different probabilistic distributions)
- Tokens (black dots)

SecAM Profile (I): a General Overview (1)



- `SecAM` relies on two profiles:
  - MARTE: analysis capabilities (among other features)
  - Dependability Analysis and Modeling (DAM): concepts shared by the dependability and security fields
- Set of stereotypes; and basic and complex types

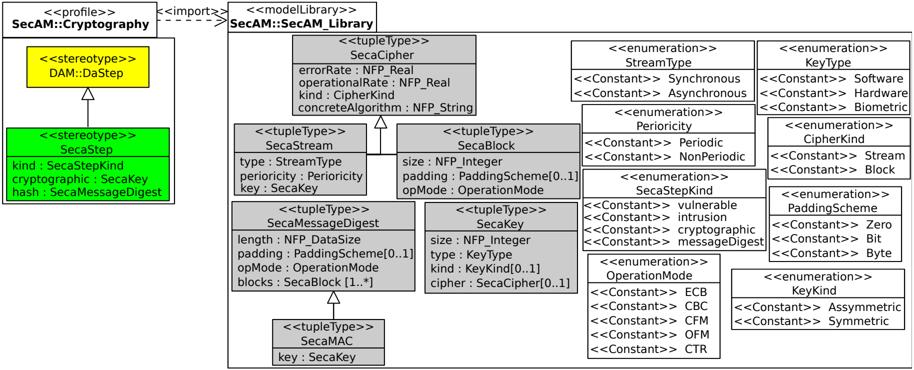
SecAM Profile (I): a General Overview (2)



Security attributes	`SecAM` **packages** (P1)	(P2)	(P3)	(P4)
Integrity	√	√		√
Availability		√	√	
Confidentiality	√	√		√
Authorisation				√
Non-repudiation	√			
Authenticity	√			

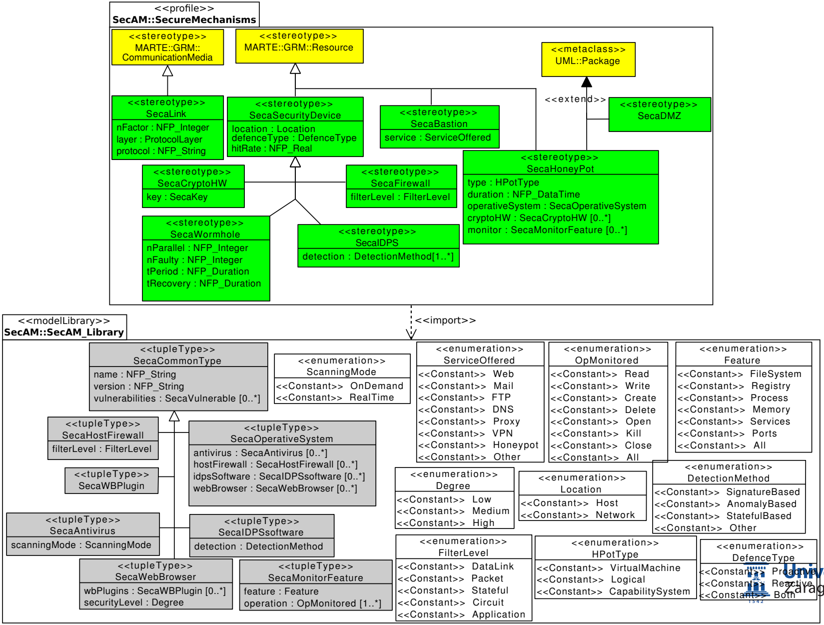
(P1): `Cryptographic`; (P2): `SecurityMechanisms`
(P3): `Resilience`; (P4): `AccessControl`

SecAM Profile (II): Cryptography package (1)



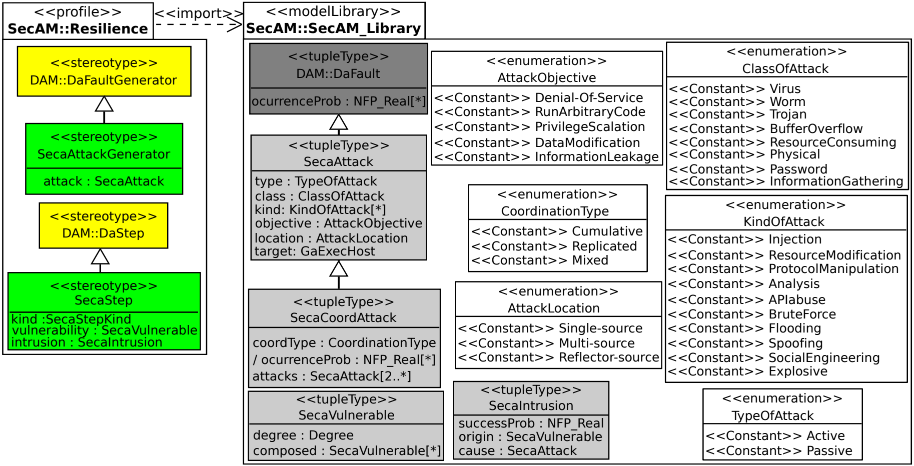
Universidad Zaragoza

SecAM Profile (III): SecurityMechanisms package



Universidad Zaragoza

SecAM Profile (IV): Resilience package



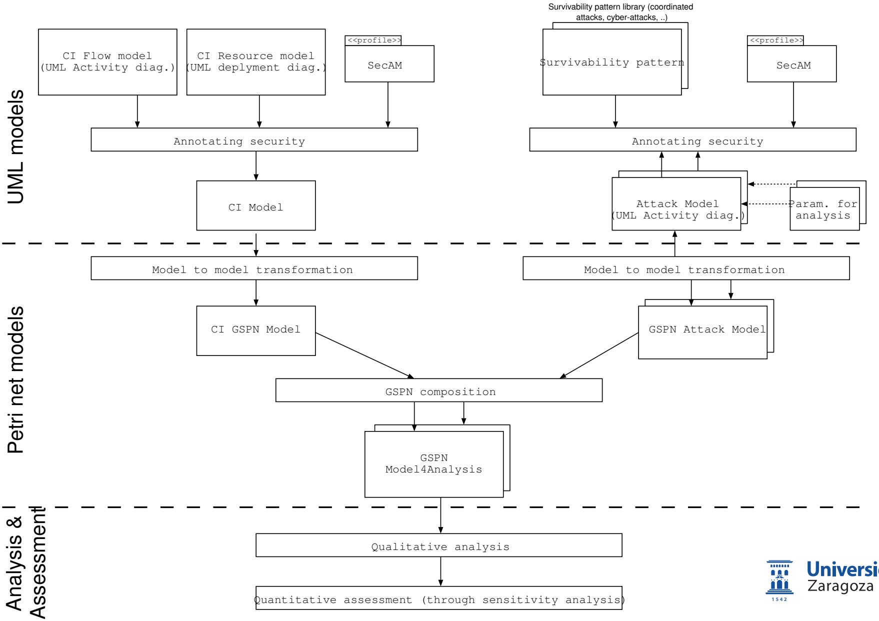
SecAM Profile (V): AccessControl package

Proposal (draft)

- Subjects, operations and objects
- Operations: kind and granted/not granted (boolean)
  - Read
  - Write
  - Access
  - Execution?
- Subjects: self-association
  - Delegation of authorisation
  - Separation of duties
- Idea: access control policies specified by OCL (UML constraints)

Universidad Zaragoza

Model-based Methodology



Case Study (I)

Saudi Arabia crude-oil pipeline network (1)

Highlights

- World's largest
  - exporter of petroleum liquids
  - crude oil producer (8-10 mmbbl/day)
- National distribution network
  - $> 9,000$ miles long

Case Study (I)

Saudi Arabia crude-oil pipeline network (2)

- Terrorist target
  - physical attacks (Abqaiq oil facility, 2006)
  - cyberattacks (Shamoon malware, 2012)

[a] Chaney and Berner. *Global: oil price update: still higher and more uncertain.* Global Economic Forum. Morgan& Stanley. 2004

Universidad Zaragoza 1542

Case Study (I)

Saudi Arabia crude-oil pipeline network (2)

- Terrorist target
  - physical attacks (Abqaiq oil facility, 2006)
  - cyberattacks (Shamoon malware, 2012)
- A 50% reduction of Saudi Arabia crude-oil output would lead to a global recession if the infrastructure could not be repaired within few months[a]

[a] Chaney and Berner. *Global: oil price update: still higher and more uncertain.* Global Economic Forum. Morgan& Stanley. 2004

Case Study (I)

Saudi Arabia crude-oil pipeline network (2)

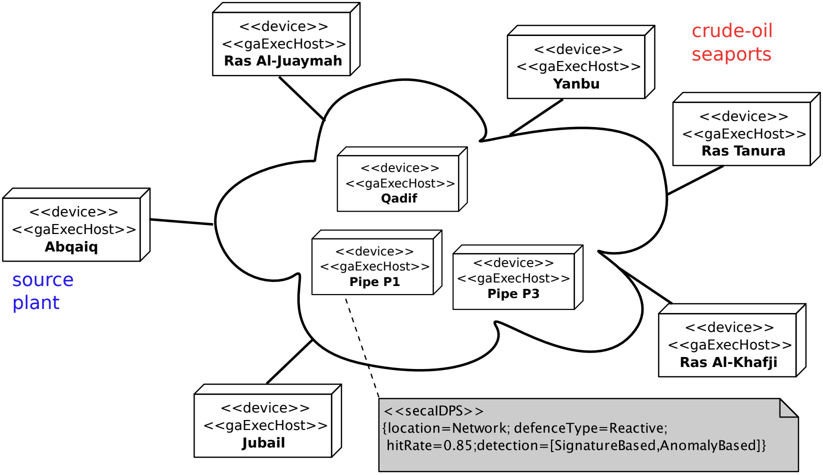
- Terrorist target
  - physical attacks (Abqaiq oil facility, 2006)
  - cyberattacks (Shamoon malware, 2012)
- A 50% reduction of Saudi Arabia crude-oil output would lead to a global recession if the infrastructure could not be repaired within few months[a]
- Survivability strategies are a must to quickly recover -hours/days- the infrastructure

---

[a] Chaney and Berner. *Global: oil price update: still higher and more uncertain.* Global Economic Forum. Morgan& Stanley. 2004

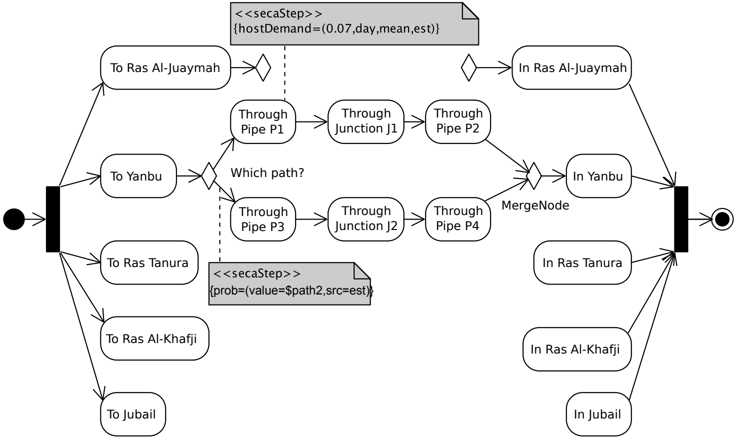
Universidad Zaragoza

Case Study (II): Distribution network model



- MARTE: devices & exec. hosts
- `SecAM`: security mechs

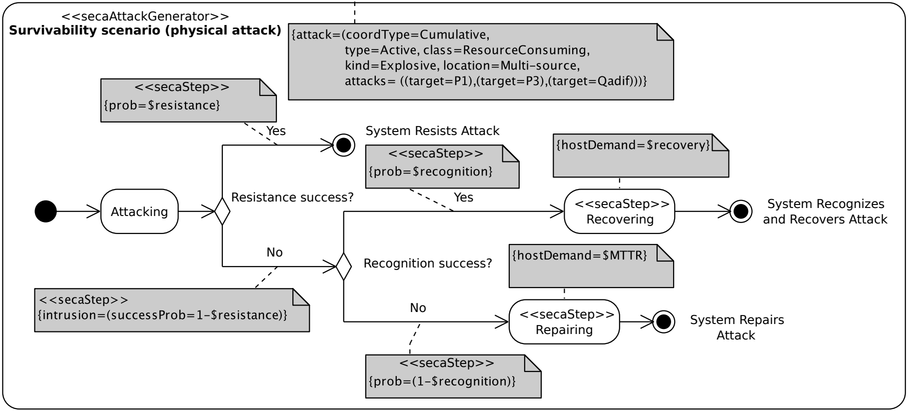
Case Study (III): Crude-oil system flow model



- `SecAM` annotations to specify
  - crude-oil traversal time in pipe, junctions
  - routing probabilities

Case Study (IV): Physical Attack (1)

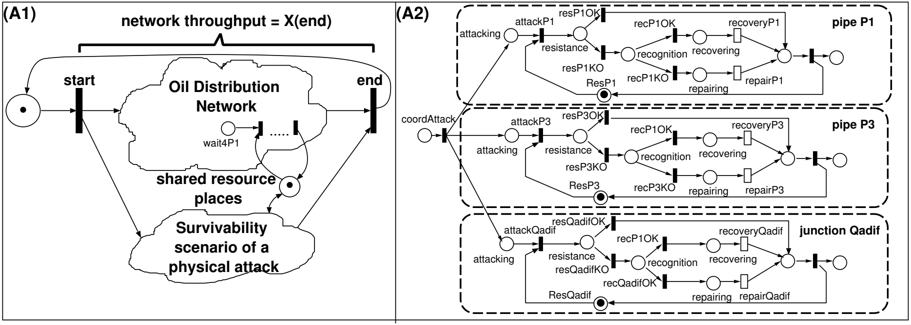
Survivability scenario



- SecAM annotations to specify:
  - Attack type and concrete target nodes in the network
  - Resistance & recognition probabilities
  - Time to recovery & repair

Case Study (IV): Physical Attack (2)

Analysis with GSPN

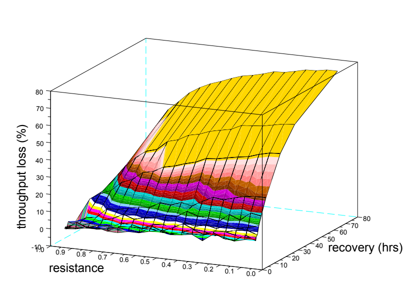


Parameters	Value(s)	GSPN transitions
resistance	[0.05-0.95]	recP1OK, recP3OK, recQadifOK
recognition	1	recP1OK, recP3OK, recQadifOK
recovery	[72-3] hrs	recoveryP1, recoveryP3, recoveryQadif
MTTR	6 months	repairP1, repairP2 repairQadif

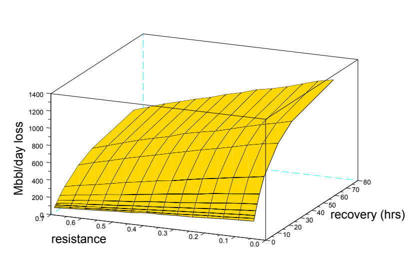
Case Study (IV): Physical Attack (3)

Analysis results

Throughput loss (%)



Mbbl/day loss

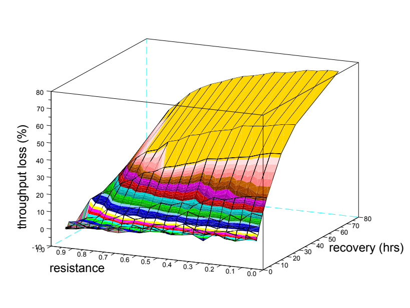


- rec < 6hrs → $X < 20\%$, $n < 240$ Mbbl/day

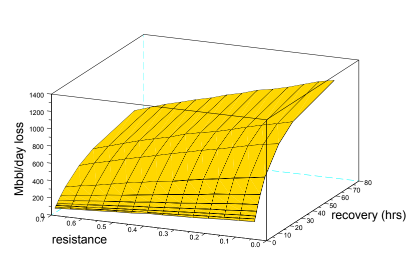
Case Study (IV): Physical Attack (3)

Analysis results

Throughput loss (%)



Mbbl/day loss

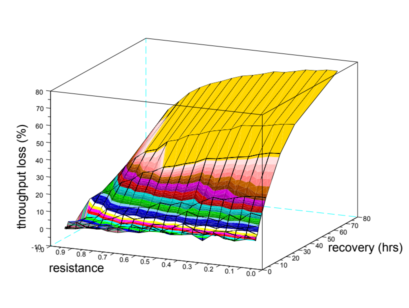


- rec $<$ 6hrs $\rightarrow X < 20\%$, $n < 240$ Mbbl/day
- res $<$ 50%, rec $\in [1-3]$days $\rightarrow X \in [40-77]\%$, $n \in [990K - 1.2M]$

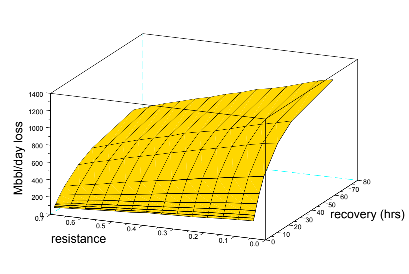
Case Study (IV): Physical Attack (3)

Analysis results

Throughput loss (%)



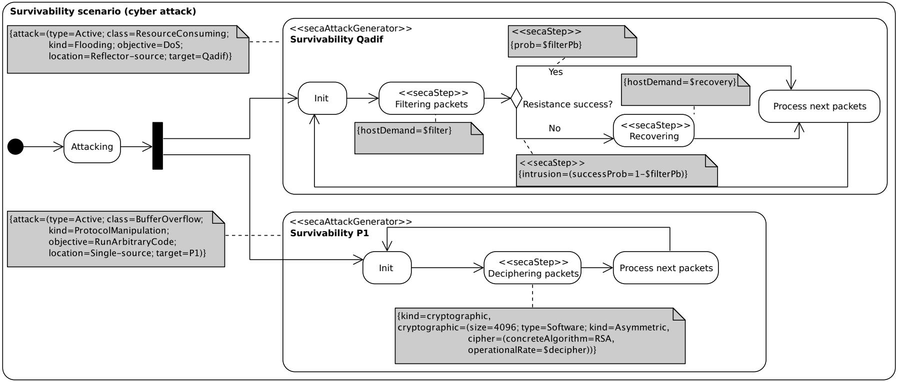
Mbbl/day loss



- rec < 6hrs → X < 20%, n < 240 Mbbl/day
- res < 50%, rec ∈ [1 – 3]days → $X \in [40 - 77]\%$, $n \in [990K - 1.2M]$
- Hard resistance solutions required to maintain $X < 50\%$
  - Example: surveillance combined with external perimeter security

Case Study (V): Cyber Attack (1)

Survivability scenario

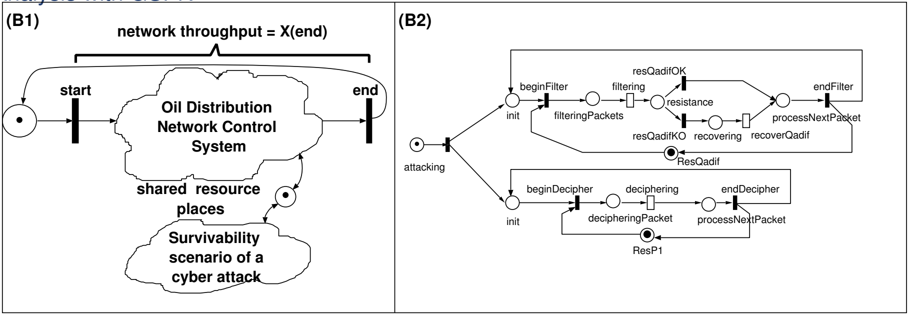


- Coordinated attack to two computation nodes
  - DoS to Qadif node & run arbitrary code to P1 node
  - Resistance strategies: IPDS & cryptographic algorithm

Zaragoza

Case Study (V): Cyber Attack (2)

Analysis with GSPN



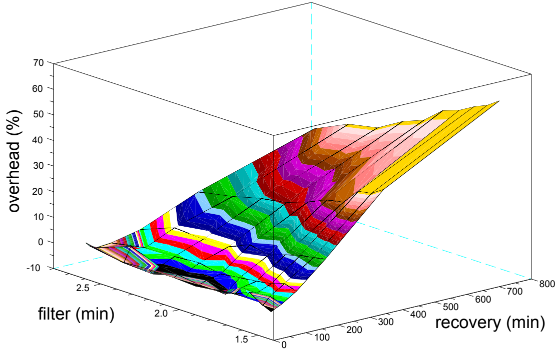
Parameters	Value(s)	GSPN transitions
filterPb	[0.50;..;0.95]	resQadifOK
filter	[1.44min;..;14.4min]	filtering
decipher	2.88 min	deciphering
recovery	[11min-12hrs]	recoveryQadif

- Overhead due filtering solution
  - `filter` and `filterPb` are in direct proportion

Case Study (V): Cyber Attack (3)

Analysis results

- rec $<$ 3hrs $\rightarrow$ $Ov < 16\%$

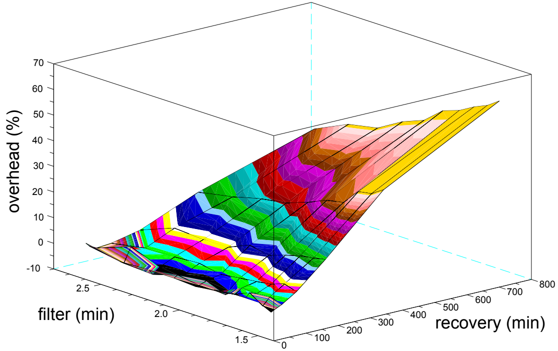


Universidad Zaragoza

Case Study (V): Cyber Attack (3)

Analysis results

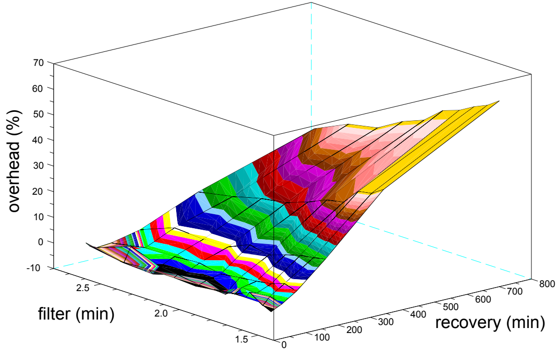
- rec < 3hrs $\rightarrow Ov < 16\%$
- rec $\in [6 - 12]$hrs $\rightarrow$



Case Study (V): Cyber Attack (3)

Analysis results

- rec < 3hrs $\rightarrow Ov < 16\%$
- rec $\in [6 - 12]$hrs $\rightarrow$
  - $Ov \sim 60\%$ for low quality filters

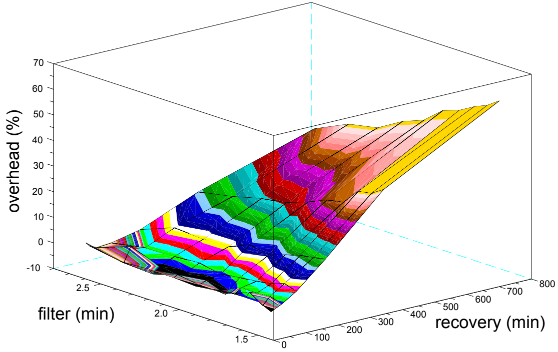


Universidad Zaragoza 1542

Case Study (V): Cyber Attack (3)

Analysis results

- rec < 3hrs → *Ov* < 16%
- rec ∈ [6 – 12]hrs →
  - *Ov* ∼ 60% for low quality filters
  - *Ov* ∼ 30% for high quality ones



Conclusions and Future Work

Conclusions

- `SecAM` enables to express security parameters and requirements
- Formal models to perform survivability analysis
- Evaluate survivability strategies under different scenarios

Universidad Zaragoza 1542

Conclusions and Future Work

Conclusions

- SecAM enables to express security parameters and requirements
- Formal models to perform survivability analysis
- Evaluate survivability strategies under different scenarios

Future Work

- Automated tool to complete transformation (and feedback!)
- Combine SecAM with other formal methods (e.g., Fault Trees or Bayesian Networks)

Universidad Zaragoza 1542

Modelling Security of Critical Infrastructures: A Survivability Assessment

Ricardo J. Rodríguez[†], José Merseguer[†], Simona Bernardi[§]
{rjrodriguez, jmerse, simonab}@unizar.es

[†]Dpto. de Informática e Ingeniería de Sistemas
Universidad de Zaragoza, Zaragoza, Spain

[§]Centro Universitario de la Defensa
Academia General Militar, Zaragoza, Spain

15 de Junio, 2016

II Jornadas Nacionales de Investigación en Ciberseguridad

Granada, España

Accepted in *The Computer Journal*. doi: 10.1093/comjnl/BXU096