Julius-Maximillians-
UNIVERSITÄT
WÜRZBURG

Bayerisches Staatsministerium für
Wirtschaft, Landesentwicklung und Energie

Hymove

versatile core avionics ranging from Satellites to launcher vehicles

AEROSPACE
INFORMATION
TECHNOLOGY

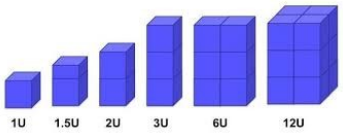
Please Ask!


Julius-Maximillians-
UNIVERSITÄT
WÜRZBURG


AEROSPACE
INFORMATION
TECHNOLOGY

Reinvent and reinvent the wheel to much wasted work

ONE avionic system for all cases?
Or reinvent the wheel every time?



First:
One for all will not work

Building Blocks + Tailoring

Building Blocks & Tailoring? Hardware is not the problem

Most experts are focusing
Just on the Hardware

The Hardware provides the Resources

Tangram
Building Blocks

The Key is the Software

How to use the building blocks in different configurations
Without having to reprogram every thing

If you just take and plug...

Emphasis
It has to be “dependable”

Intuitive:

- It work properly and will work properly and will continue working properly
- I can trust it
- No reason for worry
- System does the right thing at right time

It is not really “dependable”

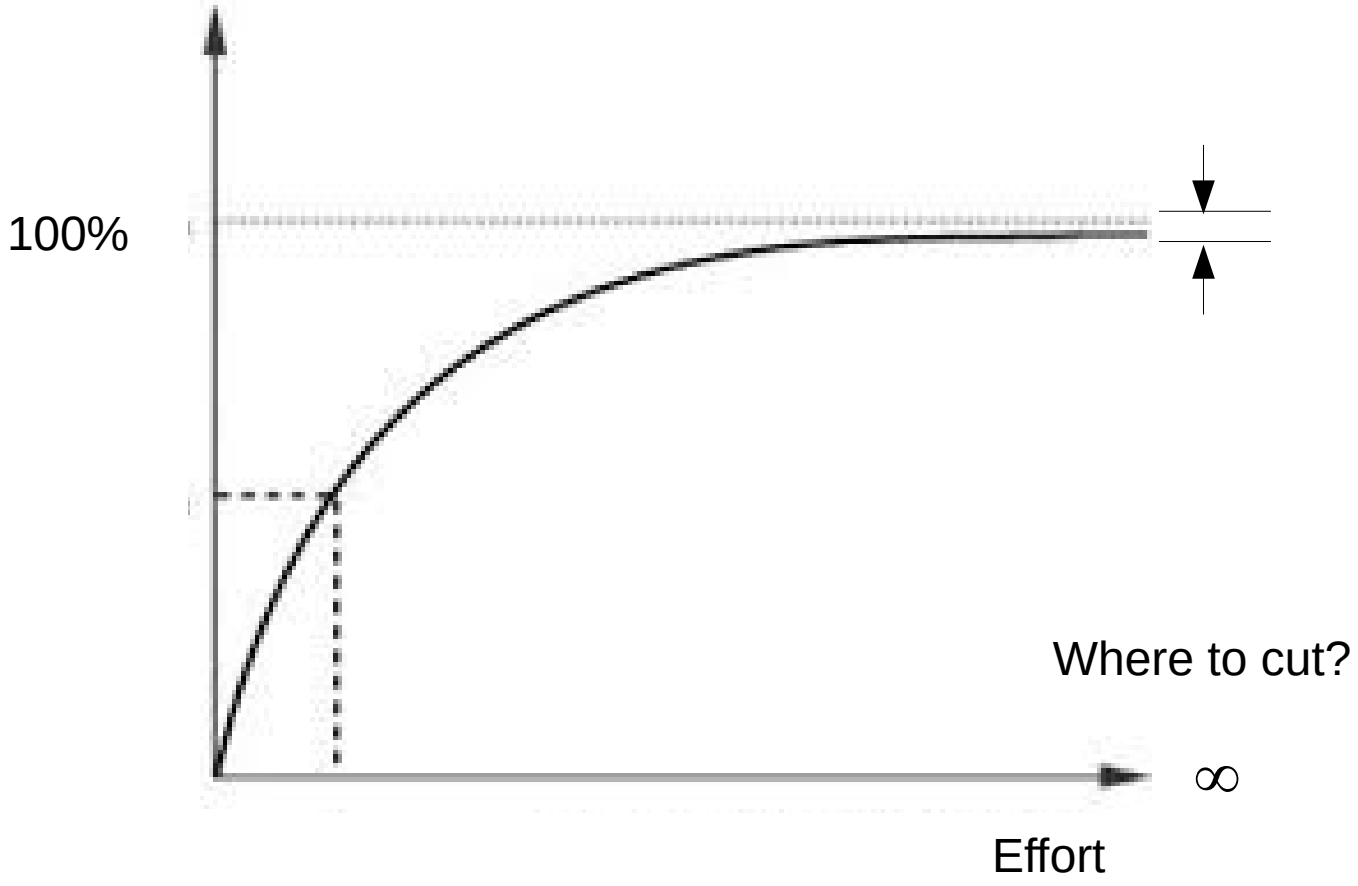
When you need it

It is doing some thing else
Is not there
Is not ready
Does something wrong/different

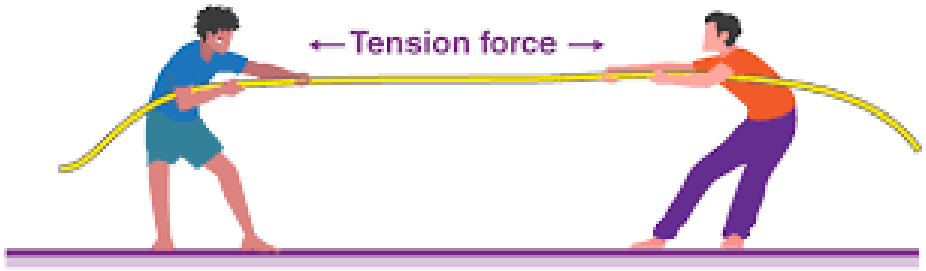
100% Dependable

Not possible!

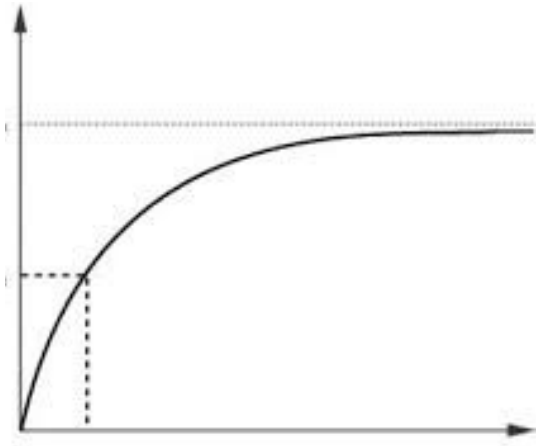
Only 99.9999999 % Dependable for one hour
Or a probability of a failure in the next hour from 10^{-9}
Or 10^{-5} in the next year



Competing targets



To raise each of them is already difficult,
and then still they are in competition.
If one takes the other loses



Dependability
Verlässlichkeit

可靠性 → 值得 信赖
trustable

安全
Security

安全	可用 性	可靠性	诚信	保密
Safety	**Availability** **Verfügbarkeit**	**Reliability** **Zuverlässigkeit**	**Integrity**	**Confidentiality**

Security <-> safety

安全

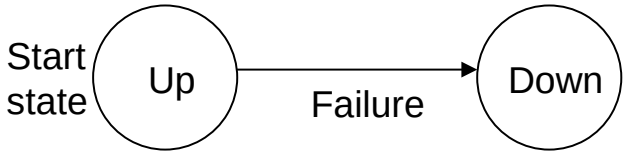
安全

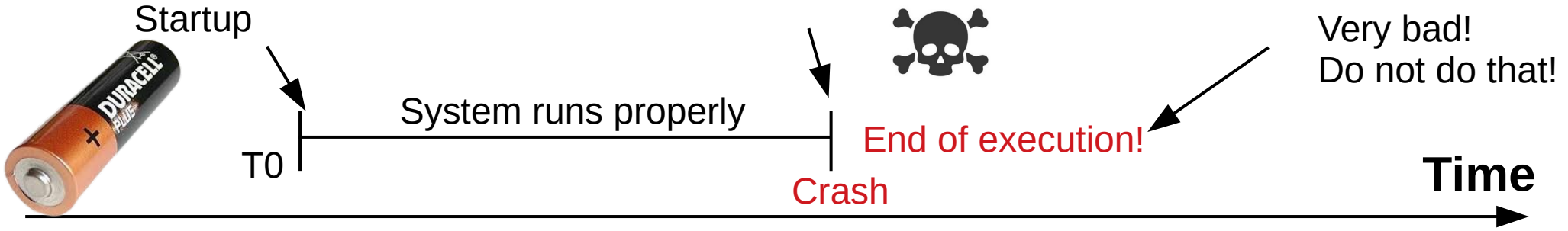
Availability <-> safety

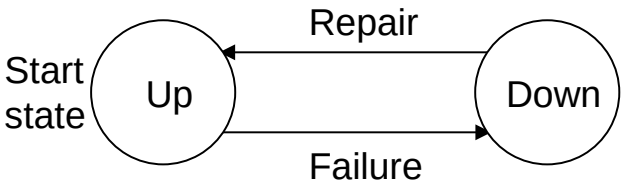
Available? You need it now, Would you use it now or bring it to the repair shop?

Competing:
Availability or Safety?

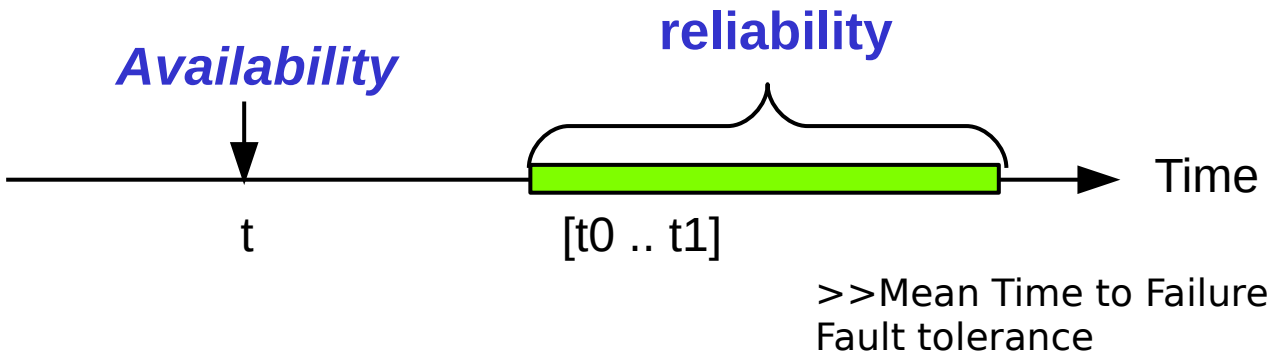
Execution course

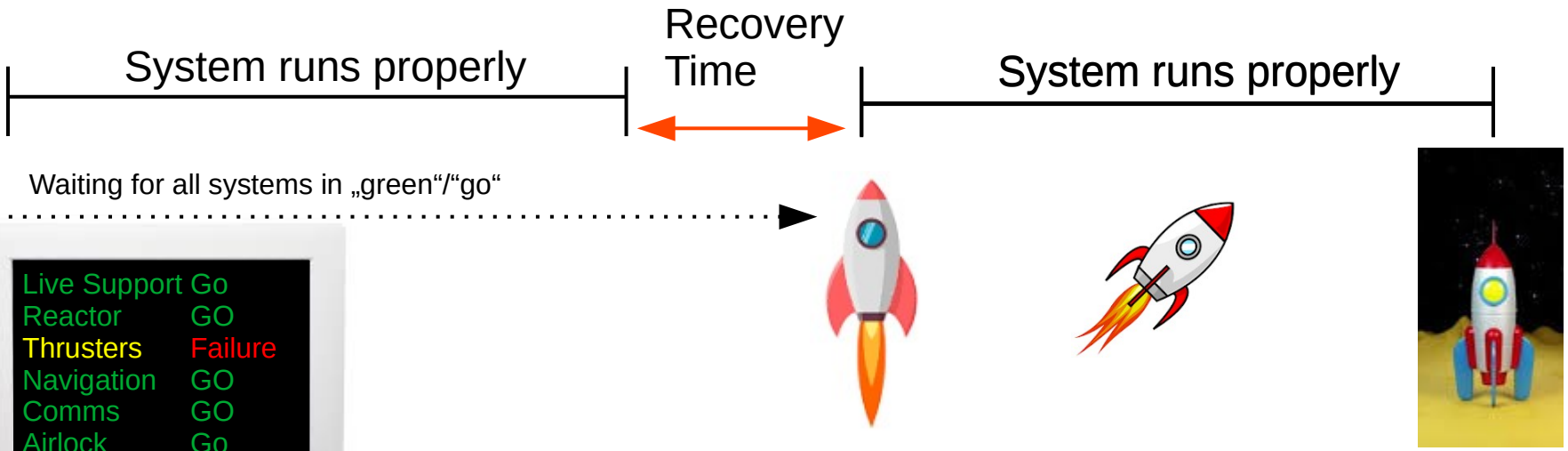






Availability and Reliability





New ways for Dependability

What is more important
(„Not more important“ is not „not important“)

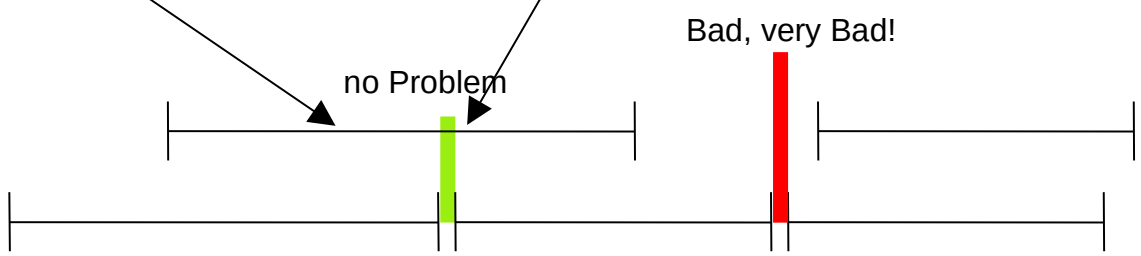
1. Aovid crashes?	No! Let it crash! : Ultrafast Restart
2.Computer?	Not computer, but the network is the most important
3. Mang complex Systems?	No!: „Irreducible complexity“
4. Robust?	No!: adaptability and self x (Diagnose … recovery)

Fault Prevention

Fault Tolerance

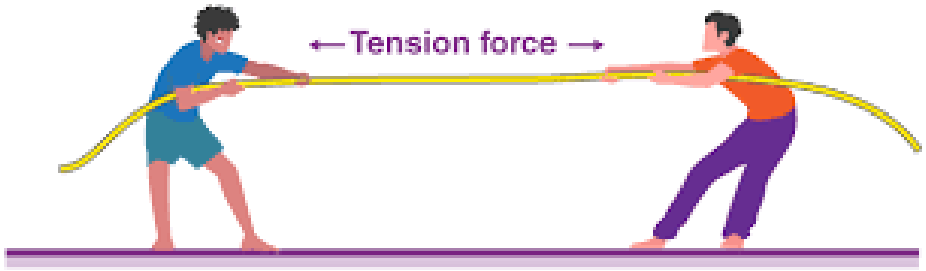
Redundancy

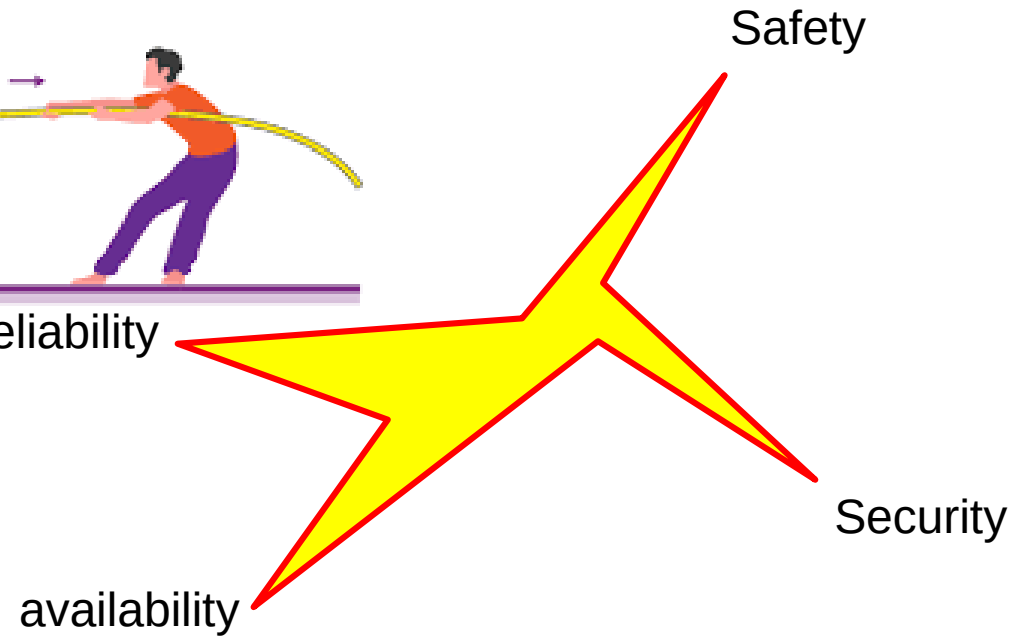
-> >Mean Time to Failure



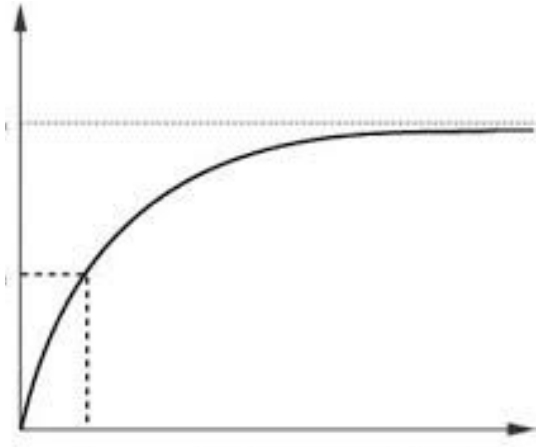
Ultra fast Recovery

Competing targets





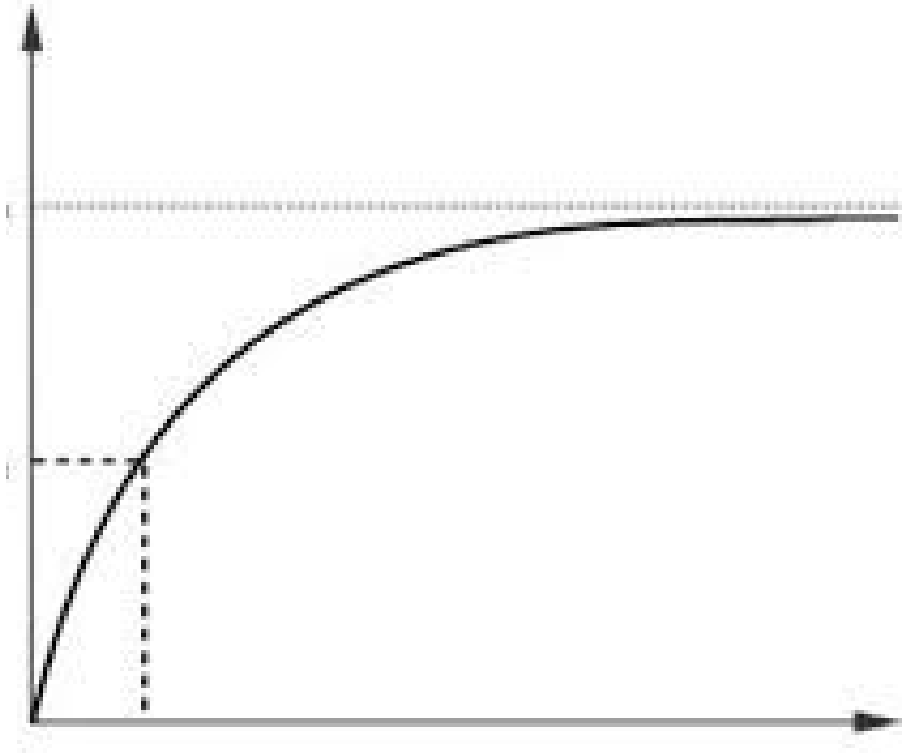
To raise each of them is already difficult,
and then still they are in competition.
If one takes the other loses



Limited, Finite Resources

Select only what you need!

You can not and you do not need
to take all!



Hymove solution (high dependability)

可用 性

Hardware and Software configurable Build blocks for

high **reliability** 可用 性

Or

high **availability** 可用 性

Or

both …If you can afford it

Verlässlichkeit:
Zuverlässigkeit + Verfügbarkeit

Hymove solution

Hardware and Software configurable Build blocks for

high **reliability**

Or

high **availability**

Or

both

Orbit
Transfer
Vehicle

You have the choice

Long-life systems: Fail-slow, Robust, High-Availability
Methods: cold-Replication (spares), error coding, monitoring, shielding

Safety-critical systems: Fail-safe, Sound, High Reliability, High-integrity
Methods: hot-Replication with voting / time redundancy

Switch from Reliability to Availability

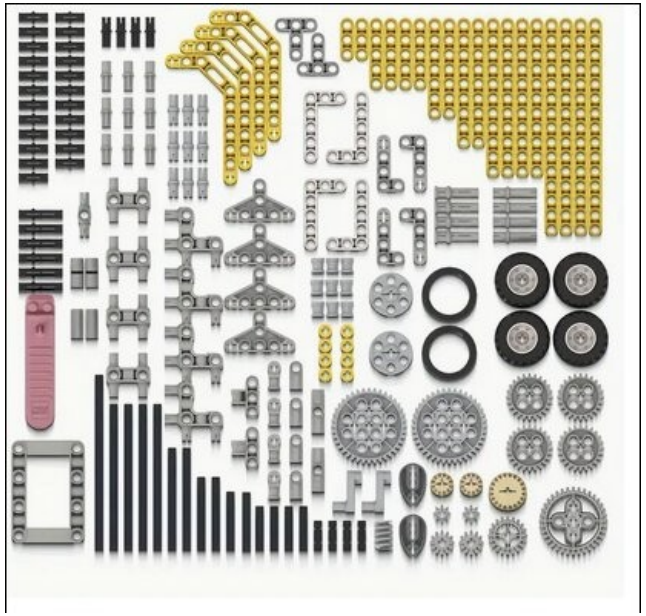
Hyimpulse Orbital Transfer Vehicle

From Launch vehicle
to long living satellite

The ability to switch from one type to other type with the same resources

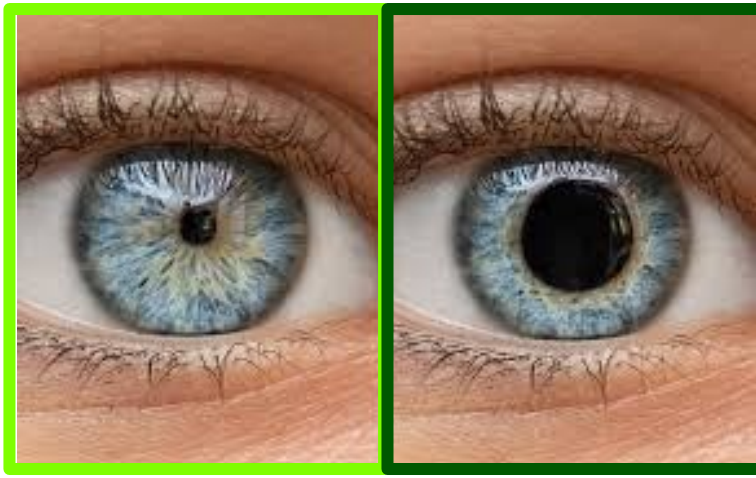
Hymove solution

Targets:



1. Static configuration (tailoring)
   for different missions
   Not a HW but a SW Challenge

2. Dynamic reconfiguration (adaptability)
   for Reliability (error masking)
   for Availability (detect and Recover)
   for different Phases of a mission.
   Not a HW but a SW Challenge



Hymove (SW) solution

Means:

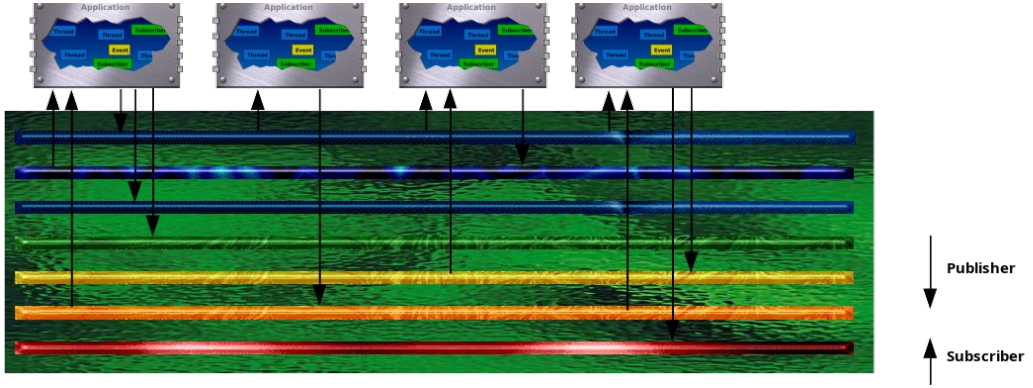
1. Continuously
   self- soundness- and plausibility- test

2. Concurrent and simultaneous
   monitoring for fault detection,
   Reconfiguration and take over

Hymove (SW) solution

Means:

3. Connection-less and location independent communication protocol
   for instant reconfiguration



4. Irreducible complexity:
   for dependability and fast Recovery

5. Ultra fast recovery: for reliability

Cold/Warm/Hot Redundancy

Cold:
The reserve hardware
Is powered off.

Long time/Long life missions
Low Power
Higher Radiation tolerance

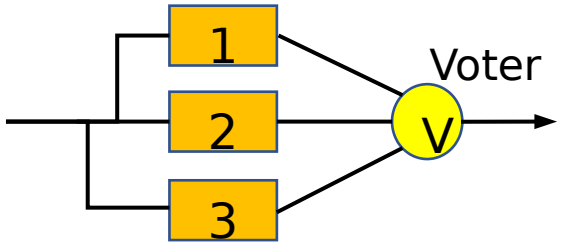
Warm
Reserve is ready to work
But its state is not up to date

Reliability for stateless systems
Fail Safe

Hot
Replicated Hardware running concurrently
All have the same Status info
same inputs

High Reliability
Error Masking
Any one can take control
At any time

Spatial/Temporal (Hot) Redundancy

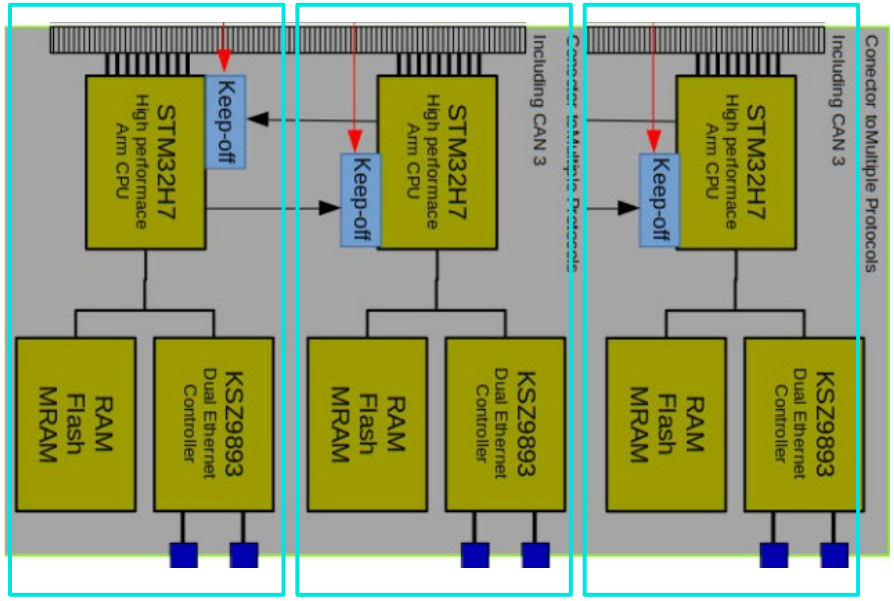


Spatial: 1,2,3: Hardware nodes
Temporal: 1,2,3: Software Processes

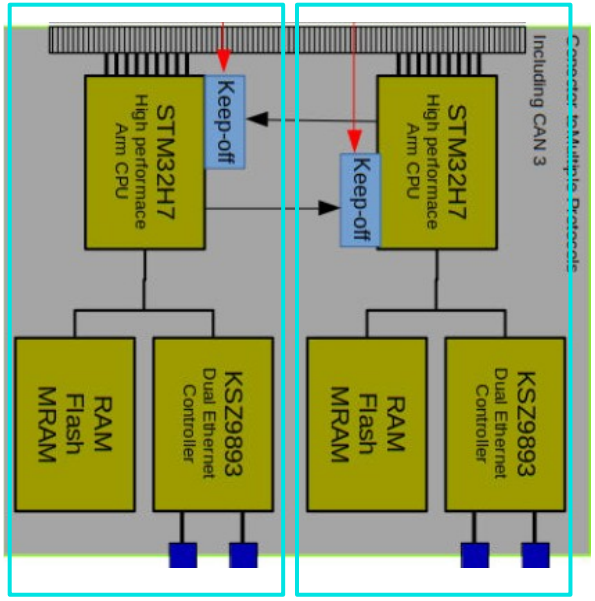
Spatial
Several (Hardware) processors
get the same input and execute
Concurrently.
Results are compared
by hardware
(Voter)

Temporal
Computations are executed
Several times in the same hardware
The comparison id done by software
Software voter

Spatial/Temporal (Hot) Redundancy



Spatial
Several (Hardware) processors
get the same input and execute
Concurrently.
Results are compared
by hardware
(Voter)

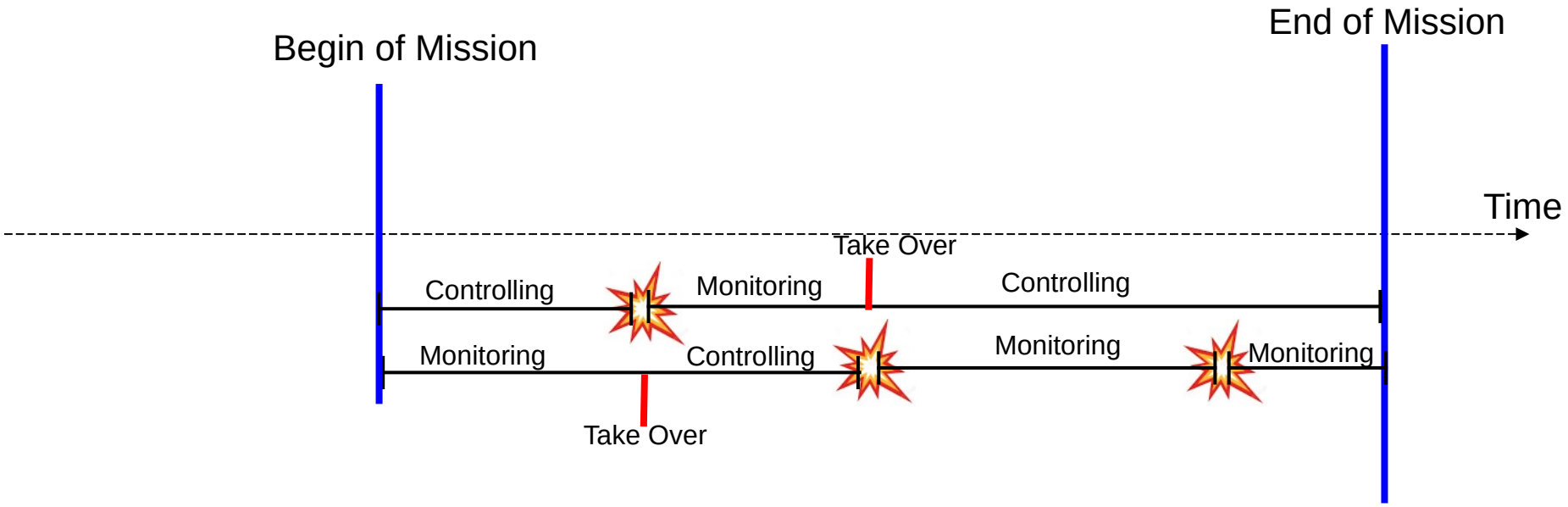


Temporal
Computations are executed
Several times in the same hardware
The comparison id done by software
Software voter

Only in case of total failure, then
We need reserve hardware
Only one pair

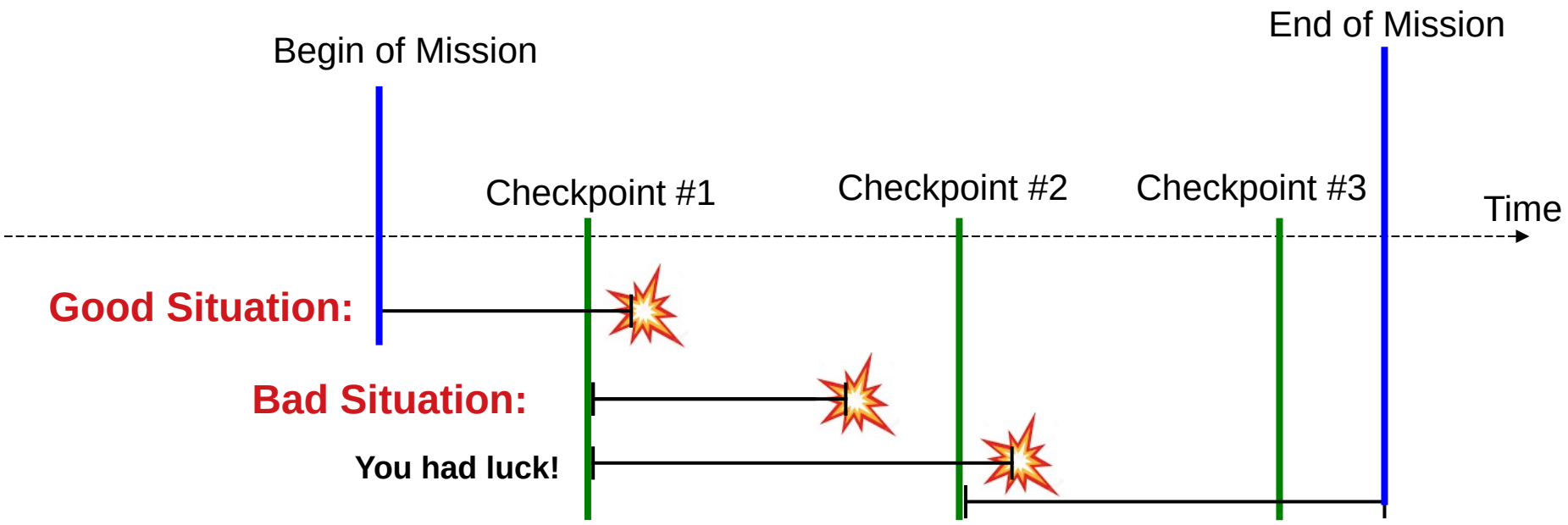
Hot Redundancy

Temporal Redundancy to detect failure
Spatial Redundancy to take over



Cold & Warm Redundancy → Write Checkpoints

But when and how often? f(mean time to failure)

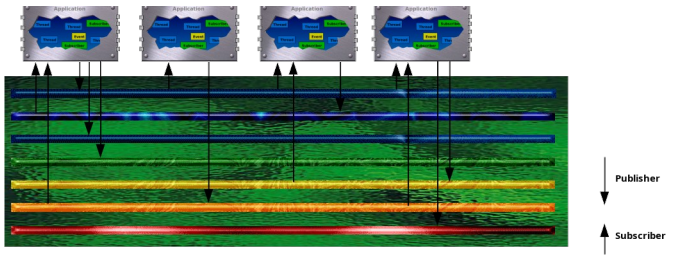


The Key is in Software
Hardware provide the resources

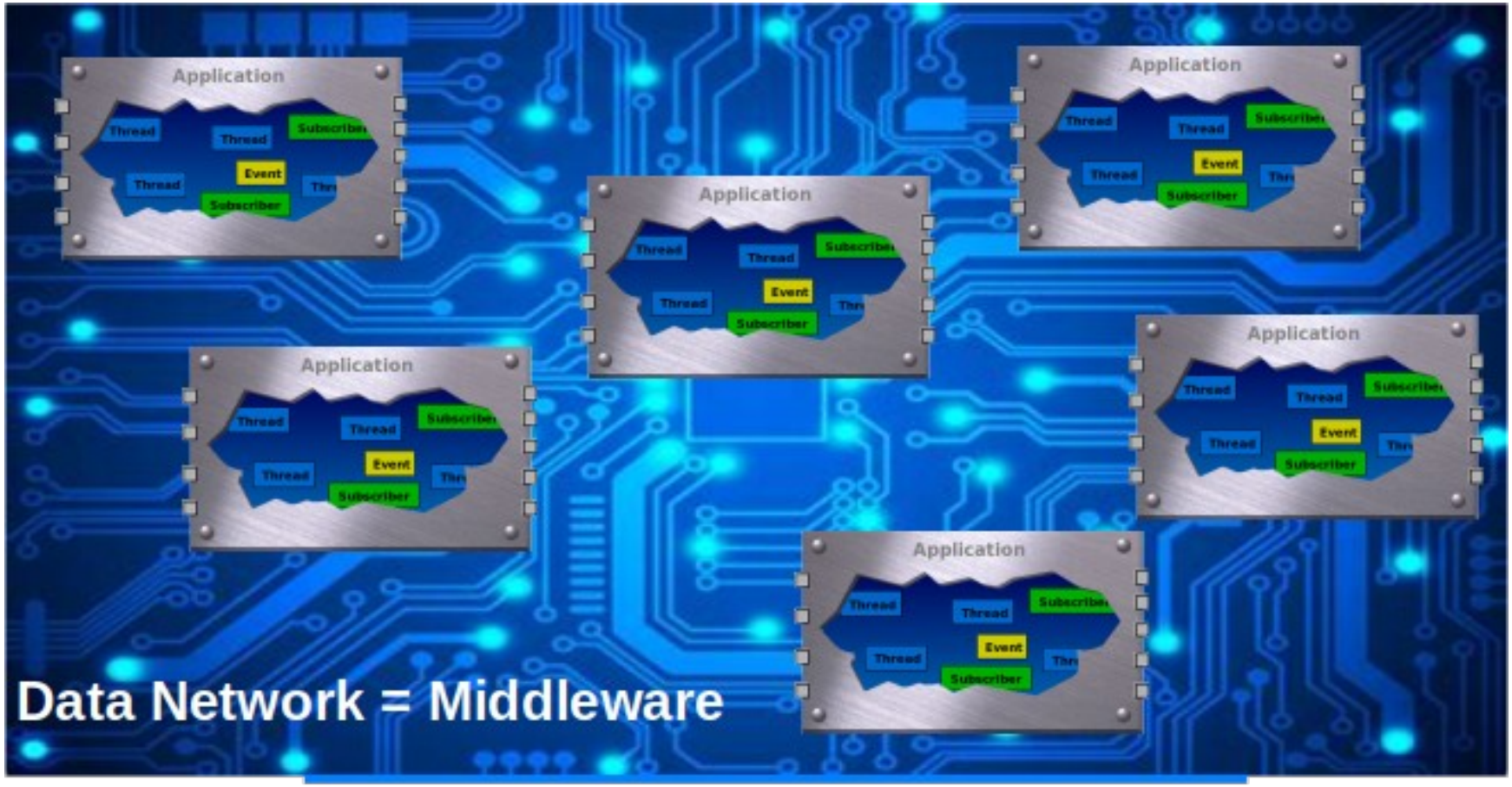
The cold, warm or hot redundancy arrangement
Is a software issue and can vary at different mission phases

Spatial (hardware redundancy) and
temporal (replicated execution) redundancy.
Is a matter of Software, combined with cold/warm/hot redundancy
We support both, dynamically

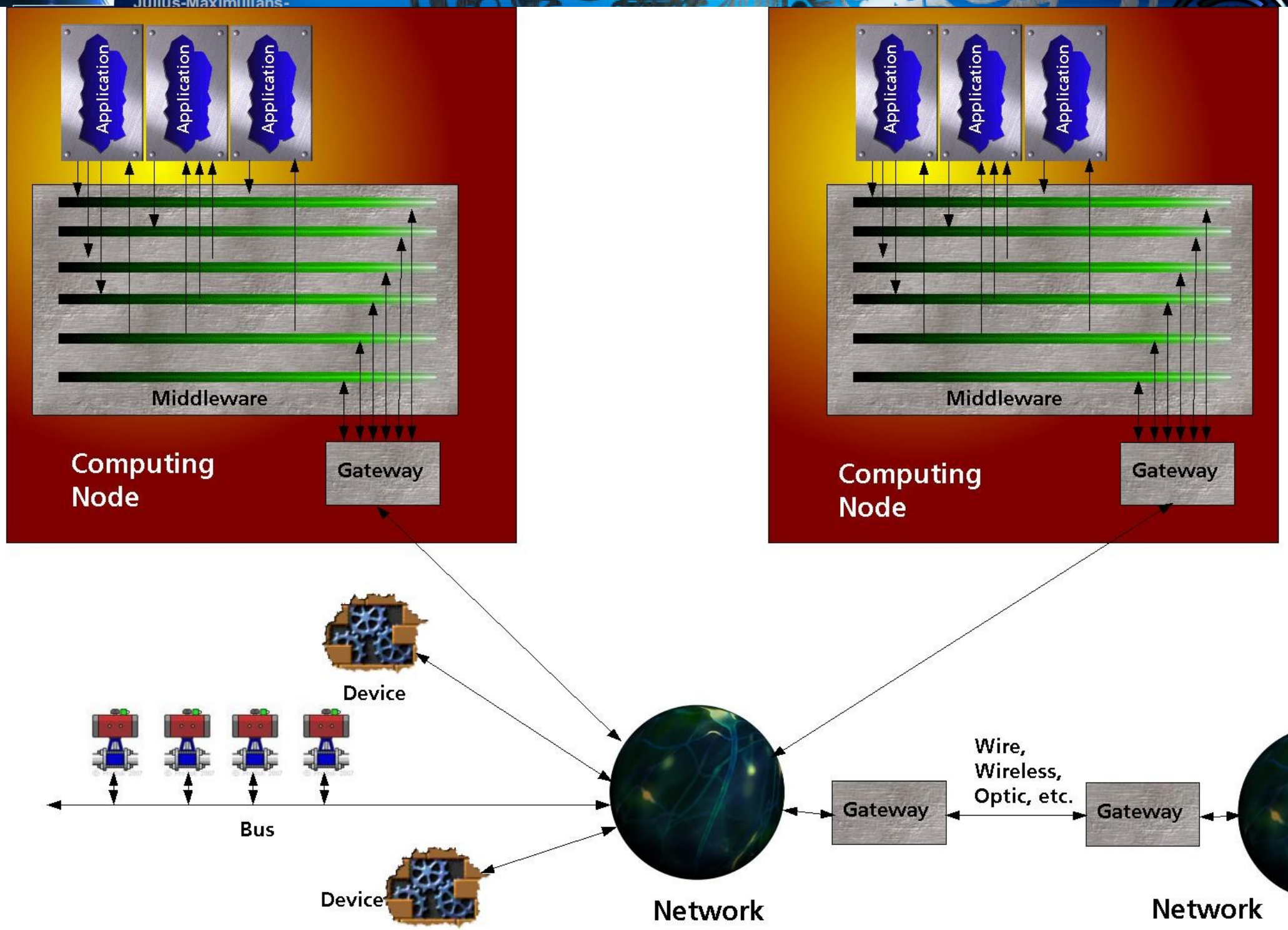
Position transparency for the communication is the factor:
Publish subscriber Middleware

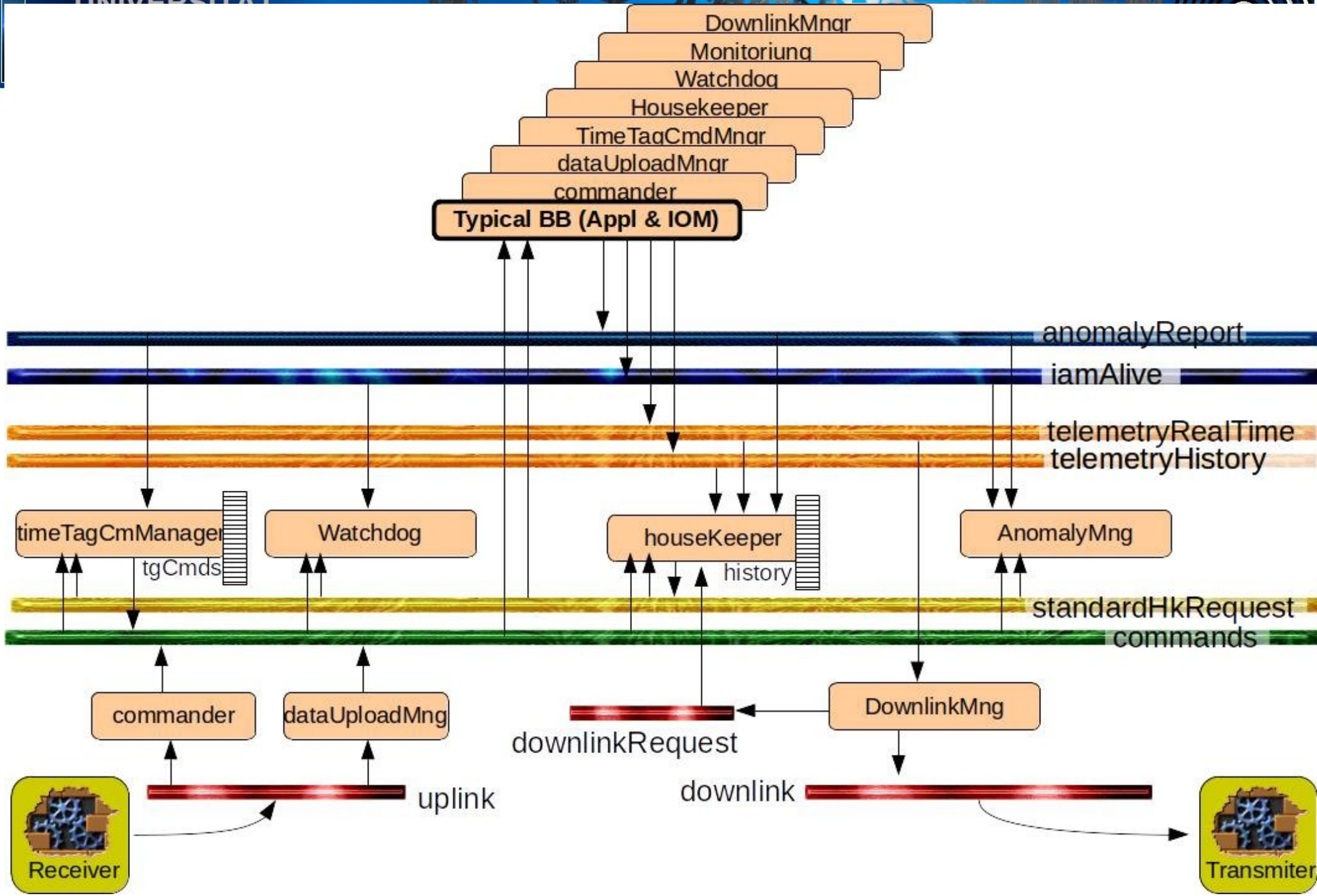


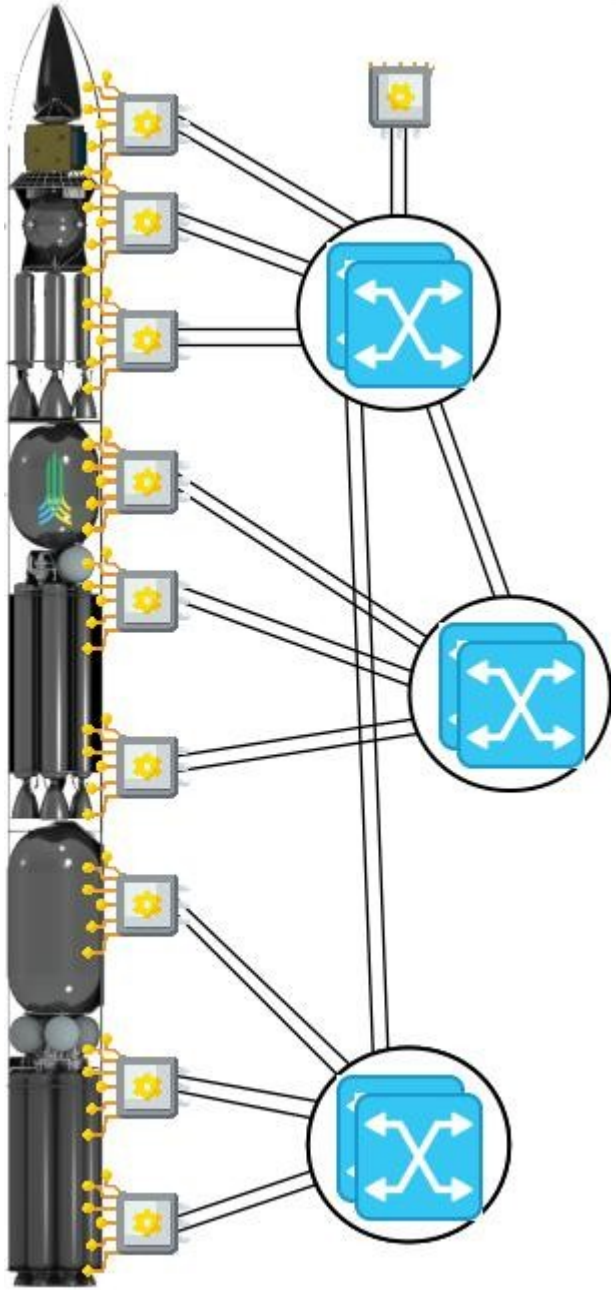
The Software Platform

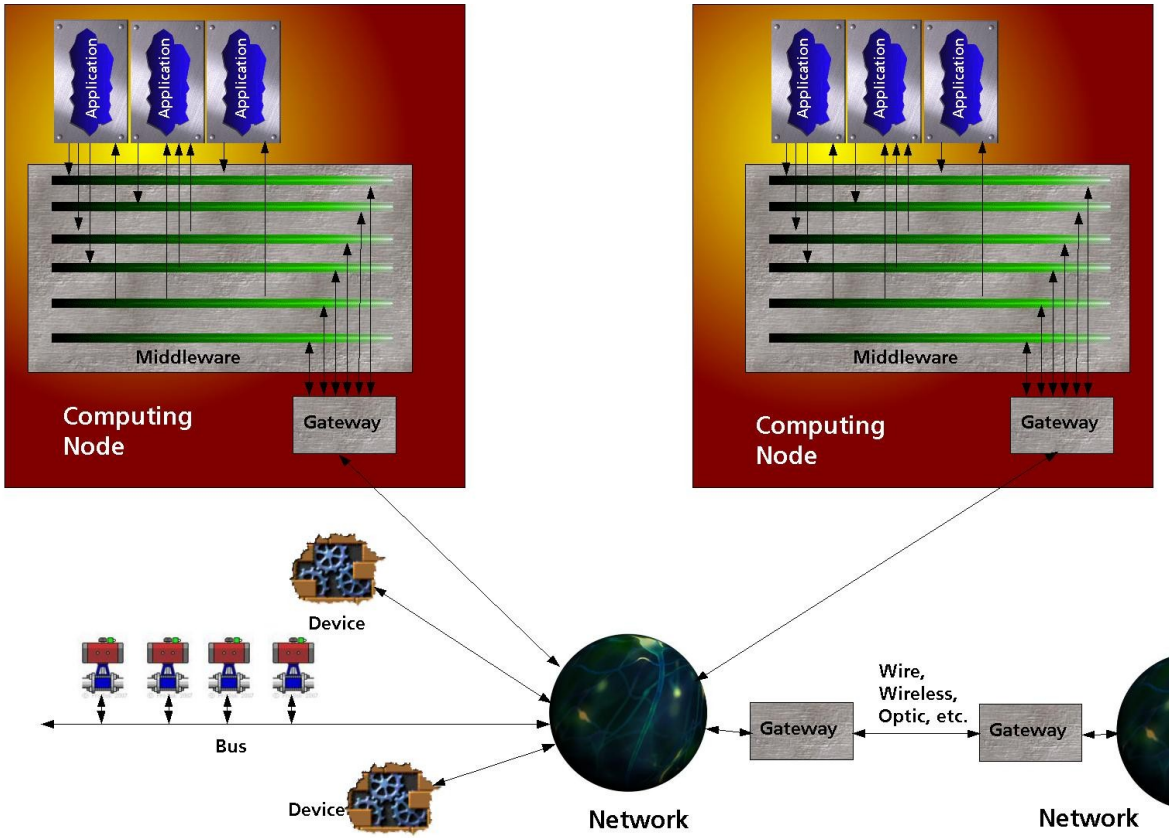


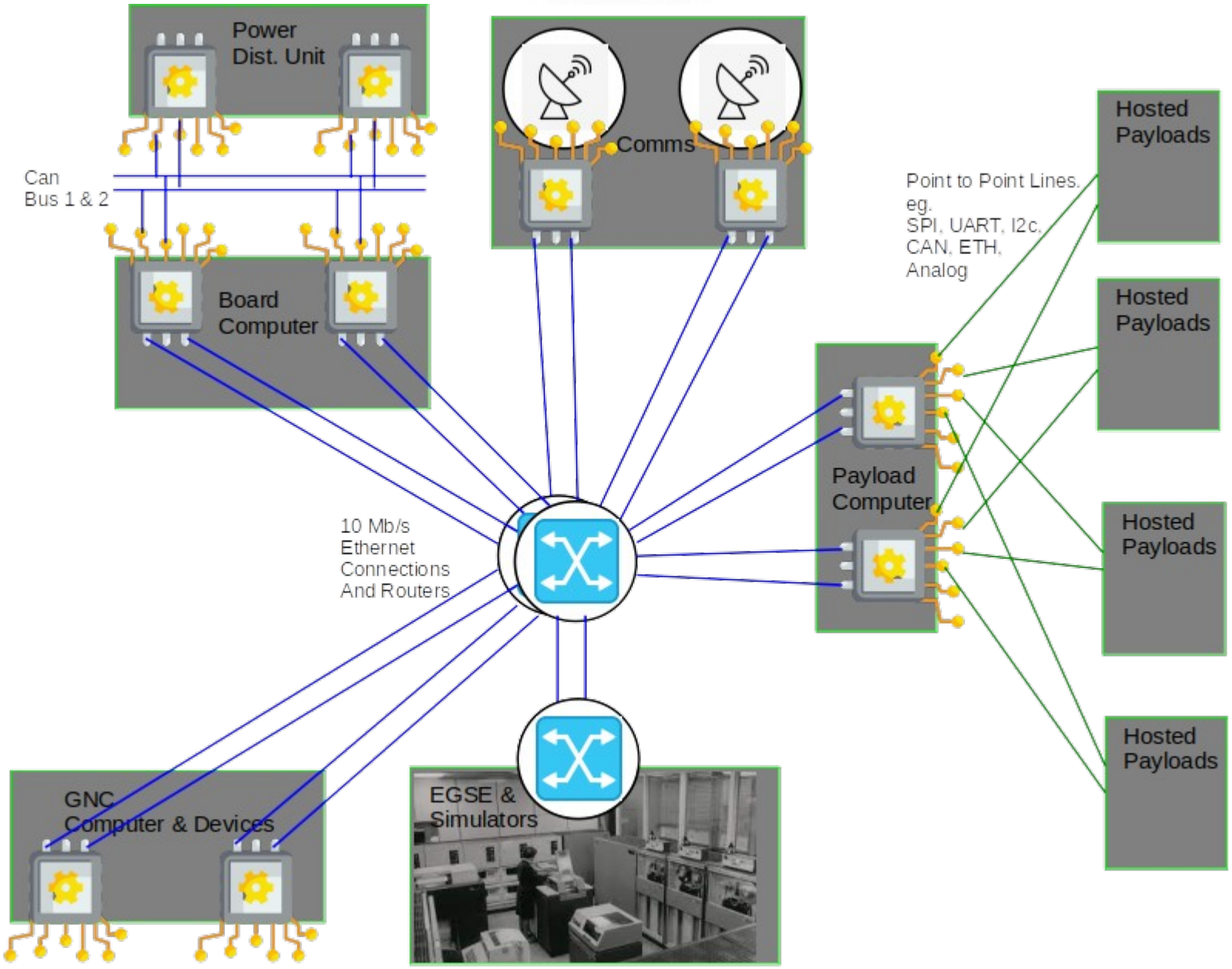
RODOS

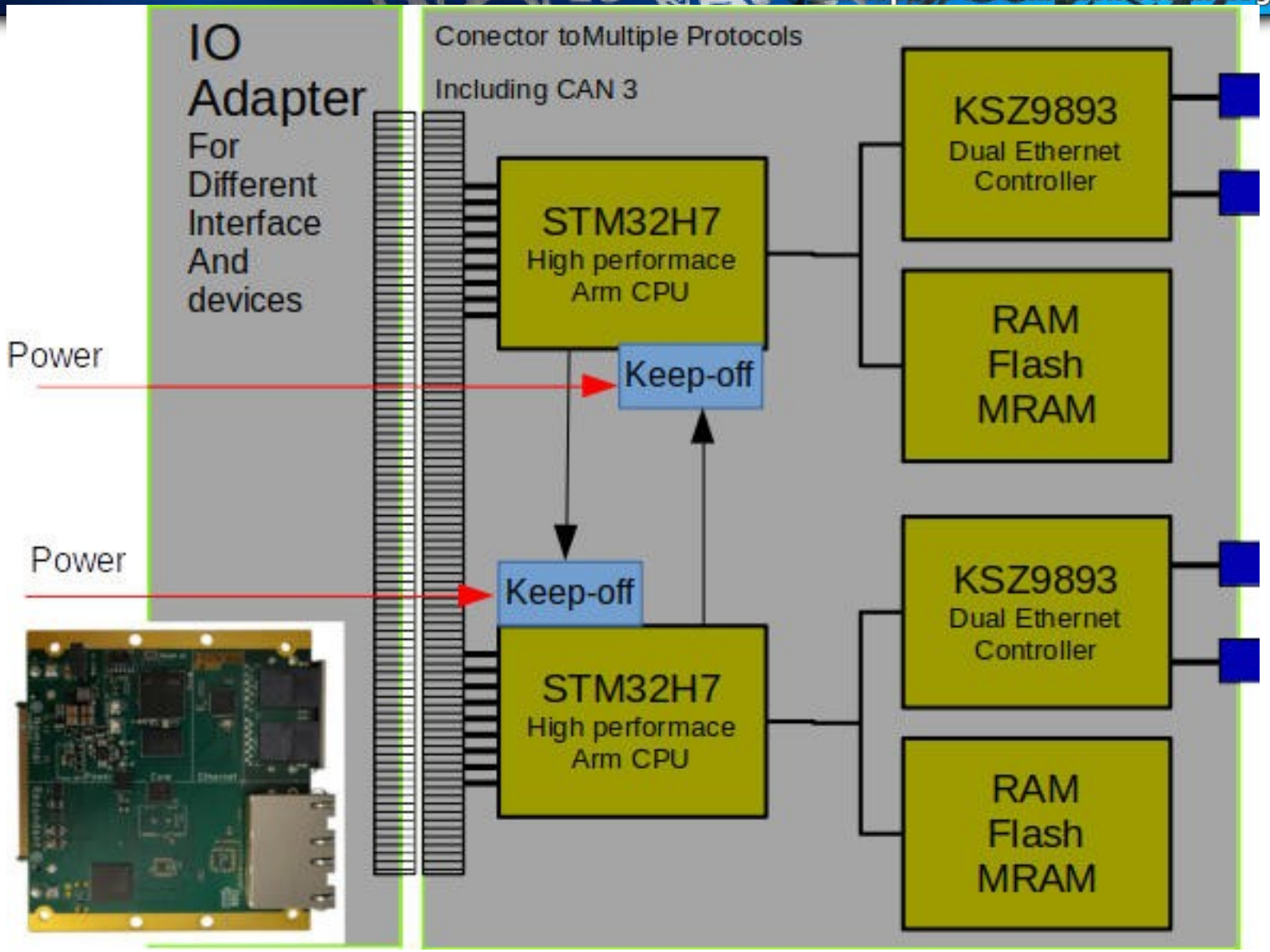

Application
Application
Application
Middleware
Computing Node
Gateway
Application
Application
Application
Middleware
Computing Node
Gateway
Device
Bus
Device
Network
Gateway
Wire, Wireless, Optic, etc.
Gateway
Network


DownlinkMngr
Monitoriung
Watchdog
Housekeeper
TimeTagCmdMngr
dataUploadMngr
commander
Typical BB (Appl & IOM)
anomalyReport
iamAlive
telemetryRealTime
telemetryHistory
timeTagCmManager
tgCmds
Watchdog
houseKeeper
history
AnomalyMng
standardHkRequest
commands
commander
dataUploadMng
downlinkRequest
DownlinkMng
uplink
downlink
Receiver
Transmiter

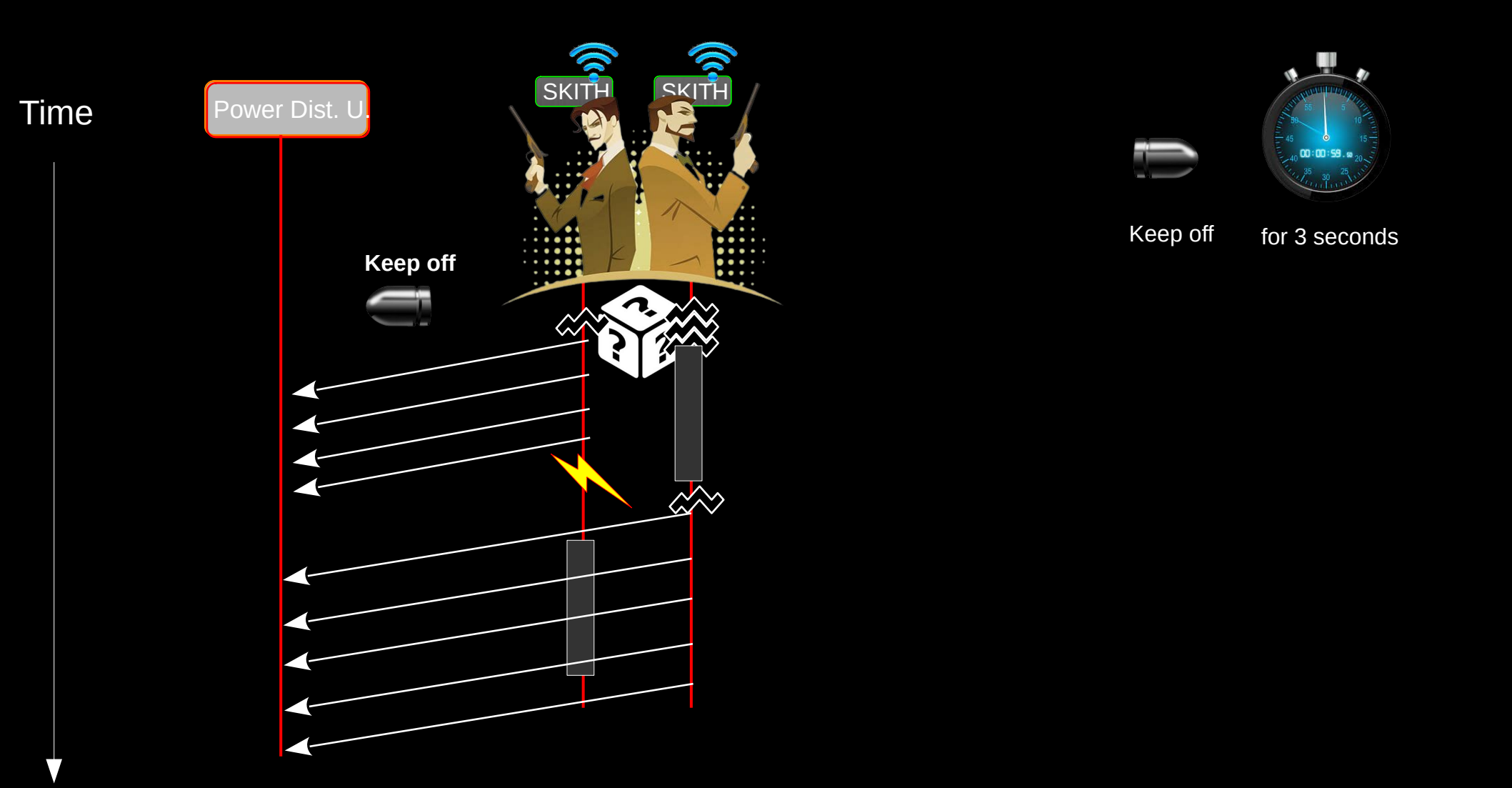


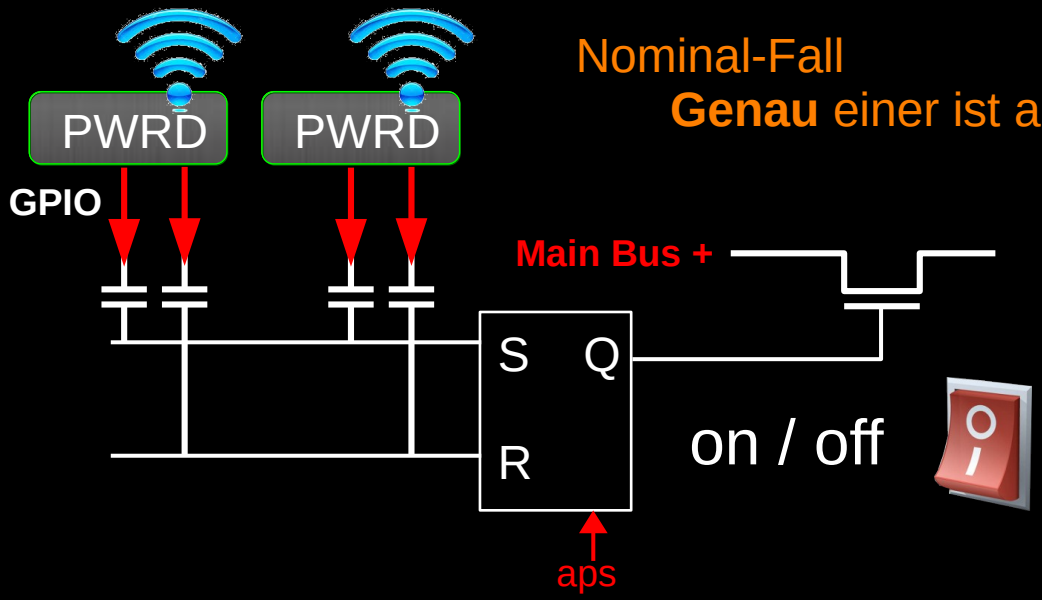

Application
Application
Application
Middleware
Computing Node
Gateway
Application
Application
Application
Middleware
Computing Node
Gateway
Device
Bus
Device
Network
Gateway
Wire, Wireless, Optic, etc.
Gateway
Network


Power
Dist. Unit
Comms
Can
Bus 1 & 2
Board
Computer
Point to Point Lines.
eg.
SPI, UART, I2c,
CAN, ETH,
Analog
Hosted
Payloads
Hosted
Payloads
Payload
Computer
10 Mb/s
Ethernet
Connections
And Routers
Hosted
Payloads
Hosted
Payloads
GNC
Computer & Devices
EGSE &
Simulators


IO
Adapter
For
Different
Interface
And
devices
Conector toMultiple Protocols
Including CAN 3
STM32H7
High performace
Arm CPU
KSZ9893
Dual Ethernet
Controller
RAM
Flash
MRAM
Power
Keep-off
Power
Keep-off
STM32H7
High performace
Arm CPU
KSZ9893
Dual Ethernet
Controller
RAM
Flash
MRAM

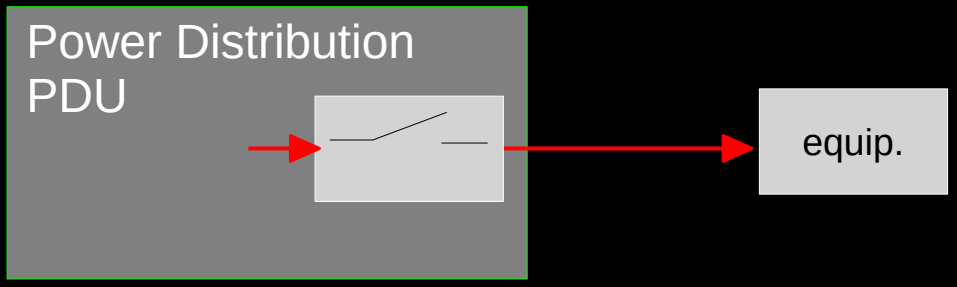
There can be only one
Es darf nur einen geben!

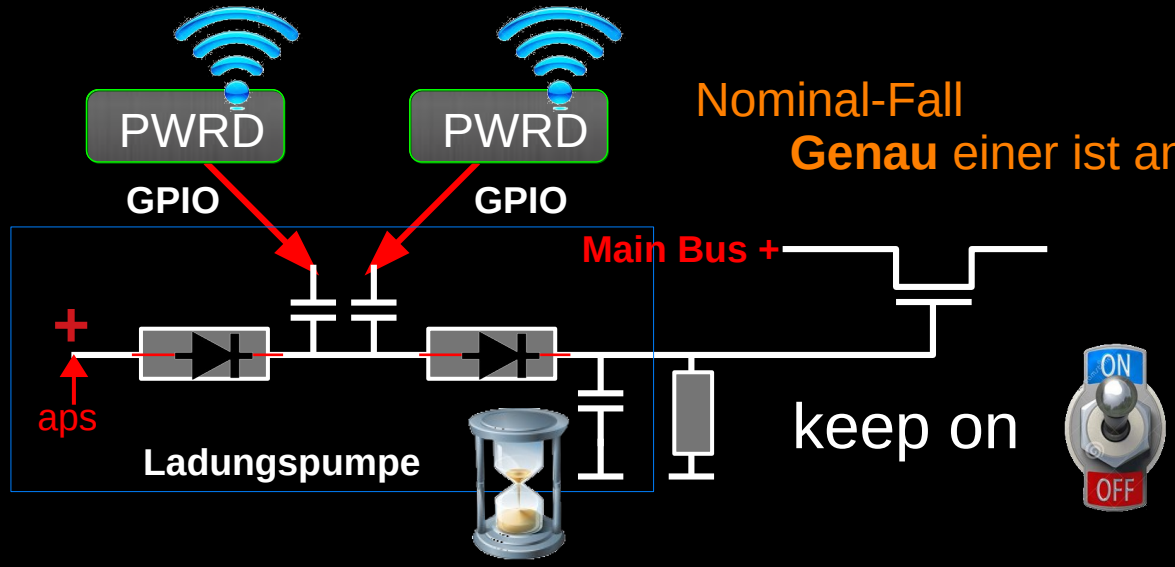

Time
Power Dist. U.
SKITH
SKITH
Keep off
Keep off
for 3 seconds



Nominal-Fall

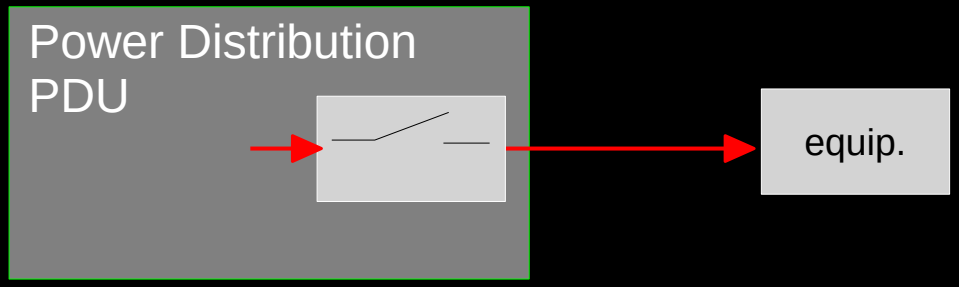
Genau einer ist an

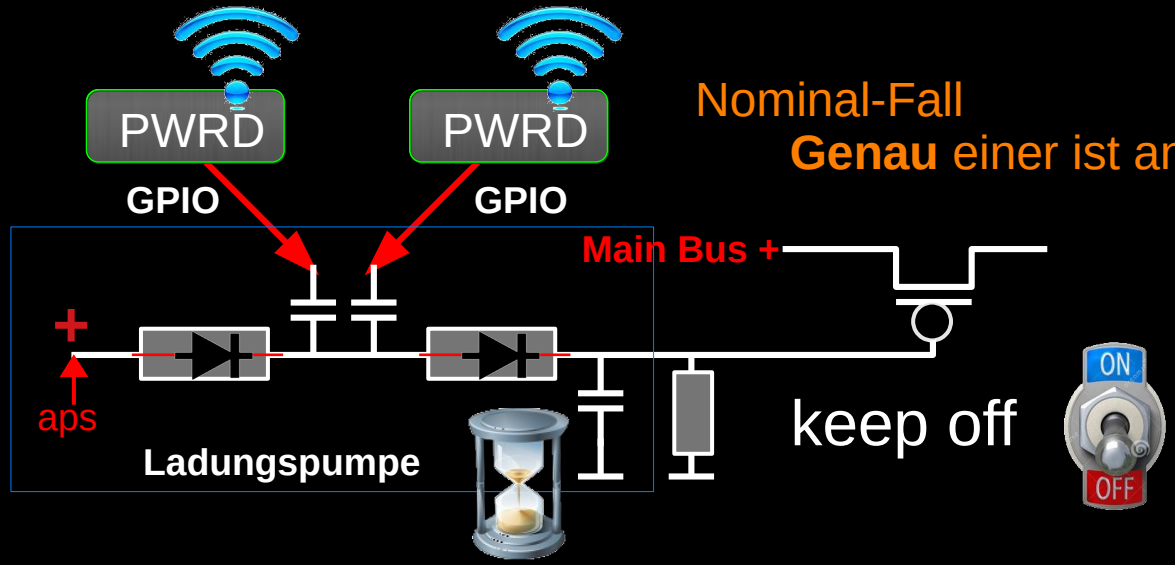




Nominal-Fall

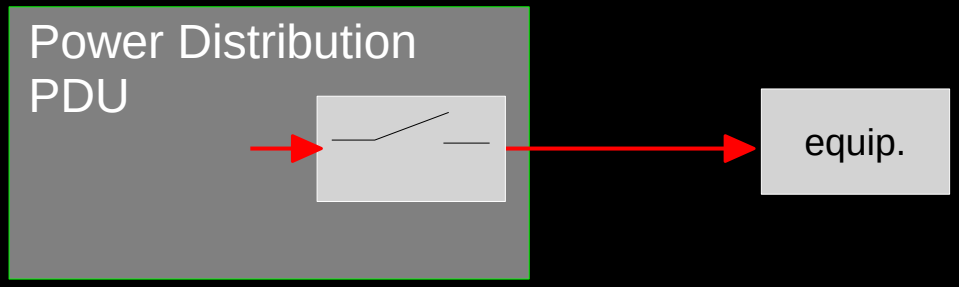
Genau einer ist an





Nominal-Fall

Genau einer ist an



谢谢

Julius-Maximillians-
UNIVERSITÄT
WÜRZBURG

Bayerisches Staatsministerium für
Wirtschaft, Landesentwicklung und Energie

Aerospace Information Technology