ETHERNOVIA

TRANSFORMING HOW CARS OF THE FUTURE ARE BUILT

REVIEW OF TIME REDUNDANCY IN AUTOMOTIVE | MARCH 2022

IEEE contribution

ETHERNOVIA
TRANSFORMING HOW CARS OF THE FUTURE ARE BUILT

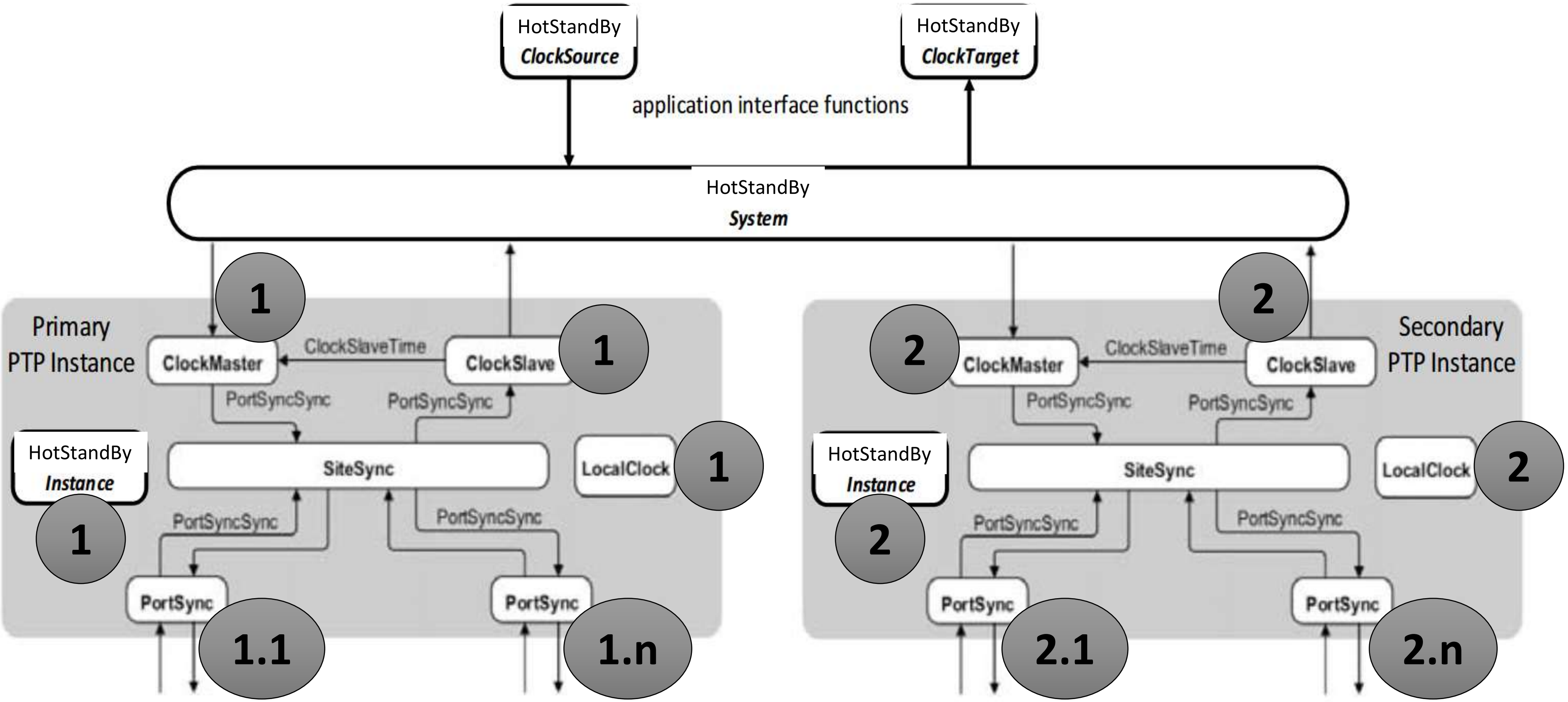
Disclaimer

- This presentation shows my personal current understanding of IEEE Std 802.1AS-2020 and IEEE P802.1ASdm-0d5.

- I am well aware of the goals of the P802.1ASdm project, but think they might fall short of a better solution with broader application, if we accept additional changes to IEEE Std 802.1AS-2020.

- This presentation is meant as a question towards the goals of IEEE P802.1ASdm with respect to extended use-case considerations.

ASdm - Model of hot standby redundancy for time synchronization



ETHERNOVIA
VIRTUALIZING VEHICLE COMMUNICATION

HotStandBySystem States

17.10.1 HotStandbySystemState: State of the HotStandbySystem for this hot standby timescale. The variable is an enumeration that takes one of the following values:

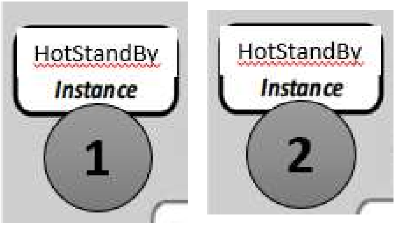
a) INIT: Initialization after the HotStandbySystem powers on and is enabled. In this state, the system is waiting for both PTP Instances to synchronize.

b) REDUNDANT: Both PTP Instances are synchronized according to the requirements of the respective application or TSN profile. Time synchronization is redundant.

c) FAULT: One PTP Instance is synchronized, and the other PTP Instance is faulted (not synchronized). Time synchronization continues to meet the requirements of the respective application or TSN profile. Time synchronization is not redundant.

d) HOLDOVER: Both PTP Instances are faulted (not synchronized). The HotStandbySystem is adjusting phase/frequency of its local time using the data stored in REDUNDANT or FAULT state, but that local time will eventually drift relative to other time-aware systems. During HOLDOVER state, time synchronization might not meet the requirements of the respective application or TSN profile.

HotStandBy Instance(s) States



17.5.1 hotStandbyInstanceState: State of the PTP Instance with respect to requirements of the respective application or TSN profile. The variable is an enumeration that takes one of the following values:

NOT Synced!

a) NOT_CAPABLE: For one or more external ports that is enabled for PTP, the neighbor is not exchanging the messages that are required for conformance to this standard.

Synced!

b) SYNCED: Time is synchronized to the requirements of this standard and the respective application or TSN profile.

NOT Synced!

c) SYNC_TIMEOUT: On the external port in SlavePort state, the port failed to receive time sync event messages according to the requirements of this standard.

d) NOT_QUALITY: Time synchronization does not conform to the quality requirements of the respective application or TSN profile.

Management Entity

IEEE Std 802.1AS-2020 IEEE P802.1ASdm-0d5

17. Hot Standby Redundancy for Time Synchronization

17.1 General

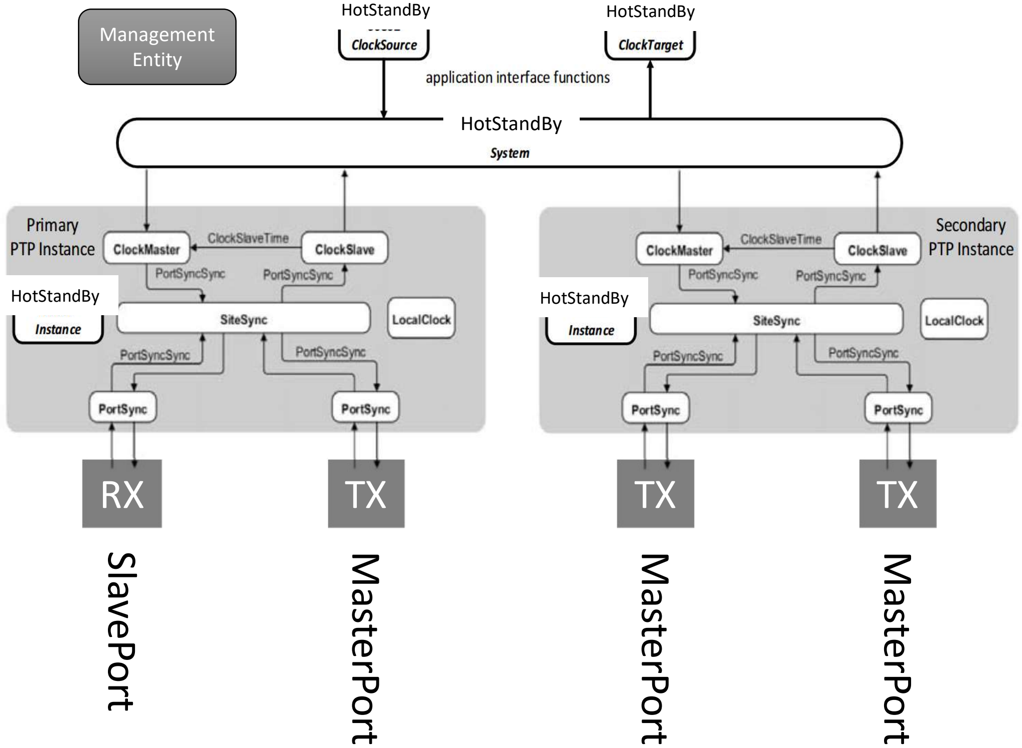
For time synchronization using this standard, hot standby redundancy refers to disabling the Best Master Clock Algorithm (BMCA), and statically configuring two distinct domains in the network. When hot standby is used for a timescale, the time-aware system operates two PTP Instances simultaneously, each in its own domain. One of the domains is considered the primary domain, and the other domain is considered the secondary domain. If the time-aware system is initially using the primary domain, and if the time-aware system and/or a link fails for that domain, the time-aware system immediately begins using the secondary domain. The change from one domain to the other occurs seamlessly, i.e., without a discontinuity in time that causes the respective application or profile requirement to be exceeded.

10.3.6.2 PTP Port state assignments when external port configuration is used

If external port configuration is used, one of the states MasterPort, SlavePort, PassivePort, or DisabledPort is assigned to each PTP Port by an external entity, as described in this subclause.

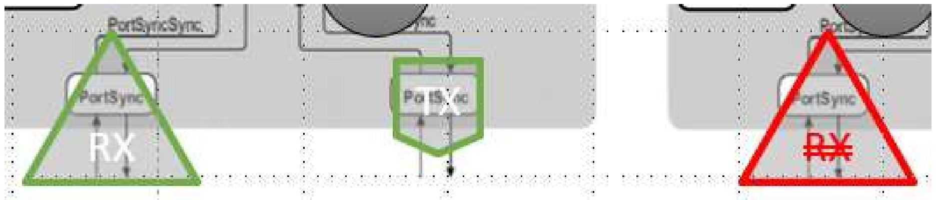
The DisabledPort state is assigned if portOper is FALSE (see 10.2.5.12), ptpPortEnabled is FALSE (see 10.2.5.13), or asCapable is FALSE (see 10.2.5.1).

The member externalPortConfigurationPortDS.desiredState (see 14.12.2) is used by an external entity to set the state of the respective PTP Port to MasterPort, SlavePort, or PassivePort. When this member is set, its value is copied to the per PTP Port local variable portStateInd (see 10.3.15.1.5). If portOper, ptpPortEnabled, and asCapable are all TRUE for this PTP Port, the PTP Port state is set equal to the value of externalPortConfigurationPortDS.desiredState by copying the value of this member to the element of the selectedState array (see 10.2.4.20) for this PTP Port.



ETHERNOVIA
VIRTUALIZING VEHICLE COMMUNICATION

Port States



SlavePort receiving timing information according to the requirements.

MasterPort transmitting timing information.

SlavePort NOT receiving timing information according to the requirements.

Port roles for both PTP Instances (Domains) are configured by the ManagementEntity.

Port roles and states of the respective PTP Instances (Domains) are known to the HotStanByInstance.

Are Port states known to the ManagementEntity?

Split Functionality

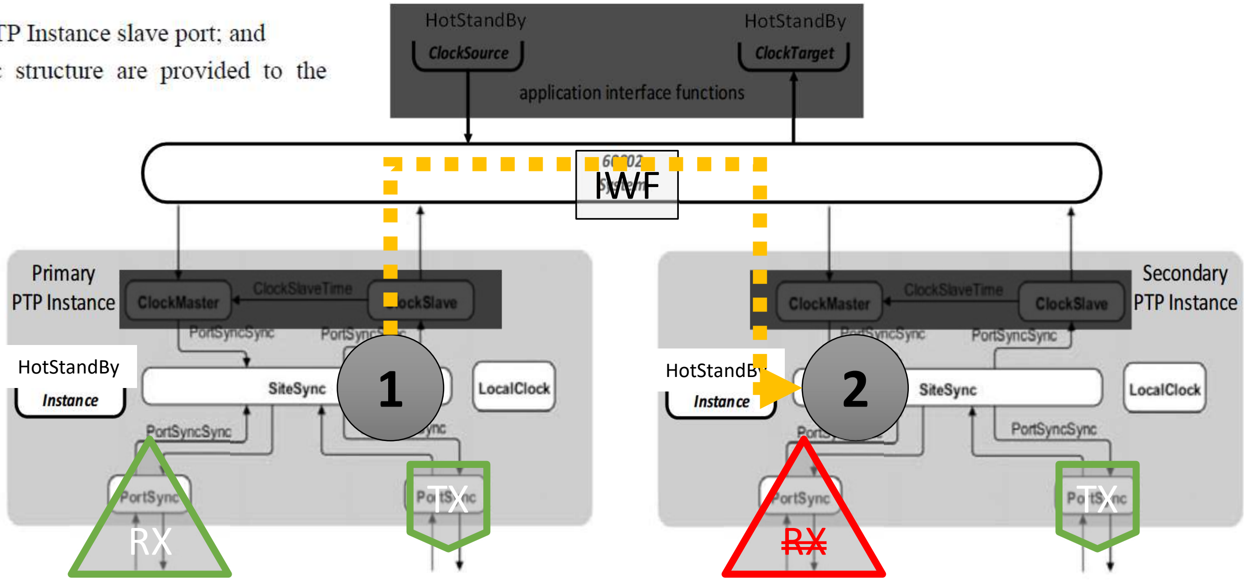
17.6.3.3.2.2 Split Functionality

The HotStandbySystem shall provide an interworking function (IWF) that transfers time synchronization information from the primary PTP Instance to the secondary PTP Instance when the secondary PTP Instance is in the NOT_SYNCED state. The IWF provides the most recently received PortSyncSync structure of the primary PTP Instance SiteSync entity to the secondary PTP Instance SiteSync entity, as follows:

a) The domainNumber is changed from the primary PTP Instance domainNumber to the secondary PTP Instance domainNumber;

b) localPortNumber is changed to the portNumber of the secondary PTP Instance slave port; and

c) All other members of the primary PTP Instance PortSyncSync structure are provided to the secondary PTP Instance SiteSync entity unchanged.



IEEE P802.1ASdm-0d5

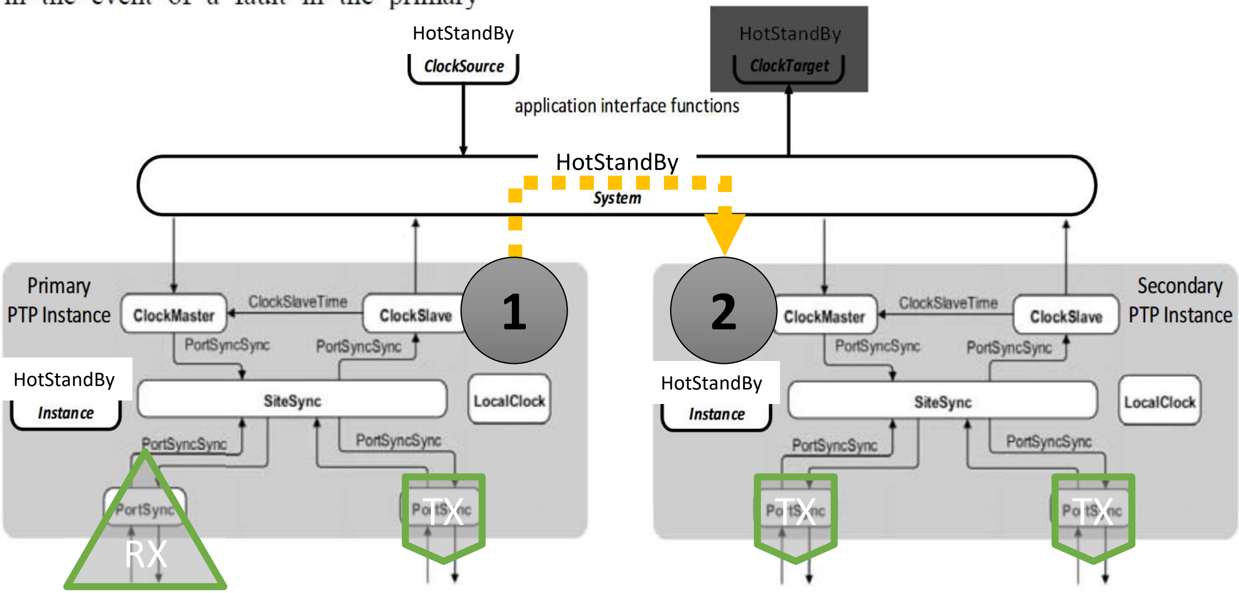
ETHERNOVIA
VIRTUALIZING VEHICLE COMMUNICATION

Secondary Grand Master

17.6.3.2 Secondary grandmaster

17.6.3.2.1 Secondary grandmaster in REDUNDANT state

When the secondary PTP Instance is grandmaster (i.e., no external port in SlavePort state), and the HotStandbySystemState is REDUNDANT, the HotStandbySystem shall transfer phase, frequency, clockSourceTimeBaseIndicator (see 10.2.4.8), clockSourceLastGmPhaseChange (see 10.2.4.10), and clockSourceLastGmFrequencyChange (see 10.2.4.11) from the ClockSlave of the primary PTP Instance to the ClockMaster of the secondary PTP Instance (see Figure 17-1). By using phase from the primary PTP Instance, the secondary grandmaster can maintain continuity in the event of a fault in the primary grandmaster.



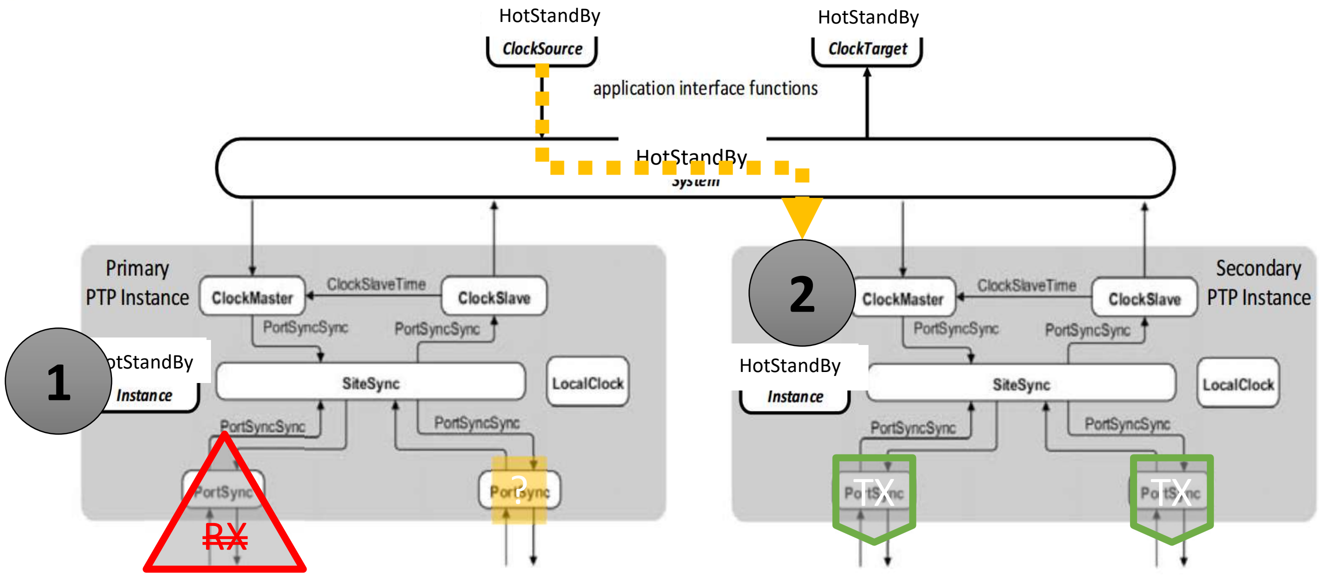
Secondary Grand Master

17.6.3.2.2 Secondary grandmaster in NOT_REDUNDANT state

When the secondary PTP Instance is grandmaster (i.e., no external port in SlavePort state), and the HotStandbySystemState is NOT_REDUNDANT, the HotStandbySystem shall transfer phase, frequency, clockSourceTimeBaseIndicator (see 10.2.4.8), clockSourceLastGmPhaseChange (see 10.2.4.10), and clockSourceLastGmFrequencyChange (see 10.2.4.11) from the ClockSource to the ClockMaster of the secondary PTP Instance (see Figure 17-1). If no external source of time is implemented, the ClockSource is equivalent to the LocalClock.

IEEE P802.1ASdm-0d5

Loss of sync-input in Domain 1 causes discontinuity in Domain 2 and terminates sync-output on Domain 1, if LogSyncInterval is fixed in the network.



ETHERNOVIA
VIRTUALIZING VEHICLE COMMUNICATION

Holdover prevented by syncLocked

IEEE Std 802.1AS-2020

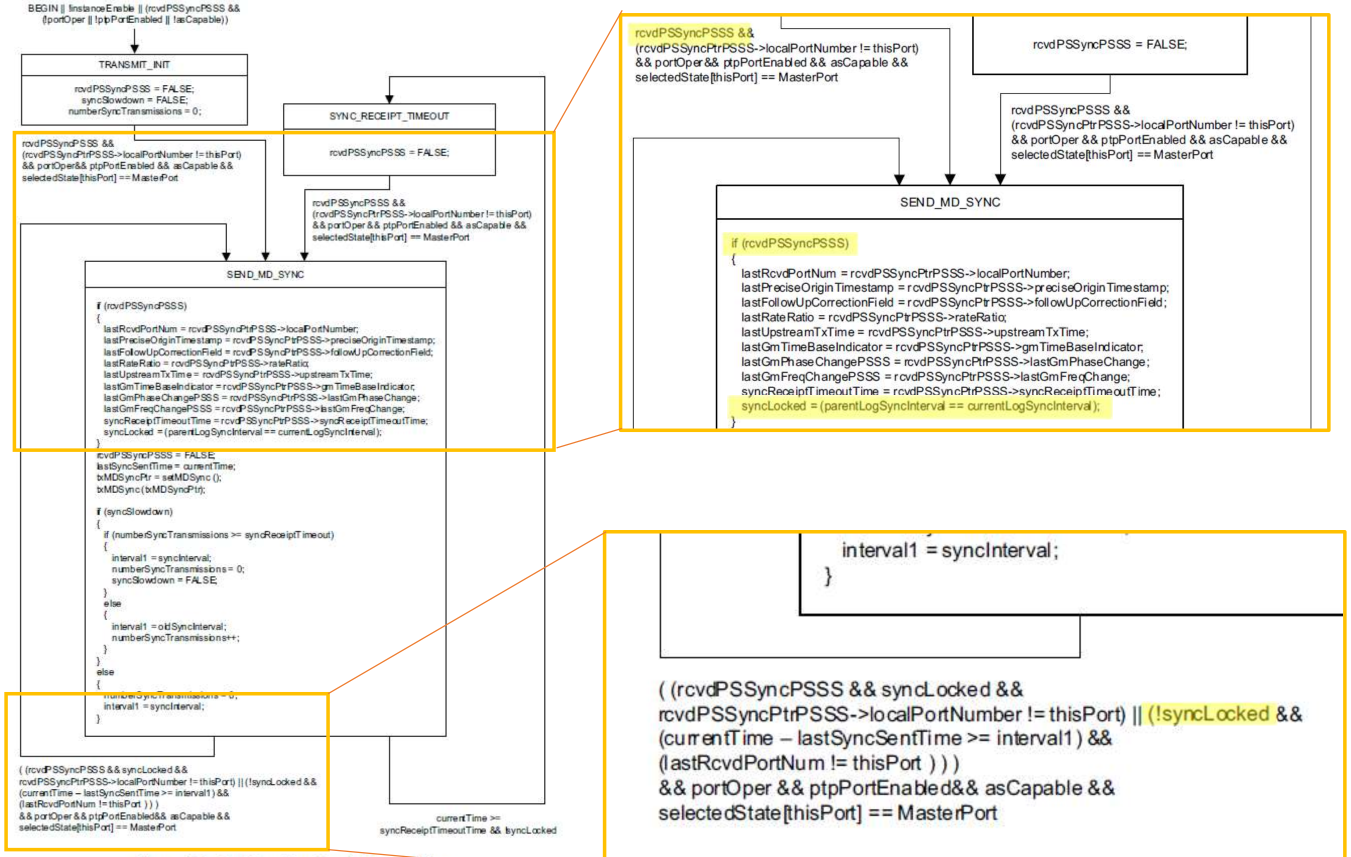


Figure 10-8—PortSyncSyncSend state machine

If all stations use the same LogSyncInterval, then syncLocked will always TRUE.

If syncLocked == TRUE, there will be no continued transmission of Sync-Messages.

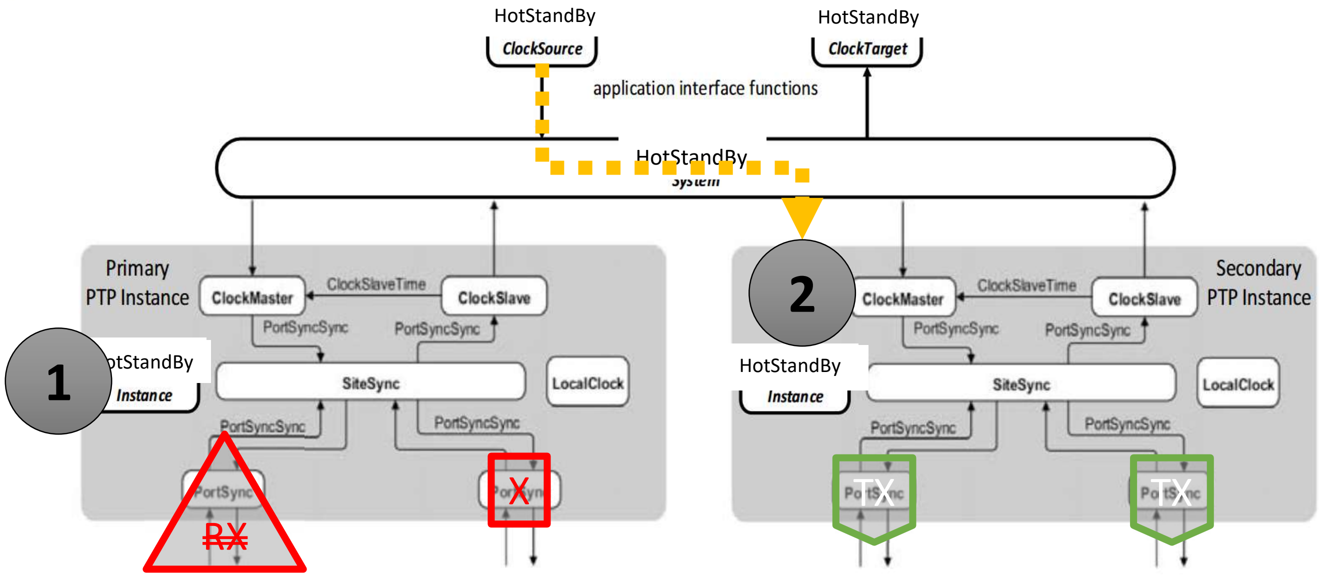
ETHERNOVIA
VIRTUALIZING VEHICLE COMMUNICATION

Secondary Grand Master - not redundant

17.6.3.2.2 Secondary grandmaster in NOT_REDUNDANT state

When the secondary PTP Instance is grandmaster (i.e., no external port in SlavePort state), and the HotStandbySystemState is NOT_REDUNDANT, the HotStandbySystem shall transfer phase, frequency, clockSourceTimeBaseIndicator (see 10.2.4.8), clockSourceLastGmPhaseChange (see 10.2.4.10), and clockSourceLastGmFrequencyChange (see 10.2.4.11) from the ClockSource to the ClockMaster of the secondary PTP Instance (see Figure 17-1). If no external source of time is implemented, the ClockSource is equivalent to the LocalClock.

Loss of sync-input in Domain 1 causes discontinuity in Domain 2 due to input change and terminates sync-output on Domain 1, if LogSyncInterval is fixed in the network.



Duplicate Functionality?

- Both Secondary Grand Master and Split Functionality transfer time information from one domain to the other in certain error conditions
- Secondary Grand Master
  - Requires at least a ClockSource, one ClockMaster, and one Clock Slave
  - Domain 1 NOT-synced leads to loss of time information transmission for all Domain 1 MasterPorts (if LogSyncInterval is fixed) and discontinuity of time information transmission for Domain 2, due switch from primary clockSlave to clockSource
- Split Functionality
  - Can work without ClockSource, ClockTarget, ClockMaster, and Clock Slave - a constellation you will likely see in a time-aware bridge
  - Domain 1 NOT-synced leads to loss of time information transmission for all Domain 1 MasterPorts (if LogSyncInterval is fixed)
  - Domain 2 NOT-synced leads to discontinuity of time information transmission for Domain 2, due switch from secondary slave port to primary slavePort

Should we adapt our goals?

If we opened up IEEE P802.1ASdm to further changes in IEEE Std 802.1AS-2020, could we find a solution that

- does not require two solutions to transfer time between the two domains?
- minimizes the potential discontinuities (time input changes) in at least some error cases?
- minimizes the loss of time information transmission on master ports for one domain in at least some error cases?
- allows a single TimeSource to feed two Domains in one device?

Towards a new approach

Draft proposal for discussion!

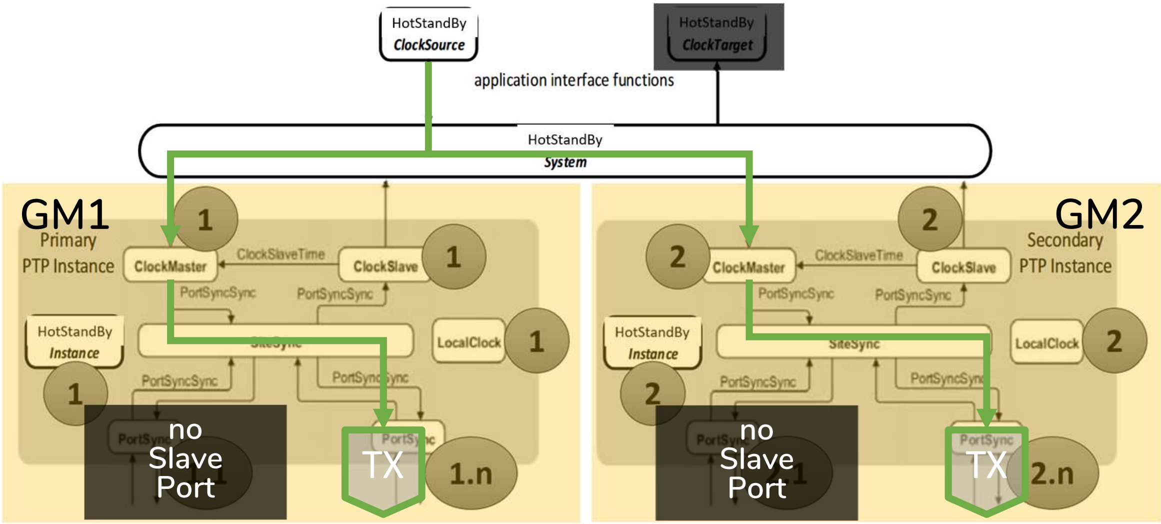
In an engineered network with a network wide statically configured LogSyncInterval and managed port states (no BMCA)

- do we need to worry about time distribution rings?
- can we (then) allow Domain 2 to Domain 1 time information transfers in some error cases?
- should we enable holdover, which would also have benefits without HotStandby (Avnu concept)?
- should we enable the comparison of the two Domains at application layer?

And could we do this within the schedule of IEEE P802.1ASdm?
Or do we want/need a new project?

Redundant Grand Master

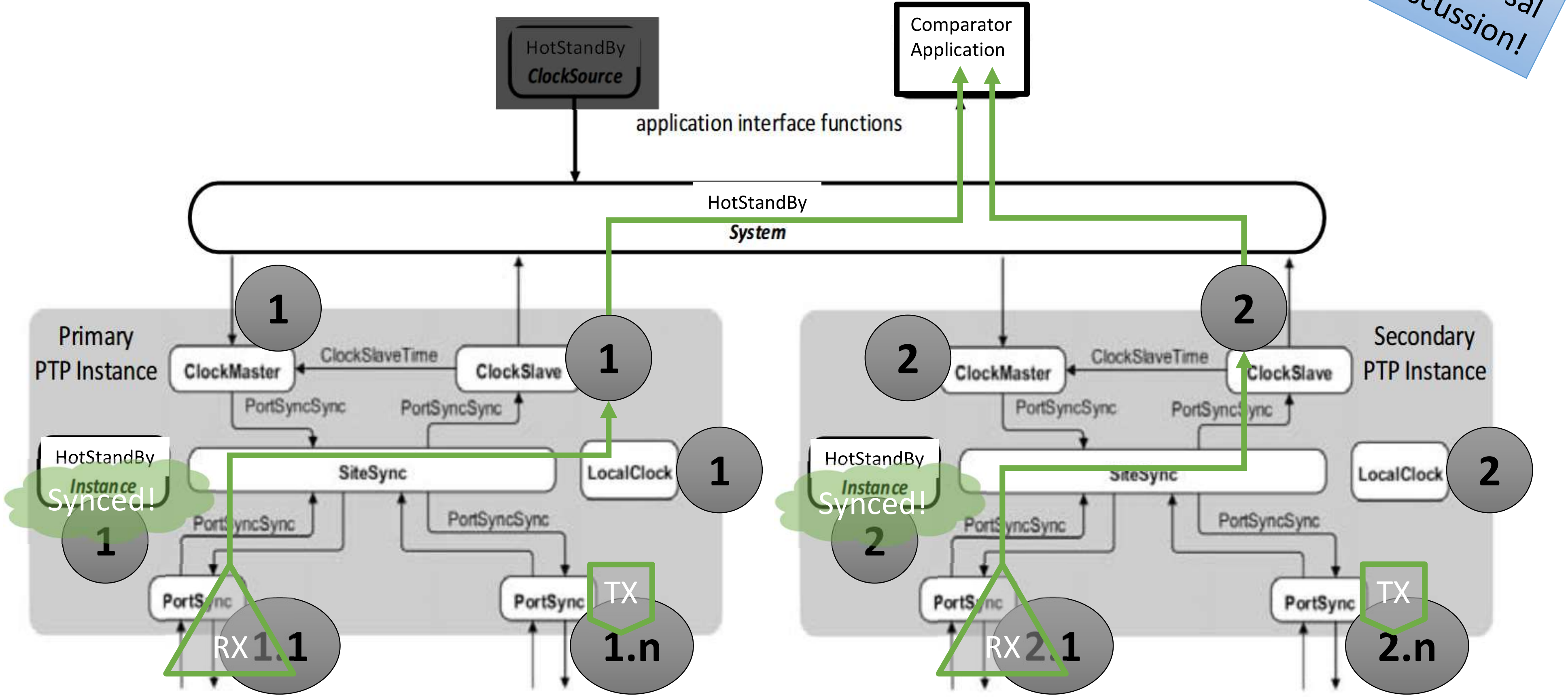
Draft proposal for discussion!



ETHERNOVIA
VIRTUALIZING VEHICLE COMMUNICATION

Comparator Application

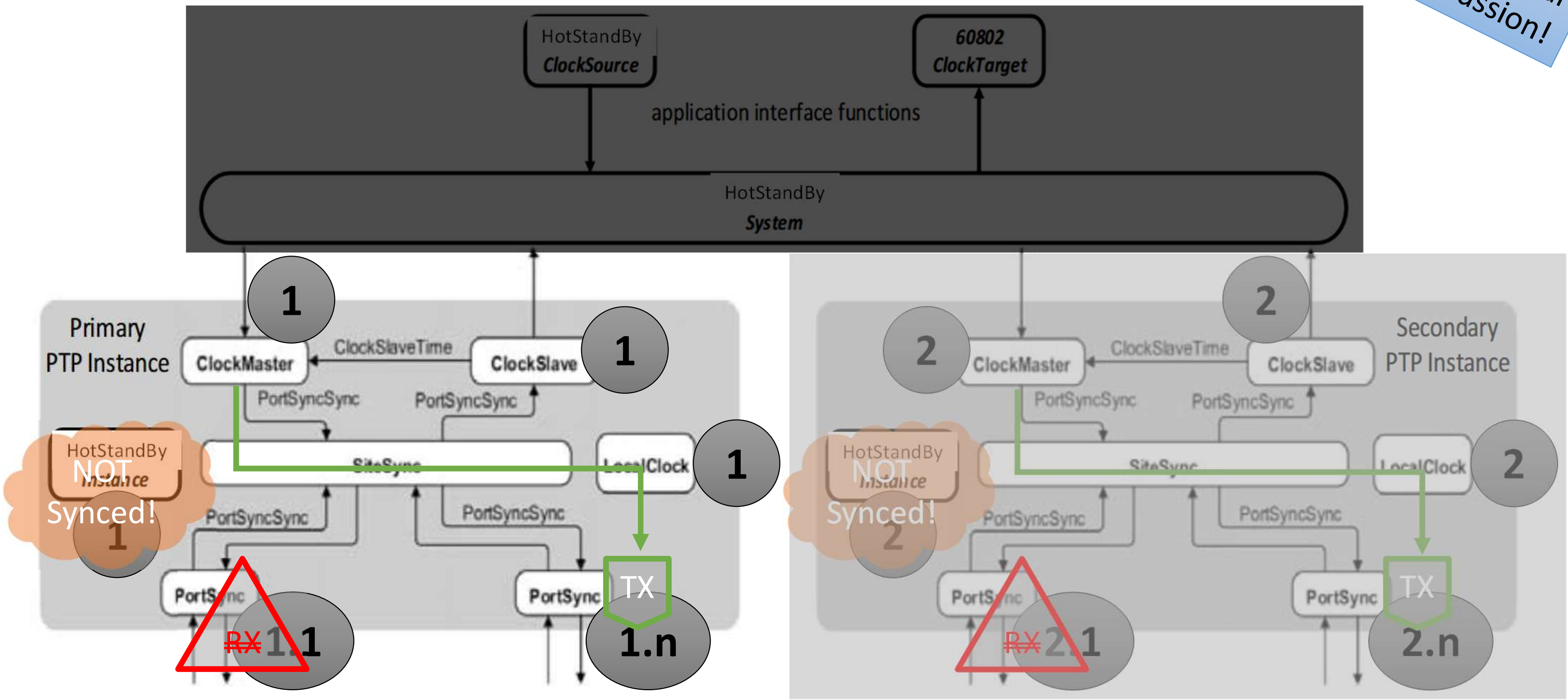
Draft proposal for discussion!



ETHERNOVIA
VIRTUALIZING VEHICLE COMMUNICATION

Holdover

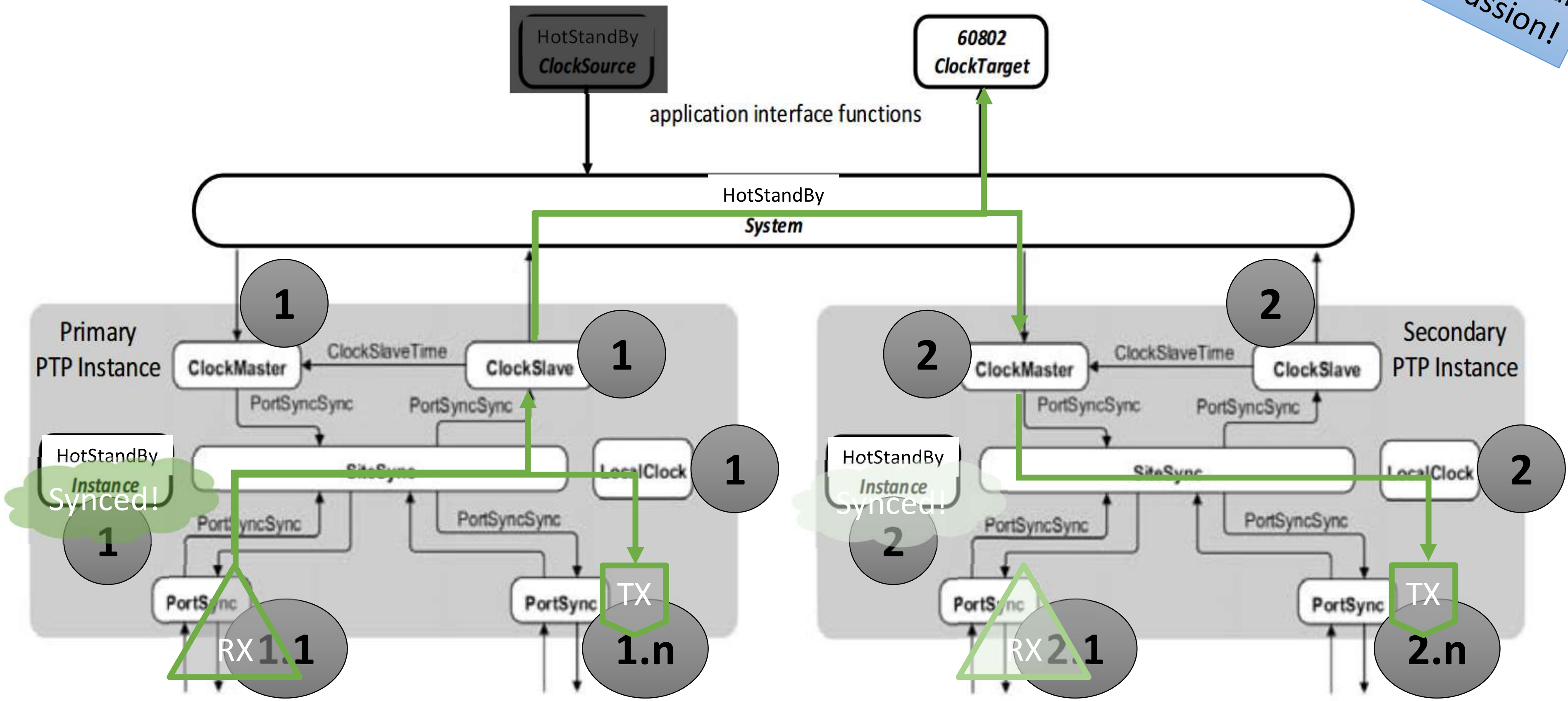
Draft proposal for discussion!



ETHERNOVIA
VIRTUALIZING VEHICLE COMMUNICATION

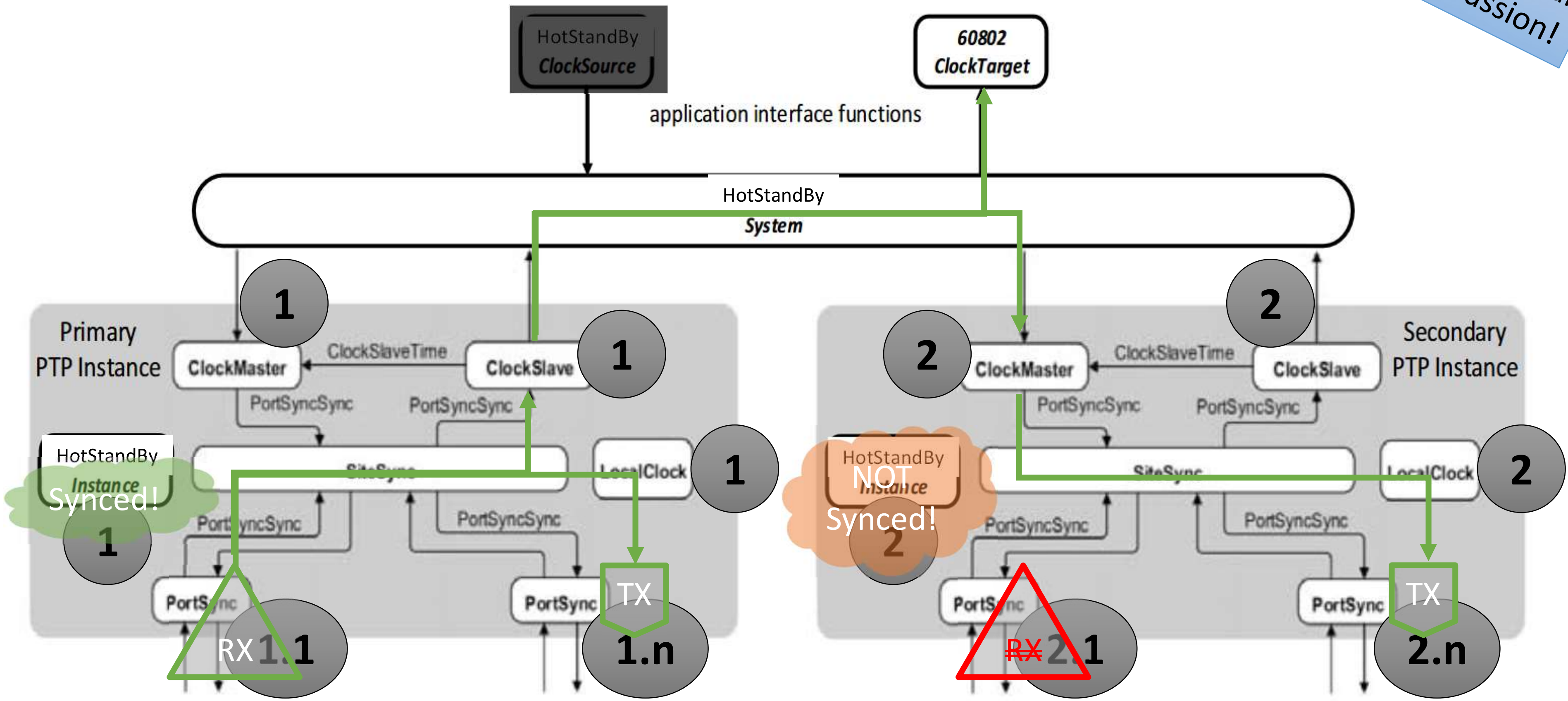
Redundant Backup

Draft proposal for discussion!



NOT-Redundant Domain 2 Failed

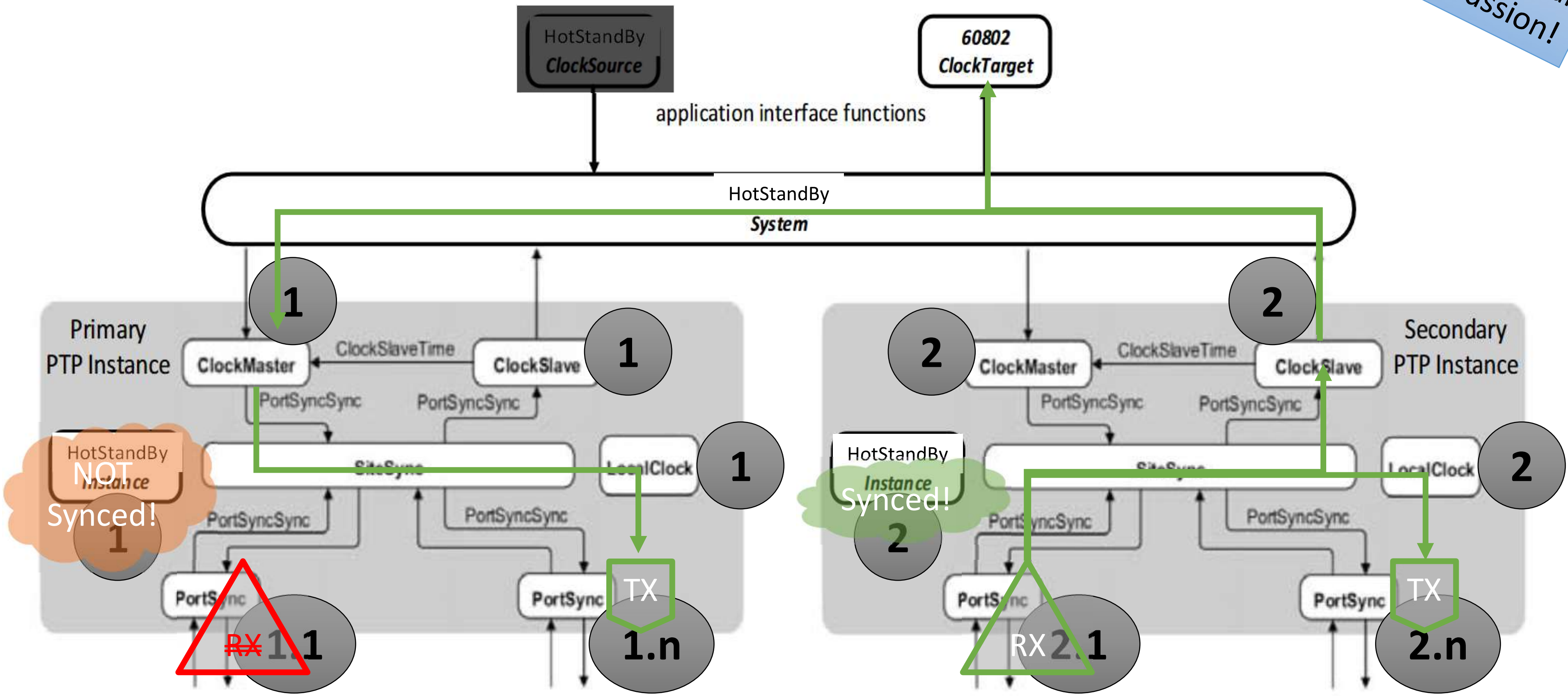
Draft proposal for discussion!



ETHERNOVIA
VIRTUALIZING VEHICLE COMMUNICATION

NOT-Redundant Domain 1 Failed

Draft proposal for discussion!



ETHERNOVIA
VIRTUALIZING VEHICLE COMMUNICATION


THANK YOU
ETHERNOVIA
VIRTUALIZING VEHICLE COMMUNICATION