Analysis and Optimization of TTEthernet-based Safety Critical Embedded Systems

MSc Thesis Presentation

Radoslav Hristov Todorov
s080990

DTU Informatics
Department of Informatics and Mathematical Modeling

Content

- Project Backlog
- Basics
  - IMA, TTEthernet, AFDX
- Motivation
  - Architectures, Constraints, Problem Definition
- End-to-end Analysis
  - Prelimenary Analysis
- Approaches
- Trajectory Approach
  - Formula
  - (II) Indirect Influence and Time-Triggered (TT) influence
- Case Studies
  - Results
- Implementation
  - Algorithm explanation
- Directions for further development

Project Backlog

1st step
- In this period were researched the technologies: TTEthernet, AFDX
- Some general knowledge about the avionics industry was gained

2nd step
- At this stage was developed a mock-up of the problem formulation
- Some sample configurations were sugested for input of the problem

3rd step
- It was made a complete research of similar problematic
- All possible methods for solution were evaluated

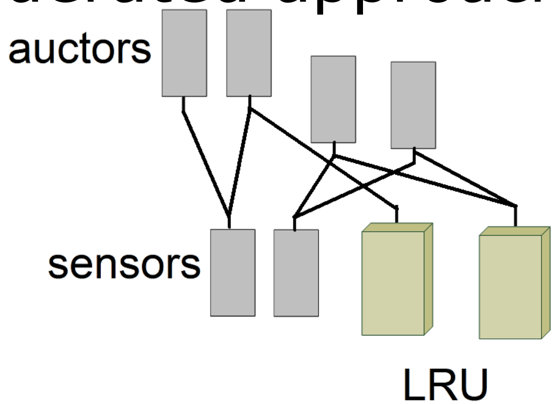
4th step
- A first version of the prototype software was developed
- Some experiments were tested

5th step
- The software was extended
- The proper test cases were chosen for the project

6th step
- The report work was done; Results were observed
- Final corrections were implemented

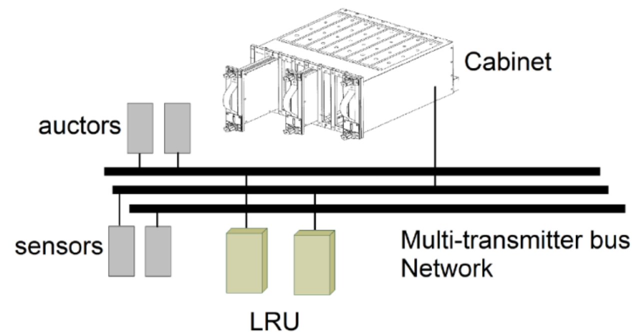
Project Research –
From federated approach to IMA, AFDX and TTEthernet

Federated approach

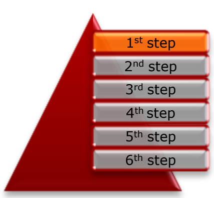


- Integrate several software functions
- Non-transparent fault propagation
- Hard maintenance

IMA approach

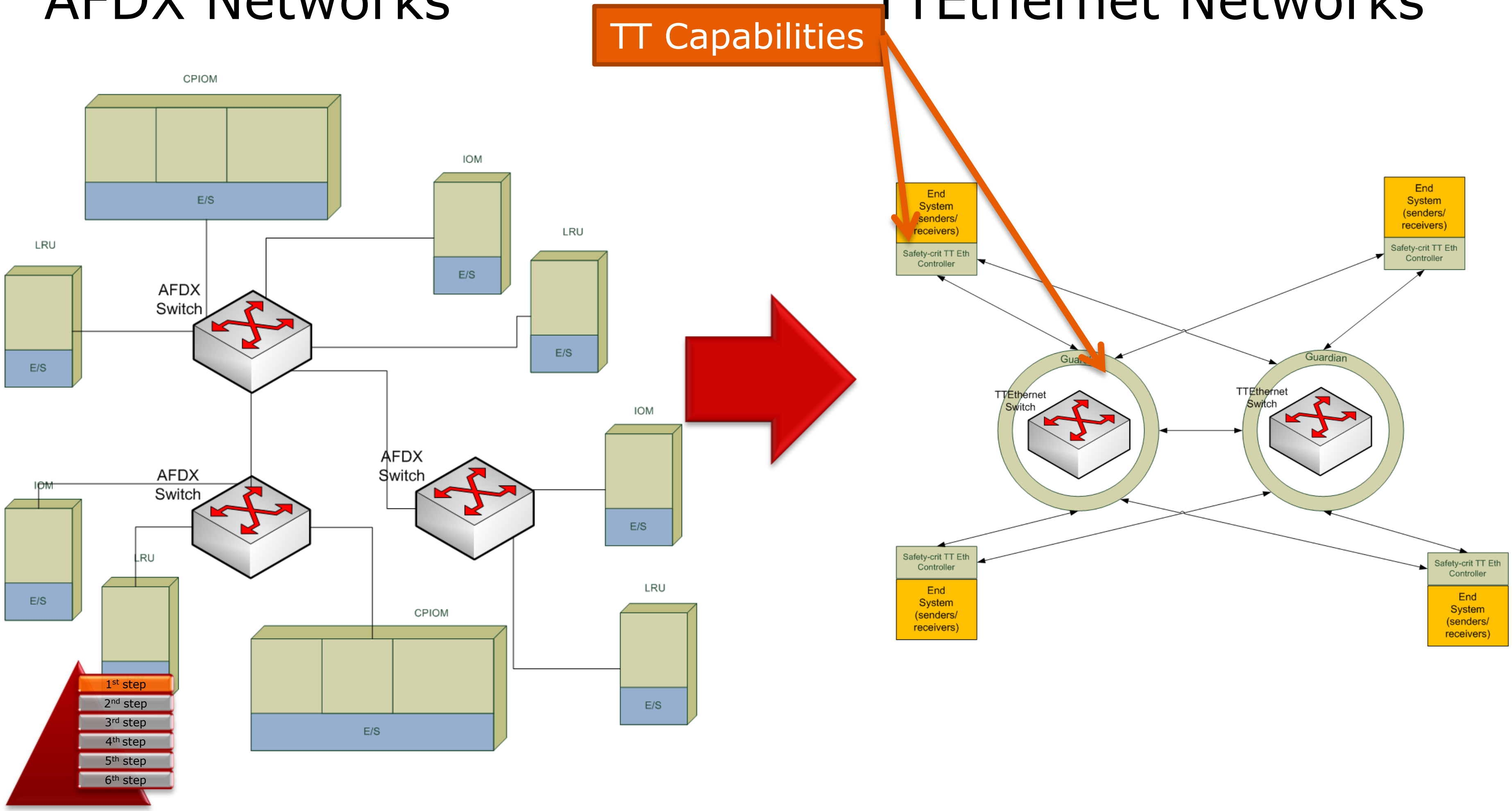


- Integrated Modular Avionics (IMA)
- Functional modules
- Cabinet equipment
- “virtual backplane"



Project Research – From federated approach to IMA, AFDX and TTEthernet

AFDX Networks | TTEthernet Networks



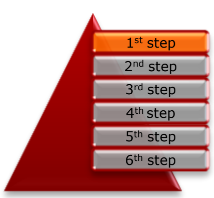
Project Research –
From federated approach to IMA, AFDX and TTEthernet

AFDX Networks

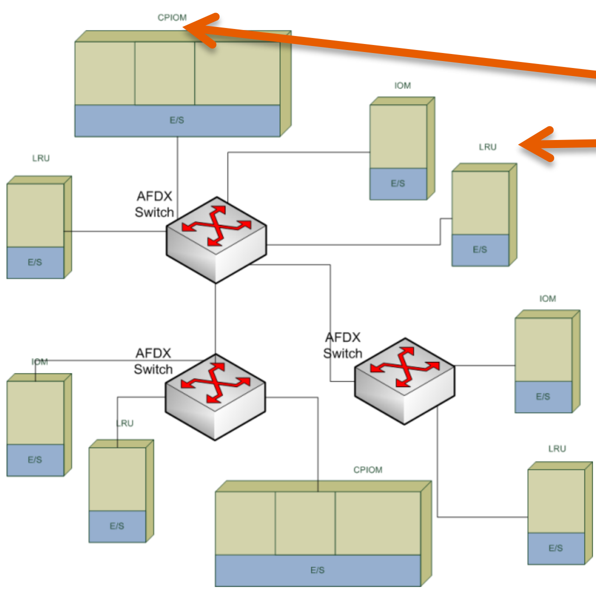
- Connect different equipment
- Allows different design topologies
- Based on well-known Ethernet technology
- Rate-Constrained (RC) messages communication

TTEthernet Netwokrs

- The same as AFDX newtorks plus Time-Triggered (TT) and Best-effort (BE) messages /traffic classes
- Utilize asynchronous and synchronous communication
- Fault-tolerant capabilities
- Global time
- Special Time-Triggered (TT) Ethernet switches
- Capabilities for system-level partitioning and distributed computing



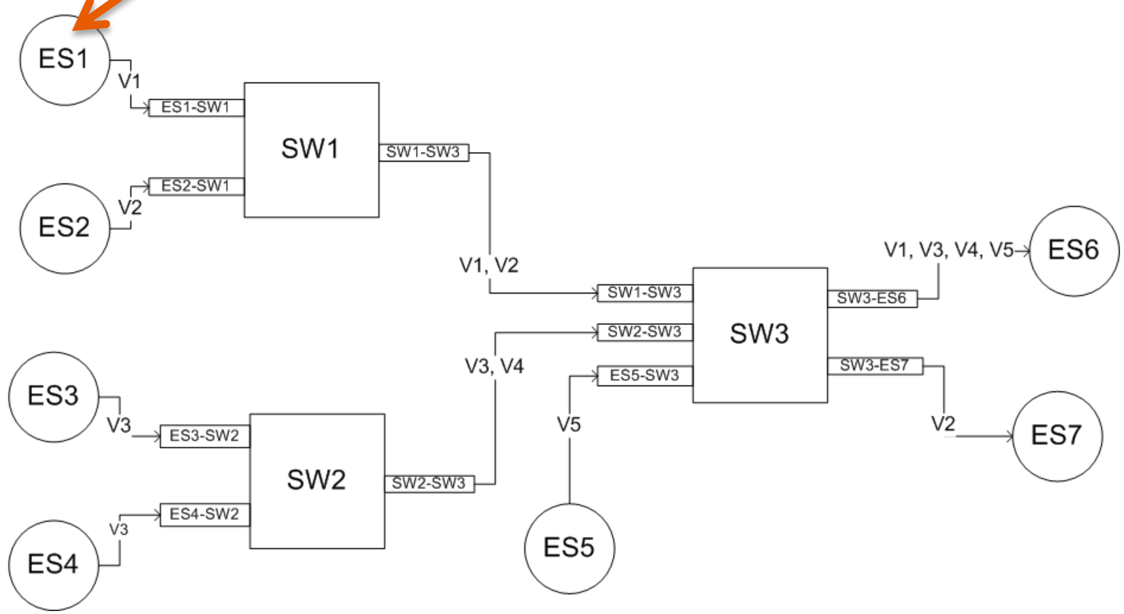
Problem Formulation – Hardware architecture

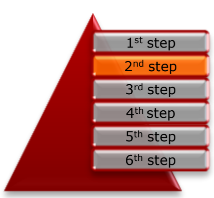


CPIOM Module

/LRU/ IOM

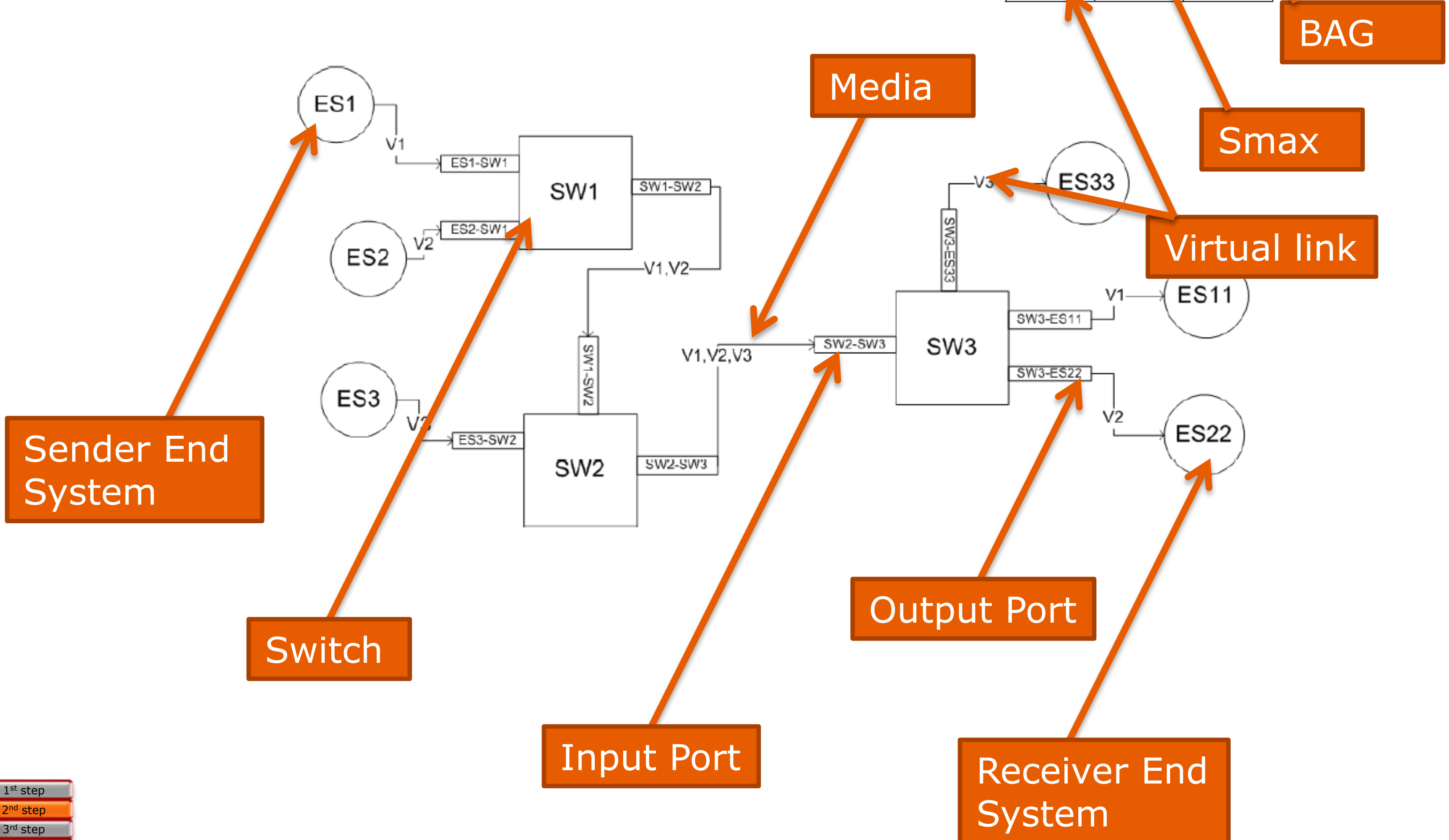
are presented by End Systems

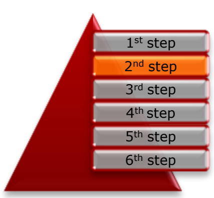




Problem Formulation – Basic Notations

VL	S_{max}	BAG
V_1	3000	500
V_2	2000	500
V_3	1000	500

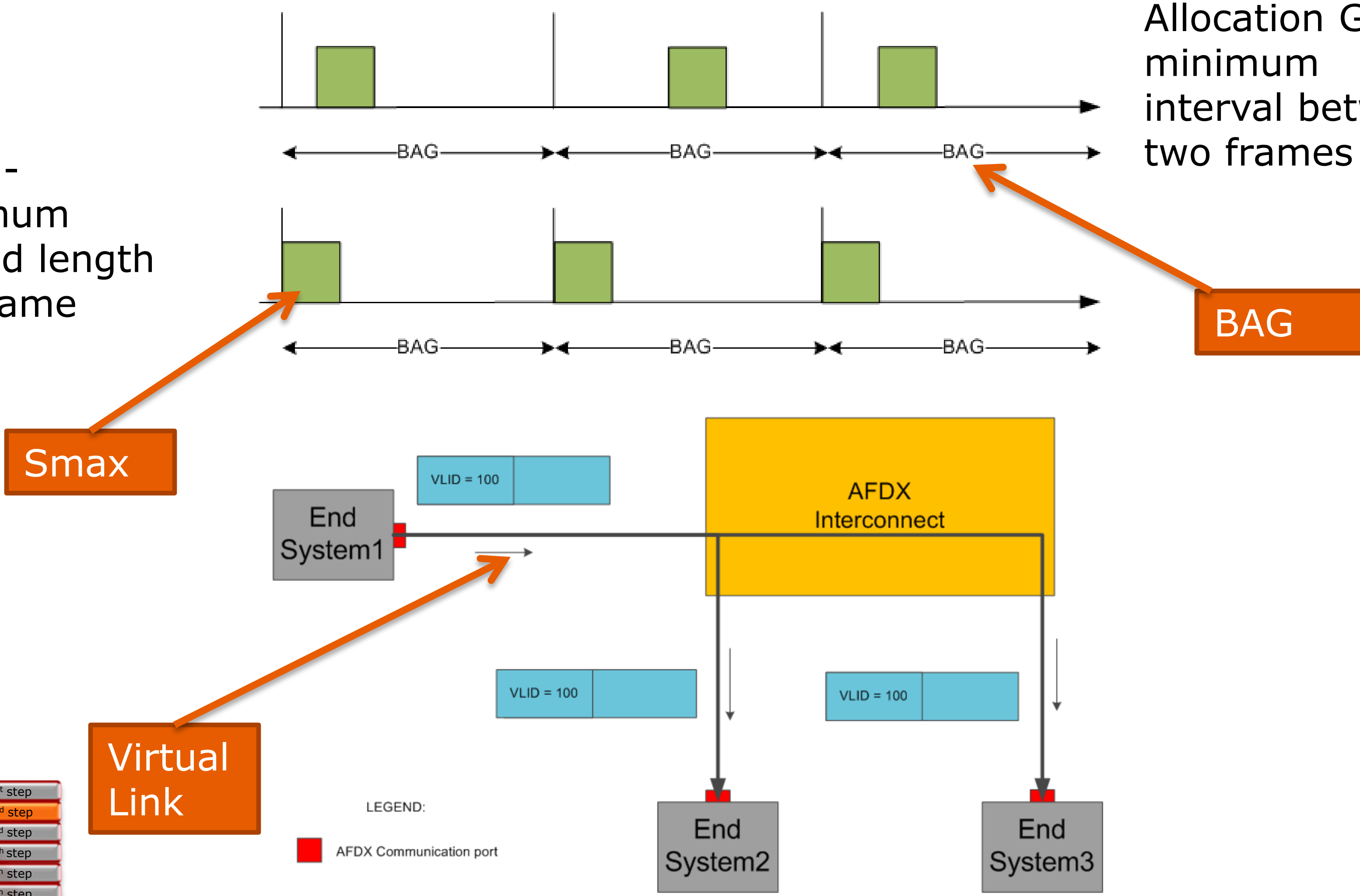


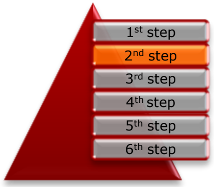


Problem Formulation – Design Considerations

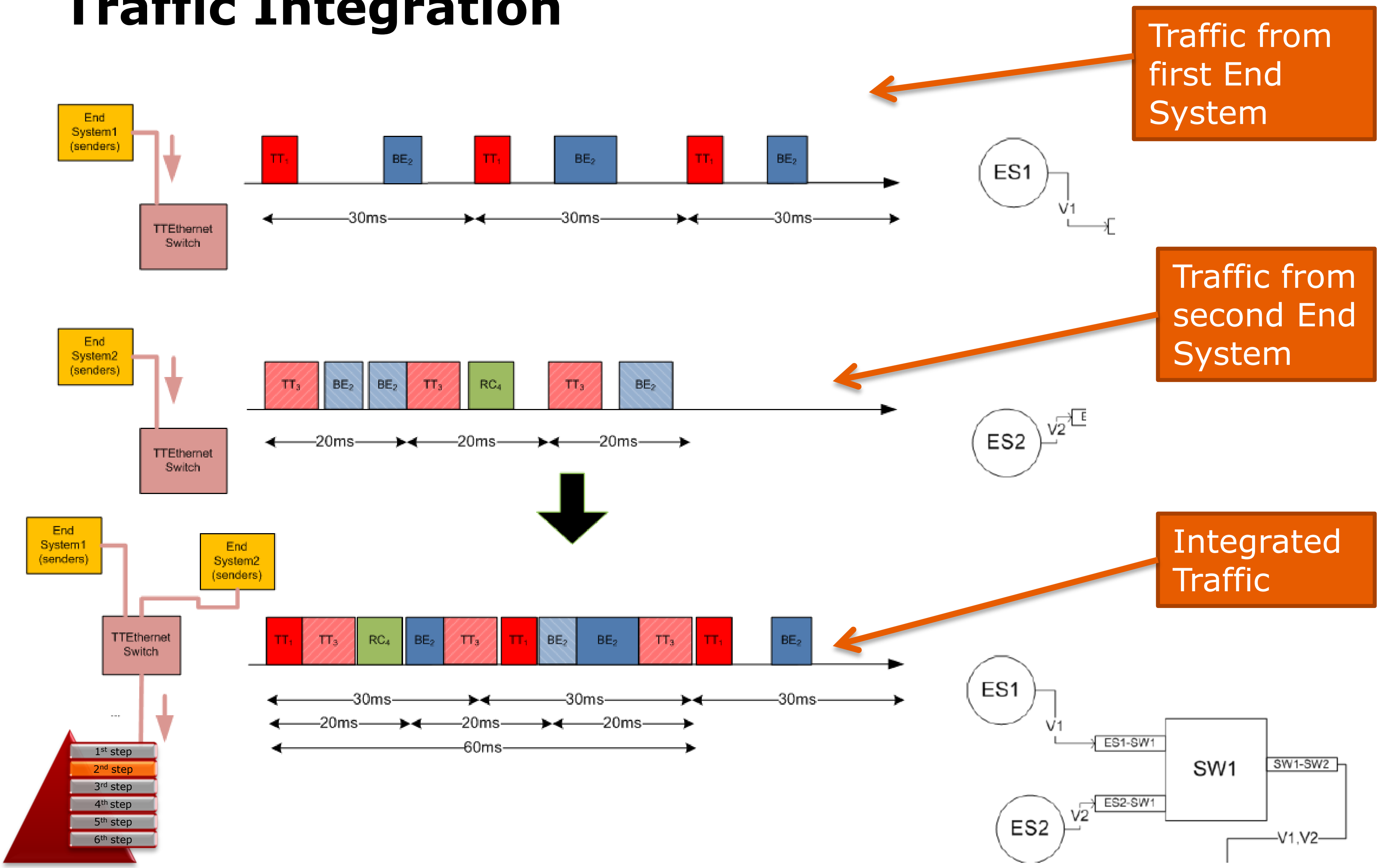
BAG (Bandwidth Allocation Gap)– minimum interval between two frames

Smax - maximum allowed length of a frame





Problem Formulation – Traffic Integration



Problem Formulation – Given

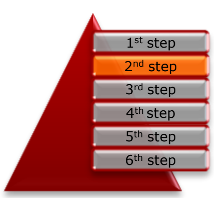
- Given:
  1. The described **architectures** so far
  2. An **application** that has:
     - Time-Triggered (TT) messages
     - Rate-Constrained (RC) messages
- Given Constraints:
  1. Time-Triggered (TT) /static/ messages take precedence
  2. Time-Triggered (TT) traffic is set offline
  3. Time-Triggered (TT) messages setup consists from:

$$< T; D; S_{max}; S_{min}; \text{start-uptime} >$$

  4. Rate-Constrained (RC) messages setup consists from

$$< T = BAG; S_{max}; S_{min} >$$

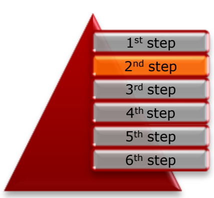
Input



Problem Formulation – Determinate

Additional aspects:
- it could be an AFDX network (only RC mesages)

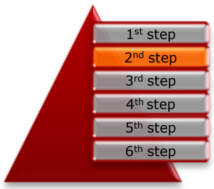
- We are interested in the produced "end-to-end" delays
- We define Scenario I and II for the problem formulation:
  - Scenario I is related to a case where the Time-Triggered (TT) messages are already defined (the problem is how to define them as a table of Time-Triggered constraints) and is required to be done optimizations for the Rate-Constrained (RC) messages.
  - Scenario II is related again to optimization of Rate-Constrained (RC) traffic but in this case the parameters related to them are optimized



Problem Formulation – Goals

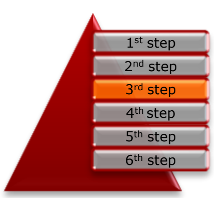
- To avoid packet loss i.e. none of the switches buffers will overflow
- To minimize the end-to-end delay messages, which is necessary to maintain the deterministic nature of the AFDX networks
- To integrate and test the results with networks carrying mixed traffic (Rate-Constrained (RC) and Time-Triggered (TT) messages).

Even the hardware design allows enormous buffering, the second problem still has to be solved



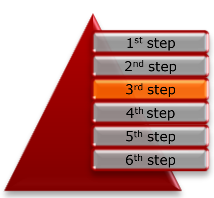
Methods for calculations of End-to-end delays

Method name	Advantages	Disadvantages	References
Network calculus	Conventional and well known	Leads to impossible scenarios and higher values than the real bounds	[31]
Grouping technique	Decreases the end-to-end delays for specific scenarios	Covers only dedicated scenarios depending on the configuration	Private case in [26]
Simulation approach	Easy to implement and understand	Covers only specific scenarios; could not be used to give guarantees for the results	[20], [24]



Methods
for calculations of
End-to-end delays (2)

Method name	Advantages	Disadvantages	References
Time automata modelling	Exact calculation of the modelled configurations	Can be applied only to scenarios with a limited number of nodes	-
Stochastic network calculus	Improves some of the disadvantages of the Network Calculus approach	Considered as hard to understand due the complexity of the theory	[23], [24]
*Heuristic optimization methods over network calculus**	*Tighter experimental results for the bounds compared to the Network Calculus method*	*Requires a lot of experimental work*	*[25]*



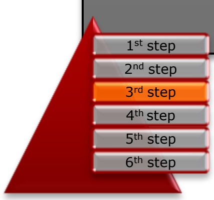
** Optimization approach*

Methods for calculations of End-to-end delays (3)

Method name	Advantages	Disadvantages	References
*Heuristic optimization methods over network calculus with priority assignments**	*Tighter experimental results for the bounds compared to the network calculus method*	*Requires a lot of experimental work and the results are not comparable with whose any other approach*	*[25]*
*Stochastic network calculus with priority assignments**	*Enables priorities to be set for the traffic flows*	*The results are not comparable with those of any other method*	*[18]*
Trajectory approach	Easy to understand and to implement; Shows tighter bounds than the network calculus approach	Analysis includes pessimism which cannot be avoided owing to the nature of the method	[26]

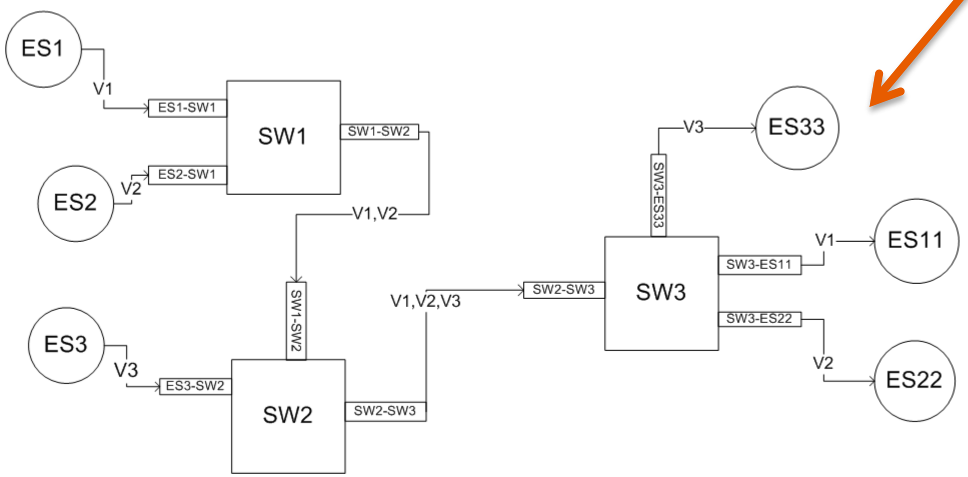
** Optimization approach*

Selected approach



Trajectory Approach
What the approach is calculating?

Input



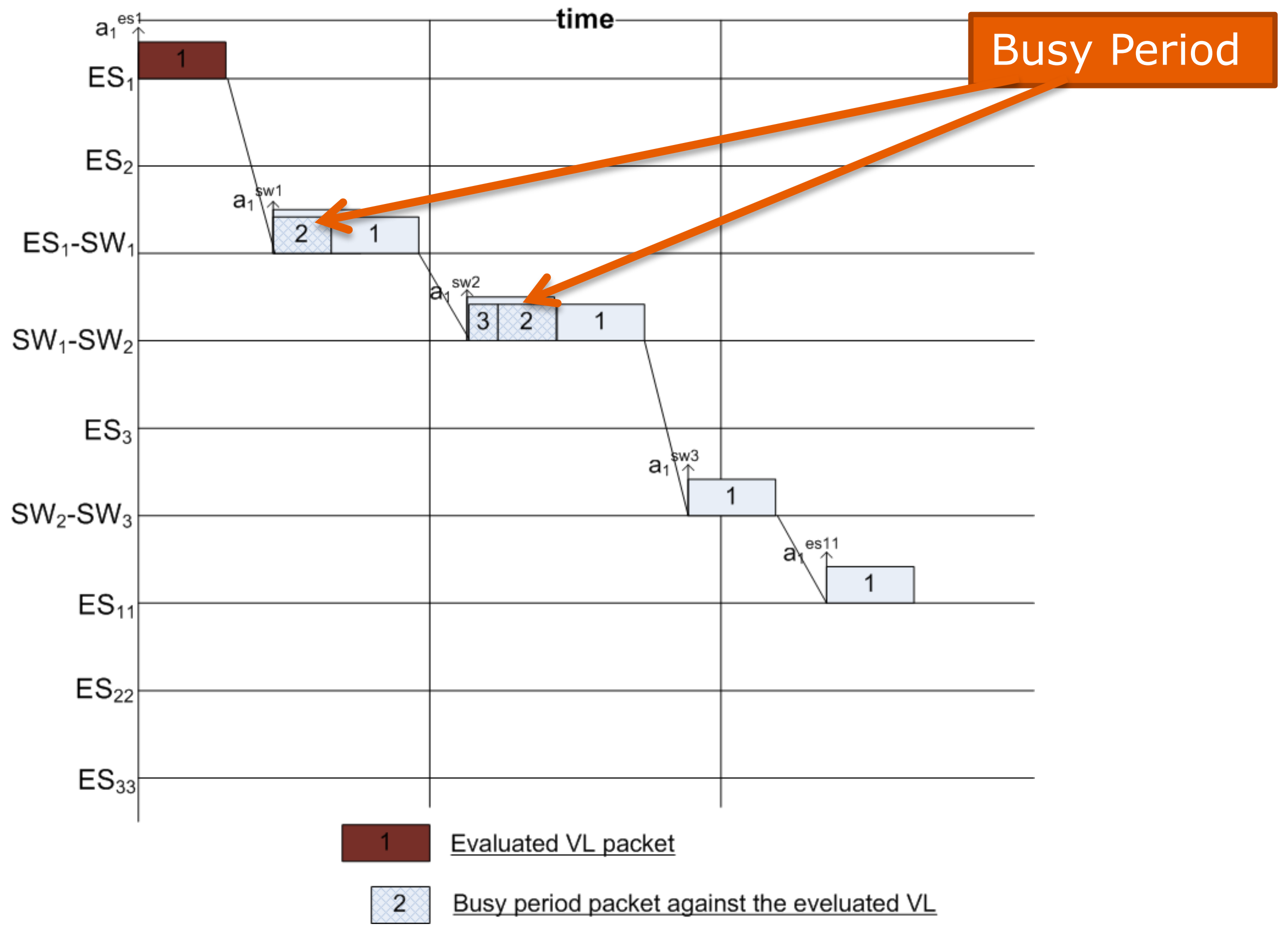
VL	S_{max}	BAG
V_1	3000	500
V_2	2000	500
V_3	1000	500

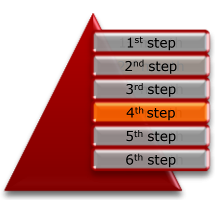
- The approach is based on the analysis of the worst-case scenario for a packet on the basis of its trajectory through the nodes in the network.

- It considers the <u>longest calculated busy period</u> of a message (i.e. all other possible transmissions before the current one or in other words a period of time in which there is at least one message for transmission before the current one in the output buffer of a switch.).

Trajectory Approach
What the approach is calculating?

- In the terms of the example the situation can be presented as the following:

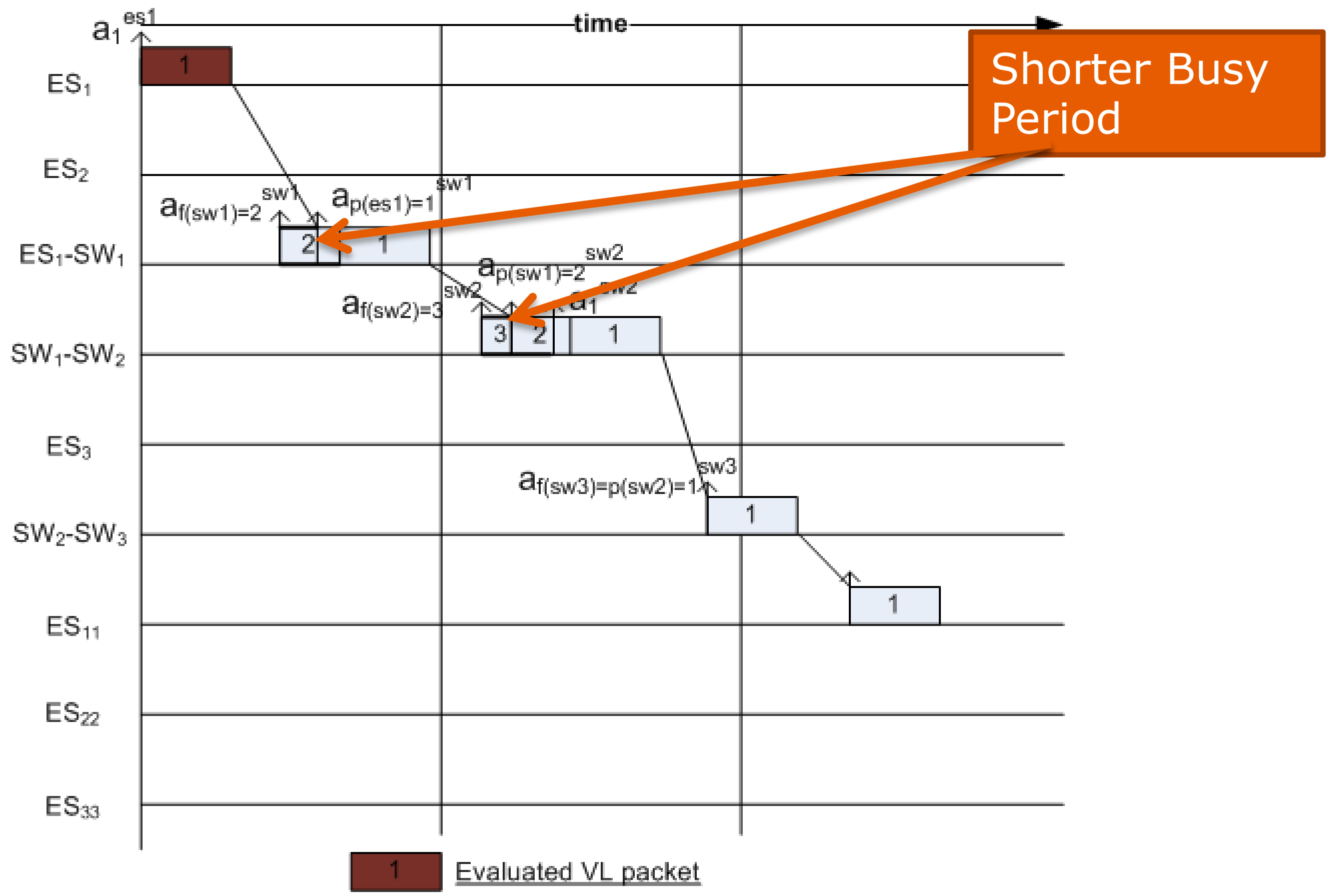


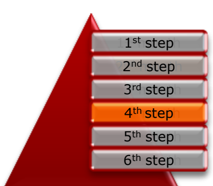


Trajectory Approach

What the approach is calculating?

- Actually, in real the delays are smaller values and almost never reach their peaks:

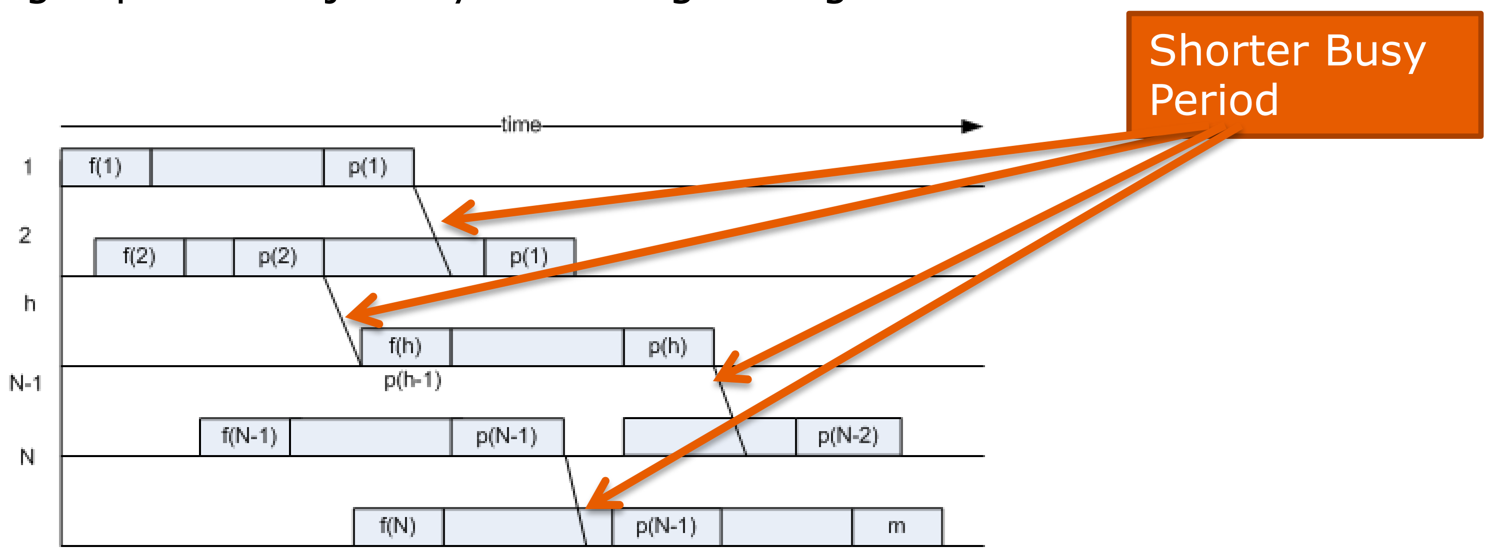




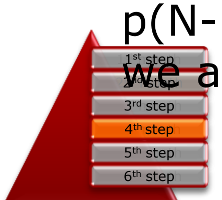
Trajectory Approach

What the approach is calculating?

- The approach is called “Trajectory” because describes the delay of the messages per its trajectory according the figure:



Where f(N)- the first packet processed in the busy period in node N and p(N-1) the first packet processed between f(N) and the packet in which we are interested



Prelimenary Formula for calculation of the Rate-Constrained (RC) message delays

$$D_{p_m} = T_{s_m} + LD_{F_{p_m}} + SD_{F_{p_m}} + WD_{F_{p_m}} + T_r$$

Total end-to-end delay of message F_{pm}

Latency of the source end system. More specifically:

$$T_{s_m} = t_o + t_c + t_s$$

T_{sm} contains time for obtaining data, fragmentation of it and sending costs

Transportation costs. More specifically:

$$LD_{F_{p_m}} = nbl_{p_m} \times L$$

Transmission delay in switches. More specifically:

$$SD_{F_{p_m}} = nbs_{p_m} \times (S_{F_{p_m}}/R)$$

Where S_{Fpm} is the size of the message and R the capacity of the link

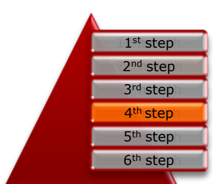
$$WD_{F_{p_m}} = \sum_{Sk \in nbs_{p_m}} WD_{F_{p_m}}(Sk)$$

Transmission delay in switches output ports. Mores specifically:

$WD_{F_{p_m}}(Sk)$ is the delay in the output port buffer S_k

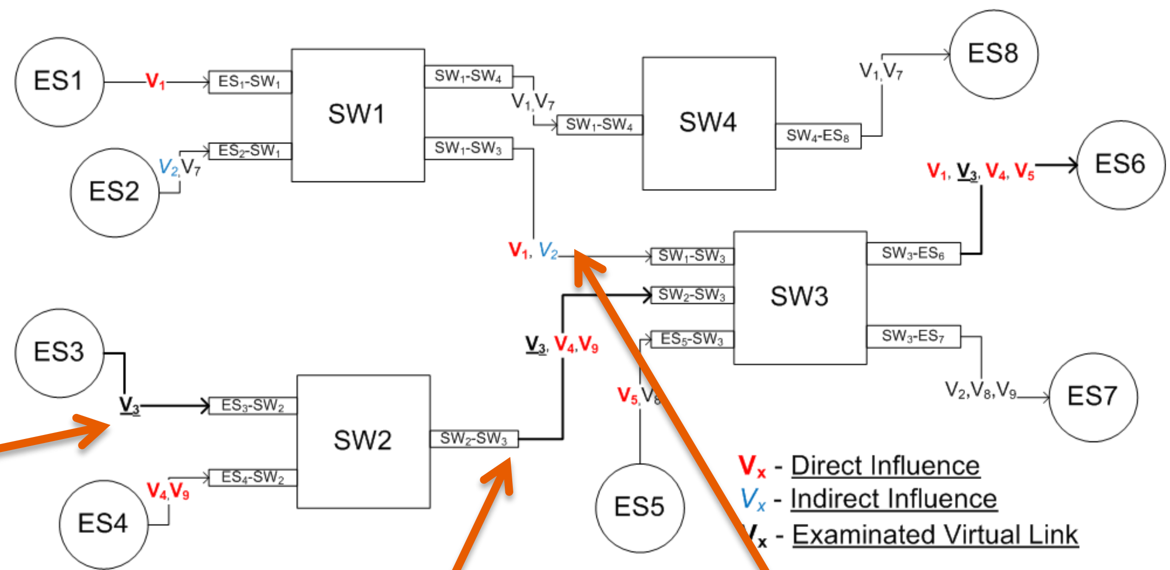
Latency in the destination system

The real problem



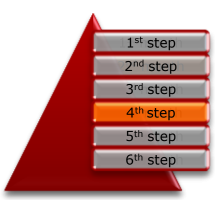
Classification of the virtual links in the system

- Example system:



Virtual Link that is examinated

- How V_x is influenced by the rest of the the virtual links in terms of the end-to-end delay?

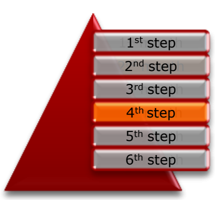


Output port that has contention problem

Indirect influence by V_2

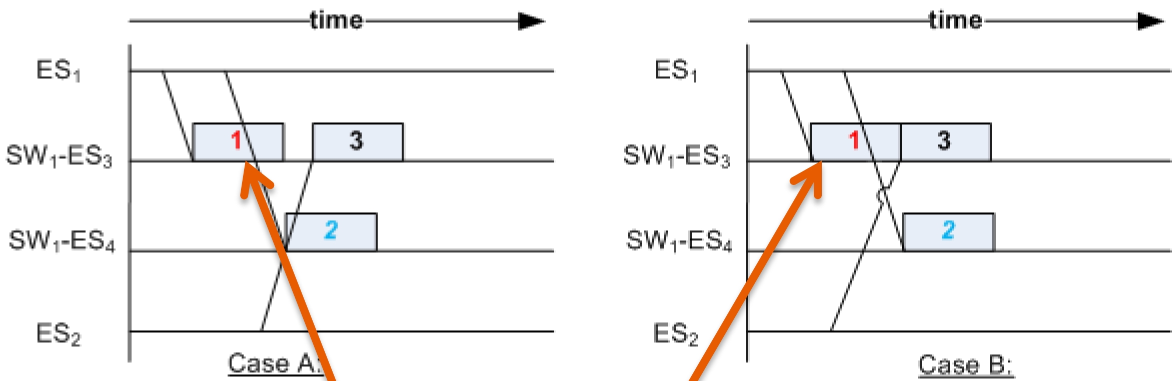
Classification of the virtual links in the system

- There are 2(or 3) classes of virtual links:
  - Direct Influence (DI) virtual links – paths or partial paths which share at least one output buffer
  - Indirect Influence (II) virtual links – paths or partial path which do not share output buffers with but share at least one output buffer with a Direct Influence (DI)or Indirect Influence (II) path.
  - No Influence – paths or partial paths which cannot be classified as either Direct Influence (DI) or Indirect Influence paths.
- Our next task is to research how far Indirect Influence (II) is important for the analysis and how much impact it has on the end-to-end delays.

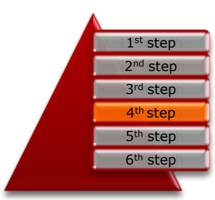


Classification of the virtual links in the system

- Virtual link V_1 has the first message from all virtual links ready for transmission



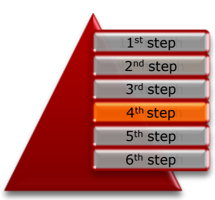
Virtual Link V_1 is the first emited one. V_3 simply depends on the arrival of the message



Classification of the virtual links in the system

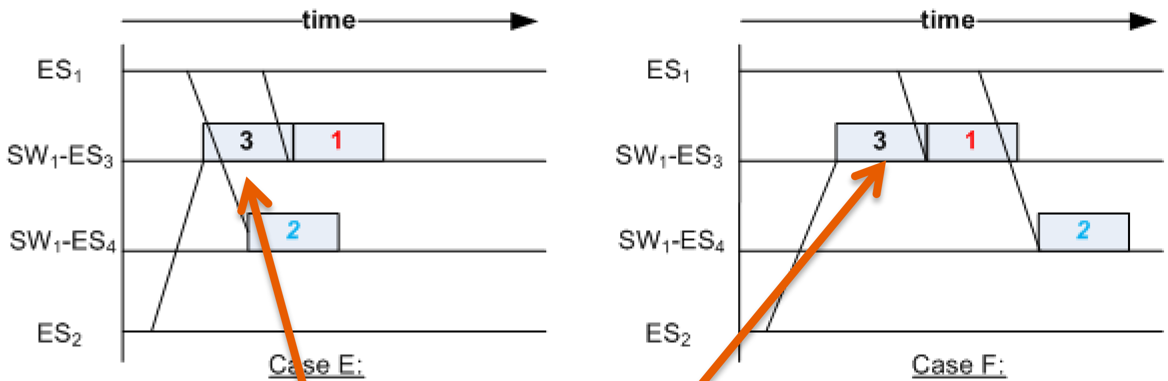
- Virtual link V_2 has the first message from all virtual links ready for transmission

Virtual Link V_2 is the first emited one. V_3 depends on the arrival of the message from V_1 in Case C

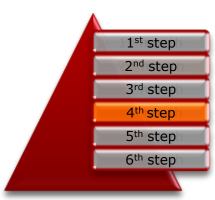


Classification of the virtual links in the system

- Virtual link V_3 has the first message from all virtual links ready for transmission



Virtual Link V_3 is the first emited one and any firther investigation is not required



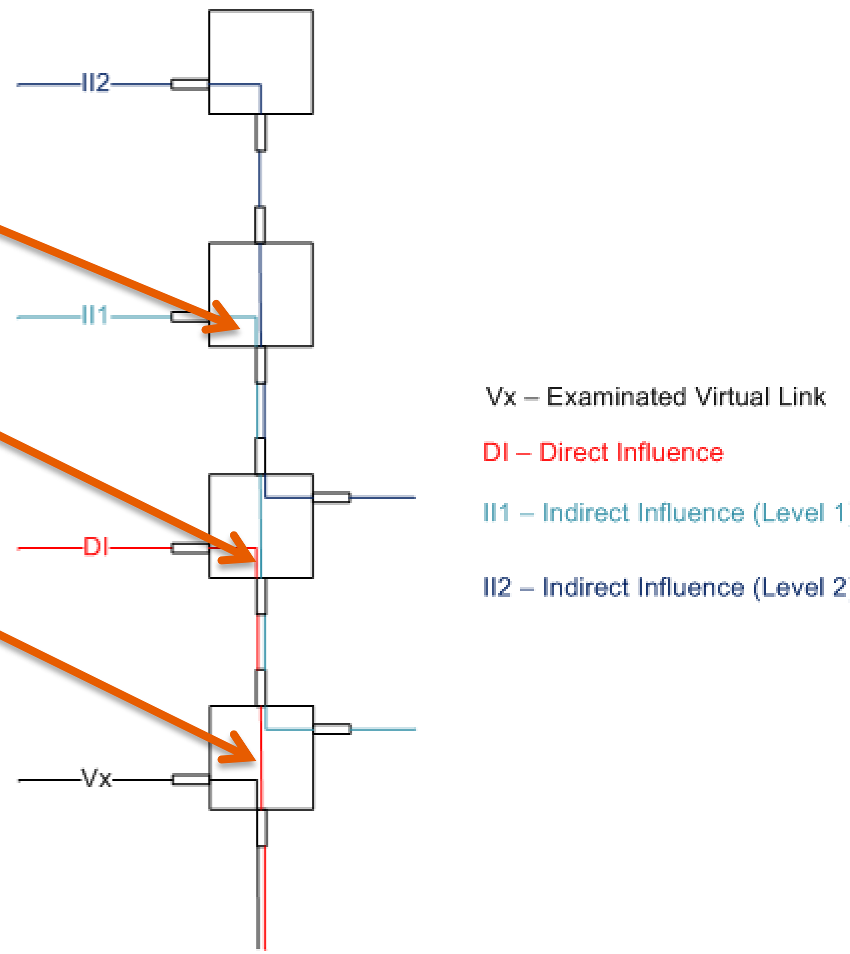
Classification of the virtual links in the system

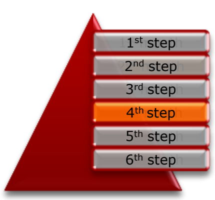
- The Indirect Influence (II) can exist on multiple levels

Indirect Influence (II2)

Indirect Influence (II1)

Direct Influence (DI)





Trajectory Approach

Short description of the formula in one slide

$$R_i = \max_{t \geq -J_i} (W_{i,t}^{last_i} + C_i^{last_i} - t)$$

$$W_{i,t}^{last_i} = \sum_{j \in [1,n]; j \neq i; \mathcal{P}_i \cap \mathcal{P}_j \neq \emptyset} \left(1 + \lfloor \frac{t + A_{i,j}}{T_j} \rfloor \right)^+ \times C_j + \left(1 + \lfloor \frac{t + J_i}{T_i} \rfloor \right) \times C_i + \sum_{h \in \mathcal{P}_i; h \neq last_i} \left(\max_{j \in [1,n]; h \in \mathcal{P}_j} \{C_j\} \right) - C_i + |\mathcal{P}_i + 1|.L_{max}$$

Processing time from packets crossing virtual link i

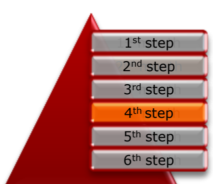
Processing time from packets of virtual link V_i

Worst case end-to-end response time of any message from virtual link i

Processing time for longest packet of virtual links V_j

Processing time for virtual link V_i packet

Delays from path

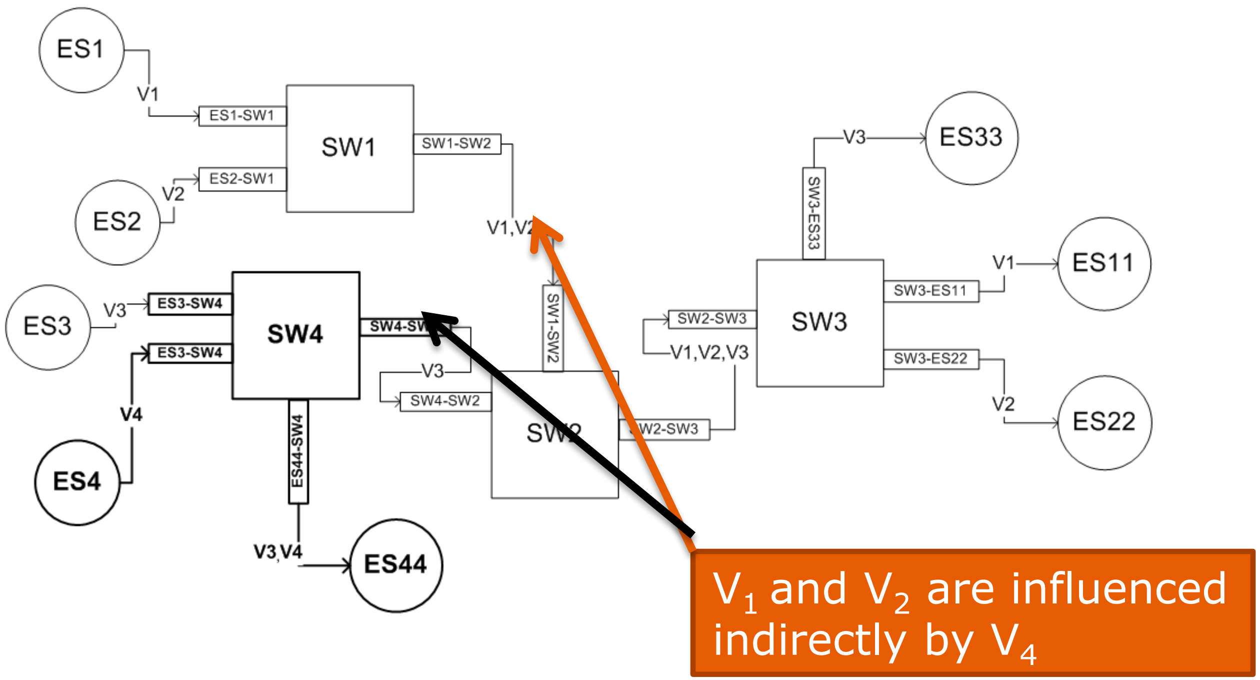


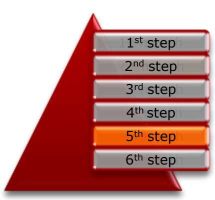
$$A_{i,j} = \min(S_{max_i}^{first_{j,i}} = W_{i,t}^{last_{i,j}} - S_{min_j}^{first_{j,i}}; t) - M_i^{first_{i,j}} + S_{max_j}^{first_{i,j}} + J_j$$

$$C_i^h = C_i = S_{max}/R$$

Enhancement to the Trajectory Approach
Including of Indirect Influence (II) virtual links

- Until now all the experiments were conducted with virtual links that have only Direct Influence (DI) crossing virtual links:

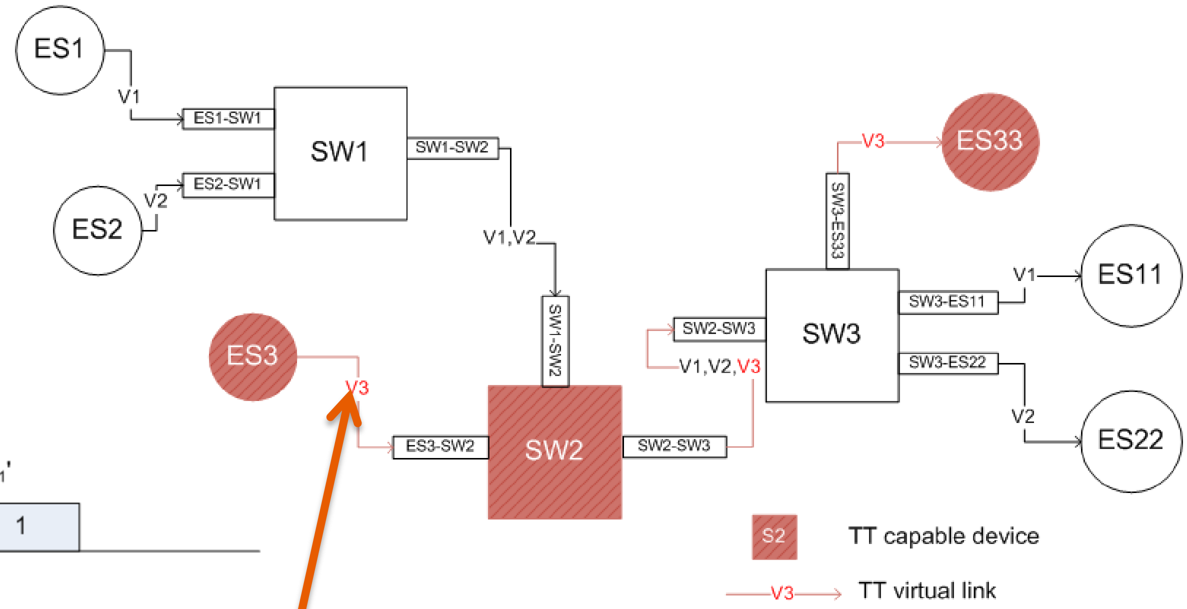


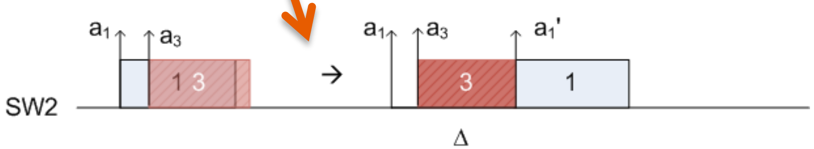


Enhancement to the Trajectory Approach
Including of Time-Triggered (TT) messages

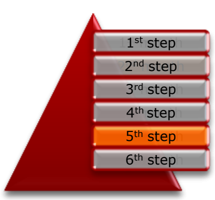
- Until now all the experiments were conducted with virtual links that have only Rate-Constrained (RC) messages:

3 – Time-Triggered (TT) message is predefined and **1** – Rate-Constrained (RC) message has to wait





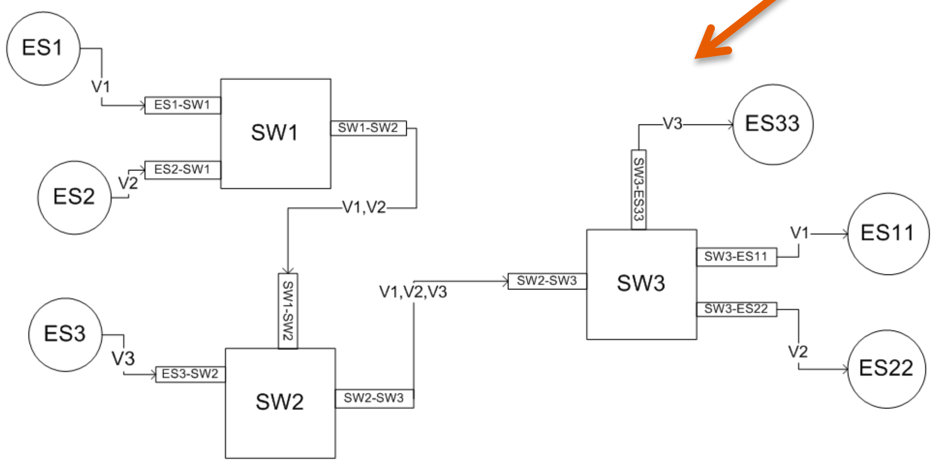
V_3 – Time-Triggered (TT) messages



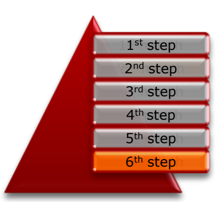
Results
Trajectory Approach

Input

- Several tests were conductuted
- In the report are presented two test cases
  - Case Study 1:



VL	S_{max}	BAG
V_1	3000	500
V_2	2000	500
V_3	1000	500

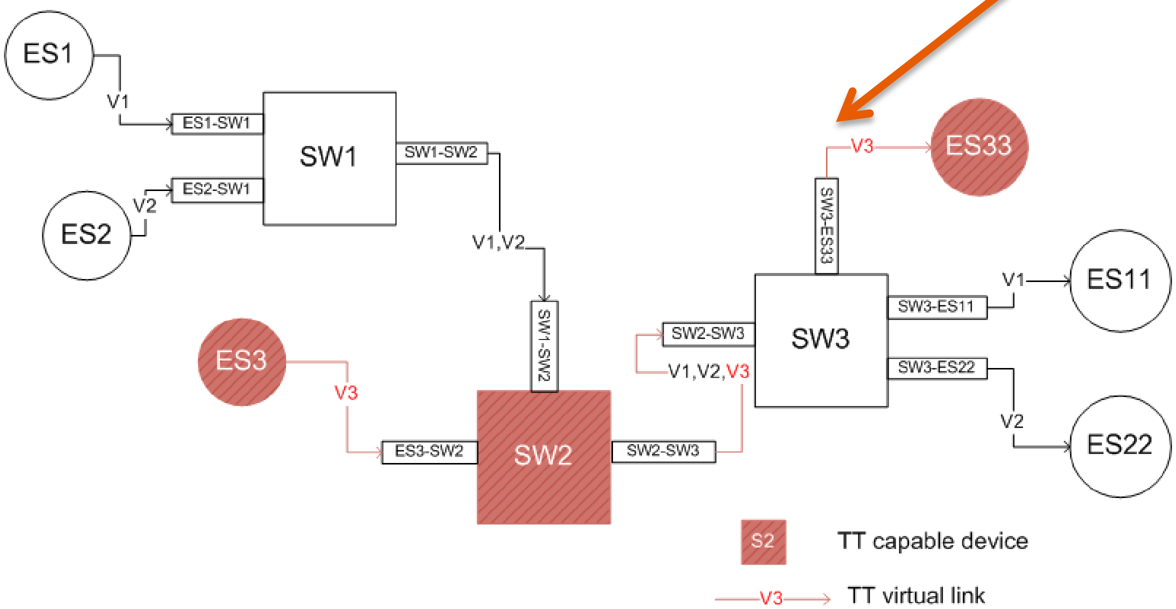


Results

Trajectory Approach –
Extenstion with Time-Triggered (TT) messages

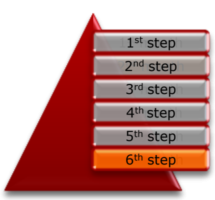
– Case Study 1A:

Input



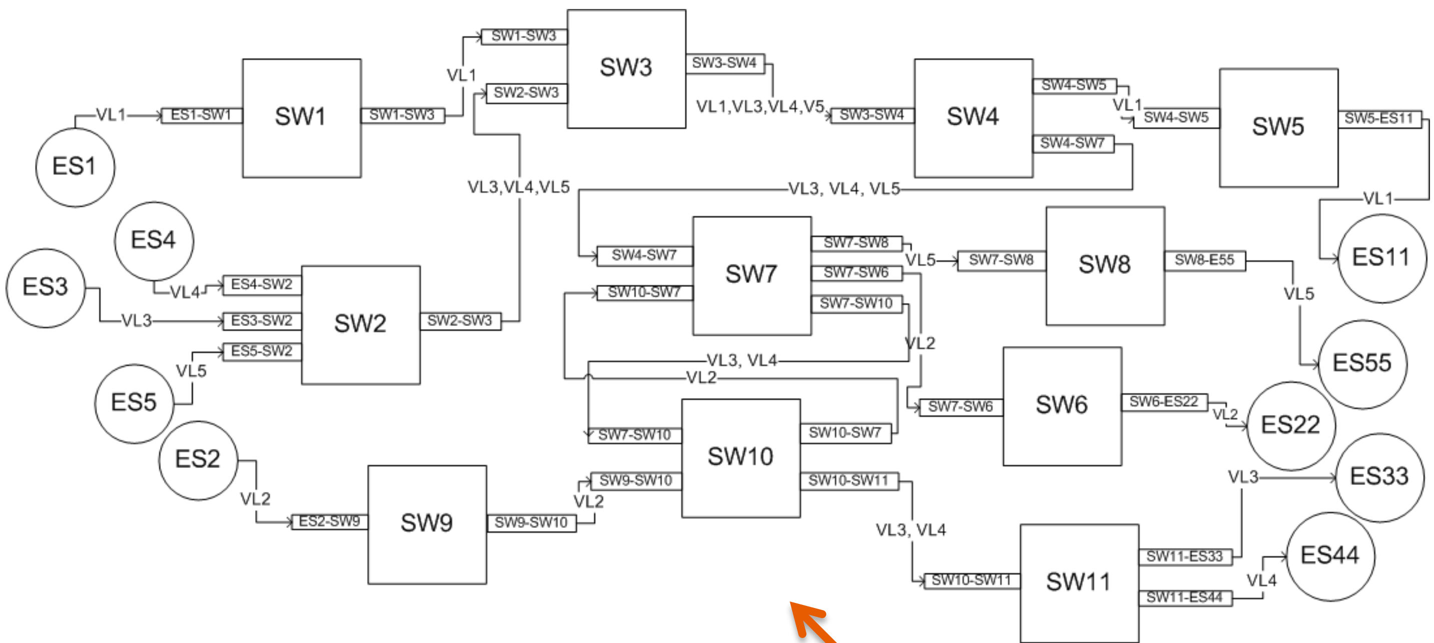
VL	S_{max}	BAG
V_1	3000	500
V_2	2000	500
~~V_3~~	~~1000~~	~~500~~

Predefined time slots



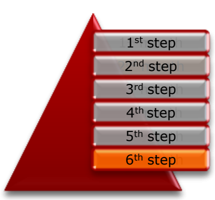
Results
Trajectory Approach

– Case Study 2:



Input

VL	S_{max}	BAG
V_1	4000	360
V_2	4000	360
V_3	4000	360
V_4	4000	360
V_5	4000	360



Implementation of the Trajectory Approach

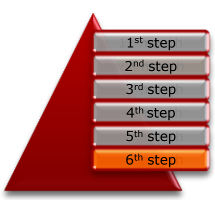
based on the formula and case study 1

Smax	V_1	V_2	V_3
ES	●		
SW_1	●		
SW_2	●		
SW_3	●		

$A_{i,j}$ V_1	V_2	V_3
SW_1	●	●
SW_2	●	●
SW_3		

$A_{i,j}$ V_2	V_1	V_3
SW_1		
SW_2		
SW_3		

$A_{i,j}$ V_3	V_1	V_2
SW_1		
SW_2		
SW_3		



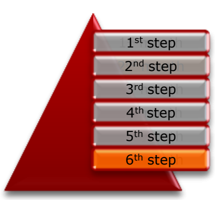
Time-Triggered Message calculations follow the same formula

Implementation of the Trajectory Approach

next to the Holistic

for every V_i **do**
  for $h = first_i$ to $last_i$ **do**
    if $h \neq last_i$ **then**
      calculate $S_{max} = W_{i,t}^{last_i} - t + C_i^h + L_{max}$
    end if
    if $h = last_i$ **then**
      calculate $R = W_{i,t}^{last_i} - t + C_i^h$ with the last S_{max} values
      $R^* = R + [AditionalCost]$
    end if
  end for
end for

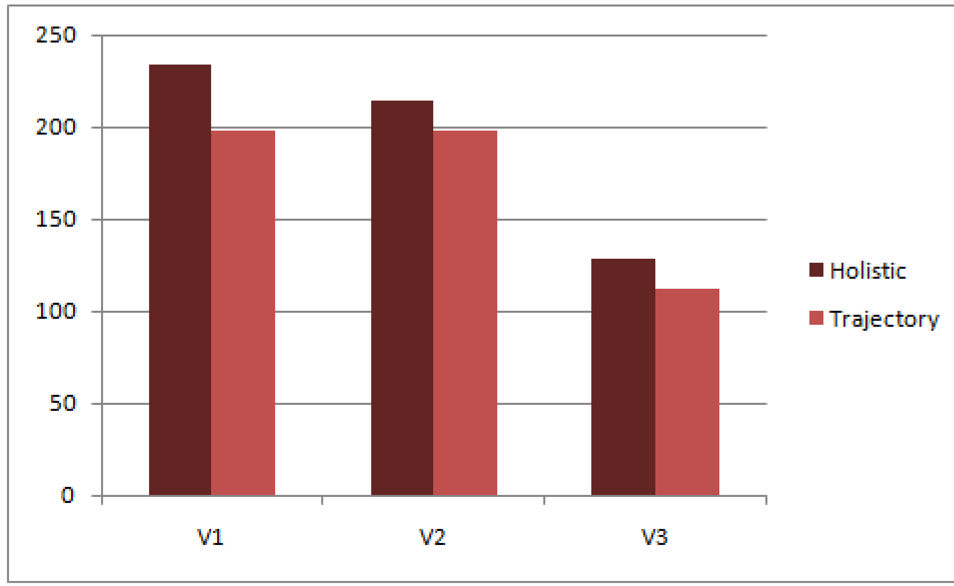
for every V_i **do**
  $R_i + = C_i^{IngressEndSystem} + L_{max}$
  for $h = first_i$ to $last_i$ **do**
    if $\exists V_j \bigcap V_i; V_j \in h; V_j \int \mathcal{S}_{TT}$ **then**
      ∇ = locate next time slot between two TT messages enough to transfer all $\sum_{j=\forall V \bigcap V_i; V_j \in h} + C_i^h$
      if $\nabla < \sum_{j=\forall V \bigcap V_i; V_j \in h} C_j^h$ **then**
        repeat
          locate next time slot between two TT messages
        until $\nabla \geq \sum_{j=\forall V \bigcap V_i; V_j \in h} C_j^h$
        $R_i + = \nabla$
      end if
    end if
    $R_i + = \sum_{j=\forall V \bigcap V_i; V_j \in h} C_j^h$
    $R_i + = C_i^h + L_{max}$
  end for
end for



Results
Trajectory Approach

– Case Study 1:

VL	$Holistic$	$Trajectory$
V_1	234	198
V_2	214	198
V_3	128	112

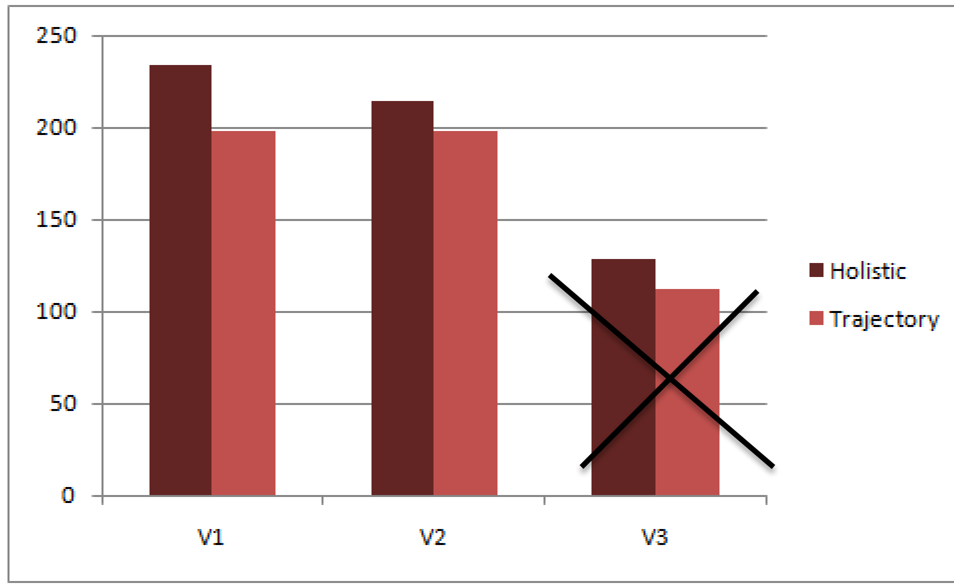


- With the term “holistic" we refer to a method for calculating the entire worst-case response times incurred in transmission of a message from a virtual link assuming the worst-case

Results
Trajectory Approach
Extenstion with Time-Triggered (TT) messages

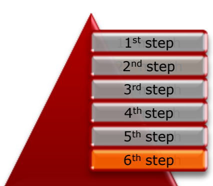
– Case Study 1A:

VL	$Holistic$	$Trajectory$
V_1	234	198
V_2	214	198
~~V_3~~	~~128~~	~~112~~

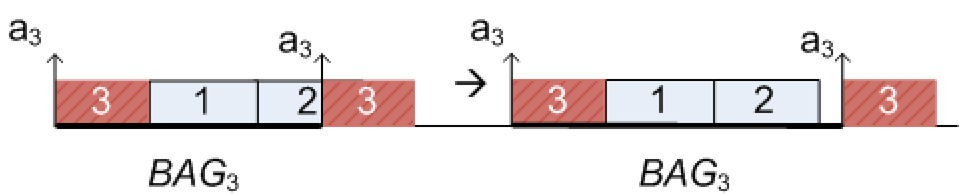


The same results were achieved.

There is no **t** which can change the results



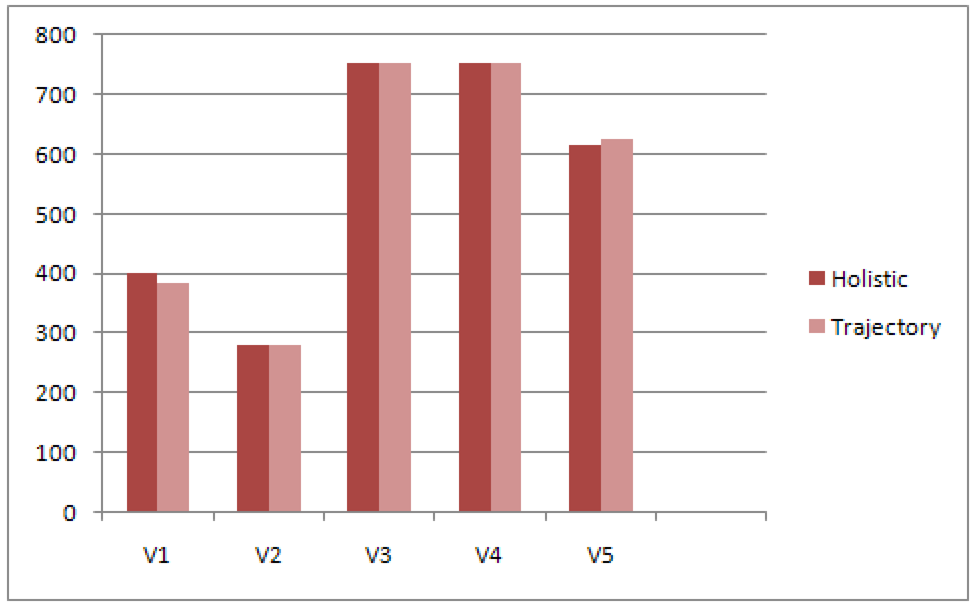
Additionaly:



Results
Trajectory Approach

– Case Study 2:

VL	$Holistic$	$Trajectory$
V_1	400	384
V_2	280	280
V_3	752	752
V_4	752	752
V_4	616	626



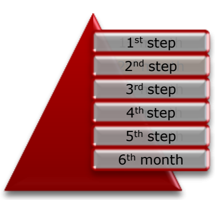
- With the term “holistic" we refer to a method for calculating the entire worst-case response times incurred in transmission of a message from a virtual link assuming the worst-case

Conclusion
Possible extensions

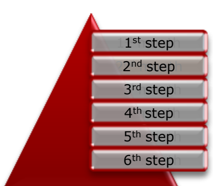
- Influence of the computation time inside the end nodes. An end node is usually subject to contention from several logical partitions that have to cooperate over the usage of the single resource CPU

- Intercommunication between different synchronization domains in these networks. As previously explained, the topology could be complex, and this calls for additional assumptions for the calculations of the worst-case response times

- Best-Effort (BE) traffic with the rest of the ongoing traffic (Rate-Constrained (RC) and Time-Triggered (TT) traffic). A quantitative or quality method should be developed which can show or predict the trends of the behaviour of this traffic class.



Thank you for your time!



Radoslav Todorov