Reliability in a White Rabbit Network

Maciej Lipinski, Javier Serrano, Tomasz Wlostowski, CERN, Geneva, Switzerland
Cesar Prados, GSI, Darmstadt, Germany

White Rabbit (WR) is a time-deterministic, low-latency Ethernet-based network which enables transparent, sub-ns accuracy timing distribution. It is being developed to replace the General Machine Timing (GMT) system currently used at CERN and will become the foundation for the control system of the Facility for Antiproton and Ion Research (FAIR) at GSI. High reliability is an important issue in WR's design, since unavailability of the accelerator's control system will directly translate into expensive downtime of the machine.

Introduction

Reliability is defined as the ability of a system to provide its services to clients under both routine and abnormal circumstances. Thus, we identify critical services of a White Rabbit Network (WRN) based on the study of WR's requirements (Table 1). We then analyze each critical service to identify possible reasons for their failure and propose targeted counter-measures to increase reliability. Finally, their impact on the overall system reliability is studied to identify the highest contributor and the focus for the further studies.

Requirement	GSI	CERN
Max latency	100 s	1000 s
CM failure rate	$3.17 \cdot 10^{-12}$	$3.17 \cdot 10^{-11}$
CMs lost per year	1	1
d_{max} from DM	2km	10km
CM size	200-500 bytes	1200-5000 bytes
Accuracy		1 s to 2ns

***Table 1**. The requirements are defined by GSI and CERN as the prospective users of WR to control their accelerators.*

Information distributed over the WRN (types of services) :

❶**Time** is distributed from a switch/node called Timing Master (TM) to all the other nodes/switches in the network. The deviation between the clock of the TM and that of any other node/switch is called *accuracy.*

❷**Data** is exchanged among all the nodes. However, the critical data is the one sent by a Data Master (DM) carrying sets of commands (events) which are organized into Control Messages (CM) - **Control Data (CD)**. The worst-case upper bound of their delivery latency (*Max latency*) from the DM to any node in the network, regardless of its location (d_{max} *from DM*), is required to be guaranteed – this is a *determinism* requirement.

The reliability of the WRN relies on the deterministic delivery of the Control Data (CD) to all the designated nodes and their sufficiently accurate and stable time synchronization. Unreliability is translated into the number of Control Messages (CMs) considered lost (not delivered, delivered corrupted or in a nondeterministic way) in a given period of time. During this time, the synchronization must be always of the required quality. Quantitative requirements of the accelerator facilities are listed in Table 1.

The failure study resulted in dividing the problem of reliability in the WRN into sub-domains:

- **Determinism** of the data delivery latency which varies with cable length, the number of hops (switches) it has to traverse to reach its destination and the traffic load.
- **Synchronization resilience** against element failure, switch-over between redundant elements and the variation of external conditions.
- **Data resilience** against data loss or corruption due to the physical medium imperfections and switching between redundant elements of the network.
- **Topology redundancy** to eliminate Single Points of Failure (SPoF). Due to the one-to-all character of information distribution in the WRN, all the elements of the WRN are considered SPoF.

Deterministic packet delivery

- A carefully configured and properly used WRN offers deterministic Ethernet frame delivery.
- The upper-bound delay latency can be verified by analysis of **publicly available source code.**
- The analysis (Table 2) revealed that GSI's requirement (100µs over 2km) is not fulfilled with the currently implemented *store-and-forward* solution.
- It was proposed to use the highest priority broadcast Ethernet traffic only for the Control Data and implement the *cut-through* method for this traffic. The analysis results (Table 2) show a significant improvement for the proposed *cut-through* method.

CM Size [bytes]	CM deliery latency			
	Store-and-forward		Cut-through	
	GSI	CERN	GSI	CERN
500	221 s	283 s	76 s	118 s
1500	285 s	325 s	102 s	142 s
5000	324 s	364 s	162 s	202 s

***Table 2.** Control Message (CM) delivery latency estimation, the requirement by CERN is 1000 µs and by GSI is 100µs.*

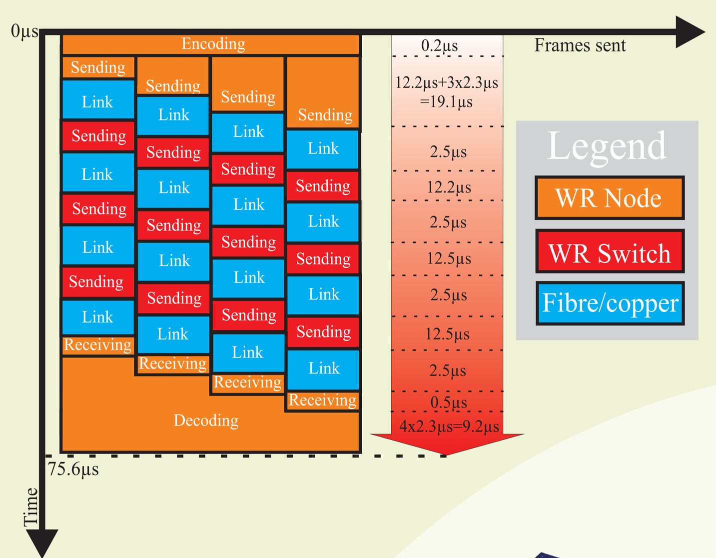
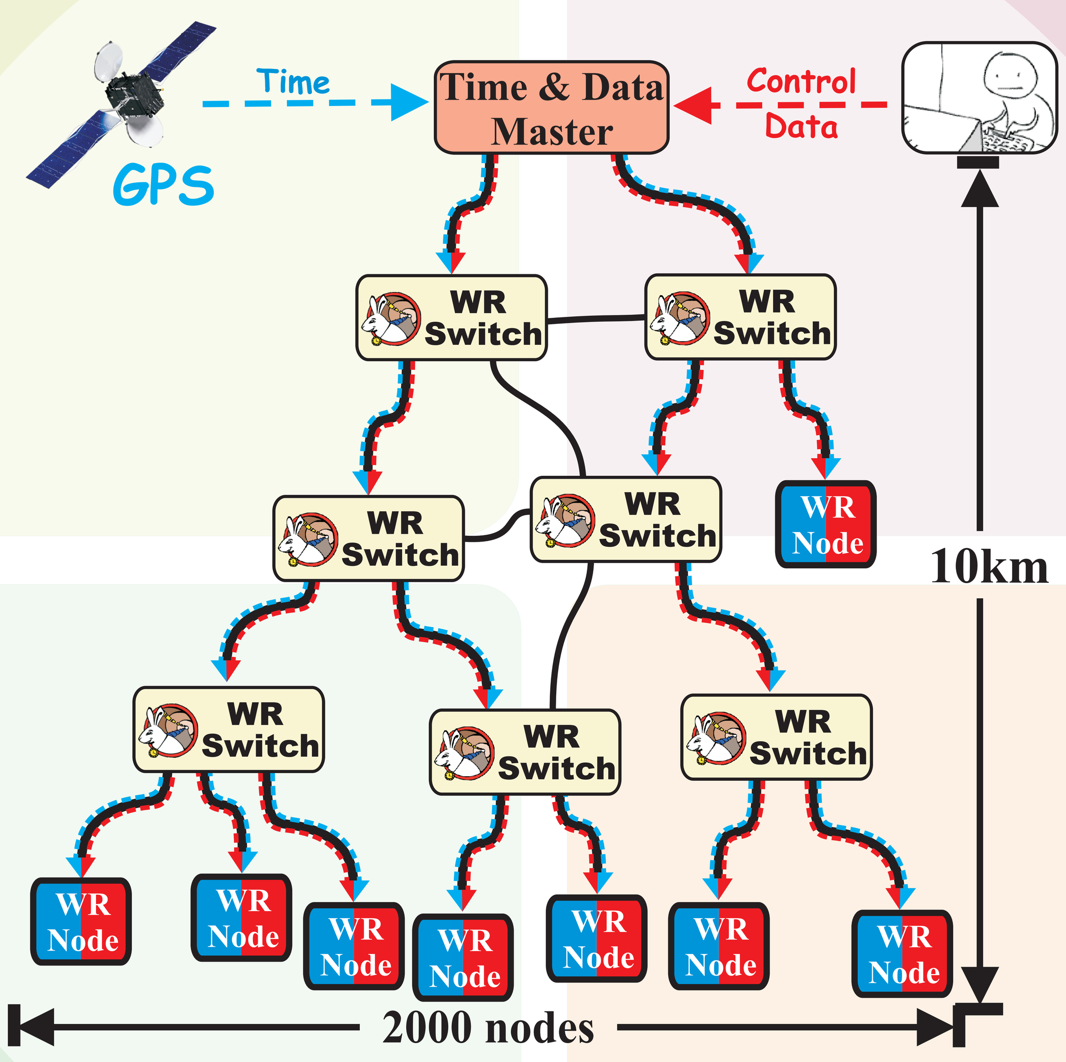


***Figure 1.** Control Message latency estimation.*



Synchronization resilience

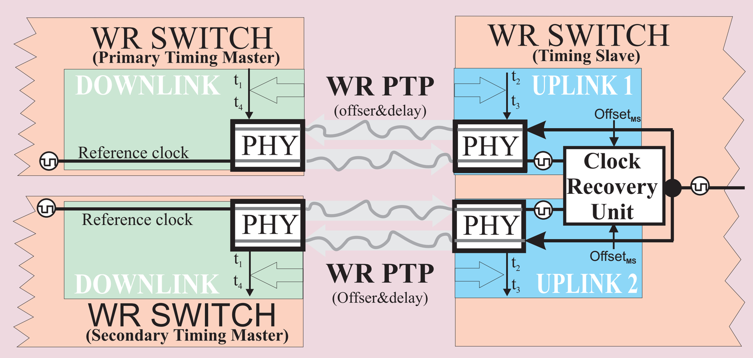


***Figure 2.** Seamless switch-over between redundant uplinks.*

Synchronization quality can deteriorate due to :

- ☑ Failure of network elements (resolved by network topology redundancy)
- ☑ Variation of external conditions, i.e. temperature (resolved by the used PTP protocol)
- ☐ Switch-over between redundant sources of timing (proposed special solution)

In WR, the switch-over is heavily supported by the Clock Recovery System (CRS) of the switch and the WR extension to PTP (WRPTP). Figure 2 presents an example where a switch (timing slave) is connected (by its uplinks 1 & 2) to two other switches (primary and secondary masters) – the sources of timing. On both uplinks the frequency is recovered from the signal and provided to the CRS. Similarly, WRPTP measures delay and offset on each of the links and provides this data to the CRS. The information from uplink 1 (primary) is used to control the CRS and adjust the local time. However, at any time all the necessary information from the uplink 2 is available and a seamless switch-over can be performed in case of primary master failure.

Topology redundancy

The overall reliability is strongly dependent on the WRN topology which needs to be appropriate for the proposed solutions (SyncE, H/W-supported RSTP, determinism).

Redundancy	Switches	P	MTBF [h]
No	127	$2.08 \cdot 10^{-3}$	$5.77 \cdot 10^{3}$
Double	292	$4.71 \cdot 10^{-7}$	$2.55 \cdot 10^{7}$
Triple	495	$3.06 \cdot 10^{-11}$	$4.08 \cdot 10^{11}$

***Table 3.** WRN topologies's relibilities.*

Topology comparison:

- We consider the reliability of a network of switches.
- Each node is connected to the network with M links (each to a separate switch), where M reflects the level of redundancy.
- Rough estimations of the probability of WRN failure (Table 3) using analytic calculations for the three considered topologies show that **triple redundancy topology can barely satisfy the requirements by CERN** (Table 1).

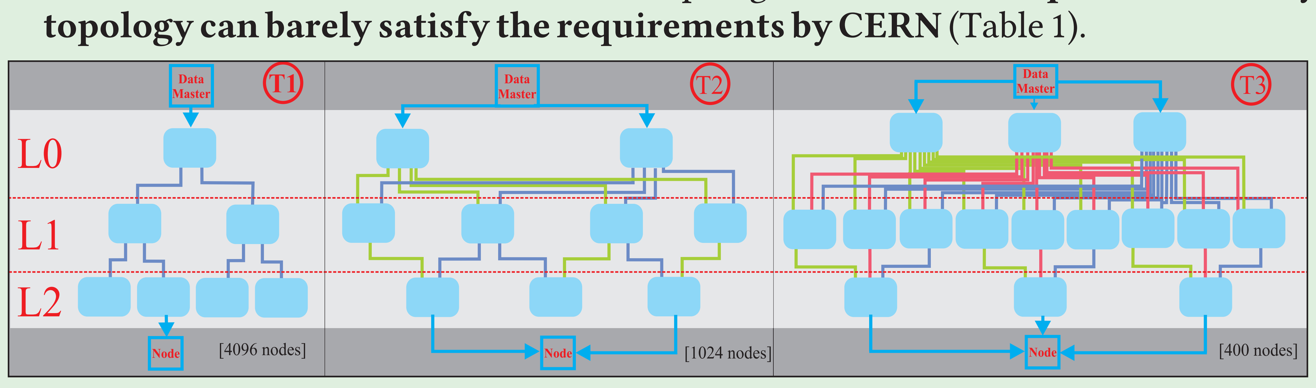


***Figure 4.** WRN topologies, Switch's MTBF of 200 000 hours.*

Data resilience

Two concacenated **Forward Error Correction** (FEC) schemes are used to decrease the loss rate of the Control Messages :

- **Reed-Solomon (R-S)** coding allows to encode k original-frames into n encoded-frames (n > k). Reception of any k encoded-frames enables to decode the original frames.
- **Hamming coding (SEC-DED)** is used to correct bit errors.

Hardware-supporting Rapid Spanning Tree Protocol (RSTP) is proposed to prevent loosing Control Messages (CMs) during the switch-over between redundant links. The maximum **convergence time of 3µs** between active and backup connections is required.

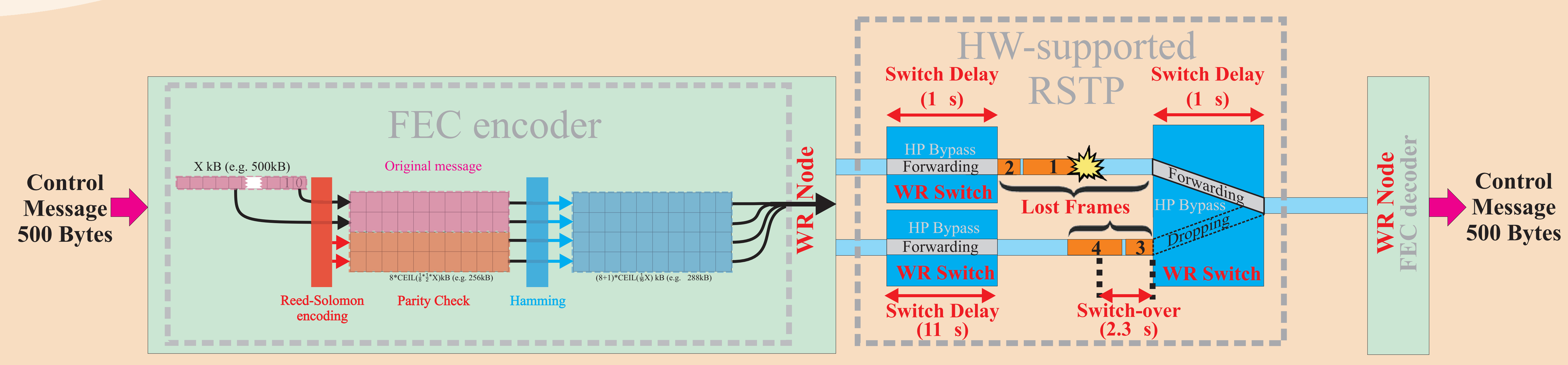


***Figure 3.** FEC & RSTP*

Conclusions

White Rabbit Network must be considered as an ordinary Ethernet network with extra optional built-in features which, when properly used, can make it robust and more reliable. The reliability study presents areas which need to be addressed to increase the reliability of a WRN. The development of WR is an on-going effort and some of the suggested solutions have been already properly investigated or developed (FEC, clock distribution) while the others need further verification (RSTP, cut-through forwarding). Suggested solutions enable to fulfill the requirements set by CERN and GSI. However the costs might trigger re-justifying of at least two of them: upper-bound latency by GSI and the number of CMs lost per year. **The network topology and its reliability calculations turned out to be the greater factor in the overall system reliability**, it is necessary to perform more precise calculations and simulations to verify the rough estimations. This mayinclude different techniques (e.g. Monte Carlo simulations) but also more real-life use cases (not available at the time of described study). Especially, we need to take into account and include into calculations the fact that not all the nodes connected to the WRN are equally critical in real-life applications.