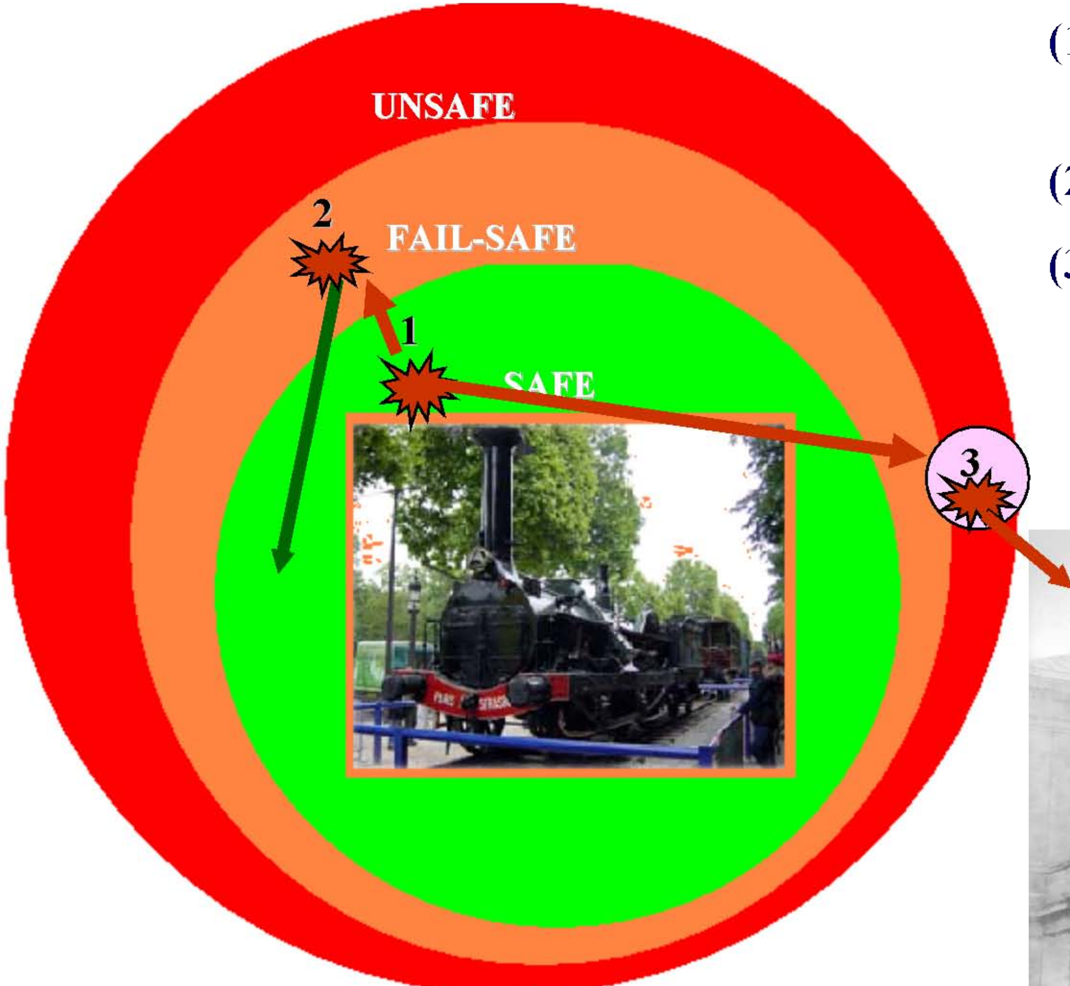
GNSS for rail
Constraints and opportunities

G. Barbu / UIC



(1) Random failures – safe by design

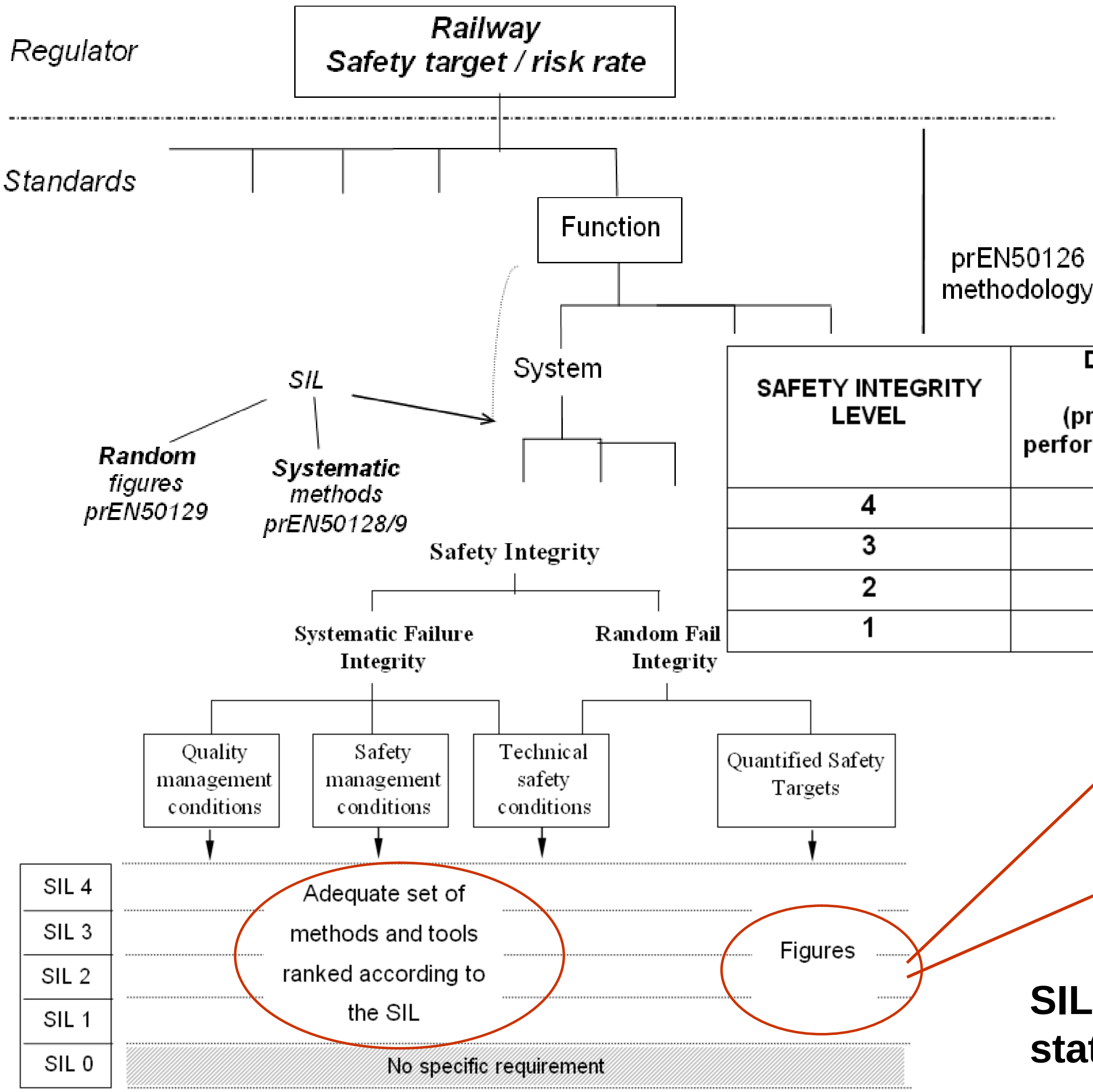
(2) Detected – safe state reached

(3) Random Residual, wrong side failures > unsafe state

potential accident!

Railway is safe by design – all imagined failures shall force a safe (or fail-safe) state

The ultimate safe state is STOP (but not like this)



Risk rate >>> Integrity risk

Quantified >>> SIL

SAFETY INTEGRITY LEVEL	DEMAND MODE OF OPERATION (probability of failure to perform its design function on demand)	CONTINUOUS/HIGH DEMAND MODE OF OPERATION (dangerous failure rate per hour and per element)
4	$< 10^{-7}$	$< 10^{-10}$
3	$\geq 10^{-7}$ to $< 10^{-6}$	$\geq 10^{-10}$ to $< 0.3\ 10^{-8}$
2	$\geq 10^{-6}$ to $< 10^{-5}$	$\geq 0.3\ 10^{-8}$ to $< 10^{-7}$
1	$\geq 10^{-5}$ to $< 10^{-4}$	$\geq 10^{-7}$ to $< 0.3\ 10^{-5}$

SIL is a probability derived from statistic data

Track data (TC, AxC, LC)

Route data (ILx)

All trains data

Line static profile data

Movement authority:

-MA-limit (MAL)

-Speed @ MAL

GSM-R / EURORADIO

On-board functions

…

-Dynamic speed profile

-Train control – speed supervision - emergency braking if no appropriate driver's reaction

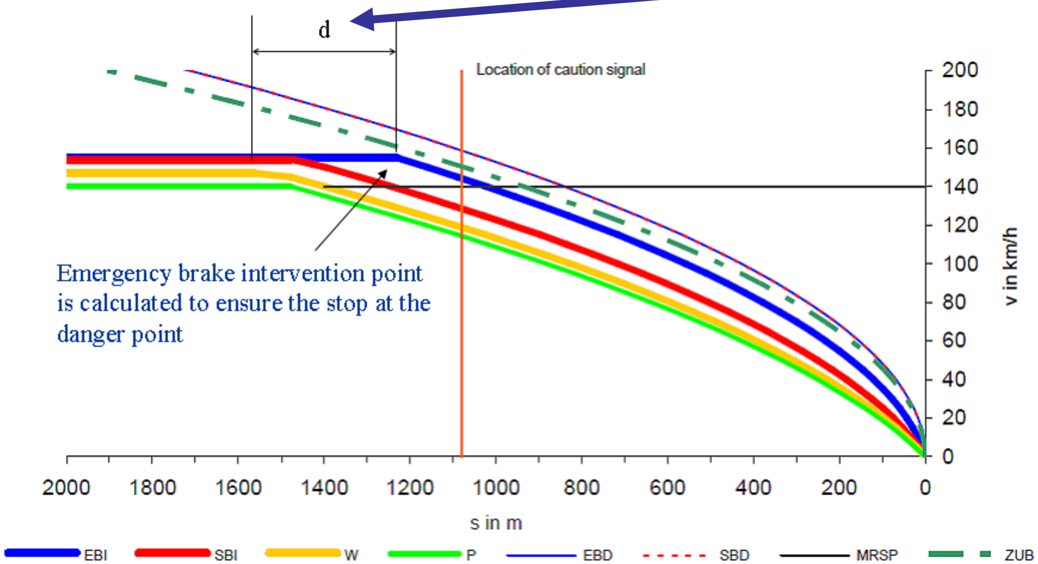
Train communicates his speed when passing a balise

Essence of the train-control safety:

-Emergency braking when:

Vi > VL

Position in the |d| limits



The consideration of various braking profiles results in spreading of intervention points over a distance d, always before the location of the caution signal

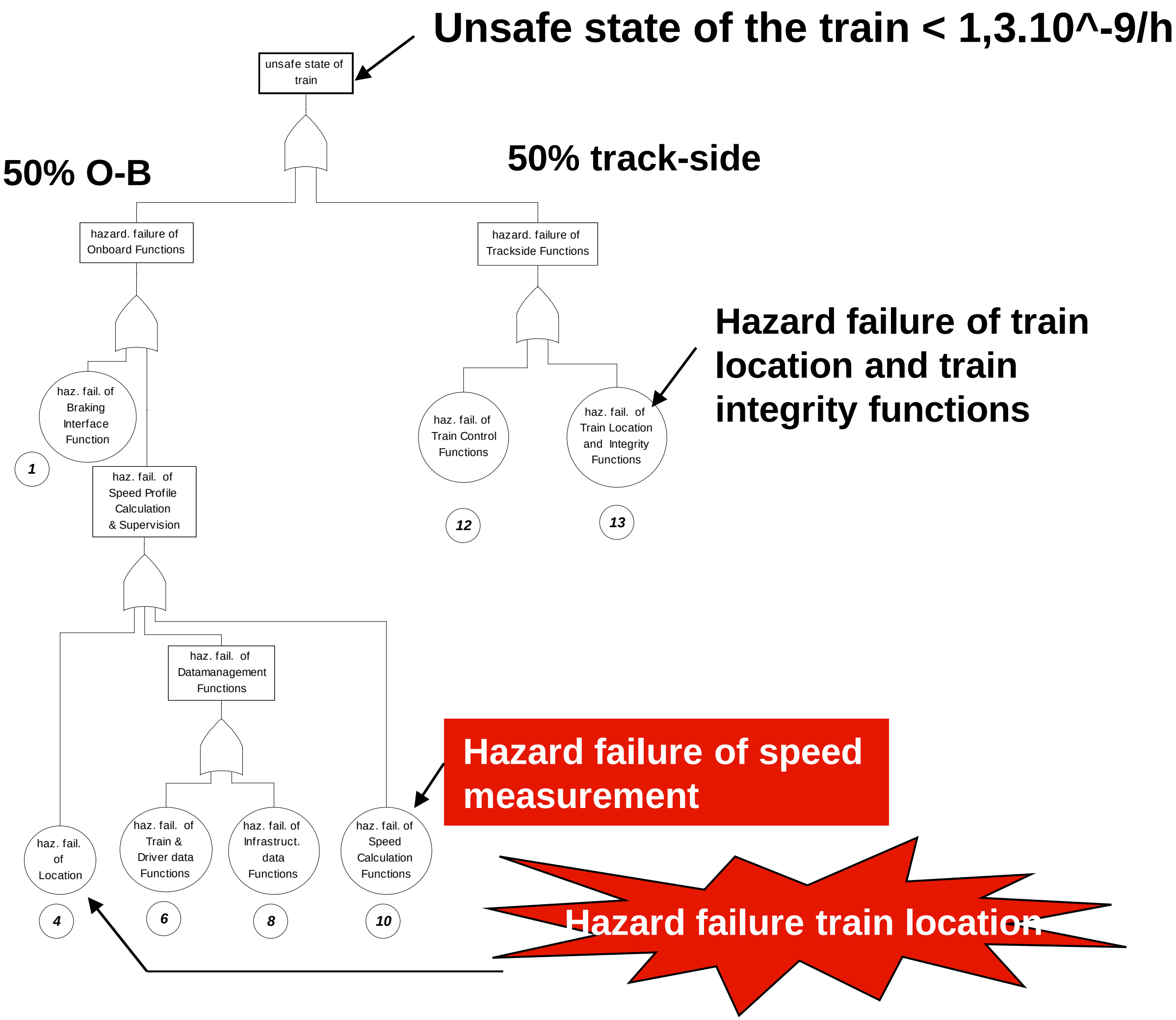
V and instant position (P) on the track are VITAL data

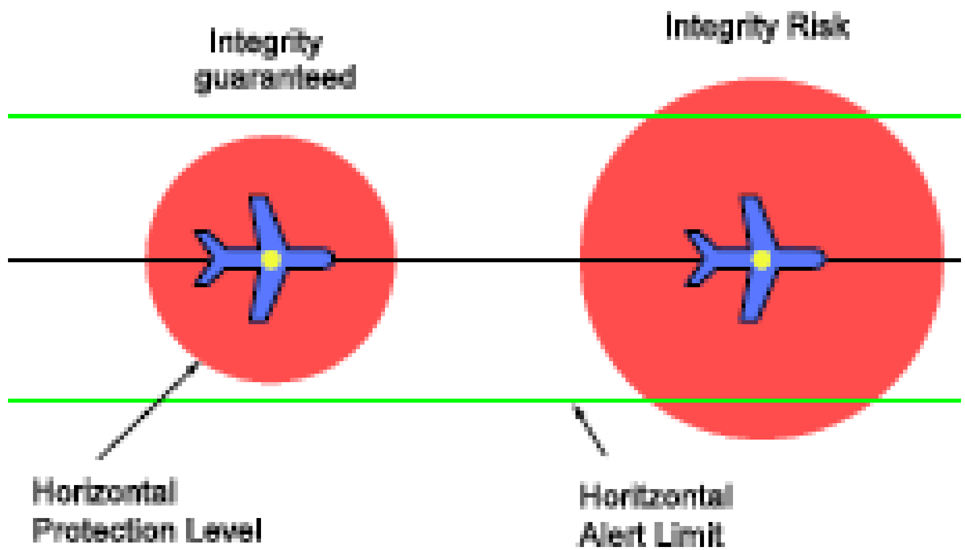
The V and P accuracies are application dependent

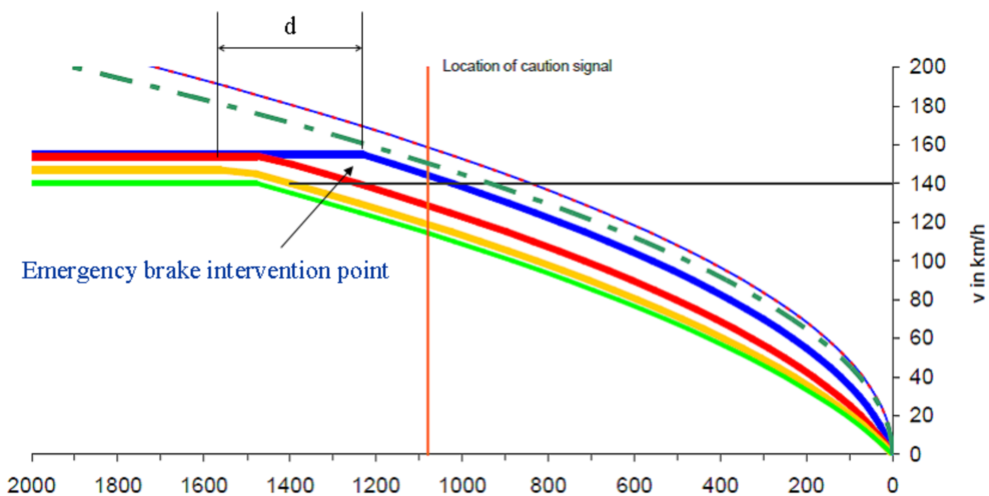
10^-9/h is a statistic figure for hazard of passenger's life

For comparison the failure rate is also expressed in events / hour

Safe behaviour of system's components is a probability but expressed in unsafe states / hour







Aviation IR (probability):

Alert limit is less than the protection level and no alert

Equivalence based on:

-Alarm for accuracy worse than the AL, when probability to occur is greater then Pa

-Time to alarm …

Railway IR (probability derived from statistic):

Position accuracy exceeds the d limit and no alert (equivalent to a non detected wrong-side failure)

GALILEO:

Each satellite can send "NOK" if failure is detected by the monitoring functions (GSS)

A NOK satellite is not included in the position computation

From de valid satellites each one is supposed to have non detected failures, and,

The user (receiver) computes for each fix:

$$P_{HMI}(VAL, HAL) = P_{IntRisk,V} + P_{IntRisk,H}$$

$$= 1 - erf\left(\frac{VAL}{\sqrt{2}\sigma_{u,V,FF}}\right) + e^{-\frac{HAL^2}{2\zeta_{FF}^2}} +$$

$$+\sum_{j=1}^{N}\left(P_{fail,sat_j}\frac{1}{2}\left(1 - erf\left(\frac{VAL + \mu_{u,V}}{\sqrt{2}\sigma_{u,V,FM}}\right)\right)\right.$$

$$\left.+\frac{1}{2}\left(1 - erf\left(\frac{VAL - \mu_{u,V}}{\sqrt{2}\sigma_{u,V,FM}}\right)\right)\right) +$$

$$+\sum_{j=1}^{N}\left(P_{fail,sat_j}\left(1 - \chi^2_{2,\delta_{u,H}}cdf\left(\frac{HAL^2}{\zeta_{FM}^2}\right)\right)\right)$$

If P_{HMI} > IR threshold Alarm is triggered

EGNOS:

$$\sigma_i^2 = \sigma_{flt,i}^2 + \sigma_{UIRE,i}^2 + \sigma_{air,i}^2 + \sigma_{tropo,i}^2$$

$$VPL_{EGNOS} = K_V\sqrt{\sum_{i=0}^{N} s_{V,i}^2\sigma_i^2}$$

- A new XPL is estimated for each computed solution (fix at RIM)
- Integrity alert is triggered (sent from GEO) if XPL > XAL

For each computed solution the IR is in range of 2,5.10^-7; Assumed to be continuous for the 150 s ; AL@20 sigma; TTA < 6 s

(B. Forsell; V. Oehler a.o.)

GALILEO

The requirements (aviation) specify a combined integrity risk – GSS combined with RECEIVER

The IR is evaluated for each failure mechanism and is scaled to a specified XPL; the sum of all contributions is compared with the required IR

Currently, the GAL system design has IR threshold and the XPL corresponding to the specification of aviation critical operations; TTA is a best achievable from the GALILEO architecture

EGNOS

UDRE and UIRE are evaluated by RIMs and include TROPO and AIR residual error models (EGNOS grid)

The (aviation) requirements specify fixed allocation for HPL and VPL – IR results from error exceed condition

The IR is evaluated at each time instant by RIMs, uploaded to GEO and re-sent to user within the ESTB message

Faultless assumption for satellites

Consequences for the rail user:

EGNOS imposes less stringent availability requirements – faultless assumption

GALILEO presents a more realistic IR conception – but the integrity system design is scaled to the aviation requirements (IR threshold and the VAL and HAL specified for the aviation critical operation)

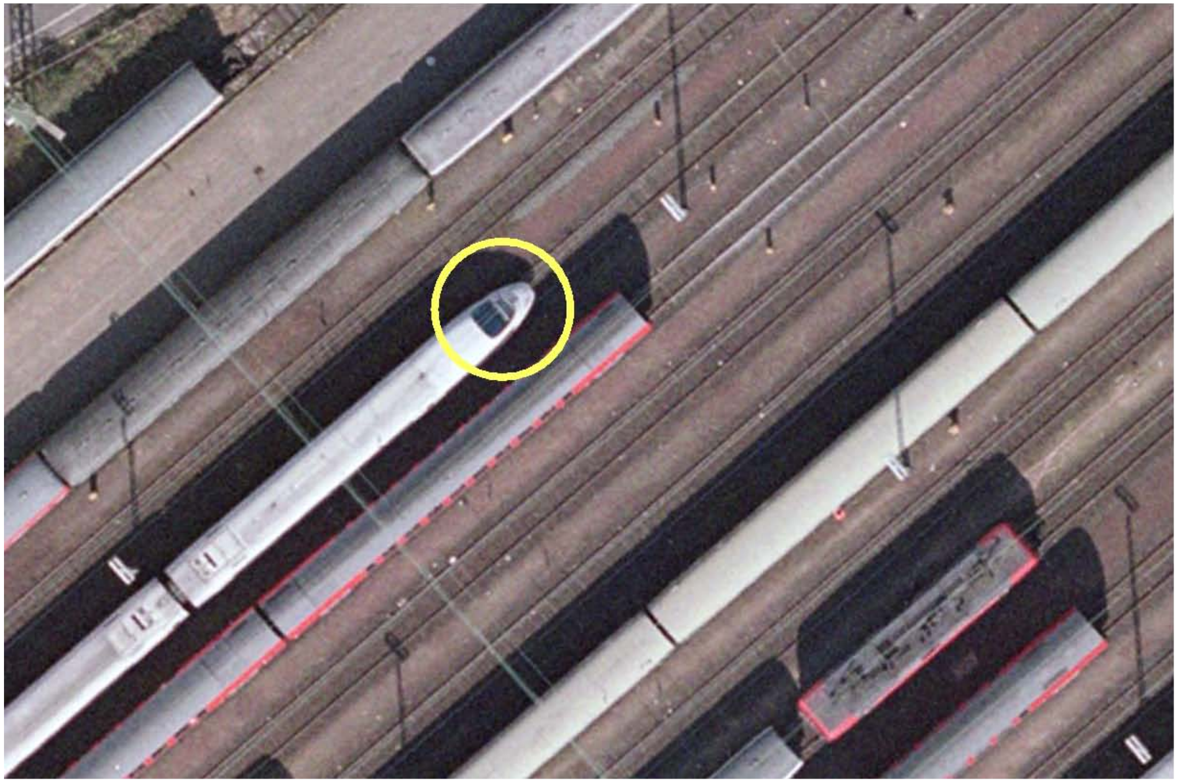
Interpretation:

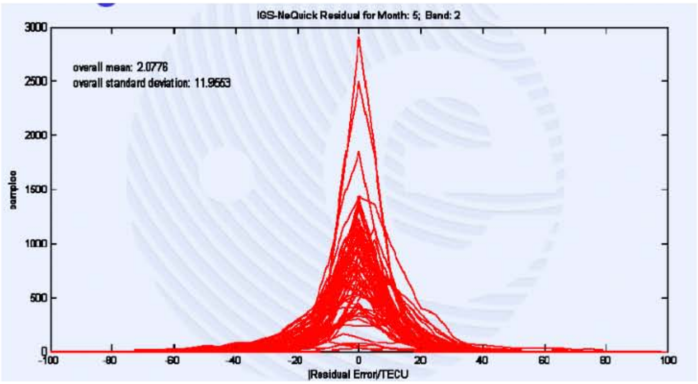
- IR=3,5.10^-7 is the probability for AL > 20σ and TTA > 6 s for every moment of time
- If no other communication arrives, this probability is valid for the next 150 s from the moment of initial communication – this is a specific aviation req.
- The simple calculation P/h = (3600/150)*IR to “reflect” a rail requirement is not correct
- At the user terminal (GALILEO receiver), IR is updated for each fix, is associated to each fix calculation and is based on every 30 s updates of the SISA and SISMA;

Practical rail requirements from ETCS: Train position for awakening which is the line where the train will start ?

Accuracy requirements: H_err < 1,5 m SIL3 in "demand mode of operation", IR < 10^-6

Is it possible in static mode



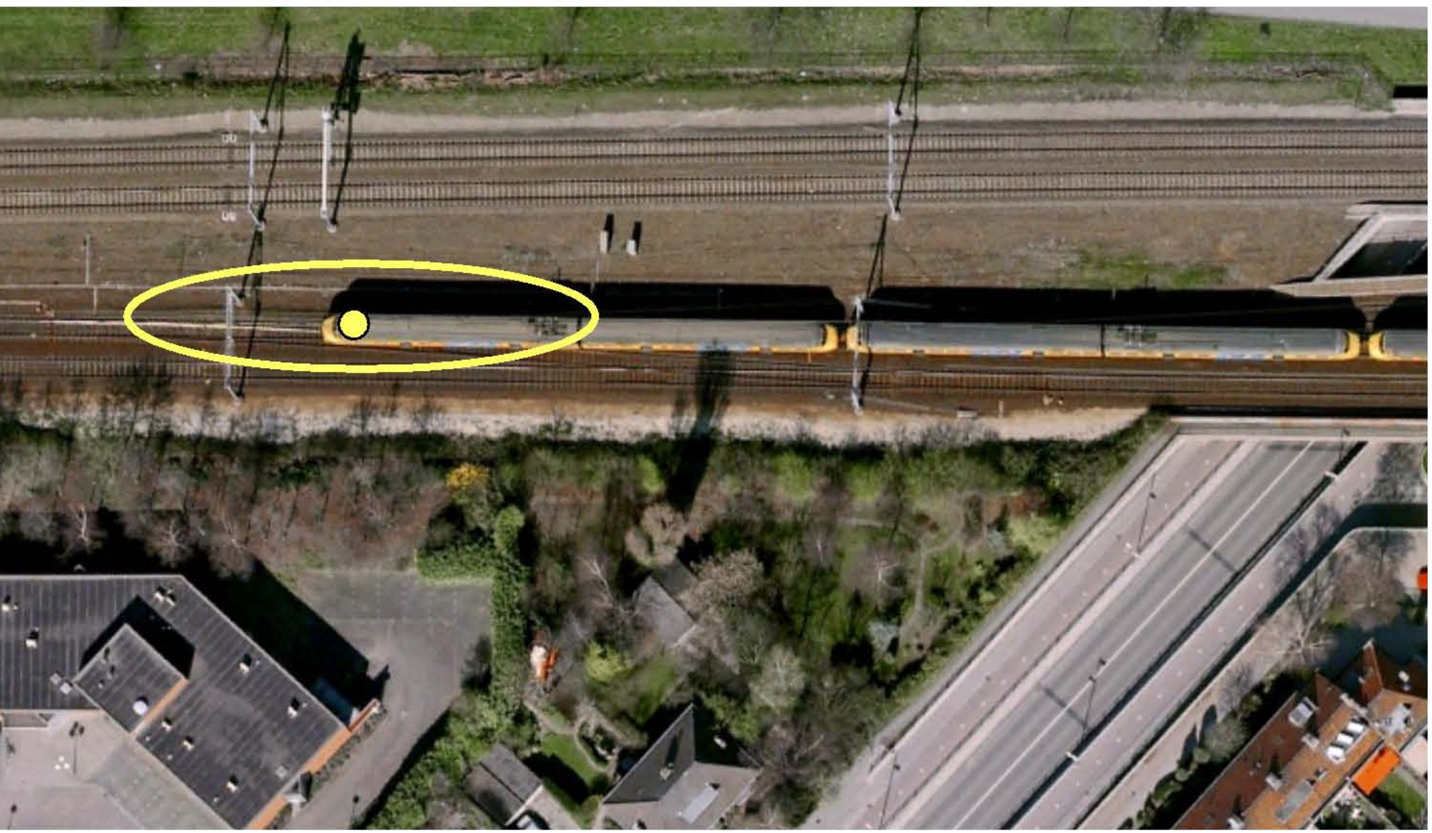


Regression on 600 samples indicates rapid convergence to 1m (ESA simulation)

Train absolute position – all operations, especially low traffic density lines, local and regional lines

AL ~ 20m but IR < 4,1.10^-12 (Probability expressed as events / hour)

Genuine GALILEO SoL satisfies accuracy but not integrity



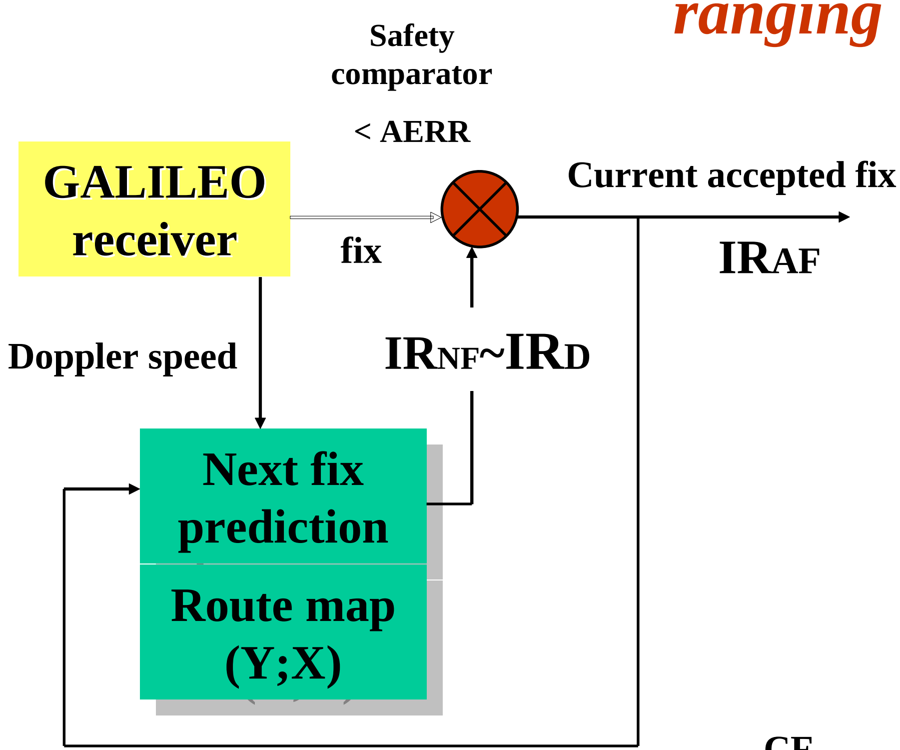
Observation:

Not each fix is necessary

Discard fixes with greater error than HAL

Use only fixes with high integrity

Apply known 2from 2 voting: Predict the next position on the track using speed determination independent from its calculation by ranging



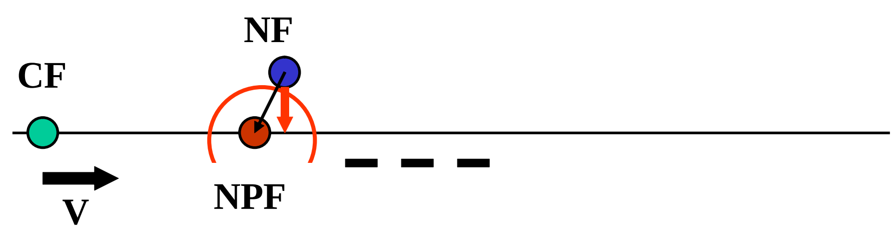
IR of the route map is very low << 10^-16

True statements:

Train does not significantly change speed over T=1s (fix rate = 1 Hz)

Doppler speed is independent of ranging but is in the same integrity as ranging [1]. DV accuracy is in ~mm/s

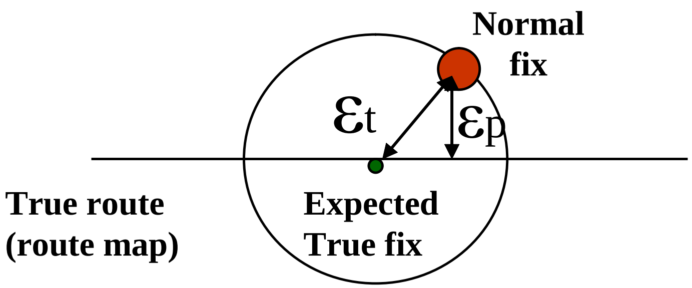
Contribution of Safety comparator to the IR degradation is neglectable

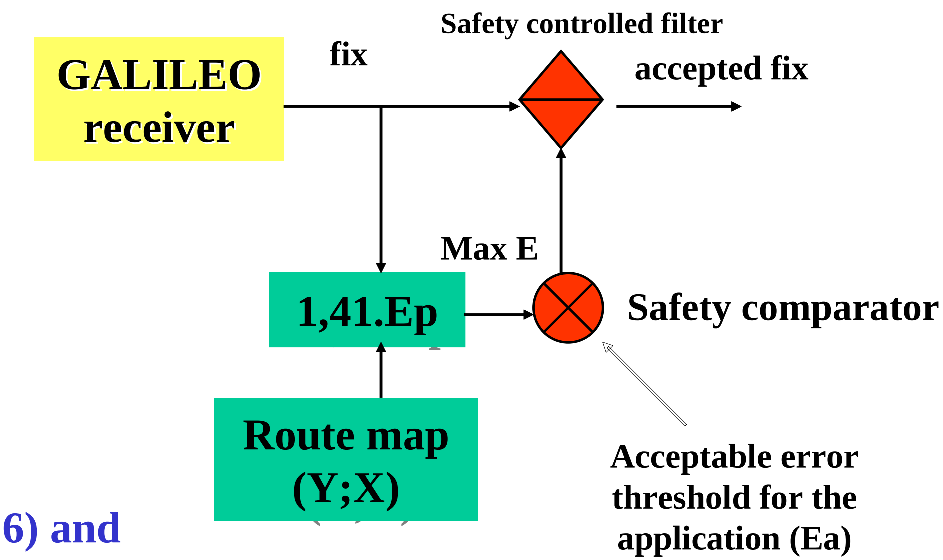


$$IR_{AF} \sim IR_{F}.IR_{D} = 6{,}25.10^{-14}$$ (Bayes)

[1] A. Simsky & F. Boon, Septentrio Belgium

Simplification: use the projection of the fix on the true route





$$MaxE \leq \sqrt{2} \cdot Ep$$

True statements:

Route map is high integer (IR_{RM} <<10^-16) and independent from the GALILEO fixes

Consequence: $IR_{EP} \sim IR_{RM}$

Safety comparator and safety controlled filter are SIL 4 devices (continuous operation mode)

SC function:

-If Max E < Ea command accept fix

-If Max E > Ea command reject fix

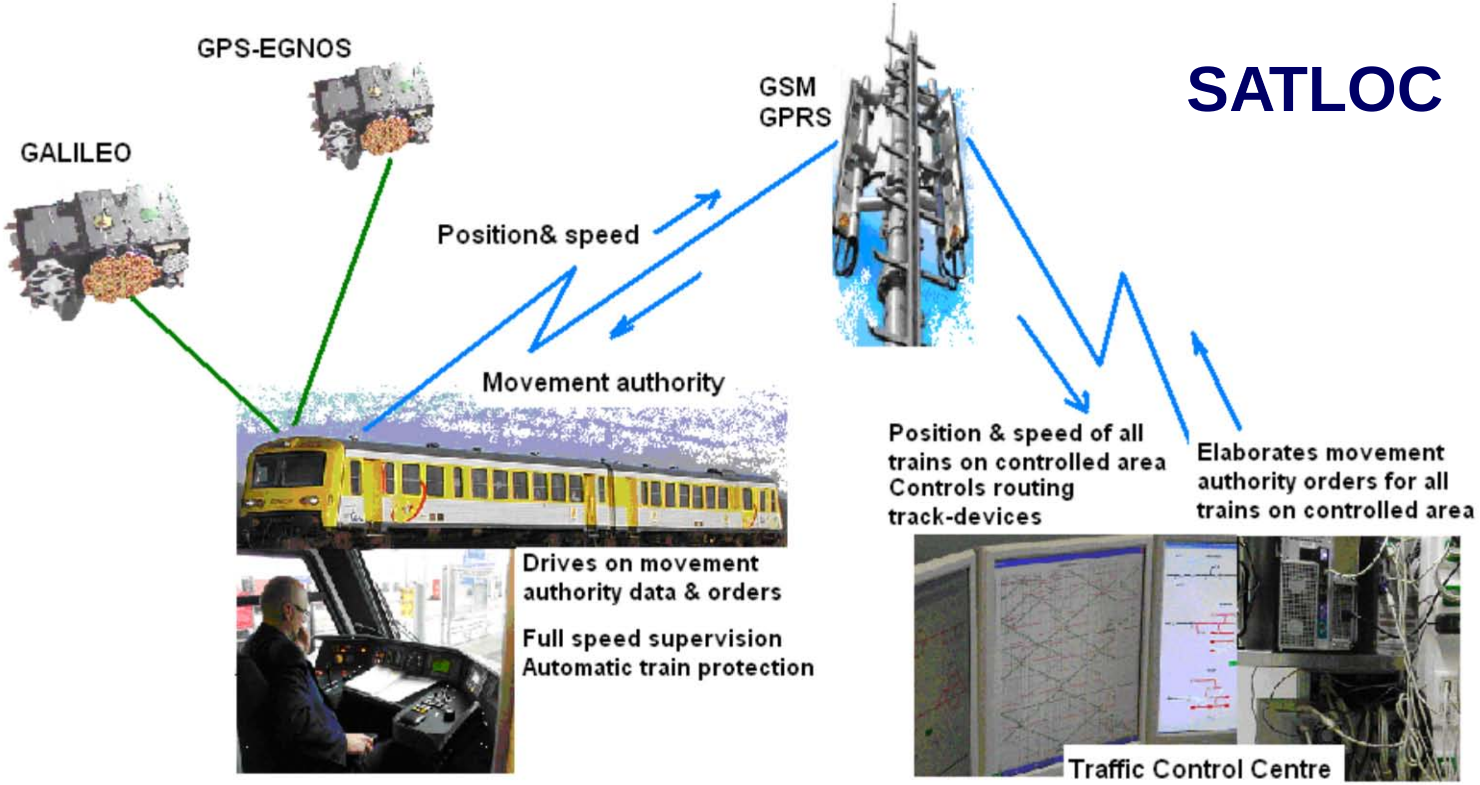
$IR_{AF} < IR_{RM} * IR_{SC} <$ 10^-16

Facilitators:

-UIC “GEORAIL” proposal for standards

-Strategy: certification of SIS performance & software receiver

GNSS immediate compliant application



Principle of satellite & radio-controlled train operation for safety and efficiency on low traffic secondary lines which are not submitted to the EC interoperability by ETCS