Connected or autonomous trains?

Alessandro Fantechi

University of Florence,
Dipartimento di Ingegneria dell'Informazione,
Italy

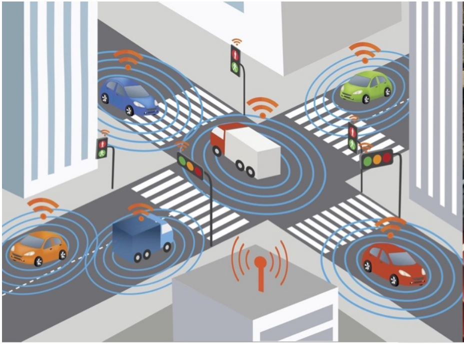
RSSRail 2019, Lille
June 2019

UNIVERSITÀ
DEGLI STUDI
FIRENZE
DINFO
DIPARTIMENTO DI
INGEGNERIA
DELL'INFORMAZIONE

Outline

1. Introduction
2. Connection vs. autonomy
3. Current connected trains
4. Future Connected trains
5. Safety concerns
6. Autonomy and performability
7. Conclusions

Connected cars vs. autonomous car driving



Connected cars and autonomous car driving

Connection

safety and full automation of car transportation globally ensured by

- vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication (**Connected cars**)
- on board artificial intelligence (**Autonomous driving**)

The concept of **connected cars** is based on availability of ubiquitous high band communication links:
cars negotiate the resolution of conflicts by playing distributed algorithms (V2V), or by asking help to equipment deployed along the roads and at crossings (V2I).

Autonomy

As an evolution of current driver assistance systems, **autonomous cars** elaborate information harvested by on-board sensors to provide the knowledge needed to an automated driver.

- Connection and autonomy complement each other, and will be eventually merged in future automated cars.
- (Connection aims at conflict resolution, Autonomy at safe distancing)

Current *connected trains*

- Wide deployment of ERTMS-ETCS systems → already witnesses the achievement of high safety standards by means of distributed control algorithms that span over geographical areas and are able to safely control large physical systems.
- ERTMS-ETCS is known as already able to support full automation of train driving:
  - it provides the basic safety layer
  - over this layer an automatic driving mechanism can be implemented in place, or beside, the human driver
- → *Connected trains* paradigm is already implemented in railways at a much more advanced point w.r.t what is current practice in the automotive domain, due to the widely deployed technological instrumentation of infrastructure.

ERTMS/ETCS

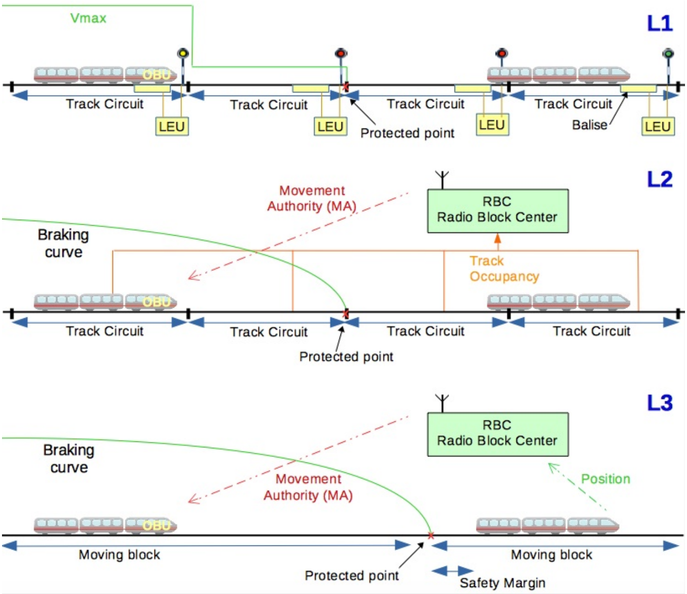
European Railway Traffic Management System (ERTMS)

- international standard that aims to improve interoperability, performance, reliability, and safety of modern railways.
- ERTMS relies on European Train Control System (ETCS): an Automatic Train Protection (ATP) system which continuously supervises the train, ensuring that the safety speed and distance are not exceeded.
- ERTMS/ETCS specified in the standard at four main levels of operation

ERTMS/ETCS levels

- **Level 0 (L0)**: non-ETCS compliant lines
- **Level NTC (L0-NTC)**: ETCS-compliant trains equipped with additional Specific Transmission Modules (STM) for interaction with legacy signalling systems (National Train Control).
- **Level 1 (L1)**: ETCS installed on lineside and on board; spot transmission of data from track to train via *Eurobalises*.
- **Level 2 (L2)**: As L1, but Eurobalises only used for exact train position detection. Continuous data transmission via GSM-R with the Radio Block Centre (RBC) gives the *Movement Authority (MA)* to driver. Lineside equipment → train integrity detection.
- **Level 3 (L3)**: As L2, but on board train location and train integrity supervision. No lineside equipment.

ERTMS/ETCS levels



Level 3

Moving block

- Currently still in development, improves upon the current Level 2:
  - by removing wayside equipment for detecting occupancy of track circuits
  - by giving on-board odometry system the responsibility to compute train position and speed.
- with moving block, headways between trains can be considerably reduced.
- Accuracy on position reporting required for safe distancing suggests more odometry sensors, plus data fusion algorithms.
- Moving block currently implemented in CBTC metro systems.

Automated driving - ATO

- Automatic driving is responsibility of Automatic Train Operation (ATO) system, subject to a safety enforcing ATP system (such as ETCS).
- ATO manages train running from one station (or predetermined operational stopping point) to the next, automatically adjusting the train speed with appropriate traction and braking commands.
- Automatic control of speed and acceleration is performed by the ATO, respecting the required operating conditions and the limits imposed by the ATP, with the goal to optimize the compliance to a set of possibly conflicting requirements, such as timetable respect, energy efficiency, passenger comfort, equipment durability, etc.
- The ATO can replace the driver also in other operations (opening and closing doors, initial train setup, etc.), making unnecessary the presence of a human operator on board.
- Although ATO takes autonomous local decisions to this respect, the actual degree of train autonomy is almost null: all the (safety-critical) decisions in a CBTC system are centralized in a Zone Controller (ZC - analogous to the RBC of ETCS).
- State-of-art within CBTC “closed system" solutions on urban lines, but ATO on main lines is still far, due to the high interoperability requirements of “open" railway systems constituted by large, complex interconnected railway networks operated by many different train types.
- Indeed, the automated freight heavy rail line recently opened in Australia is also a closed system, with one only type of train.

Interlocking - IXL

- responsible to grant to a train the exclusive access to a *route*: a route is a sequence of track elements that are exclusively assigned for the movement of a train through a station or a junction.
- an IXL simply receives requests of reservations, and grants reservations or not on the ground of safety rules, until the reservation has been fully used (the track is again free) or has been safely revoked.
- It is not a burden of the interlocking to look for alternative routes in case the requested one is busy, in order to optimise traffic throughput parameters, nor to guarantee that a train does not enter a not reserved track. These two functions, when automated, are responsibility of Automatic Train Supervision (ATS) and ATP systems respectively.
- *connection between a train and an IXL is usually either through optical signals that the driver must manually obey, or mediated by an ATP system.*

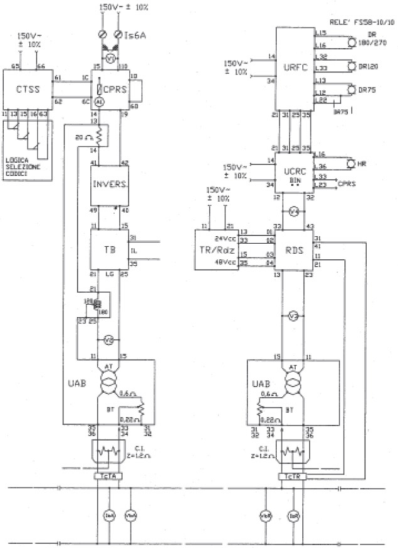
Current *connected trains*: points of view

- "Connected trains" systems are indeed distributed systems:
  composed of a network of computing *nodes* connected by communication links.
- Main critical control decisions are however typically taken at specific nodes of the network (e.g. ETCS Radio Block Centre - RBC), that collect data from the other nodes for this purpose, and are communicated to the other nodes in a master/slave fashion.
- Evolution goes in the direction of a more dynamic connection among mobile components, in which decisions are actually taken in a distributed way, asking for distributed consensus algorithms.
- *limiting factor : independence of infrastructure managers w.r.t. train operators: the former tend to centralize control on the traffic over the infrastructure they manage, while the latter have to ask the former, and pay, for access to the infrastructure.*
- Autonomous decisions appear to have a far less important role in train control systems, due to the strongly infrastructure-based nature of railway operations.

Distributed control

- Railway lines are by nature geographically dispersed, so system distribution typically reflects geography:
  a line is divided in sections, a station is divided in zones, etc.,
  with a separate control of each part in order to reduce complexity and equipment costs, to minimize cabling, or to obey to different authorities over the line.
  But within the section, or zone, the control is still centralised.
- A recent trend has even seen the diffusion of “multistation interlocking" systems: centralization of the interlocking functions of all the stations of a line.
- Avoiding proprietary interfaces and protocols between the different systems, that generate *vendor locking*, through the definition of standard interfaces and communication protocols. (The whole story of ERTMS/ETCS is about this issue: interoperability between trains, infrastructures and equipment produced by different vendors and/or managed by different entities).
- One driving factor against distribution is related to maintenance costs: the dispersion of technological equipment needing a frequent maintenance over kilometers of lines hosting a continuous train traffic is a highly costly and highly risky activity.
- For the same reasons, if a particular functionality requires massively distributed equipments put in operation along a line, it would be an important advantage that they exhibit **zero-maintenance** throughout its operating life. The latter characteristic is hence a must for future systems that exploit a finer granularity of distribution.
- These centralisation trends seem to contrast the advent of pervasive, distributed intelligence to support fine grained, distributed decision systems, as advocated in advanced *cyber-physical systems* to attack complexity.

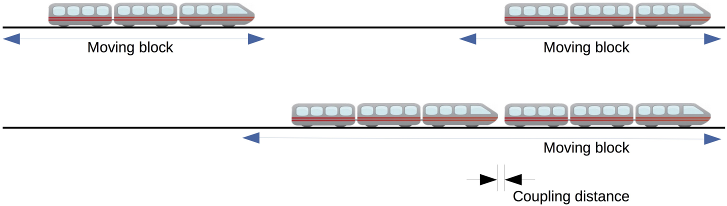
Legacy distributed decision



BACC

- Indeed, distributed decision can be found even in old, electromechanical signalling systems: e.g. Italian BACC (Automated Coded Currents Block) is intrinsically distributed.
- BACC: fixed-block ATP based on relay technology: at any border between two sections, an alternate current, with a specific code modulation, is injected on the rails in front of the coming train: the train short circuits the rails so that no current is present on the track behind it, and an on-board equipment brakes the train if no code is detected in front.
- The injected code at a section border is depending on the (sensed) code of the previous section, so that the code read by the train tells how many sections are actually free in front of the train.
- The equipment that decides the information to be injected in the rail for delivery to the train is distributed in a chain on the line:
- the protection algorithm is naturally geographically distributed.

Future Connected trains - Virtual coupling



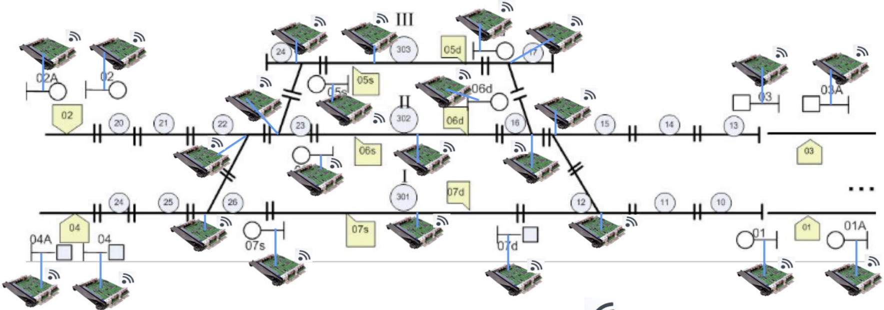
- Innovative method of train formation:
- multiple trains running one behind the other, without physical contact,
- distance comparable to mechanical coupling,
- enabling maximisation of the line capacity
- in VC the strict cross control between coupled trains has to be negotiated locally, with a *train to train communication*, since it requires a precision on the relative distance between the trains that cannot be supported by ETCS-like systems.

Distributed Interlocking

- Centralised interlockings are complex and costly to design and especially to be certified against safety guidelines.
- Therefore it seems sensible to consider a distribution of the interlocking logic over a network of computing nodes, with a granularity pushed to the limit of one controller node for each element of the track layout.
- Every physical track element is equipped with a tiny computer, which knows the routes that interest the associated element, and receives and interprets route booking, release, and cancellation requests, dialoguing with the computers of adjacent elements.

Distributed Interlocking

Distributing Interlocking logic: the SaRDIn concept



Not in the next agenda (5 to 10 years) of the railway industry.

But patents already issued for similar concepts:

US patent 8820685 B2, 2014.

US patent 20120323411 A1, 2012.

control room

Distributed Interlocking

- The overall safety of the controlled layout can only be achieved by ensuring that the information on the routes reserved for incoming trains are properly shared in a consistent way by all distributed processors associated to the concerned elements.
- A distributed mutual exclusion algorithm is played between the nodes corresponding to track elements, triggered by route requests coming from the trains or from a dispatcher;
- different algorithms, depending on the way information is allocated to nodes and trains and passed between them (T2I)
- even a distributed consensus algorithm between trains to reach a common decision about allocation of a route could be adopted (T2T negotiation)

Fully automated train operation

Extending the principles of ATO systems to envisage a fully automated main line train:

- A train is given a mission in terms of:
  - starting time and location,
  - destination,
  - intermediate stops,
  - possibly, the required timetable,
  - a map of the lines to be traversed, with alternative paths if any, and with speed profile.
- information is transmitted to the train at the beginning of the journey or at run-time, or section after section, or continuously asked by the train: this choice has to consider many factors (geography, different jurisdictions, the possibility of real-time changes and different modalities adopted in different sections of the mission).
- A train tries to accomplish at best its mission by reserving in advance the resources that it needs, autonomously asking for the needed extensions of its EoA (End of Authority), or asking for the exclusive access to a route through a station or a junction to a (centralised or distributed) interlocking system.

Fully automated train operation

Extending the principles of ATO ... (cont.):

- At any prospected conflict between trains, complex distributed consensus algorithms can be envisaged to take the role of preserving safety while optimizing resource usage and line capacity.
- A train, in case of conflict, can choose an alternative route, if available and convenient.
- Existence of standard interfaces and protocols for T2T, T2I, I2I communication.
- A train moves at a speed, below the braking curve given by the current safety envelope, and is optimal w.r.t. the objectives of timetable respect, energy efficiency, not uselessly triggering emergency brakes, etc...
- The items above are not safety-critical, since safety is guaranteed by underlying ATP.
- At any moment, the train should release resources that were allocated to it, and have already been consumed. The sooner the resources are released, the sooner they are available to other trains, improving the capacity of the railway network. This concept is called, for interlocking system, *sequential release.*
- Safety concerns are raised by this issue, that should be taken in charge by ATP.
- Interoperability with human-driven trains has to be guaranteed.

- *Autonomous decisions* play a minor role in this picture, dominated by communication-based centralised and distributed decisions.
- Importance of *autonomous positioning*.

Safety concerns - Qualitative safety

Safe train motion usually defined in a qualitative manner:

- inability of a train to travel beyond a *protected point* or *EoA* (depending on the kind of of protection mechanism) established in front of the train.
- At any time, the span of tracks from the current train position to the protected point constitute a ***safety envelope*** within which the train can freely move.

This generic notion of safety envelope includes:

- distancing from previous train (responsibility of ATP - Fixed or Moving block - or Virtual Coupling) along the line,
- and the reservation of a path in junction areas (responsibility of IXL), if any.
- *The safety envelope can be defined as the minimum of the track spans given by these two contributions.*

Safety envelope

- Other constraints: e.g. switches in front of the train are locked in their position so that they do not move when the train passes over them, level crossing barriers are locked in a closed position, signals show specific aspects, etc...
- In general, we can look at this issue as a mutual exclusion problem: **in order to proceed a train needs to have an adequate set of resources exclusively allocated to it**: the amount and characteristics of such resources define the maximum extent and speed of safe train motion.
- Notice that in such a distributed mobile system, communication timing and latencies have to be taken into account together with train speed in the definition of the safety envelope, by adding proper safety margins that typically reduce the span of the safety envelope.

Safety concerns - Quantitative safety

EN50126 standard: functions that in case of malfunction may cause catastrophic effects are rated at SIL4, equated to a Tolerable Hazard Rate (THR) of 10^{-9} failures per function per operation hour.
Under the probabilistic perspective, considering the safety envelope concept discussed above, safety of train motion is guaranteed when it is demonstrated that the sum of the probabilities that:

- *i*) a train goes beyond its safety envelope (e.g. the received MA),
- *ii*) the train is given an erroneously permissive safety envelope (e.g., a longer MA),

does not exceed the THR limits.

When distributed consensus algorithms are used for safety-critical control functions, is the fundamental result of [Fischer Lynch Paterson 85]: *distributed consensus cannot always be reached in presence of asynchronous, possibly faulty, communication*.
Evaluating the probability of not reaching consensus can provide other figures for a quantitative analysis of safety.
However, the most sensible way to deal with this problem is by setting timeouts for a distributed consensus round, that bring the system in a fail-safe state, moving the problem from safety to availability.

Uncertainty

- Advanced train control system require accurate measure of position and speed of trains
- *Uncertainty* over such measures, quantified as an error interval around the measured quantity of interest.
- Uncertainty in positioning is usually managed by allowing for a longer safety margin, by assuming a maximum uncertainty threshold.

- A satellite positioning device, as used in avionic satellite navigation, gives, together with a position estimation a so called *protection level*, a statistical bound error computed so as to guarantee that the probability of the (unknown) real position error exceeding the protection level is smaller than or equal to a target value (called *integrity risk*).
- i.e. the interval (given by the protection level) around the estimated position does not contain the real position with probability less than the integrity risk.
- The target integrity risk can be computed in relation to the desired THR.
- However, a typical satellite position receiver gives a greater THR w.r.t. that of SIL4 functions, and hence sensor fusion with other odometry devices is needed to lower the THR

Security for safety

- A further challenging aspect related to the integrity of exchanged vital data is *security*, due to the trend to keep communication costs to an acceptable level by recurring at open protocols and media.
- The CENELEC standard EN50159, as well as recent developments in security and encryption techniques, attempt to mitigate this concern: the so called *cyber-physical security* research area, addressing other domains both in transportation and other pervasive computing applications (e.g. IEC62443 standard for security of industrial automation and control systems), has produced also results for the railway signalling domain.
- A general message from this body of literature is that it is currently possible to adopt security countermeasures that make security attacks (such as counterfeiting plausible MA) with catastrophic consequences very unlikely. Rather, more concern is raised about the possibility of denying communication, which may trigger emergency breaking and extensive denial of service.

Autonomy as a mean to performability of automated operation

- Inheriting autonomous cars technology → move more and more intelligence onboard trains, to let them take autonomous decisions, with little help of ground-based infrastructure.
- However, the physics of train motion, that requires long stretches of free track to attain high speeds, limits the actual possibility to adopt autonomy in train control.

Performability, availability, capacity

- Actually, the primary objective of introducing technological advances in train traffic control is not safety (already very high standards of railway safety), but rather improving KPIs such as performability (often intended as adherence to expected timetables), availability of transport service and transport capacity, ("liveness properties", that often conflict with safety objectives.)
- The complexity of the considered system makes the occurrence of a safe-fail block rather probable, causing the partial or full unavailability of transport service.
- e.g. an ETCS train cannot move if no MA has been received due to any computation or transmission fault
- A careful evaluation of safety characteristics of a modern complex signalling system cannot therefore ignore an adequate analysis of availability attributes, in order to ensure an appropriate transport capacity, with the related operation cost effectiveness, through techniques of quantitative evaluation of these attributes.

Autonomy in degraded modes

Due to the strong infrastructure-based nature of railways, autonomy would appear not to have a main role in the future of train control systems.
However, in future fully automated train driving the possibility of taking autonomous decisions in place of the driver will be essential.
In both following scenarios, the *safety envelope* in front of the train is not negotiated with the infrastructure or with other trains, but is autonomously determined.

First scenario – Degraded modes of operation

- In order to allow trains to proceed even when a threat to safety does not allow full performance, ETCS defines degraded modes of operation, to be entered when the "Full Supervision" mode (the normal mode of operation, as described above) is no longer supported by the system.
- More responsibility is given to the driver, in different operational non fully supervised modes: Limited Supervision, Staff Responsible, OnSight, Shunting are the most relevant ones.
- When an ATO system is substituting the driver, it should be able to cope with degraded modes, with no connection with any RBC or other external supervising entity.
- An autonomous driving system equipped with obstacle detection sensors and artificial vision may play the role of the driver, moving the train at reduced speed according to the operational procedures that are foreseen for the OnSight mode, trying to switch back to Full Supervision as soon as connection is recovered.

Second scenario – Light rail autonomous vehicles

- Tramways and light rail vehicles normally use little signalling, and safety is for most part responsibility of the human driver *(on-sight driving)*.
- Obstacle detection and artificial vision techniques inherited by the automotive domain, together with connection to control centers and tram to tram communication may be used to substitute the human driver.
- Autonomous trams experiments of this kind have already be shown at the last Innotrans fair.

AI

- A sensitive issue on autonomous driving is that advanced capabilities of autonomous decisions (such as artificial vision systems) are often based on Artificial Intelligence techniques that are not easily certifiable with a deterministic approach based on testing or formal verification, and indeed appear to be banned as *Not Recommended* by EN 50128.
- Possibly, the widespread adoption in automotive applications will favour the acceptance of these techniques as “proven in use" software, especially considering that trains move in a much more predictable environment than cars, hence favouring reliability of machine learning techniques.

Conclusions

Conclusions

- **Indeed, nothing is concluded, everything is still to be developed...**
- enjoy your work in this amazing domain!!!

Some advertising....

DisCoRail 2019 - **International Workshop on Distributed Computing in Future Railway Systems**

DisCoRail 2019 is a satellite workshop of DisCoTec 2019,
held on June 17, 2019
at Denmark Technical University (DTU) in Lyngby, Denmark.

`https://www.discotec.org/2019/discorail`

Thanks

- Davide Basile
- Andrea Bonacchi
- Maurice ter Beek
- Laura Carnevali
- Alessio Ferrari
- Stefania Gnesi
- Gloria Gori
- Anne Haxthausen
- Franco Mazzanti
- Andrea Piattino
- Daniele Trentini

SISTER
SIgnalling & Sensing

2014 2020 POR CreO
PROGRAMMA OPERATIVO REGIONALE
CRESCITA e OCCUPAZIONE

Shift2Rail

ASTRail

DITECFER
DISTRICT FOR RAIL TECHNOLOGIES
HIGH SPEED SAFETY & SECURITY