(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 3 929 892 A1

# (12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
**29.12.2021 Bulletin 2021/52**

(21) Application number: **20182410.9**

(22) Date of filing: **26.06.2020**

(51) Int Cl.:
***G08G 1/065*** *(2006.01)* ***G08G 1/0965*** *(2006.01)*
***G08G 1/0967*** *(2006.01)* ***G07B 15/06*** *(2011.01)*

(84) Designated Contracting States:
**AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR**
Designated Extension States:
**BA ME**
Designated Validation States:
**KH MA MD TN**

(71) Applicant: **Hitachi, Ltd.**
**Tokyo 100-8280 (JP)**

(72) Inventors:
- **KOJIMA, Takao**
  **85445 Schwaig-Oberding (DE)**
- **OISHI, Yuji**
  **06560 Valbonne (FR)**
- **KATSUTA, Keiichi**
  **Tokyo, 100-8280 (JP)**
- **OGATA, Takehito**
  **Tokyo, 100-8280 (JP)**

(74) Representative: **MERH-IP Matias Erny Reichl Hoffmann**
**Patentanwälte PartG mbB**
**Paul-Heyse-Strasse 29**
**80336 München (DE)**

## (54) TRAFFIC CONTROL SYSTEM

(57) A Traffic control system 100 for managing the flow of vehicles within a predefined sector of a road, the predefined sector being divided into subsections and the traffic control system having a plurality of traffic control devices 1a-d connected to a network, each traffic control device is configured to control the flow of the traffic in a subsection of the predefined sector and comprises at least one communication unit 20 for receiving or transmitting data from a remotely located communication unit, wherein the communication unit 20 is configured to receive an entry request from a vehicle 10 approaching the subsection before entering said subsection, and transmit one token 2a-d with one entry permission flag 3a-d for said subsection to said vehicle 10 in response to said entry request, if at least one token 2a-d and at least one entry permission flag 3a-d is stored in a data storage space 13 linked to said subsection.

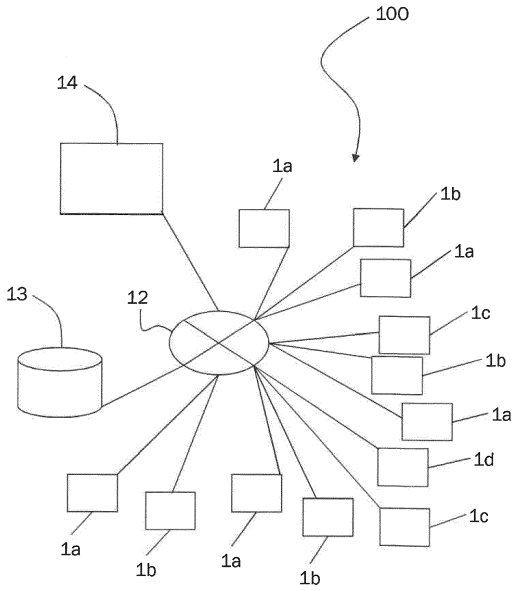



Fig. 1

EP 3 929 892 A1

## Description

**[0001]** The present disclosure relates to a traffic control system for managing the flow of vehicles within a predefined sector of a road, such as a crossing or a round-about, and it relates to a computer program product comprising computer-readable instructions that can be executed in a computer system including one or more computers. In particular, it is provided an automated traffic control for a controlled sector (without traffic lights) which requires reduced/minimal computational and data transmission resources. Preferably, even specific traffic situations can be controlled in which, e.g., emergency vehicles request priority for entering or passing the controlled sector of the road. The safety of the automated traffic control and automated driving is increased, too.

## Background

**[0002]** Traffic flow management especially in urban areas with a high density of traffic is increasingly important for avoiding traffic jams and for ensuring a high level of safety. Automated solutions are known which however require high computational performance/power and which may not cover specific traffic situations (comprehensively) or which require additional high computing resources for handling specific traffic situations. For example, there are systems which predict the future travelling trajectories of all vehicles in a controlled sector or around a controlled sector and which perform a control based on the trajectories for avoiding collisions. Other systems inform autonomously driving vehicles about the presence of an emergency vehicle nearby. The control techniques are described by US 2019/130739A1 and US 2019/302781 A1.

**[0003]** As mentioned above, the required computational resources are immense and specific traffic situations, such as the occurrence of an emergency vehicle or the like, are not reflected or require additional high computational effort.

## Problem and Solution

**[0004]** It is an object of the herein described disclosure to provide a solution which, in particular, includes an automated traffic control system for safely managing the flow of vehicles within a predefined sector of a road and a computer program product which can safely and in an automated manner control the traffic, wherein the required computational resources and the required data transmission resources are minimized, preferably even when handling specific traffic situations. This is solved by the appended claims.

**[0005]** The following aspects may be provided in particular:

A Traffic control system for managing the flow of vehicles within a predefined sector of a road. The controlled sector may be a crossing, a round-about or any other part of a road at which lanes overlap with each other. Further, the sector may also be any part of a road if entry restrictions shall be applied thereto. The predefined sector may be divided into subsections.

**[0006]** The traffic control system may include one or more traffic control devices communicably connected to a network. The network may be any type of network, such as a local area network (LAN), a wide area network (WAN) such as the Internet, a cellular network, a satellite network, or a combination thereof, wired or wireless. The connection may be wireless and/or wire-based. Each of the one or more traffic control devices may be configured to control (manage) the traffic in one or more subsections of the predefined sector, wherein preferably each traffic control device is assigned to one predefined subsection which it controls. Further, each traffic control device may comprise at least one communication unit for receiving or transmitting data. Preferably, the data exchange is performed with a remotely located communication unit wireless. Preferably, the remotely located communication unit is installed in a vehicle, in another traffic control apparatus, or the like.

**[0007]** The communication unit may be configured to receive an entry request from a vehicle approaching the subsection that is controlled by the traffic control device including said communication unit which has received the request. Further, the communication unit may be configured to transmit (issue) one token combined (together with) one entry permission flag for said subsection to the vehicle in response to the entry request. The transmission/issuance is performed if at least one token and at least one entry permission flag is stored in a data storage space associated with (linked to, related to, assigned to, communicably connected to, included in) the traffic control device controlling the subsection for which entry was requested.

**[0008]** Further, the traffic control system may include or may be (communicably) connected to one or more data storage space(s) which may be configured to store one or more tokens and one or more entry permission flags for each subsection of the predefined sector of the road. The tokens may be stored in advance and/or tokens may be created within predefined rules by the traffic control device if needed. The tokens may be a data unit which is not different for different subsections, in other words the tokens are preferably identical or universally usable for the different subsections. The entry permission flag may be another data unit which includes specific information about its validity; specifically, each entry permission flag may be configured to be valid for a predefined (preferably single) subsection and this information may be included in the entry permission flag/data unit. The tokens and entry permission flags (entry permission or permission) may be data strings or data packages and preferably the tokens may be data units which are configured to carry information from a sender to a receiver (data transport vessel/unit) and the entry permission flags preferably may at least include information which

indicate the subsection for which entry is granted. Modified tokens or modifications of tokens are envisaged and are explained further below.

**[0009]** The data storage space may be a physical memory or a database on a physical storage means and it may include databases, tables or the like for storing data, such as the tokens and the permission flags. Preferably, the storage space links each subsection of the sector of the road to a storage sub-space (physical or within a software database).

**[0010]** The traffic control device or the system itself may be configured to increase the number of tokens/entry permission flags (for the respective subsection) in the data storage space if a token/an entry permission flag was received (for the respective subsection). This applies also for the case that a token/entry permission flag was transmitted which results in a decrease of the number.

**[0011]** The token and entry permission system allows creating an entry permission/denial system for the controlled sector of the road including one or more subsections on an automated basis which ensures high safety especially in view of avoiding collisions between vehicles. The complexity and the required computational resources are reduced because there is no need for complex computing tasks, such as determining travelling trajectories or the like. Tokens and permissions are issued like returnable tickets based on which the traffic is managed safely. The system is also flexible with regard to its implementation because the system can be established based on software (except the physical storage and the network including computing resources) only, based on hardware (except the data exchange), or based on a flexibly adjustable combination of both. Data transmission between the communication units is also reduced due to the minimal data information that is required to be exchanged (in particular token and entry permission flag which both can be very small in regard of their data size). Small data size being transferred also increases the reaction times of the system advantageously (reduced latency) which increases the overall control safety even further.

**[0012]** In a further preferred aspect the predefined sector of the road may include overlapping lanes (like in a crossing, an intersection or a round-about), the sector may be divided into subsections and/or each traffic control device may be configured to control/manage the traffic within one predefined subsection of the plurality of subsections. A preferred scenario of application is a crossing or a round-about where preferably each part in which lanes overlap defines a subsection.

**[0013]** The data storage space may be configured to store information about which traffic control device is assigned to (linked to, associated with, related to) control the traffic within which subsection. This may be stored in a table, a database, or any other suitable data format. A vehicle, after it has entered a specific subsection within which the traffic is controlled by a designated traffic control device, may return the received token and the received entry permission flag to another traffic control device, i.e. a different/second traffic control device. Said other traffic control device (second/different) may be configured to return/transmit the entry permission flag returned from the vehicle to the traffic control device that issued the entry permission flag to the vehicle and to forward/transmit a token (any one in its storage or the specific token returned from the vehicle) to a further control device, i.e. a third one.

**[0014]** The above general configuration of the system in which the entry permission flag is returned to the issuing traffic control device while the token is passed on to a further (third) traffic control device allows balancing the number of tokens in each traffic control device (or the data storage space associated therewith) in a simple computer operation while a high safety of the traffic control is ensured. As an example, if the token would be returned to the issuing traffic control device immediately, the traffic within the controlled sector may not be safely controlled, e.g. if a plurality of vehicles request entry to different subsections of the controlled sector of the road.

**[0015]** Further, if considering a scenario in which each subsection of the sector may allow only a single vehicle at the same time, the disclosed system could be configured so that each traffic control device has a single token and entry permission flag. If the token (and the entry permission flag) is issued to a first vehicle, no further token is available so that any further request of a second vehicle will not be granted until the first vehicle has passed the subsection and until the entry permission flag was returned to the issuing traffic control device.

**[0016]** Neatly, the present disclosure allows that the initial/default token distribution can be restored without needing to know which traffic control device has issued a token. Hence, no further computational intelligence needs to be provided which would take care of a correct token distribution. The tokens are "simply" passed to another traffic control device until restoration of the initial/default distribution.

**[0017]** Data traffic can be reduced, computational complexity/resources is/are reduced and a safe handling of the traffic management is established.

**[0018]** In a further preferred aspect the tokens issued by the traffic control devices may be identical to each other, and the entry permission flags may be configured to be valid only for a specific subsection. This supports the above technical advantages, in particular it ensures that an initial configuration of the system can be restored without complex computer operations and without high data communication traffic.

**[0019]** In a further preferred aspect the data storage space may be configured to store information about which traffic control device is assigned to control the traffic within which subsection, wherein each subsection may be labelled (numbered/marked or otherwise characterized) according to a predefined order and each traffic control device may be labelled according to a predefined order. The data storage space may include infor-

mation about which subsection with a specific label is linked to which traffic control device having a specific label. In other words, preferably, the linking between the control unit (traffic control device) and the control target (a specific subsection) is stored in the data storage space and preferably it may be stored in a central database or the like. The order of the subsections and traffic control devices may be exemplified by a crossing. Assuming that two streets each have two lanes which cross each other and assuming that the area in which the two streets cross each other is the controlled sector of the road. Then, as one possible example, the sector may be divided into four subsections, one subsection for each area in which two different lanes overlap each other. Each of the four subsections may be connected/assigned to one traffic control device and each subsection/traffic control device may be labelled according to an order, e.g. a numbering running counter-clockwise or clockwise. E.g., subsection and traffic control device labelled no. 1, subsection and traffic control device labelled no. 2, and so on.

**[0020]** The numbering is storable with low complexity, e.g. in a table connecting the numbers or letters with subsections and traffic control devices.

**[0021]** Preferably, the predefined order is circularly connected/arranged/numbered so that each subsection and each traffic control device of the sector of the road, respectively, is adjacent to one previous and one next subsection and traffic control device, respectively. In the above example, if N subsections/devices would be required in the controlled sector, the subsection/device no. 1 would be stored to be adjacent with the subsections/devices no. N and 2, respectively. The "circular connection/numbering" allows to realize a redistribution of tokens with low complexity and reduced computational efforts.

**[0022]** In a further preferred aspect a vehicle which has entered a subsection m within which the traffic subsection is controlled by a traffic control device N returns the received token and the received entry permission flag to a traffic control device m+1 which is next in the predefined order and which is configured to control the traffic in a next subsection m+1 into which the vehicle may enter. The traffic control device m+1 which has received the token and the entry permission flag of the subsection m may be configured to return/transmit the entry permission flag of subsection m to the traffic control device m that issued said entry permission flag of subsection m and to forward/transmit a token (any token from the storage can be passed on; it may be the same token that was returned from the vehicle) to a further next traffic control device m+2 according to the predefined order, and each further traffic control device may be configured to forward a token until a token is received by the traffic control device which issued a token to the vehicle.

**[0023]** The traffic control device that issued the token is easily identifiable because the connected data storage space includes one token less than it should/it included in the initial distribution setup. In other words, preferably, the traffic control device which issued the token to a vehicle may be identified by the number of tokens in the data storage space.

**[0024]** In a further preferred aspect each traffic control device may include an entry permission control unit configured to grant a vehicle entry into a predefined sector, if said vehicle holds a token combined with an entry permission flag for said sector. Vehicles which do not hold it may be refused to enter a subsection for which they do not have the permission. If the vehicle is an automated or self-driving vehicle, the entry permission control unit may issue a signal to the vehicle's controller including the stop or entry command. If the vehicle is driven by a human, the signal may be displayed to the driver acoustically, optically or the like. Safety is ensured effectively and without requiring high volumes of data transfer.

**[0025]** The entry permission control unit may not be necessary in the traffic control system/device if vehicles include a unit which prevents them from entering a subsection without holding the required entry permission. In automated vehicles the unit may stop the vehicle automatically, while human drivers may be stopped by a warning.

**[0026]** In a further preferred aspect a traffic control device may be configured to issue a token combined with one or more reservation options for one or more subsequent subsections and linked to a specific vehicle. Each traffic control device holding a token with reservation option may issue the token with reservation option only to the vehicle to which said token with reservation option is linked. This allows handling a traffic scenario in which a vehicle requests entry into the controlled sector indicating that not only a single subsection will be crossed, but two or more. The reservation option may be enabled, e.g., by adding an additional data part to the token which includes the information about the reservation and the vehicle for which it was issued.

**[0027]** For example, in the above example according to which a crossing has four subsections: A vehicle which intends to cross the crossing straightly, would have to travel through two subsections. The vehicle may hence request entering the first subsection (the first with regard to its travelling direction) and indicate that it will furthermore need to enter the next subsection (the next in the straight travelling direction) after having passed the first subsection. The request may be automatically transmitted from the vehicle to the traffic control system, e.g. based on the route set in the navigation system or based on a route set by a trajectory planner of an artificial intelligence driver. As a result of the reservation option, the vehicle may smoothly pass the crossing without interruption due to other vehicles or the like. Again, also such a specific driving scenario can be managed without a great increase of the complexity of the control system. The computational resources need not to be increased significantly and the data volume transferred can be kept low. Safety is ensured by the explained configuration at all times.

**[0028]** In a further preferred aspect each traffic control device may include an emergency vehicle priority mode and/or a unit which switches the modes. Alternatively or additionally, the overall system may include such a unit. The unit configured to be activated by an emergency/priority vehicle requesting entry into one or more subsections of the predefined sector of the road. If the emergency vehicle priority mode unit switches the operational mode of the traffic control device to an emergency vehicle priority mode, the traffic control device may be configured to create a temporary token and a temporary entry permission flag which may be issued to the emergency vehicle requesting entry. The temporary token and the temporary entry permission may be different to the tokens and the entry permission flags used in the normal operation mode, ie they may be distinguished, e.g. by adding/modifying the data forming the token/permission. The temporary token may be generated upon the request of the emergency vehicle in the system or the traffic control device to which the request was directed. At the same time, when the request is received from an emergency vehicle, the traffic control device may be configured to check whether it has already issued a (normal) token and an (normal) entry permission flag (e.g., by checking the number of tokens/permissions in the data storage compared to the default/initial number). If it is determined that another (normal, not emergency/priority) vehicle, ie other than the emergency vehicle, holds an entry permission flag for the subsection into which the emergency requires to enter, the traffic control device may be configured to force said vehicle (by issuing a return request) to return said token and the entry permission flag before the temporary token and the temporary entry permission flag is issued to the emergency vehicle. As soon as the token and the entry permission flag is returned to the traffic control device, the traffic control device is configured to issue the temporary token with the temporary entry permission request immediately to the emergency vehicle. The priority/emergency vehicle may be a police car, a fire vehicle, an ambulance vehicle, etc.

**[0029]** The temporary token and the temporary entry permission flag may be transmitted to the next traffic control device when the emergency vehicle has entered the (first) subsection and the next traffic control device may be configured to erase the temporary token and to return the temporary entry permission flag to the traffic control device which has issued the temporary entry permission flag. When the traffic control device which has issued the temporary entry permission flag has received the temporary entry permission flag, it may be configured to erase the temporary entry permission flag and to re-issue any token and any entry permission flag to a vehicle which forcibly returned the token and the entry permission flag before.

**[0030]** Also the specific driving scenario of an emergency or priority vehicle which wants to enter the controlled sector can be managed without a great increase of the complexity of the control system. The computational resources need not to be increased significantly and the data volume transferred can be kept low. Safety is ensured by the explained configuration at all times while the emergency vehicle can pass the sector with high priority.

**[0031]** In a further preferred aspect the temporary token may have a reservation option for one or more further subsections in order to enable a smooth passage of the emergency vehicle through all subsections of the sector which it need to pass on its target travelling route.

**[0032]** In a further preferred aspect the number of tokens and entry permission flags per subsection may be fixed. For example, the fixed predefined number may be set based on the maximum number of vehicles allowed in a subsection. The number may alternatively or additionally variably controlled based on time and density of traffic. In the latter case, it may be possible to increase the number of vehicles in the controlled sector during low traffic times, at sunny daylight conditions or the like while it may be decreased during peak traffic times, during rainy weather or the like.

**[0033]** In a further preferred aspect each traffic control device may include an emergency vehicle priority mode unit configured to be activated by an emergency vehicle requesting entry into one or more subsections of the predefined sector, and, if the emergency vehicle priority mode is activated, the traffic control system/device may be configured to control the occupancy within the predefined sector/subsection of the road. The occupancy may stand for the density of vehicles or the number of vehicles per area.

**[0034]** For occupancy control a maximum occupancy may be determined during the emergency vehicle priority mode. The maximum occupancy may be derived (determined, calculated) from the number of subsections of the predefined sector which will be crossed by the emergency vehicle. The latter may be determined based on the entry request of the emergency vehicle including, e.g. the intended travelling route, and based on the maximum capacity of vehicles inside the predefined sector of the road or a subsection at the same time.

**[0035]** The traffic control system may be configured to stop providing entry permission to a vehicle outside the sector of the road if an actual occupancy is higher than the maximum occupancy, and/or to set or adapt a delay time for the grant of an entry permission depending on the actual occupancy. The occupancy control may allow to manage the traffic situation alternatively or additionally to issuing temporary tokens and permission flags. The technical benefits explained before can be achieved with the occupancy control as well because it does not require complex computing resources, like for a trajectory-based control.

**[0036]** In a further preferred aspect, the above described control system may be realized by a computer program product comprising computer-readable instructions that, when executed in a computer system including one or more computers, cause the computer system to

perform the control as described in relation with one or more of the aspects above.

**Brief Description of Drawings**

**[0037]**

**Fig. 1** schematically shows an example of a traffic control system;

**Fig. 2** schematically shows a traffic control device;

**Fig. 3** schematically shows a vehicle control device;

**Figs. 4 to 8** schematically show a control procedure for a vehicle requesting entry into the controlled sector;

**Figs. 9 to 14** schematically show a modified control procedure including a token having a reservation option;

**Fig. 15** schematically shows a control method/control configuration performed within a traffic control device;

**Fig. 16** shows a sub-process of step S200 performed in the traffic control device;

**Fig. 17** shows the sub-procedure of step S400 performed in a traffic control device;

**Fig. 18** schematically shows a sub-procedure of step S300 performed in a traffic control device;

**Figs. 19 to 23** schematically show a procedure of a modification including an entry request of an emergency vehicle;

**Fig. 24** schematically shows a modification of the procedure according to Fig. 16 in regard of an emergency control mode selection step (S500);

**Fig. 25** shows a sub-procedure of step S500 (control mode selection performed in a traffic control device);

**Fig. 26** shows a modification of step S400 including the emergency/priority mode performed in a traffic control device;

**Fig. 27** schematically shows a sub-procedure of step S300 performed in a traffic control device;

**Figs. 28 to 30** shows a process/configuration of a vehicle-based control device;

**Figs. 31 and 32** schematically show the effect of the emergency mode on the controlled sector and normal vehicles being rejected/unable to enter;

**Fig. 33** schematically shows a modified traffic control device including a traffic density monitoring unit;

**Fig. 34** shows a procedure of controlling the traffic within the controlled sector based on the priority control mode and an acceptance delay of granting a permission to enter;

**Figs. 35 to 38** schematically show a procedure in which an emergency vehicle is given priority access to the controlled sector based on an occupancy control;

**Fig. 39** shows an example of calculating a maximum occupancy within a controlled sector;

**Fig. 40** shows a table of an example for calculating the occupancy within a roundabout including proposed equations for calculating the occupancy.

**Detailed Description of Exemplary Embodiments**

**[0038]** In the following, preferred aspects and examples will be described in more detail with reference to the accompanying figures. Same or similar features in different drawings and examples are referred to by similar reference numerals. It is to be understood that the detailed description below relating to various preferred aspects and preferred examples are not to be meant as limiting the scope of the present disclosure.

**[0039]** Fig. 1 shows an example for a traffic control system 100 as disclosed herein according to which a plurality of traffic control devices 1a-d are connected to a network 12. In this example, one or more of the plurality of traffic control devices 1a-d being connected to the network 12 may be grouped to control one specific sector of a road. The sector being controlled may preferably be a crossing, a roundabout or any other sector of a road in which lanes are overlapping. The number of sectors being controlled by the traffic control system 100 is generally not limited, however, of course, a plurality of traffic control systems 100 can be provided. It is an advantage of the herein described disclosure that traffic lights are not necessary for the sectors being controlled.

**[0040]** Furthermore, one or more data storage spaces 13 are included or communicably connected to the traffic control system 100. Fig. 1 shows one data storage space 13 which may, however, be a plurality or which may be sub-divided into a plurality of sub-units of the data storage space 13. Furthermore, a computing apparatus/unit 14 may be connected to the network 12. The computing apparatus/unit 14 may be a single unit or may include/be a plurality of computing units or sub-units. The traffic control devices 1a-d being shown in Fig. 1 may be implemented by software and/or by hardware.

**[0041]** In the case the traffic control devices 1a-d are implemented by software, these devices 1 may be stored as computer program products within a data storage space such as indicated by reference sign 13 in Fig. 1.

**[0042]** If the traffic control devices 1 are implemented by hardware, they may be installed at the very sector of

the road being controlled by the one or more traffic control devices 1a-d related/associated/assigned to said sector. A combination of a software and hardware implementation is as well possible; for example, a hardware device may be installed at the controlled sector, while a part of its functionality is provided as a computer program product installed at a physical memory of the traffic control device 1a-d or the data storage space 13 connected remotely to the network 12. The computing unit 14 may as well be implemented in each of the traffic control devices 1, especially when the hardware implementation is used. The (communication) connection between the hardware traffic control devices 1 and the network is either established by a wired connection and/or can be enabled via a wireless connection to the network.

**[0043]** Fig. 2 schematically shows one example for the configuration of a traffic control device 1 being implemented as a hardware or a software unit. One module/sub-unit of the traffic control device 1 is a communication unit 20 connected to a data receiving/transmission component 20a. Furthermore, an entry permission control unit 21 may be included in the traffic control device 1, as well. In case of a hardware implementation of the traffic control device, the units 20 and 21 may be implemented within a traffic control device internal memory, while the unit 20a/component 20a may be established by an antenna. In case of a software implementation, the units/components 20, 20a and 21 may be composed of software modules. The functionality of the traffic control device 1 and its sub-units will be described in detail below.

**[0044]** Furthermore, a vehicle which is traveling on the road and which wants to enter a controlled sector, may also be equipped with a vehicle control device 30 which is exemplarily shown by Fig. 3. As it is usually implemented in a vehicle control device 30, it may be connected to sensing unit(s) 34 as well as actuation unit(s) 35 for controlling the driving of the vehicle. These units may be connected with can be a vehicle control unit 33 which is a sub-unit of the vehicle control device 30. Furthermore, in regard of the traffic control system 100 being disclosed herein, the vehicle control device 30 may also include a communication unit 31 as well as an entry permission control unit on the vehicle side 32 and a data receiving/transmitting unit 31a. The units 31, 31a, and 32 may be configured to communicate in a wireless manner with the before described traffic control devices 1a-d. If the traffic control devices 1a-d are not implemented by hardware, but as a software/computer program product, the communication unit 31 of the vehicle may be configured to directly communicate with the network 12 in which the traffic control devices 1a-d are implemented.

**[0045]** Now a control method/configuration being performed/enabled by the traffic control system 100 will be described. The method described may either be claimed by a method claim directly, a computer program product being enabled to perform said method and/or the traffic control system/apparatus being configured to perform the respective method steps.

**[0046]** Figs. 4 and 5 show a first step within a procedure included in the disclosure described herein. In this first step, a (first) vehicle 10a approaches a controlled sector of a road which is in this example a crossing of two roads each having two lanes, wherein the lanes and their driving directions are indicated by short arrows in the middle of each lane. The sector is shown by the virtual circle that is divided into four subsections in this example. The circle is divided by the virtual broken straight lines in the middle of the two roads which also divide the lanes from each other. Of course, other sectors of a road than a crossing may be controlled and of course more or less subsections may be provided for a controlled sector. Returning to the example of Fig. 5, each virtual sub-sector is virtually labeled, wherein the labels are stored in the storage space 13; here the Figures use the exemplary labels "area A", "area B", "area C", and "area D". In Figs. 4 and 5, the vehicle 10a approaching the controlled sector approaches the subsection labeled "area B" which it wants to pass (indicated by the broken arrow ahead of vehicle 10a in Fig. 5). Accordingly, an entry permission for area B needs to be granted to the first vehicle 10a by the traffic control system 100 which is responsible for the crossing shown by Fig. 5.

**[0047]** Figs. 4 and 5 further schematically show that four traffic control devices 1a to 1d are provided for controlling the subsections area A to area D of the controlled sector. In other words, in the traffic control system 100 controlling the depicted sector of a road, each subsection of the sector of the road is controlled by a single traffic control device 1a-1d. Each traffic control device 1a to 1d is assigned to/related to/associated with one specific subsection "area A" to "area D". Furthermore, it is schematically shown that in this example each traffic control device 1a to 1d holds one entry permission (in the following called entry permission flag) 3a to 3d and each traffic control device 1a to 1d holds on token 2a to 2d. This is the default/initial configuration of the exemplary traffic control system 100 when no vehicle is inside the controlled sector. This exemplary traffic control system 100 will be used to describe the present disclosure in more detail. Variations thereof are envisaged, such as providing more or less traffic control devices 1a-1d, providing more than one token or entry permission to each traffic control device 1, and the like.

**[0048]** As soon as the communication unit of the vehicle 31 has issued a request for an entry permission to the traffic control device 1b (Fig. 5 arrow pointing from the vehicle 10a to the device 1b) which is in charge of/assigned to controlling area B of the controlled sector, the traffic control device 1b will issue one token 2b combined with one entry permission flag 3b via the communication unit 20 to the communication unit of the vehicle 31. The transmission of the token with the entry permission flag 2b, 3b (shown as 2b') is shown in Fig. 6, wherein the arrow pointing from the traffic control device 1b to the vehicle 10a indicates the wireless transmission between

these two communication units 20 and 31. As one can see from Fig. 6, the traffic control device 1b does not have any further token or entry permission flag after transmitting one of each to the vehicle 10a.

**[0049]** If the traffic control devices 1 are a hardware implementation, a data storage space/memory within each traffic control device 1 may hold the data relating to the token/entry permission flag. Alternatively, the token and the entry permission flag data/information may also be stored in a central memory/data storage space 13 connected to the network 12 and, more specifically, in a subsection of the data storage space 13 which is specifically linked/related to a traffic control device 1. The related data storage space of subsection "area B" and traffic control device 1b is empty after the transmission of the only token 2b and the only entry permission flag 3b to the vehicle 10a. It is noted that in this example, only a single token and only a single entry permission flag are stored in the data storage space linked to one specific traffic control device 1. However, more than one token and entry permission flag may be stored therein. The latter may be the case if, for example, the subsections, such as "area B", are large enough for taking up more than one vehicle at the same time.

**[0050]** Fig. 7 shows the next step in which the vehicle 10a is allowed to enter the subsection "area B" because it holds the entry permission flag combined with the token issued by the traffic control device 1b being in charge for "area B". Instead of returning the combined token with the entry permission flag 2b' to the traffic control device 1b which issued it to the vehicle 10a, the vehicle 10a transmits the combination of the token and the entry permission flag 2b' to the traffic control device 1c which is in charge of the next area in the predefined order/ in the itinerary/ possible itinerary of the vehicle 10a. The vehicle 10a returns/transmits the combined token and entry permission flag 2b' after it has entered into the area for which the entry permission flag is valid. In this example of Fig. 7, it is subsection "area B". As one can now see in Fig. 8 combined with Fig. 7, the next traffic control device 1c which has received the token 2b from the vehicle 10a temporarily holds two tokens 2b and 2c within its related data storage space/sub-space. Therefore, the traffic control device 1c holds one token more than in the default setup of the traffic control system 100. Therefore, the excess token 2c is transmitted to a next traffic control device in the order of the traffic control devices which is traffic control device 1d in the herein shown in example. Since the tokens 2 are identical to each other, it is only about the total number of tokens being stored in a data storage space 13 related to each traffic control device 1. After having received the token 2 from the traffic control device 1c, the traffic control device 1d would have one excess token and, therefore, transmits one token to the next traffic control device 1a in Fig. 8. The same holds for the traffic control device 1a and, therefore, it transmits the excess token being shown as token 2a in Fig. 8 to the next traffic control device which is the traffic control device 1b in Fig. 8. Since in this example, the traffic control device 1b has originally issued a token to the vehicle 10a, it is short of tokens by one and, therefore, stops circulating the tokens so that the default setup/distribution of tokens is reestablished. Further (preferably at the same time), instead of circulating it, the entry permission flag 3b, which is not identical to the other entry permission flags 3 of other subsections of the controlled sector, is returned to the originally issuing traffic control device 1b. In other words, the entry permission flag 3b being valid for the subsection "area B" having reference sign 3b in Fig. 8 is returned from the traffic control device 1c to the traffic control device 1b which has issued it. With this step, the default distribution/setup of tokens 2 and entry permission flags 3 is reestablished. Since the vehicle 10a has no further entry permission flag to any other subsection of the controlled sector, it either has to stop within the subsection "area B" or it has to leave the subsection "area B" exiting the controlled sector as it is shown in this example depicted by the arrow in Fig. 8.

**[0051]** If the vehicle 10a is an automatically driven vehicle, preferably the vehicle 10a will proceed according to its itinerary which in the depicted case of Figs. 4 to 8 would mean that it automatically leaves the crossing by turning right after having entered the subsection area B. Otherwise, if the vehicle 10a would have an itinerary according to which more than one sector has to be passed, the vehicle 10a will request to an entry permission into the next sector on its itinerary.

**[0052]** The above described control example assumes that the vehicle 10a does not need to pass more than one subsection of the controlled sector. In the following example, the control method is modified to allow the vehicle 10a to travel smoothly through more than one subsection which shall be subsections being labeled as "area B" and "area C" in Fig. 9.

**[0053]** Fig. 9 shows the situation that after having requested entry into the subsection "area B", a token combined with an entry permission flag 2b' was issued by the traffic control device 1b to the vehicle 10a. However, as a modification, the vehicle 10a has indicated to the traffic control device 1b that it needs to enter not only subsection "area B" but also subsection "area C". The indication may be conveniently performed by submitting the itinerary via a navigational system of the vehicle 10a to the communication unit 20 of the traffic control device 1 or it may be requested by a driver. Other options are of course possible, too. Having received the specific request for entering more than one subsection of the controlled sector, a reservation option being indicated by reference sign 6 is added to the data package of the token 2b and the entry permission flag 3b being summarized as 2b' in Fig. 9. The reservation option 6 may be additional data which may, for example, include the information about the specific vehicle (such as an identification number) and the areas for which entry is requested. However, it may also suffice for reducing data transmission/data traffic that only the vehicle ID is included in the reservation option 6.

**[0054]** After the vehicle 10a has entered the first subsection area B and after it has returned the data package including the combination of the token and the entry permission flag 2b' as well as the reservation option 6 to the next traffic control device 1c, Fig. 10 shows the next step(s) according to which the tokens are circulated as described before until each of the other traffic control devices 1d, 1a, and 1b have its original number of tokens. The entry permission flag 3b is returned from the traffic control device 1c to the issuing traffic control 1b as described before. However, the traffic control device 1c holds/maintains the token 2b which has the reservation option 6; i.e. it starts the circulation of tokens 2 based on the token 2c which does not have the reservation option 6. Then, the vehicle 10a, when it is inside the subsection "area B", requests entry into the subsection "area C" to the traffic control device 1c in charge for controlling the traffic within the subsection "area C" (its intended itinerary is shown by the broken arrow in Fig. 10).

**[0055]** In order to highlight the technical effect/benefit of this modified method, it is assumed that in the moment at which the first vehicle 10a requests entry, a second vehicle 10b approaches the area C subsection and requests entry into subsection "area C", too. This is depicted in Fig. 11. In this situation and this example in which only one vehicle can enter a subsection at the same time, the traffic control device 1c can only allow one of the two vehicles 10a, 10b to enter into subsection "area C".

**[0056]** According to the present disclosure, the traffic control device 1c holds the token 2c which is modified by a reservation option 6. The reservation option 6 includes data relating to the ID of the first vehicle 10a. Therefore, the traffic control device 1c easily determines that it may issue/transmit the token 2b including the reservation option 6 to the first vehicle 10a only; i.e. not to the second vehicle 10b. This is shown in Fig. 12 in which it is schematically indicated that the request of the second vehicle 10b is rejected temporarily while a package including the token 2b and the entry permission flag 3c for entering subsection "area C" is transmitted to the first vehicle 10a. In other words, a permission to enter area C is only granted to the vehicle 10a to which the reservation option 6 belongs while all other vehicles are rejected in their attempt to enter the same subsection of the controlled sector at this time.

**[0057]** With the permission granted, the vehicle 10a enters into the subsection "area C" and returns the package of a token including the entry permission flag indicated by 2b' according to the method described before. Fig. 13 shows an example in which the vehicle 10a returns the combination 2b' to the next traffic control device 1d. Then, since the vehicle 10a has requested entry only into the subsection area "area C", the reservation option attached to the token 2b is deleted and the vehicle 10a leaves the controlled sector after subsection "area C". Depending on the format of the request message (or signal), the vehicle may request entry into a plurality of areas at once - in this example, "area B" and "area C"; or one request message (or signal) includes one entry request only and a new request is issued for each area to be entered. The deletion of the reservation option 6 has the consequence that all tokens 2 included in the traffic control system 100 are rendered identical again. The recirculation of tokens 2 is then performed as described before and, as described before as well, the entry permission flag 3c for the subsection "area C" is returned by the traffic control device 1d to the issuing traffic control device 1c. Figure 14 shows: After, the vehicle 10a has left the controlled sector exiting subsection "area C" and after default setup of the traffic control device 1c was restored, the traffic control device 1c can grant the request of the second vehicle 10b by issuing a package of a token and an entry permission flag 2c' for the subsection "area C" so that the second vehicle 10b may enter. The arrows between the second vehicle 10b and the traffic control device 1c show the further request of the second vehicle 10b and the grant thereof.

**[0058]** The above described configuration of the traffic control system 100 allows an automation of vehicle traffic within intersections, roundabouts, etc. which can be used by vehicles driven by a human driver or a machine safely. The exchange of tokens and entry permission flags, which are (small) data strings or packages including the minimum information necessary for the above described procedures, does enable to reduce the size of the data transmission/bandwidth of the connections (and it also reduces the latency times), and to reduce the complexity of the computing operations needed, e.g. it is not necessary that the system 100 or any of the travel control devices 1a-d calculates trajectories of the vehicles or the like. A very safe, ultrafast, and low complex traffic control is enabled which has the options to control even specific traffic situations, which will be further explained below.

**[0059]** The flowcharts related to the before described configuration/method implemented with the traffic control system 100 are now described in connection with Figs. 15 to 18. The steps being described in the following may preferably be performed within the traffic control device 1 and its sub-units, the communication unit 20 and/or the entry permission management unit 21. Communication preferably takes place with the communication apparatus of the vehicle 30 and its sub-units.

**[0060]** Fig. 15 shows a high-level flowchart of steps related to receiving and analyzing a message which is, for example, the entry request received by the communication unit 20 and issued/transmitted from a vehicle's communication unit 31. This is shown as step S101 in Fig. 15.

**[0061]** Further, if it was analyzed that an entry permission is requested, this processed within step S200 and its sub-steps. After step S200, the step S300 (including sub-steps) is performed according to which a token 2 and a permission 3 is returned/issued to a traffic control device 1. Step S300 preferably includes the sub-steps for recirculating tokens 2 and for returning entry permission flags 3 to the respective traffic control devices 1a to 1d

as discussed in connection with the before described Figures. A further step S102 may be added which includes the sending of messages; in this optional setup, when performing steps 200/300 et seq., a message/signal/request is not sent or transmitted. The sending/receiving of a message/signal/request between e.g. communication unit(s) 20 and/or 31 can be performed within/by step(s) S102. If step S102 is not provided, the sending/receiving of messages may also be integrated within the general control flow.

**[0062]** Fig. 16 shows the sub-steps of step S200, especially the analyzation whether entry to a subsection is requested. If this is decided to be positive ("yes" in step S201), the procedure according to the entry permission control related to step S400 and its sub-steps is performed. The sub-steps of step S400 are shown by Fig. 17.

**[0063]** Fig. 17 shows a first step of the entry permission control (step S401) which is to check whether the traffic control device 1 to which the request was transmitted holds an entry permission flag 3 in its related data storage space 13 or its internal memory. If step S401 is decided positively ("yes"), it is determined in step S402 whether a token 2 is stored for said traffic control device 1, too. If this is positively decided ("yes"), it is checked in step S403 whether the available token 2 has a reservation option 6 for a vehicle 10. If this is not the case ("no"), a permission is issued to the vehicle 10 which has requested entry into the specific subsection being controlled by the related traffic control device (in step S407). The permission is preferably granted by submitting a combination of a token 2 and an entry permission flag 3 for the subsection.

**[0064]** If, however, the token 2 is reserved, step S407 cannot be performed and step S404 is performed according to which it is checked whether the reservation option 6 of the token 2 matches with the ID of the vehicle requesting entry. If this is positively decided ("yes"), step S406 is performed which grants, analogously to step S407, a permission for entry to said vehicle. Otherwise, if the IDs do not match, step S405 is performed in which an entry permission request is rejected at least temporarily. The same step S405 is also performed if steps S401 and/or step S402 return a negative result ("no"). In the flowchart it is explained that step S406 returns a permission to the vehicle inside the controlled sector: This is the situation as depicted in Fig. 12 which shows that a traffic control device 1c holds the token 2b with reservation option 6 for the first vehicle 10a.

**[0065]** Furthermore, Fig. 18 shows the control procedure according to the distribution of tokens 2 and permission flags 3 which is used for returning the traffic control system 100 into its default setup after a token 2 and/or an entry permission flag 3 was issued to a vehicle. In a first step S301, the traffic control device 1 (or all traffic control devices 1a-1d of a controlled sector) performing said control checks the number of tokens 2 which it has in stored in its related data storage space 13 and it also verifies if any token 2 is in its possession/storage space which has a reservation option/status 6.

**[0066]** Then, in step S302, information is acquired about returned tokens 2, especially as to a possible reservation request for reserving a token 2 and/or with regard to an entry permission for a target management subsection/area.

**[0067]** In a subsequent step S303, the number of tokens without reservation option 6, i.e. which can be circulated to a next traffic control device 1 as described before, is counted. Based on the above acquired information of steps S301 to S303, it is determined, whether there is any token(s) 2 to be circulated. This is step S304. Should step S304 determine that there are tokens 2 which can be circulated, the step S305 is performed in which non-reserved tokens 2, i.e. tokens 2 without reservation option 6, are passed/transmitted to a next traffic control device 1. After step S305 or if step S304 should return a negative result ("no"), step S306 is performed. In step S306 it is checked whether the traffic control device 1 performing the procedure of steps S300 et seq.. holds an entry permission flag 3 which is not associated/valid for the subsection being linked to said traffic control device 1. If such a "foreign" entry permission flag 3 is detected in the storage related to said traffic control device 1, it is returned with step S307 to the traffic control device 1 to which it belongs (e.g. shown in Fig. 8: device 1c returns flag 3b to device 1b). Otherwise, if only entry permission flags 3 are detected which belong to the controlled subsection of said traffic control device 1, step S308 is performed in which the entry permission flags 3 are kept by said traffic control device 1. If every traffic control device 1 within the traffic control system 100 or at least related to a controlled sector of a road performs this flow of steps, the default/original distribution of tokens 2 and entry permission flags 3 can always be reestablished quickly and without complex computational operations.

**[0068]** Next, a further modification of the above method/control setup is provided in regard of Figs. 19 to 23.

**[0069]** Fig. 19 shows the situation in which a vehicle 10a, which is a normal vehicle such as a passenger car or the like, holds an entry permission flag 3b combined with a token 2b (the combination referenced as 2b') issued by the traffic control device 1b. Hence, said vehicle 10a has the permission to enter the subsection "area B" from its actual position which is inside subsection "area A". In the moment before the vehicle 10a can enter into the subsection "area B", as depicted in Fig. 19, a priority vehicle, such as an emergency vehicle 11, requests entry into the subsection "area B". The request is communicated to the traffic control device 1b as shown by the arrow from the emergency vehicle 11 to the traffic control device 1b. In a situation as described before or in case that the emergency vehicle 11 would not be an emergency vehicle 11, but a second vehicle 10b, the request would be denied by the traffic control device 1b because it does not have any further token or entry permission flag available (in Fig. 19 the traffic control device is sche-

matically shown "empty"). The only entry permission flag 3b and token 2b combined (2b') is in possession of the vehicle 10a which is driving within subsection "area A". Therefore, it would not be possible to give priority to the emergency vehicle 11 which would result in adversary effects possibly to a person who needs quick medical assistance or the like.

**[0070]** Therefore, Fig. 20 depicts a modification relating to an emergency mode which may be activated by a not depicted emergency mode setting unit (which may be part of each traffic control device 1 or of the overall system 100). In the emergency mode, which is triggered by a request of an emergency vehicle 11, the following procedure is preferably followed. The traffic control device 1b to which the request of the emergency vehicle 11 was transmitted in this example issues a command/request to the vehicle 10a which possesses the permission for entering the controlled subsection. The request as indicated by the arrow between the control device 1b and the vehicle 10a in Fig. 20 includes the command to return the token 2b including the entry permission flag 3b to the issuing traffic control device 1, which is 1b in this example. In addition, in the emergency mode, the traffic control device 1b is enabled to temporarily create/generate a temporary token 4 including a temporary entry permission flag T being shown by reference sign 4b' in Fig. 20.

**[0071]** As shown in Fig. 21, as soon as the vehicle 10a has returned the entry permission flag including the token 2b' upon request of the traffic control device 1b (see arrow and reference sign 2b'), the temporary token including the temporary permission flag 4b' is transmitted to the emergency vehicle 11 (see the arrow and reference sign 4b'). As a consequence, the emergency vehicle 11 can immediately enter the subsection controlled by the traffic control device 1b which is subsection "area B", while the normal vehicle 10a has to stop and wait in the subsection "area A".

**[0072]** As previously described in the normal mode, the emergency vehicle 11 returns the package 4b' including the temporary token 4 and the temporary entry permission flag T to the next entry permission device 1c. This is depicted by the respective arrow in Fig. 22.

**[0073]** Fig. 23 displays the moment when the emergency vehicle 11 has returned the temporary token 4 including the temporary entry permission flag T to the traffic control device 1c which, upon receiving it, returns the temporary entry permission flag 5b to its issuing traffic control device 1b and deletes the temporary token 4b after it has received it.

**[0074]** As a further modification, if the temporary token 4b has a reservation option 6 (not shown), the token will not be deleted in accordance with the flow of steps as described before. The token 4b will only be deleted, if it has a reservation option 6, after the reservation option 6 is "consumed".

**[0075]** As further shown by Fig. 23, as soon as the temporary token T is received by its issuing traffic control device 1b, it is deleted within said traffic control device 1b and the traffic control device 1b can reissue a normal token 2b and entry permission flag 3b for the subsection "area B" to the normal vehicle 10a (see respective arrow).

**[0076]** With the above modification, it is possible that an emergency vehicle 11 is given priority without increasing the computational complexity/system complexity. The temporary token 4b may be issued with a reservation option analogously to the above described modification including the reservation option in case that the emergency vehicle 11 should request entering more than one subsection of the controlled sector.

**[0077]** The flowcharts of Figs. 24 to 27 illustrate the modifications to the method/control configuration if the emergency mode option is available. Specifically, Fig. 24 illustrates that a further step S500 including a control mode selection process is provided before entry permissions requests are checked in step S201.

**[0078]** The procedure of steps S500 following is illustrated by Fig. 25 which shows that in a step S501 it is determined whether the request was issued from a high priority vehicle, such as an emergency vehicle 11. If this is decided negatively ("no"), it is decided in step S503 whether there is already a temporary token 4 (that means that there is no emergency vehicle inside this section if the answer "no"; an 'in-use'flag is hence not set). If step S503 is decided with "no", the control mode is decided to be "normal" in step S504; i.e. no 'in-use' is flagged by the system. Otherwise, if in step S501, it is determined that a priority vehicle is requesting entry, step S502 is performed in which a temporary token 4 and a temporary entry permission flag T is added to the traffic control device 1 and its data storage space, respectively, and the control mode is switched to "emergency mode" in the next step S505. The same holds if in step S503 it is found positively that temporary tokens are existing (remaining) so that the emergency mode is activated in step S505.

**[0079]** Further, as a modification to the sub-steps including the steps S400 following, Fig. 26 shows modifications for enabling the emergency mode. Before the entry permission checking described in connection with the normal operation mode (step S401) is performed, steps S408 and S409 are processed according to which it is decided whether a priority vehicle requests entry (step S408). If this is not the case, it is decided as to whether temporary tokens 4 and entry permission flags T are already in use (step S409). If temporary tokens 4 and temporary entry permission flags T are already in use ("yes" in step S409), the request is rejected in step S405 because there is already an emergency/priority vehicle 11 inside the controlled sector; if it is defined that only one temporary token 4 and temporary entry permission flag T is allowed to be issued for the controlled sector.

**[0080]** Furthermore, as a difference to the before discussed control steps of step S400, step S410 is performed if in step S408 it was found that a priority vehicle has requested entry. Step S410 firstly asks/determines whether the traffic control device 1 has a normal entry permission 3 in its related storage (like S400 described

above) and if this is answered with "yes", a temporary entry permission flag T including a temporary token 4 is sent to the emergency vehicle 11 in step S411. Further, a status of the system that generates a temporary token 4 and a temporary entry permission flag T is switched to "in use" in step S412 (which means that an 'in-use'-flag is set) in order to avoid that another (normal) vehicle 10a may receive a grant for entry as long as the emergency vehicle 11 is within the designated subsection.

**[0081]** Otherwise, if it is found in step S410 that the traffic control device 1 to which the request was issued by the priority vehicle /emergency vehicle 11 does not have any normal tokens 2/normal entry permission flags 3 in possession (stored in the memory/data storage space 13) (or less than it has in the default setting), which means that a normal vehicle 10a already holds a permission to drive into the subsection, step S413 is performed according to which the normal entry permission flag 3 and its token 2 are demanded to be returned from the normal vehicle 10a holding them, as described before. The request from the priority vehicle 11 to enter the respective subsection is rejected in S414 as long as the normal entry permission flag 3 and its token 2 are not returned by the normal vehicle 10a; in other words, as soon as (but not before) they are returned the grant can be issued to the emergency vehicle 11 in S411.

**[0082]** Furthermore, an emergency mode checking step S415 is added which takes place after step S403 if this step S403 delivers that no reserved token 2 is available. If no reserved token 2 is available ("no" in step S403), and if in step S415, it is found that an emergency mode is active, any request from a normal vehicle 10 is rejected in step S416 while, if the emergency mode is inactive ("no" in step S415), a permission to enter the controlled subsection is granted.

**[0083]** Furthermore, with regard to the redistribution/recirculating of tokens 2 and entry permission flags 3, a modification to the sub-steps of step S300 is shown in Fig. 27, if the emergency mode is included in the traffic control system 100. Specifically, in step S302, it is additionally asked which kind of token 2 is returned (normal or temporary). Further, before step S303 and after step S302, another decision is added by step S309 which checks whether the returned token is a temporary token 4. If this is not the case ("no"), the normal operation following step S303 as described before is processed. Otherwise, if step S309 returns "yes", step S310 is performed asking whether the returned temporary token 4 is reserved. If the temporary token 4 is reserved (i.e. it has a reservation option 6), step S312 is performed which means that the temporary token 4 and the related entry permission flag T are kept so that no circulation/redistribution for this token is performed. Otherwise, should step S310 find that the temporary token 4 is not reserved, step S311 performs erasing of the temporary token 4 and its permission /entry permission flag T (which also means that the 'in-use'-flag may be cleared/erased).

**[0084]** Figs. 28 to 30 show a procedure of the control included in the vehicle control device 30; the vehicle control device 30 may be included in the traffic control system 100. Fundamentally, the procedure as shown in Fig. 28 mirrors the procedure on the "infrastructure side" so that a step S601 receives messages which are analyzed by the communication unit 31. Then, vehicle and map information are acquired by and within step S602, e. g. from the sensing unit 35 or the like of the vehicle 10. Map information may relate to the information included or generated by a navigation device (not shown), e.g. it may include itineraries, positional data, and the like. In step S700, the request for an entry permission to a traffic control device 1 is issued and in step S800 a token 2 and an entry permission flag 3 are returned to a traffic control device. Messages may be sent as shown in step S603 in correspondence with the description of S102. The substeps of step S700 are explained in Fig. 29.

**[0085]** Fig. 29: In step S701 it is determined whether the vehicle 10 is inside a controlled sector, such as an intersection or a crossing. Should the answer be "no", it is determined, whether a distance to said controlled sector is smaller than a predefined distance D (step S702). Should the intersection be farer away than the predefined distance D, step S703 is performed according to which a request to enter a subsection is issued to the respective/responsible traffic control device 1 of said subsection (such as traffic control device 1b in Fig. 5). Furthermore, should step S701 find that the vehicle 10 is already inside the controlled sector or a subsection thereof, step S704 determines whether the vehicle 10 (or its driver) has the plan to proceed within the controlled sector or not. If this should be the case, step S705 is performed and a reservation right/option 6 for the next subsection is requested.

**[0086]** As a modification to Fig. 29 and its flowchart shown therein, step S701 is not necessarily included if a reservation option 6 is not used in the traffic control system 100.

**[0087]** Furthermore, the subs-steps of steps S800 are depicted in Fig. 30 which are performable within a vehicle control device 30. The process includes the returning of a token 2 and an entry permission flag 3 to a traffic control device 1. It is determined in step S801 whether the vehicle 10 is inside the controlled sector. If this is not the case, this procedure is stopped. If it is found that the vehicle 10 is inside the controlled sector, in step S802, it is checked whether a traffic control device 1 has issued a request to return an entry permission flag 3 as well as a token 2 which was already issued to said vehicle 10. This is the case, if an emergency vehicle 11 switched the traffic control system 100 to the emergency mode. If in step S802 the answer is "no", step S803 is performed in which it is determined whether the vehicle shall exit the subsection in which it is driving presently or not. If it is decided "yes", step S804 returns the entry permission 3 including the token 2 without a reservation option 6. Otherwise, if step S805 is performed, the entry permission flag 3 and token 2 with reservation option 6 is returned.

If furthermore, in step S802, it is determined that there is a request present from a traffic control device 1 which demands the return of an entry permission flag 3 and a token 2, step S806 is performed. It is decided in step S806 whether it is possible to safely stop within the subsection in which the vehicle 10 is travelling at this moment. If this is the case, in step S807, the permission 3 is returned (with reservation option 6), while in step S808, the returning of the entry permission 3 and of the token 2 is rejected. In optional step 806 it may be found that the vehicle 10 has to perform an emergency braking or may not be able to stop in time, then the vehicle 10 may rather pass keep the entry permission; i.e. in this case the emergency vehicle 11 would have to wait and may pass the subsection briefly afterwards.

**[0088]** The effects achieved by the control including an emergency vehicle more are schematically depicted in Figs. 31 and 32. Both Figures show a virtual "stop sign" indicated by the filled black areas which cannot be passed by the normal vehicles 10a to 10d when the emergency vehicle 11 needs to enter the controlled sector. The emergency vehicle 11 has a "pass signal" indicated by the hatched area. Hence, for example, it is a technical advantage that the emergency vehicle 11 may quickly enter into the controlled sector, even though another normal vehicle 10a (see Fig. 31) holds an entry permission flag for the same subsection into which the emergency vehicle 11 needs to enter. This also applies for the case of many vehicles 10a to 10d which are inside or outside the controlled sector. They can be reliable prevented to enter the controlled sector or subsections thereof, through which the emergency vehicle 11 needs to pass. The technical implementation allows that the entire automated handling/coordination can be performed safely with minimum requirements in regard of communication bandwidth and computational resources. The control exhibits low latencies, inter alia, because of the small data packages which are exchanged.

**[0089]** A further modification option for prioritizing an emergency vehicle 11, i.e. giving it priority access to the controlled sector, is enabled by adding a traffic density monitoring unit 22 to the traffic control device 1. The traffic density monitoring unit 22 may be connected to a respective sensing unit 23 (Fig. 33). The sensing unit 23 may include a camera which monitors the traffic and it may be supported by an artificial intelligence that detects vehicles, roads, infrastructure and other traffic-relevant objects. Based on the modification of the traffic control device as shown by Fig. 33, instead of or in addition to the before described procedure including the generation of a temporary token 4 and a temporary entry permission flag T, an occupancy rate can be used to control the traffic within the controlled sector and for providing access priority to the emergency vehicle 11.

**[0090]** A first example is shown by Fig. 34 which shows possible timings for requesting and granting entry permissions to vehicles 10. Here, "[R]" indicates the timing of entry request and "[G]" indicates the timing of the grant of said request. The horizontal arrows indicate a time axis. In a normal traffic situation without an emergency vehicle 11 requesting entry to the controlled sector/a subsection thereof, a request is issued and after a very short communication caused delay, the request is granted if the token 2 and an entry permission flag 3 is available. This is depicted in the upper part of Fig. 34 and the communication caused delay is shown by the hatched areas. However, if it is switched to a priority/emergency control mode, as shown in the lower part of the schematic Figure 34, a request is not instantly granted and a delay time is added on purpose. The delay time (shown by the filled black areas) may be a predetermined delay time or a delay time being calculated for each situation depending on the present occupancy within the controlled sector. By delaying a grant to a normal vehicle 10 within or outside the controlled sector, the occupancy within the controlled sector can be reduced to such a degree that an emergency vehicle 11 can safely pass through the subsections of the controlled sector as requested.

**[0091]** Instead of or in addition to adapting the delay time, it may also be possible to force vehicles 10 inside the controlled sector to leave it on the shortest route and/orto stop issuing entry permissions to the controlled sector. Generally, the situation of an occupancy adjustment/control in an emergency case is depicted by Figs. 35 and following. Assuming that, as shown in Fig. 35, an emergency vehicle requests entry to the traffic control system 100, for example, if traffic control devices 1 are implemented only by software, the request is directly transmitted to the network 12. Then, as soon as the emergency mode is switched on, traffic density adjustment will be performed. One option of adjustment was described in connection with Figure 34 above. Another option is described as follows. The options may be combined.

**[0092]** Fig. 36 shows general considerations for an occupancy adjustment within a controlled sector. As shown in the left part of Fig. 36, an emergency vehicle 11 may need to pass the subsections "area C" and "area D" (indicated by the long unbroken arrow; the "areas A to D" are abbreviated as "A" to "D"). That means, it will have to pass two subsections of the controlled sector which has four subsections in this example. Then, it is assumed that a certain percentage of occupancy should not be exceeded so that the emergency vehicle 11 can smoothly and safely pass the controlled sector. This situation is further schematically explained by the right side part of Fig. 36. This part shows the subsections linearly aligned starting with the subsection which will be entered first by the emergency vehicle 11. In this example, subsection C would be first followed by subsections D, A, and B. Since it is a circular arrangement of subsections, the subsections B and C are shown again on the left and right side of this linear arrangement. Further, the filled black areas indicate the "stop signal" for entering this lane/subsection and the hatched areas indicate that passing is allowed. The areas with a quadratic black and white filling

indicate that these subsections may be used for adjustment of occupancy if needed.

**[0093]** Since the emergency vehicle will pass through subsections C and D, these two subsections need to be free of other vehicles; it will not pass subsections A and B so that other vehicles may be inside the subsections A and B. In other words, the maximum occupancy can be calculated based on 100% minus the maximum occupancy X% of the subsections A and B. As an example, if six normal vehicles 10a to 10f are inside the controlled sector and its controlled subsections and, hence, 57.30% (see Fig. 38) are occupied according to a calculation which is described later, one can find that, if the vehicles 10a-f are evenly distributed over the subsections as shown in the right side of Fig. 37, the occupancy rate would need to be reduced in accordance with the scheme as shown in Fig. 38. In other words, it could be found that five vehicles 10a to 10e are allowable within the controlled sector (subsection A and B would be filled), while the sixth vehicle 10f in this example is exceeding the allowable/maximum occupancy rate in the controlled sector. Therefore, the occupancy rate in the situation depicted by Fig. 37 would have to be reduced so that the emergency vehicle 11 can smoothly pass areas C and D on its intended route indicated by the bold black arrows.

**[0094]** The occupancy rate may be calculated as shown in Fig. 39 by determining the vehicle body length LB, a safety margin $L_M$, and a vehicle breaking distance

$$d_{brk} = \frac{v^2}{2a_{brk}}$$

as well as the assumed radius of the controlled sector and the number of subsections. A maximum number of vehicles 10a to 10j may look like it is shown in the right side part of Fig. 39. Then, based on the equations and example shown in Fig. 40, the occupancy rate can be determined.

**[0095]** In the example with the example values of Fig. 40 (right column), a maximum of 10.472 vehicles is possible in the example sector which means a maximum of 2.618 vehicles per subsection. Now, assuming based on Fig. 36, that at least two free areas are required so that the emergency vehicle 11 can pass from area C to D safely, one can find that a maximum of five vehicles (47.7% occupancy rate) may be allowed inside the controlled sector for fulfilling the requirement. This is calculated based on the maximum number of vehicles within one subsection and the number of subsections in which vehicles are allowable. In this example, two areas of four need to be free and two areas can be occupied by other vehicles and each area may hold 2.618 vehicles per subsection.

**[0096]** In the example as shown in Fig. 38, the number of five vehicles within the controlled sector would result in an occupancy rate of 47.7 % which is admissible because two free subsections areas A and B are provided. However, with the sixth vehicle 10f within the controlled sector, an occupancy rate of 57.3 % is returned which is too high so that a specific procedure would have to be applied for reducing the occupancy rate. In other words, in the scenario as shown in Fig. 38, with six vehicles 10a to 10f inside the controlled sector, the vehicle no. 6 (10f) would block a part of subsection D, if all other vehicles 1 to 5 (10a- e) are adjusted to be driven inside subsections A and B which the emergency vehicle 11 does not need to pass or to leave the controlled sector.

**[0097]** In the above case the sixth vehicle 10f which is too much for the controlled sector and since it is inside the controlled sector already, it would be possible to force the sixth vehicle 10f to leave the controlled sector or to stop permitting other vehicles 10 to enter the controlled sector so that the number of vehicles 10 inside the controlled sector can decrease to an allowable occupancy rate before the emergency vehicle 11 enters the controlled sector.

**[0098]** If the number of vehicles 10 inside the controlled sector is below the maximum occupancy rate, two options are preferred which are also combinable and which are applicable within the traffic control system 100 for keeping the occupancy rate below the maximum occupancy rate for the safe passage of the emergency vehicle. A first possibility in this regard is that the occupancy rate is kept below the maximum occupancy rate /threshold by stopping each normal vehicle requesting to enter the controlled sector. The second option is as described in connection with Fig. 34 that a delay time is set or adjusted for the returning of a grant for an entry permission flag based on the occupancy rate so that the occupancy rate can be kept over the time below the maximum occupancy rate as long as the emergency mode is active.

**[0099]** The present disclosure allows to provide an automated traffic control for a controlled sector which needs reduced/minimal computational resources and data transmission resources. Even specific traffic situations can be controlled in which, e.g., emergency vehicles request priority for entering or passing the controlled sector of the road. The safety of the automated traffic control and automated driving is increased.

**[0100]** Aspects/Examples of the present disclosure may be a software entirely (including firmware, resident software, micro-code, etc.), or a combination of software and hardware aspects that may be referred to as a "system". Furthermore, the present disclosure may take the form of a computer program product on a computer-readable medium having computer-executable program code embodied in the medium.

**[0101]** It should be noted that arrows may be used in drawings to represent communication, transfer, or other activity involving two or more entities. Double-ended arrows generally indicate that activity may occur in both directions (e.g., a command/request in one direction with a corresponding reply back in the other direction, or peer-to-peer communications initiated by either entity), although in some situations, activity may not necessarily occur in both directions.

**[0102]** Single-ended arrows generally indicate activity

exclusively or predominantly in one direction, although it should be noted that, in certain situations, such directional activity actually may involve activities in both directions (e.g., a message from a sender to a receiver and an acknowledgement back from the receiver to the sender, or establishment of a connection prior to a transfer and termination of the connection following the transfer). Thus, the type of arrow used in a particular drawing to represent a particular activity is exemplary and should not be seen as limiting.

**[0103]** The present disclosure may be described with reference to flowchart illustrations and/or block diagrams of methods and apparatuses, and with reference to a number of sample views of a graphical user interface generated by the methods and/or apparatuses. It will be understood that each block of the flowchart illustrations and/or block diagrams, and/or combinations of blocks in the flowchart illustrations and/or block diagrams, as well as the graphical user interface, can be implemented by computer-executable program code.

**[0104]** The computer-executable program code may be provided to a processor of a general purpose computer, special purpose computer, or other programmable data processing apparatus to produce a particular machine, such that the program code, which executes via the processor of the computer or other programmable data processing apparatus, create means for implementing the functions/acts/outputs specified in the flowchart, block diagram block or blocks, figures, and/or written description.

**[0105]** The computer-executable program code may also be stored in a computer-readable memory that can direct a computer or other programmable data processing apparatus to function in a particular manner, such that the program code stored in the computer readable memory produce an article of manufacture including instruction means which implement the function/act/output specified in the flowchart, block diagram block(s), figures, and/or written description.

**[0106]** The computer-executable program code may also be loaded onto a computer or other programmable data processing apparatus to cause a series of operational steps to be performed on the computer or other programmable apparatus to produce a computer-implemented process such that the program code which executes on the computer or other programmable apparatus provides steps for implementing the functions/acts/outputs specified in the flowchart, block diagram block(s), figures, and/or written description. Alternatively, computer program implemented steps or acts may be combined with operator or human implemented steps or acts in order to carry out an embodiment of the disclosure.

**[0107]** It should be noted that terms such as "server" and "processor" may be used herein to describe devices that may be used in certain aspects of the present disclosure and should not be construed to limit the present disclosure to any particular device type unless the context otherwise requires. Thus, a device may include, without limitation, a bridge, router, bridge-router (brouter), switch, node, server, computer, appliance, or other type of device. Such devices typically include one or more network interfaces for communicating over a communication network and a processor (e.g., a microprocessor with memory and other peripherals and/or application-specific hardware) configured accordingly to perform device functions.

**[0108]** Communication networks generally may include public and/or private networks; may include local-area, wide-area, metropolitan-area, storage, and/or other types of networks; and may employ communication technologies including, but in no way limited to, analog technologies, digital technologies, optical technologies, wireless technologies (e.g., Bluetooth), networking technologies, and internetworking technologies.

**[0109]** It should also be noted that devices may use communication protocols and messages (e.g., messages created, transmitted, received, stored, and/or processed by the device), and such messages may be conveyed by a communication network or medium.

**[0110]** Unless the context otherwise requires, the present disclosure should not be construed as being limited to any particular communication message type, communication message format, or communication protocol. Thus, a communication message generally may include, without limitation, a frame, packet, datagram, user datagram, cell, or other type of communication message.

**[0111]** Unless the context requires otherwise, references to specific communication protocols are exemplary, and it should be understood that alternatives may, as appropriate, employ variations of such communication protocols (e.g., modifications or extensions of the protocol that may be made from time-to-time) or other protocols either known or developed in the future.

**[0112]** It should also be noted that logic flows may be described herein to demonstrate various aspects of the disclosure, and should not be construed to limit the present disclosure to any particular logic flow or logic implementation. The described logic may be partitioned into different logic blocks (e.g., programs, modules, functions, or subroutines) without changing the overall results or otherwise departing from the true scope of the disclosure.

**[0113]** Often, logic elements may be added, modified, omitted, performed in a different order, or implemented using different logic constructs (e.g., logic gates, looping primitives, conditional logic, and other logic constructs) without changing the overall results or otherwise departing from the scope of the disclosure.

**[0114]** The present disclosure may be embodied in many different forms, including, but in no way limited to, computer program logic for use with a processor (e.g., a microprocessor, microcontroller, digital signal processor, or general purpose computer), programmable logic for use with a programmable logic device (e.g., a Field Programmable Gate Array (FPGA) or other PLD), discrete components, integrated circuitry (e.g., an Application

Specific Integrated Circuit (ASIC)), or any other means including any combination thereof Computer program logic implementing some or all of the described functionality is typically implemented as a set of computer program instructions that is converted into a computer executable form, stored as such in a computer readable medium, and executed by a microprocessor under the control of an operating system. Hardware-based logic implementing some or all of the described functionality may be implemented using one or more appropriately configured FPGAs.

**[0115]** Computer program logic implementing all or part of the functionality previously described herein may be embodied in various forms, including, but in no way limited to, a source code form, a computer executable form, and various intermediate forms (e.g., forms generated by an assembler, compiler, linker, or locator).

**[0116]** Source code may include a series of computer program instructions implemented in any of various programming languages (e.g., an object code, an assembly language, or a high-level language such as Fortran, C, C++, JAVA, JavaScript or HTML) for use with various operating systems or operating environments. The source code may define and use various data structures and communication messages. The source code may be in a computer executable form (e.g., via an interpreter), or the source code maybe converted (e.g., via a translator, assembler, or compiler) into a computer executable form.

**[0117]** Computer-executable program code for carrying out operations of embodiments of the present disclosure may be written in an object oriented, scripted or unscripted programming language such as Java, Perl, Smalltalk, C++, or the like. However, the computer program code for carrying out operations of aspects of the present disclosure may also be written in conventional procedural programming languages, such as the "C" programming language or similar programming languages.

**[0118]** Computer program logic implementing all or part of the functionality previously described herein may be executed at different times on a single processor (e.g., concurrently) or may be executed at the same or different times on multiple processors and may run under a single operating system process/thread or under different operating system processes/threads.

**[0119]** Thus, the term "computer process" refers generally to the execution of a set of computer program instructions regardless of whether different computer processes are executed on the same or different processors and regardless of whether different computer processes run under the same operating system process/thread or different operating system processes/threads.

**[0120]** The computer program may be fixed in any form (e.g., source code form, computer executable form, or an intermediate form) either permanently or transitorily in a tangible storage medium, such as a semiconductor memory device (e.g., a RAM, ROM, PROM, EEPROM, or Flash-Programmable RAM), a magnetic memory device (e.g., a diskette or fixed disk), an optical memory device (e.g., a CD-ROM), a PC card (e.g., PCMCIA card), or other memory device.

**[0121]** The computer program may be fixed in any form in a signal that is transmittable to a computer using any of various communication technologies, including, but in no way limited to, analog technologies, digital technologies, optical technologies, wireless technologies (e.g., Bluetooth), networking technologies, and internetworking technologies.

**[0122]** The computer program may be distributed in any form as a removable storage medium with accompanying printed or electronic documentation (e.g., shrink wrapped software), preloaded with a computer system (e.g., on system ROM or fixed disk), or distributed from a server or electronic bulletin board over the communication system (e.g., the Internet or World Wide Web).

**[0123]** Hardware logic (including programmable logic for use with a programmable logic device) implementing all or part of the functionality previously described herein may be designed using traditional manual methods, or may be designed, captured, simulated, or documented electronically using various tools, such as Computer Aided Design (CAD), a hardware description language (e.g., VHDL or AHDL), or a PLD programming language (e.g., PALASM, ABEL, or CUPL).

**[0124]** Any suitable computer readable medium may be utilized. The computer readable medium may be, for example but not limited to, an electronic, magnetic, optical, electromagnetic, infrared, or semiconductor system, apparatus, device, or medium.

**[0125]** More specific examples of the computer readable medium include, but are not limited to, an electrical connection having one or more wires or other tangible storage medium such as a portable computer diskette, a hard disk, a random access memory (RAM), a read-only memory (ROM), an erasable programmable read-only memory (EPROM or Flash memory), a compact disc read-only memory (CD-ROM), or other optical or magnetic storage device.

**[0126]** Programmable logic may be fixed either permanently or transitorily in a tangible storage medium, such as a semiconductor memory device (e.g., a RAM, ROM, PROM, EEPROM, or Flash-Programmable RAM), a magnetic memory device (e.g., a diskette or fixed disk), an optical memory device (e.g., a CD-ROM), or other memory device.

**[0127]** The programmable logic may be fixed in a signal that is transmittable to a computer using any of various communication technologies, including, but in no way limited to, analog technologies, digital technologies, optical technologies, wireless technologies (e.g., Bluetooth), networking technologies, and internetworking technologies.

**[0128]** The programmable logic may be distributed as a removable storage medium with accompanying printed or electronic documentation (e.g., shrink wrapped software), preloaded with a computer system (e.g., on sys-

tem ROM or fixed disk), or distributed from a server or electronic bulletin board over the communication system (e.g., the Internet or World Wide Web). Of course, some embodiments of the disclosure may be implemented as a combination of both software (e.g., a computer program product) and hardware. Still other aspects of the present disclosure are implemented as entirely hardware, or entirely software.

**[0129]** While certain exemplary aspects have been described and shown in the accompanying drawings, it is to be understood that such embodiments are merely illustrative of and are not restrictive on the broad disclosure, and that the aspects of the present disclosure are not limited to the specific constructions and arrangements shown and described, since various other changes, combinations, omissions, modifications and substitutions, in addition to those set forth in the above paragraphs, are possible.

**[0130]** Those skilled in the art will appreciate that various adaptations, modifications, and/or combination of the just described aspects and examples can be configured. Therefore, it is to be understood that, within the scope of the appended claims, the disclosure may be practiced other than as specifically described herein. For example, unless expressly stated otherwise, the steps of processes described herein may be performed in orders different from those described herein and one or more steps may be combined, split, or performed simultaneously.

**[0131]** Those skilled in the art will also appreciate, in view of this disclosure, that different aspects or examples of the disclosure described herein may be combined to form other aspects or examples of the disclosure.

## Claims

1. A Traffic control system (100) for managing the flow of vehicles within a predefined sector of a road, the predefined sector being divided into subsections and the traffic control system having a plurality of traffic control devices (1a-d) connected to a network, each traffic control device is configured to control the flow of the traffic in a subsection of the predefined sector and comprises
   at least one communication unit (20) for receiving or transmitting data from a remotely located communication unit, wherein the communication unit (20) is configured to

   receive an entry request from a vehicle (10) approaching the subsection before entering said subsection, and
   transmit one token (2a-d) with one entry permission flag (3a-d) for said subsection to said vehicle (10) in response to said entry request, if at least one token (2a-d) and at least one entry permission flag (3a-3d) is stored in a data storage space (13) linked to said subsection;

   the traffic control system (100) further including said data storage space (13) configured to store one or more tokens (2a-2d) and one or more entry permission flags (3a-d), wherein receiving a token (2a-d) or an entry permission flag (3a-d) increases the number of tokens (2a-d) or entry permission flags (3a-d) in said data storage (13), respectively, and transmitting a token (2a-d) or an entry permission flag (3a-d) reduces the number of tokens (2a-d) or entry permission flags (3a-d) in said data storage (13), respectively.

2. The traffic control system according to claim 1, **characterized in that** the predefined sector of the road includes overlapping lanes, the sector is divided into subsections and each traffic control device (1a-d) is configured to control the traffic within one subsection of the plurality of subsections, and
   the data storage space (13) is configured to store information about which traffic control device (1a-d) is assigned to control the traffic within which subsection; and
   a vehicle (10) which has entered a subsection within which the traffic is controlled by a traffic control device (1a-d) returns the received token (2a-d) and the received entry permission flag (3a-3d) to another traffic control device (1a-d), wherein
   said other traffic control device (1a-d) is configured to transmit the entry permission flag (3a-d) returned from the vehicle (10) to the traffic control device (1a-d) that had issued the entry permission flag (3a-d) and to forward a token (2a-d) to a further control device (1a-d).

3. The traffic control system according to at least one of claims 1 to 2, **characterized in that** the tokens (2a-d) issued by the traffic control devices (1a-d) are identical to each other, and the entry permission flags (3a-d) are configured to be valid for a specific subsection.

4. The traffic control system according to at least one of claims 1 to 3, **characterized in that** the data storage space (13) is configured to store information about which traffic control device (1a-d) is assigned to control the traffic within which subsection, wherein each subsection is labelled according to a predefined order and each traffic control device (1a-d) is labelled according to a predefined order, and
   the data storage space (13) is configured to store information about which subsection with a specific label is linked to which traffic control device (1a-d) having a specific label.

5. The traffic control system according to claim 4, **characterized in that** the predefined order is circular so

that each subsection and each traffic control device (1a-d) of the sector of the road, respectively, is connected to one previous and one next subsection and traffic control device (1a-d), respectively.

**6.** The traffic control system according to claim 4 and/or 5, **characterized in that** the predefined sector of the road includes overlapping lanes and the area of the sector in which roads or lanes are overlapping is divided into subsections and one subsection is defined for a part of the area within which two different lanes overlap, wherein
a vehicle (10) which has entered a subsection m within which the traffic is controlled by a traffic control device m (1a-d) returns the received token (2a-d) and the received entry permission flag (3a-d) to a traffic control device m+1 (1a-d) which is next in the predefined order and which is configured to control the traffic in a next subsection m+1, wherein
the traffic control device m+1 (1a-d) which has received the token (2a-d) and the entry permission flag (3a-d) of the subsection m is configured to transmit the entry permission flag of subsection m to the traffic control device m (1a-d) that issued said entry permission flag of subsection m and to forward a token (2a-d) to a further next traffic control device m+2 (1a-d) according to the predefined order, and each further traffic control device (1a-d) is configured to forward a token (2a-d) until a token (2a-d) is received by the traffic control device (1a-d) which issued a token to the vehicle (10).

**7.** The traffic control system according to claim 6, **characterized in that** the traffic control device which issued the token (2a-d) to the vehicle (10) is identified by the number of tokens (2a-d) in the data storage space (13).

**8.** The traffic control system according to at least one of the previous claims, **characterized in that** each traffic control device includes an entry permission control unit configured (21) to grant a vehicle (10) entry into a predefined sector, if said vehicle (10) holds an entry permission flag (3a-d) for said sector.

**9.** The traffic control system according to at least one of the previous claims, **characterized in that** the traffic control device (1a-d) is configured to issue a token (2a-d) combined with one or more reservation options (6) for one or more subsequent subsections and linked to a specific vehicle (10a), and each traffic control device (1a-d) holding a token (2a-d) with reservation option (6) is configured to issue said token with reservation option only to the vehicle (10a) to which said token with reservation option is linked.

**10.** The traffic control system according to at least one of the previous claims, **characterized in that** the traffic control device (1a-d) includes an emergency vehicle priority mode unit configured to be activated by an emergency vehicle (11) requesting entry into one or more subsections of the predefined sector, wherein,
if the emergency vehicle priority mode unit switches the operational mode of the traffic control device (1a-d) to an emergency vehicle priority mode, the traffic control device (1a-d) is configured to create a temporary token and a temporary entry permission flag to be issued to the emergency vehicle (11) requesting entry, and
each other vehicle (10), if holding a token (2a-d) and an entry permission flag (3a-d) of the subsection for which the emergency vehicle (11) requests entry, is forced by the traffic control device (1a-d) to return said token and the entry permission flag before the temporary token and the temporary entry permission flag is issued to the emergency vehicle (11).

**11.** The traffic control system according to claim 10, **characterized in that** the temporary token and the temporary entry permission flag are transmitted to the next traffic control device (1a-d) when the emergency vehicle (11) enters the subsection and the next traffic control device (1a-d) is configured to erase the temporary token and to return the temporary entry permission flag to the traffic control device (1a-d) which had issued the temporary entry permission flag; wherein when the traffic control device which has issued the temporary entry permission flag has received the temporary entry permission flag, said traffic control device is configured to erase the temporary entry permission flag and to re-issue a token and an entry permission flag to the vehicle (10) which forcibly returned a token and an entry permission flag before.

**12.** The traffic control system according to claim 10 or 11, **characterized in that** the temporary token has a reservation option (6) for one or more further subsections.

**13.** The traffic control system according to at least one of the previous claims, **characterized in that** the number of tokens (2a-d) and entry permission flags (3a-d) per subsection is either fixed based on the maximum number of vehicles (10) allowed in the subsection or is variably controlled based on time and density of traffic.

**14.** The traffic control system according to at least one of the previous claims, **characterized in that** each traffic control device (1a-d) includes an emergency vehicle priority mode unit configured to be activated by an emergency vehicle (11) requesting entry into one or more subsections of the predefined sector, wherein

if the emergency vehicle priority mode unit switches the operational mode of the traffic control device (1a-d) to an emergency vehicle priority mode, the traffic control device (1a-d) is configured to control the occupancy within the predefined sector of the road.

**15.** The traffic control system according to at least one of the previous claims, **characterized in that** the traffic control system (100) is configured to determine a maximum occupancy during the emergency vehicle priority mode which is derived from the number of subsections of the predefined sector which will be crossed by the emergency vehicle (11), the number being determined based on the entry request of the emergency vehicle (11), and based on the maximum capacity of vehicles (10) being inside the predefined sector of the road at the same time.

**16.** The traffic control system according to claim 15, **characterized in that** the traffic control system (100) stops providing entry permission to a vehicle (10) outside the sector of the road if an actual occupancy is higher than the maximum occupancy, and/or to set or adapt a delay time for the grant of an entry permission depending on the actual occupancy.

**17.** A computer program product comprising computer-readable instructions that, when executed in a computer system including one or more computers, cause the computer system to perform the control of the traffic control system according to at least one of the previous claims.

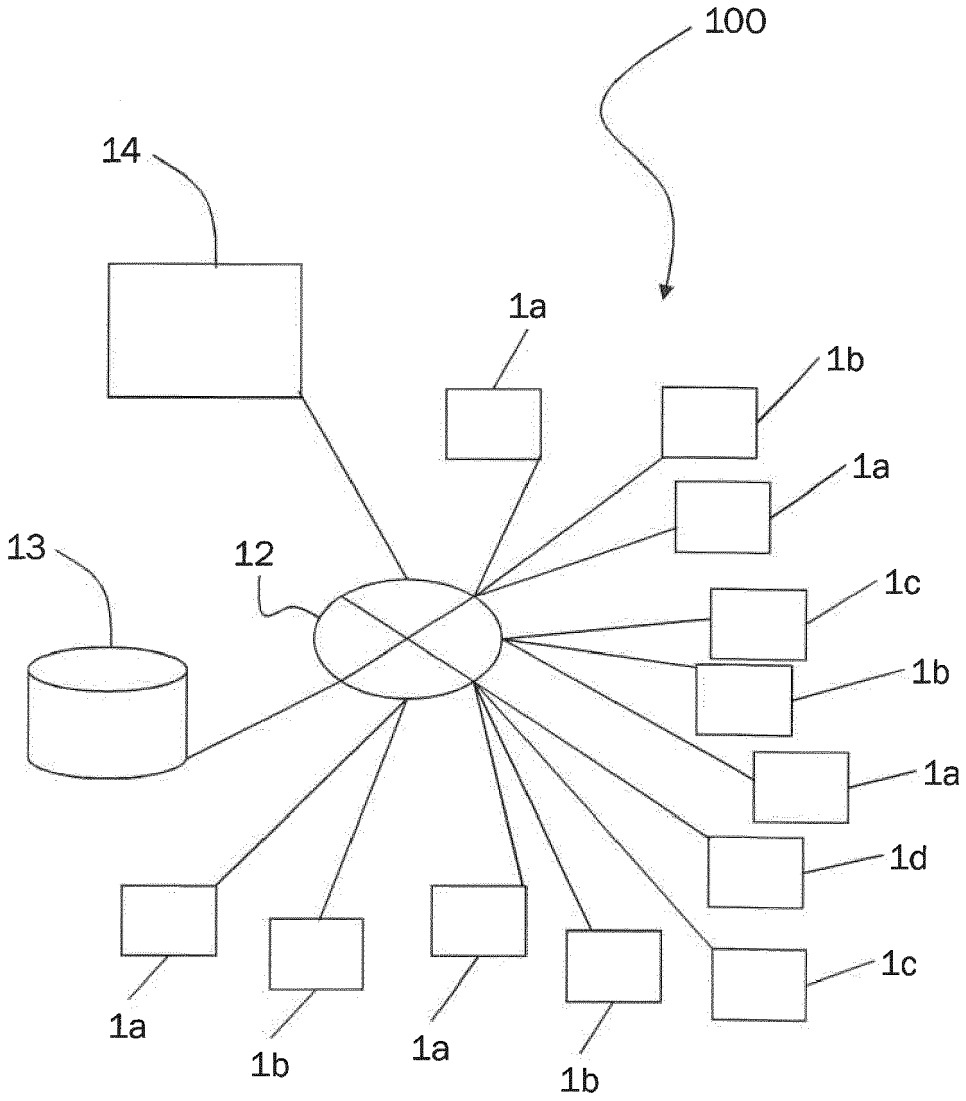



Fig. 1

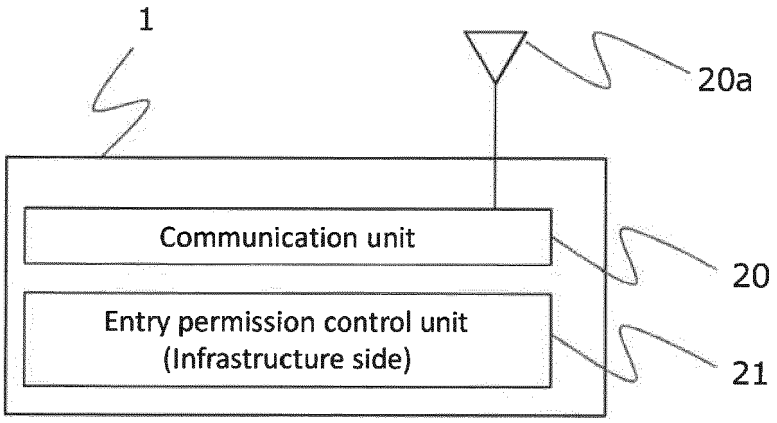

1
20a
Communication unit
20
Entry permission control unit
(Infrastructure side)
21

Fig. 2

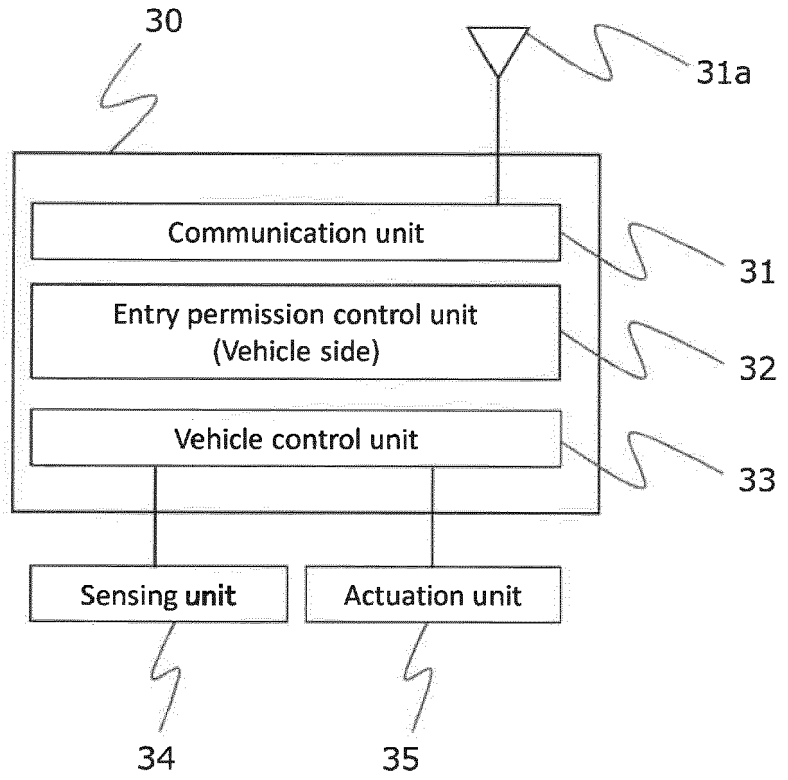

30
31a
Communication unit
31
Entry permission control unit
(Vehicle side)
32
Vehicle control unit
33
Sensing unit
Actuation unit
34
35

Fig. 3

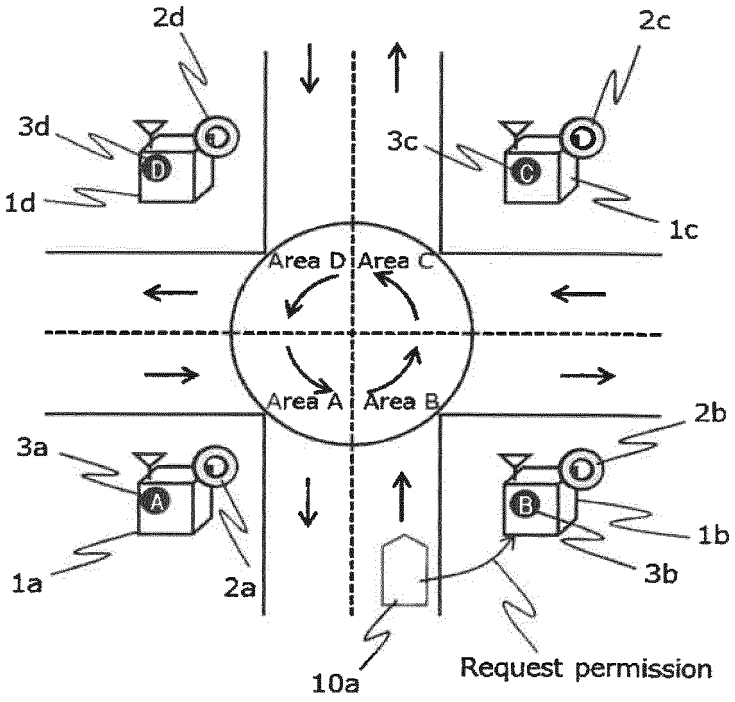
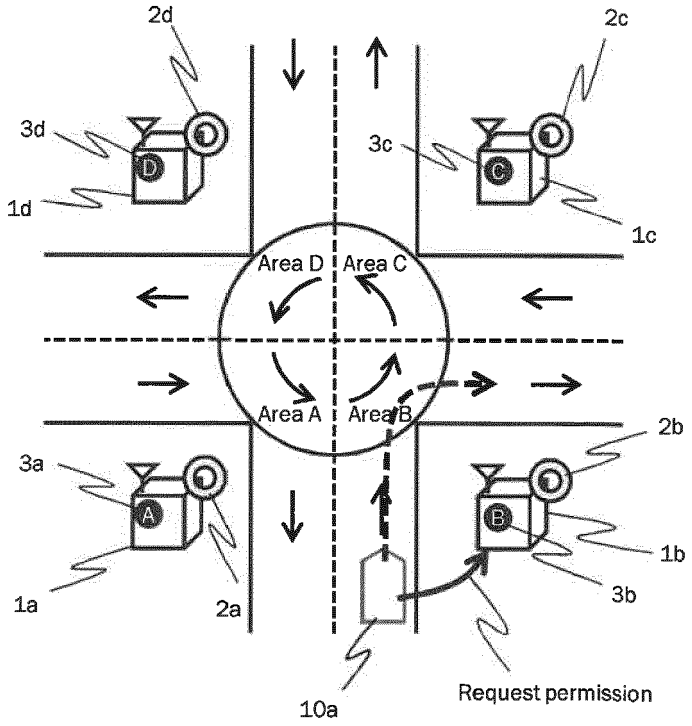
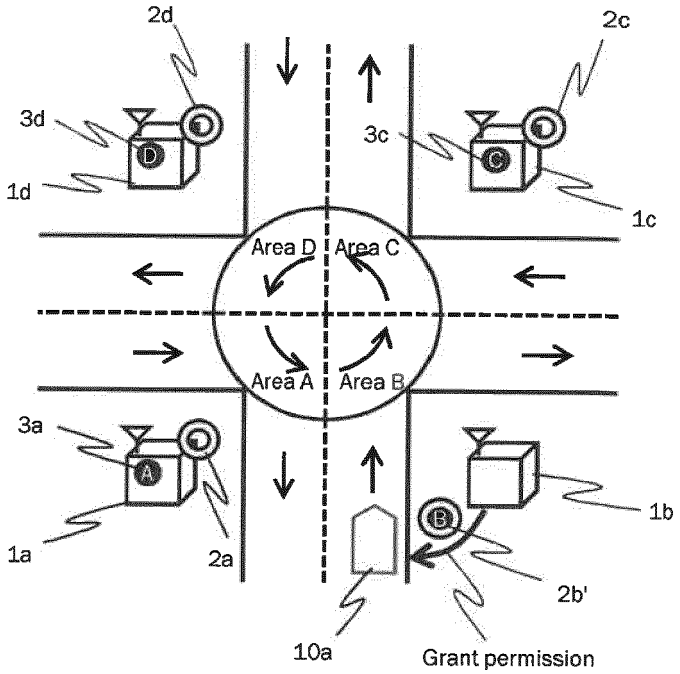



Fig. 4



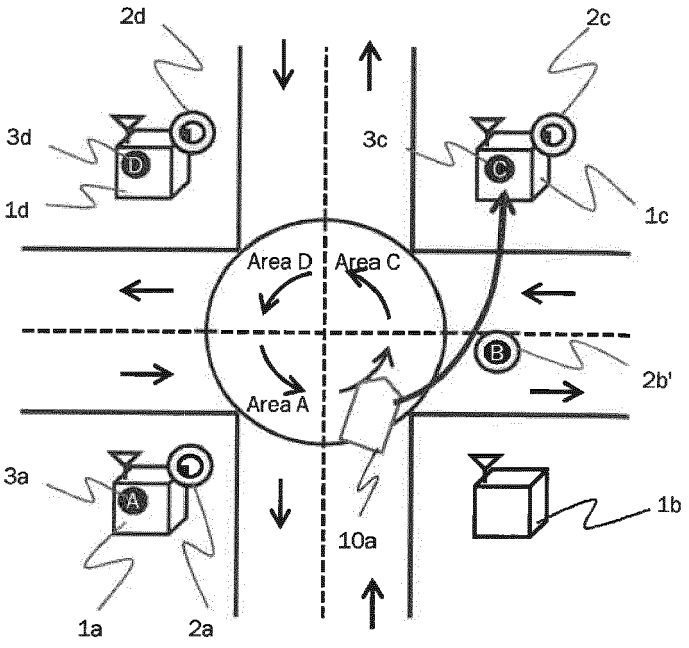

[1] Request permission

Fig. 5



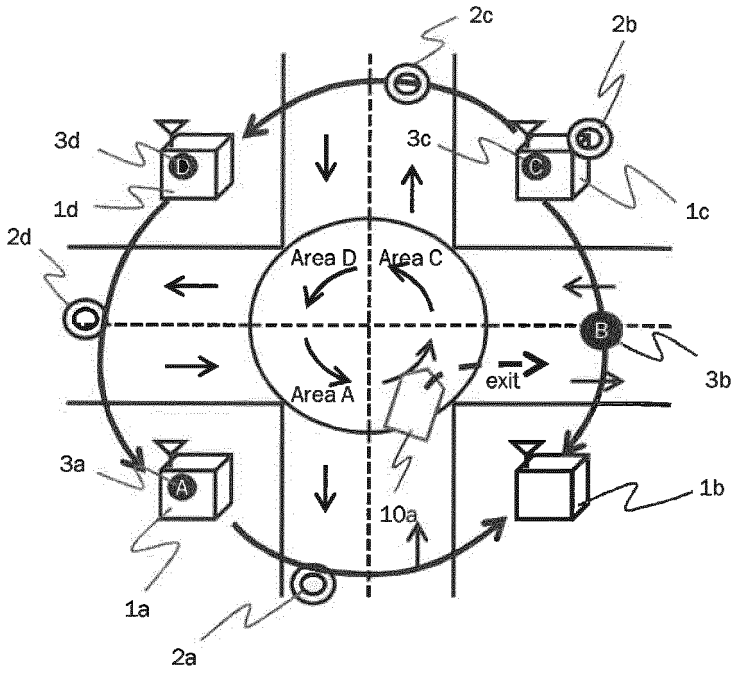

[2] Grant permission

Fig. 6



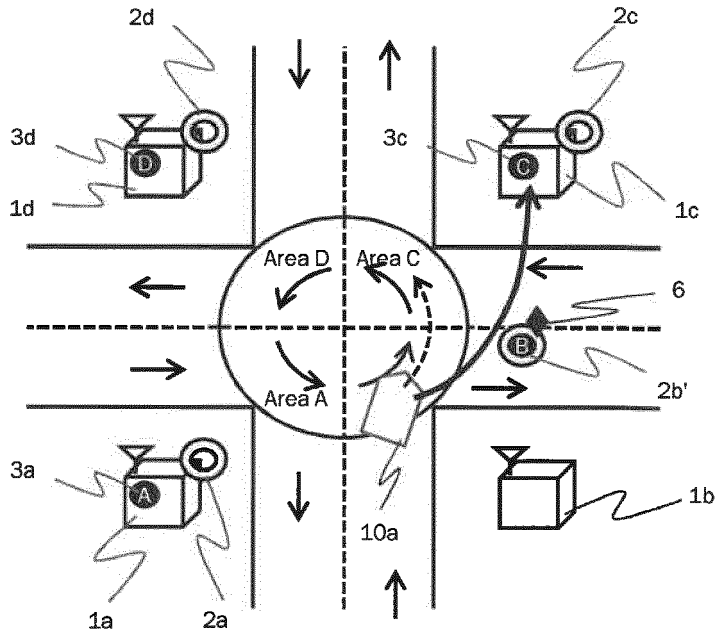

[3] Return token and permission

Fig. 7



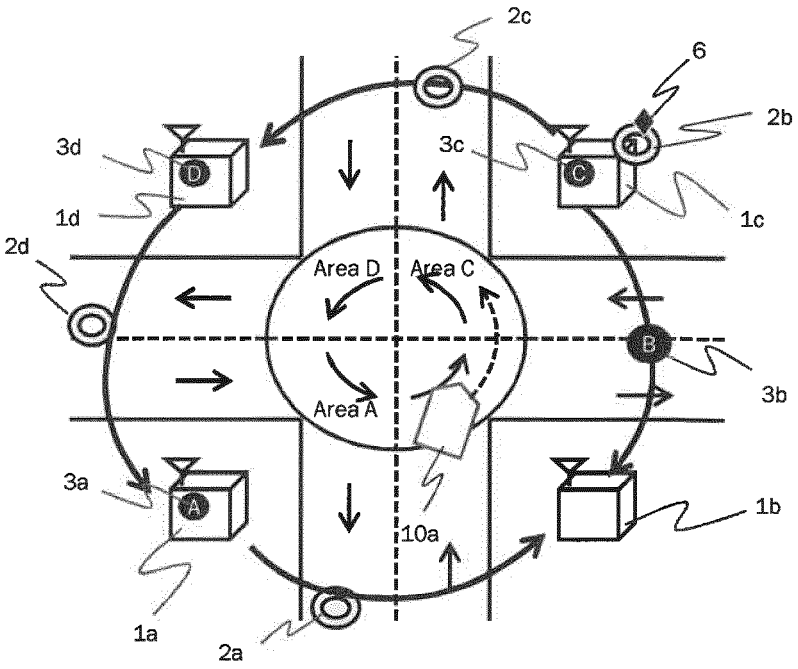

[4] Return permission to the original position and circulate tokens

Fig. 8



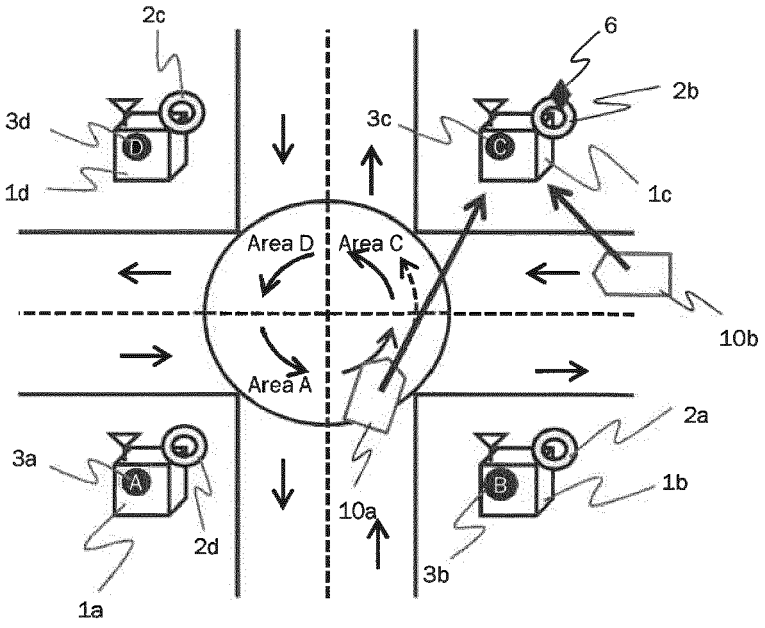

[3'] Return token and permission with reservation option

Fig. 9



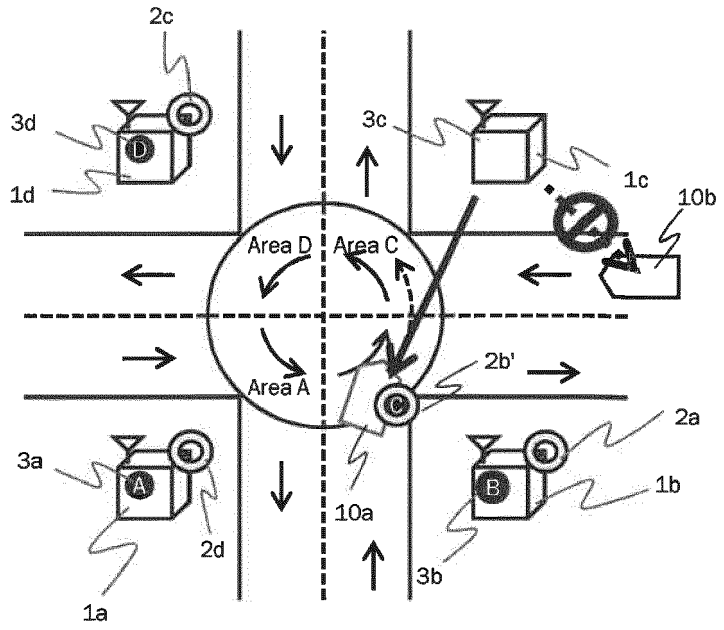

[4] Return permission(B) to the original position and circulate tokens

Fig. 10



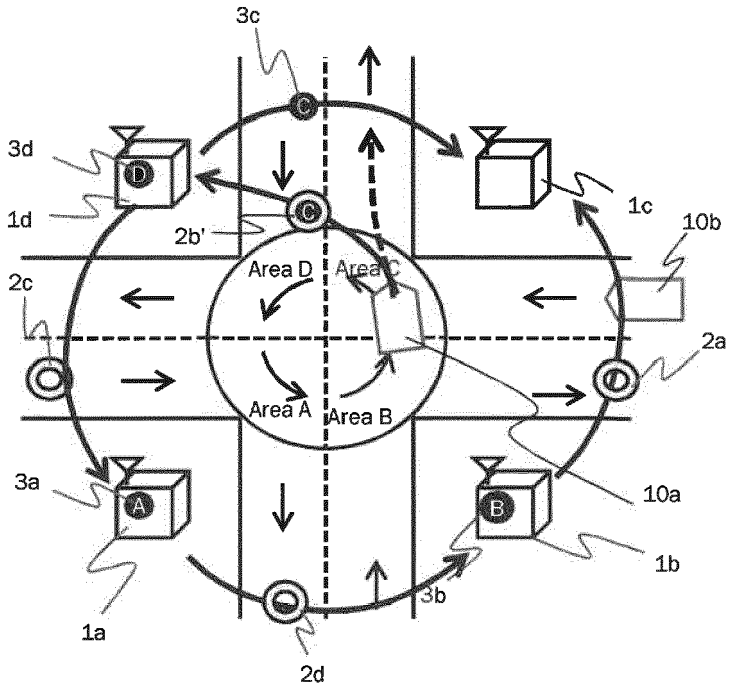

[5] Request permission for Area C (from 10a and 10b)

Fig. 11



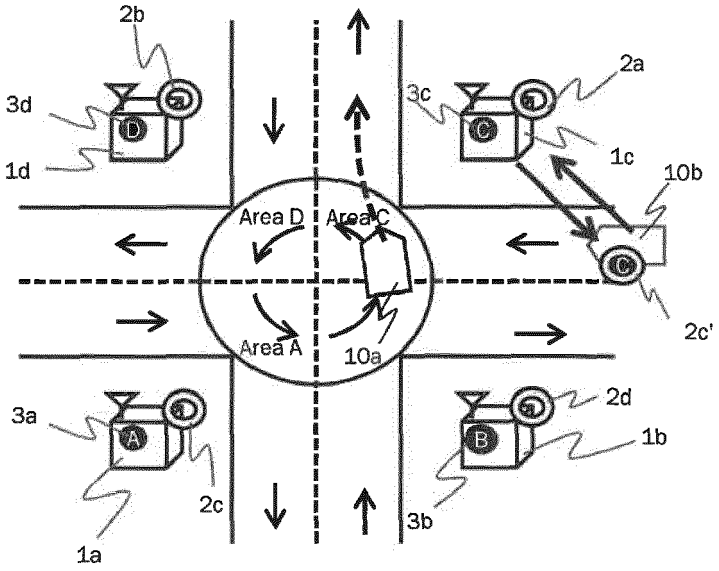

[6] Grant permission to vehicle 10a based on the reservation option (Reject request from 10b)

Fig. 12




[7] - Return token and permission(2b')
- Circulate tokens(2c, 2d, 2a)
- Return permission(3c) to 1c

Fig. 13




[8] - Request and grant permission to vehicle(10b) - Vehicle(10a) exits the intersection

Fig. 14

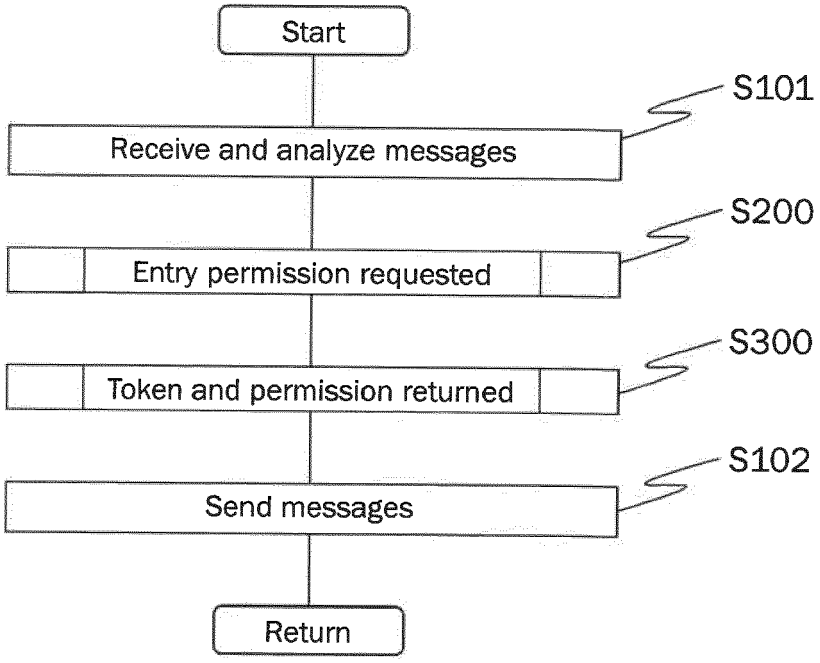

Start
S101
Receive and analyze messages
S200
Entry permission requested
S300
Token and permission returned
S102
Send messages
Return

Fig. 15

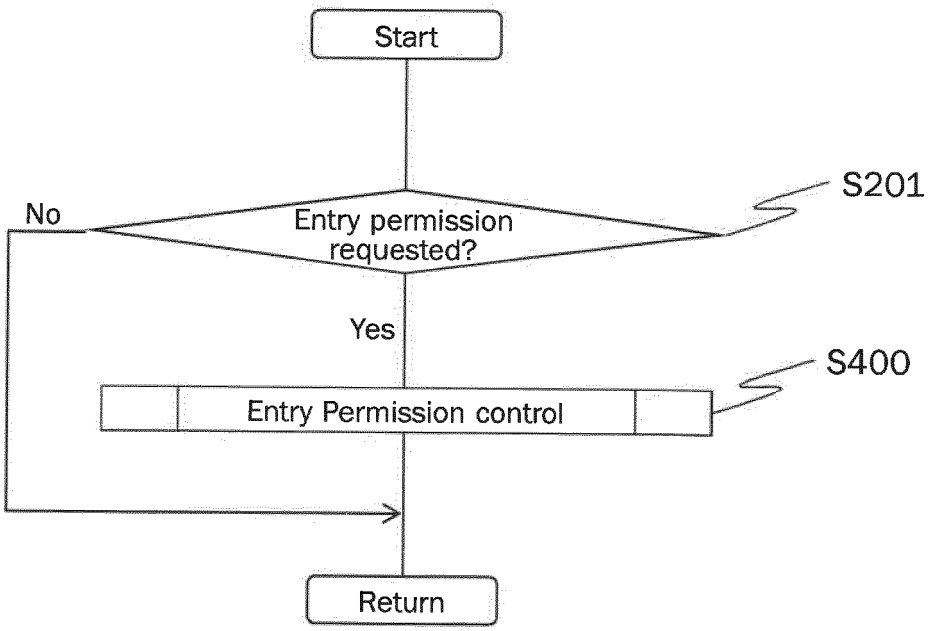

Start
S201
No
Entry permission requested?
Yes
S400
Entry Permission control
Return

Fig. 16

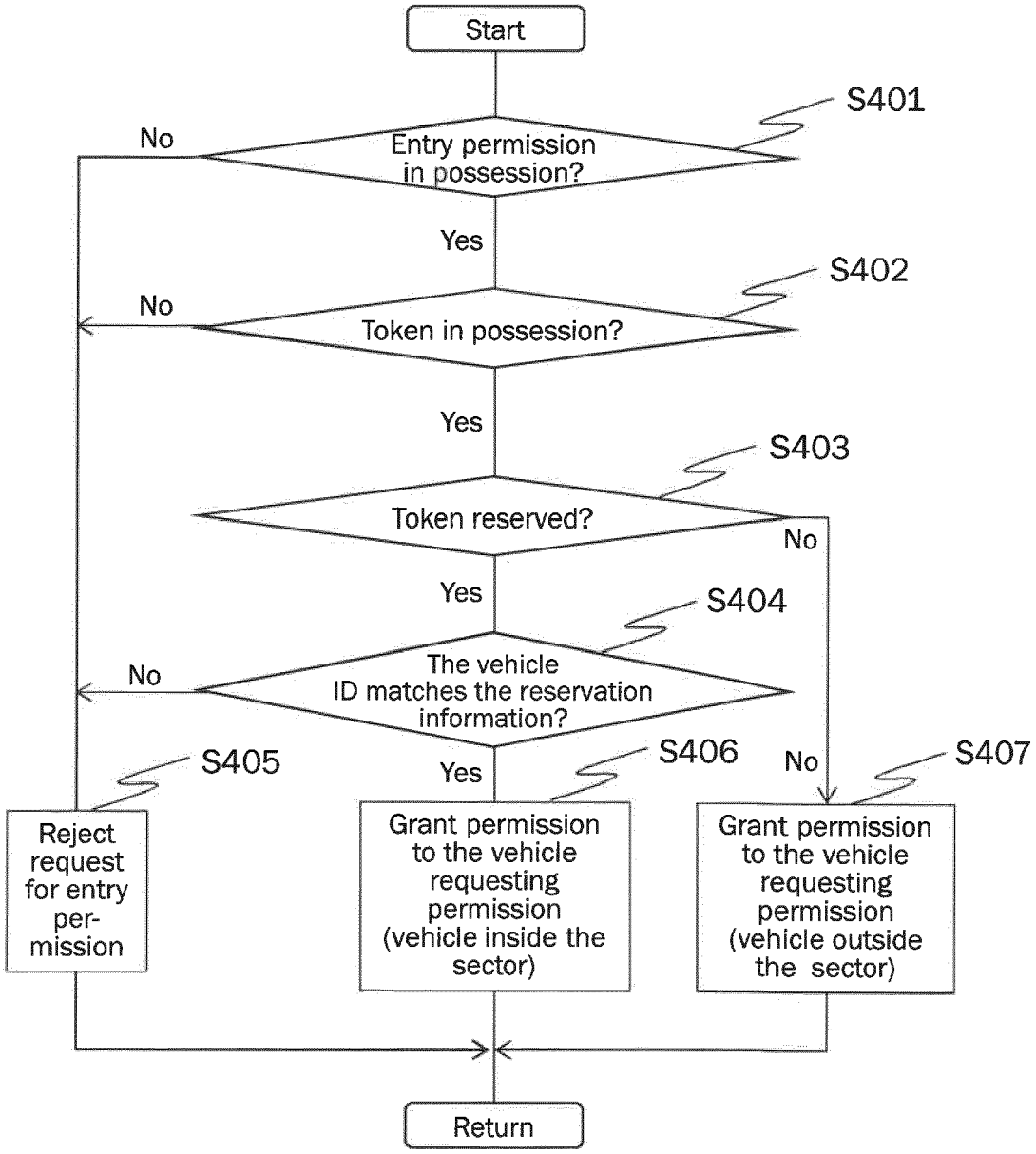

Start
S401
Entry permission in possession?
No
Yes
S402
Token in possession?
No
Yes
S403
Token reserved?
No
Yes
S404
The vehicle ID matches the reservation information?
No
Yes
S405
S406
No
S407
Reject request for entry per-mission
Grant permission to the vehicle requesting permission (vehicle inside the sector)
Grant permission to the vehicle requesting permission (vehicle outside the sector)
Return

Fig. 17

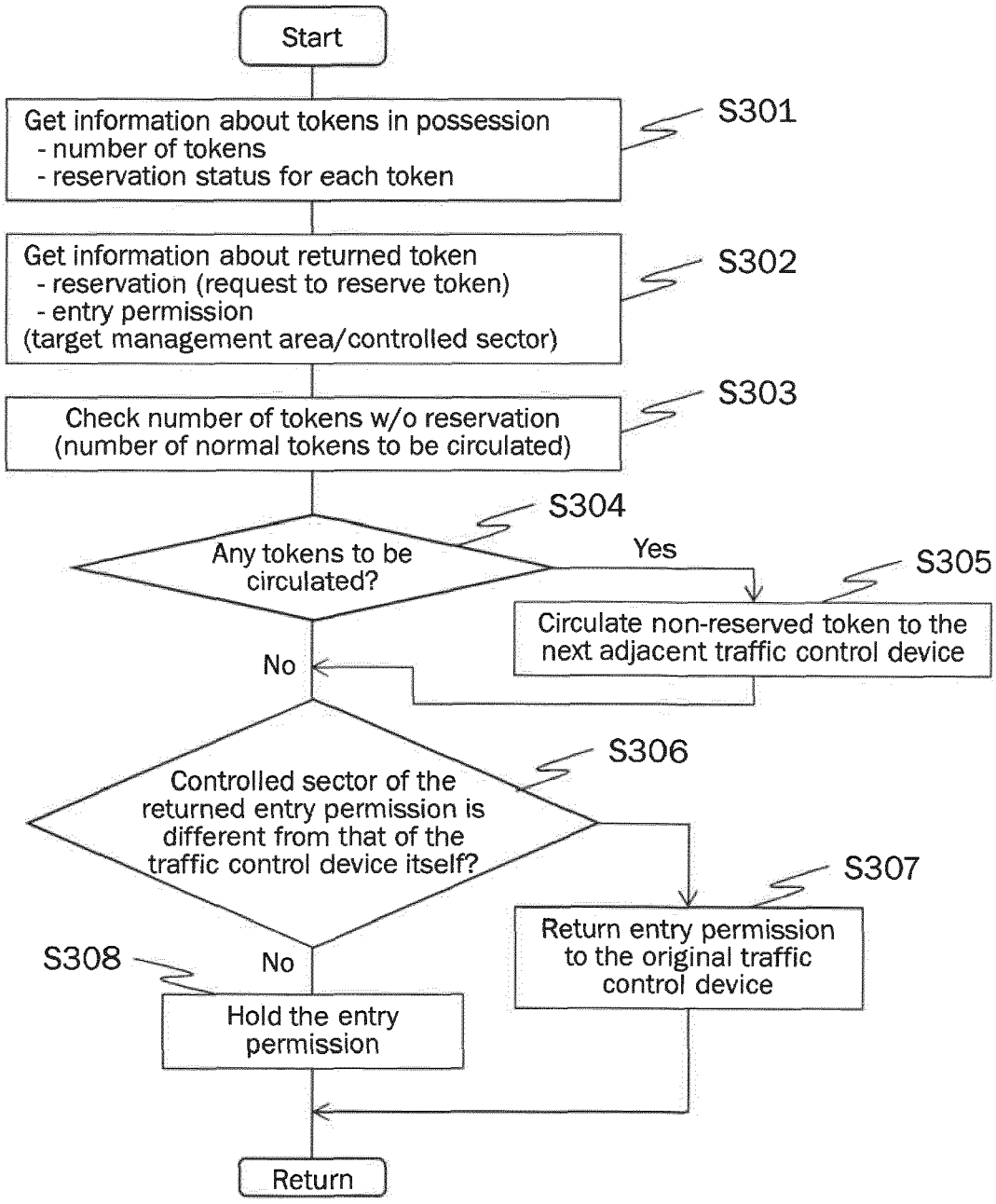
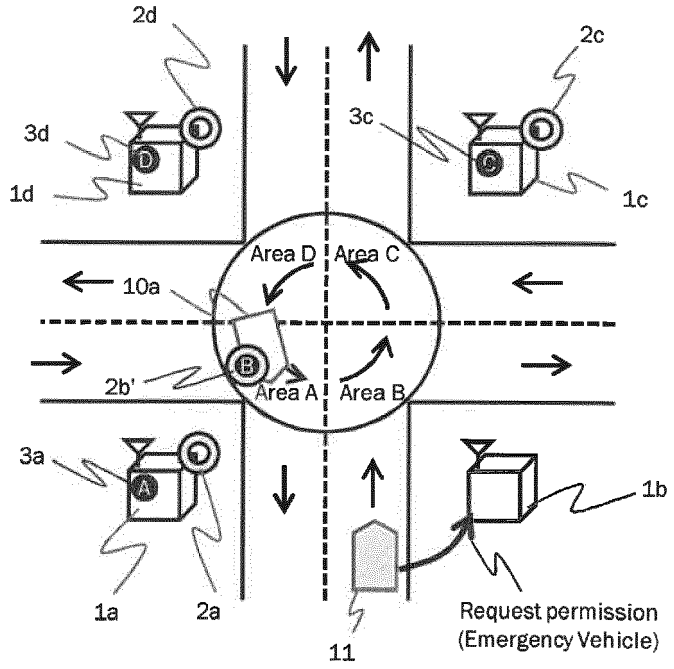
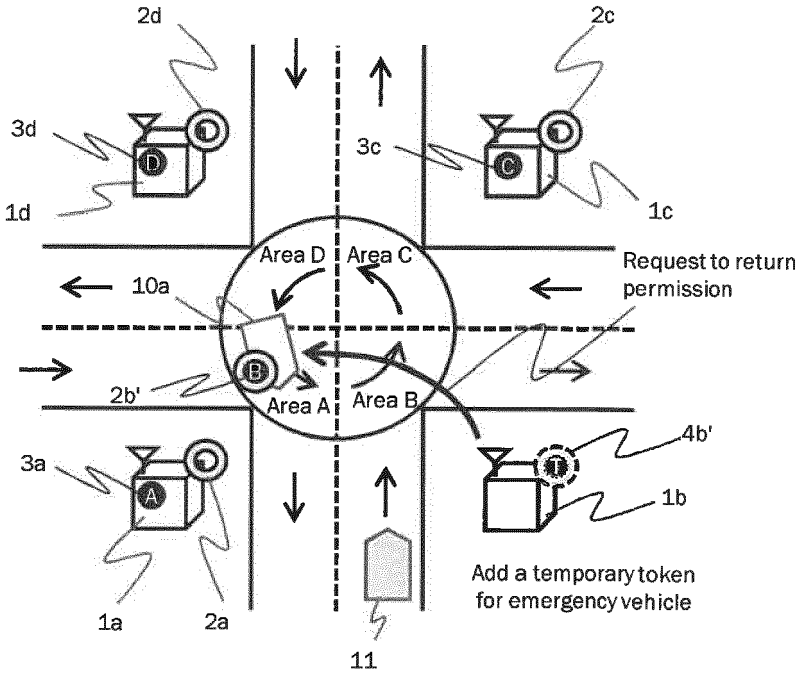

Start
Get information about tokens in possession
- number of tokens
- reservation status for each token
S301
Get information about returned token
- reservation (request to reserve token)
- entry permission
(target management area/controlled sector)
S302
Check number of tokens w/o reservation
(number of normal tokens to be circulated)
S303
S304
Any tokens to be circulated?
Yes
S305
Circulate non-reserved token to the next adjacent traffic control device
No
S306
Controlled sector of the returned entry permission is different from that of the traffic control device itself?
S307
Return entry permission to the original traffic control device
S308
No
Hold the entry permission
Return

Fig. 18



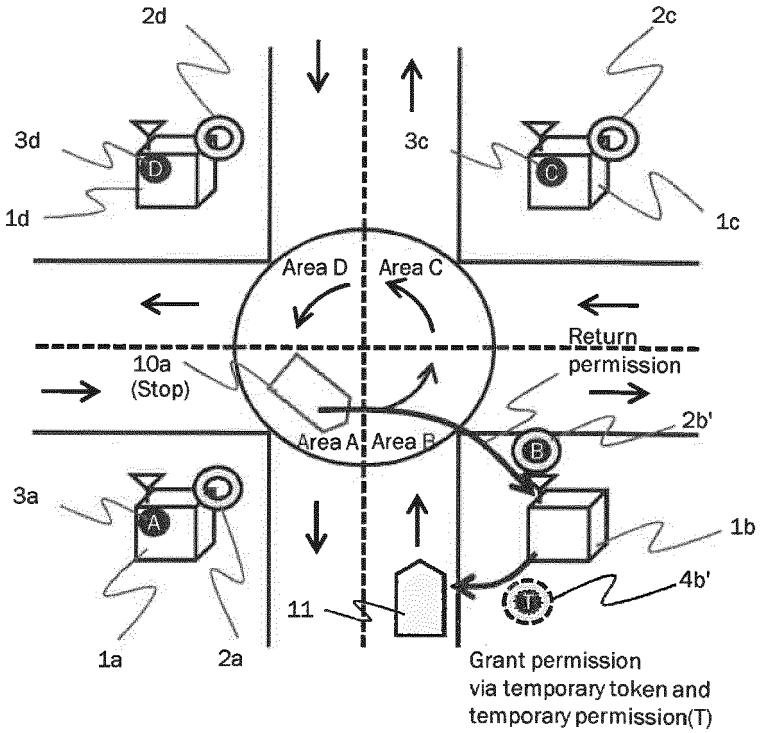

[1] Request permission by an emergency vehicle

Fig. 19



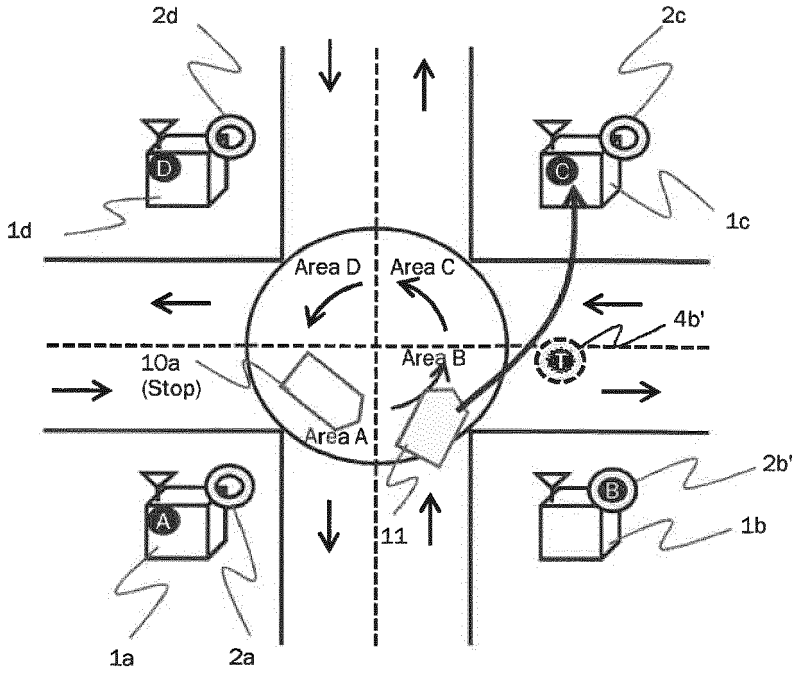

[2] Add a temporary token with priority reservation

Fig. 20



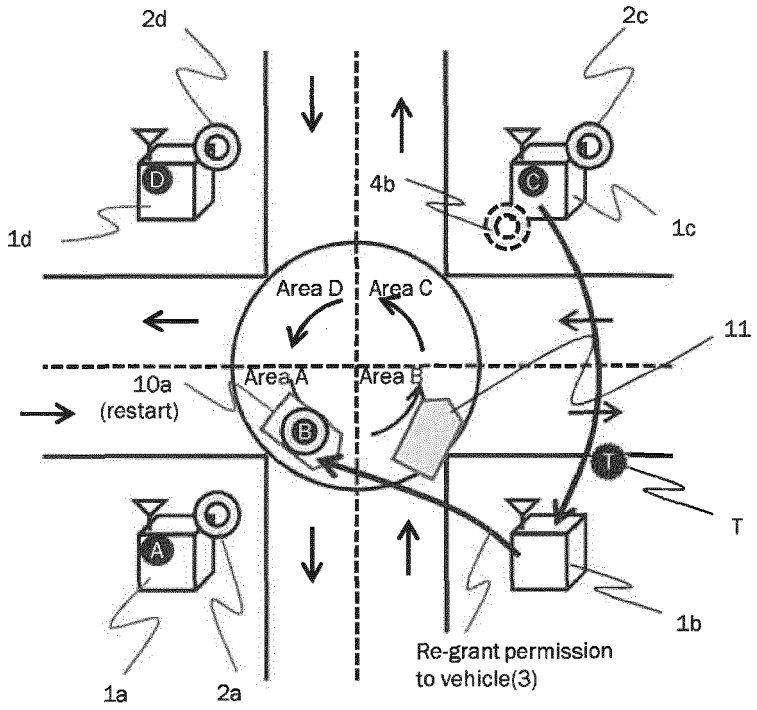

[3] Grant temporary permission to emergency vehicle

Fig. 21




[4] Return temporary token with permission

Fig. 22




[5] Return temporary permission to 1b and re-grant permission to the vehicle(3)

Fig. 23

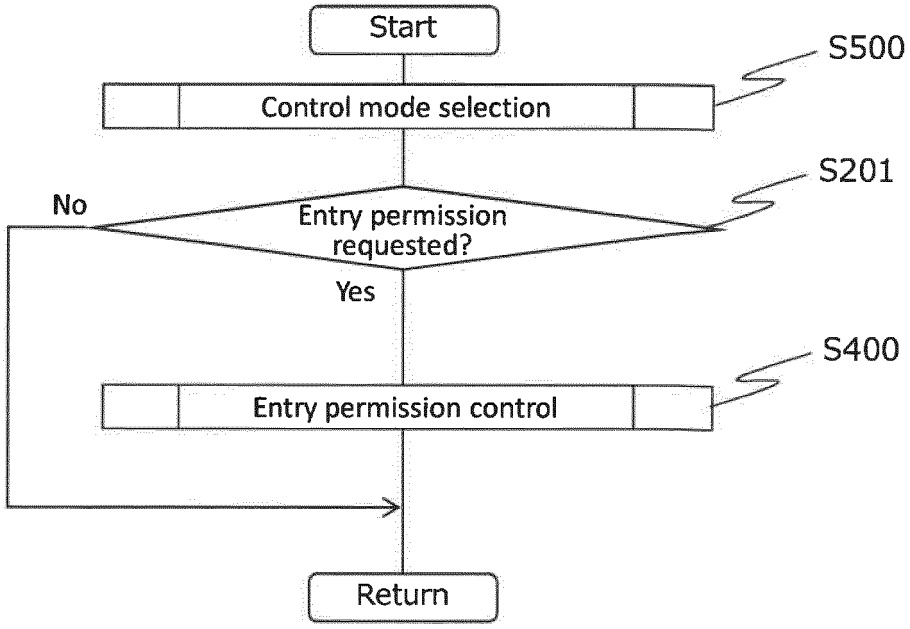

Start
S500
Control mode selection
S201
No
Entry permission requested?
Yes
S400
Entry permission control
Return

Fig. 24

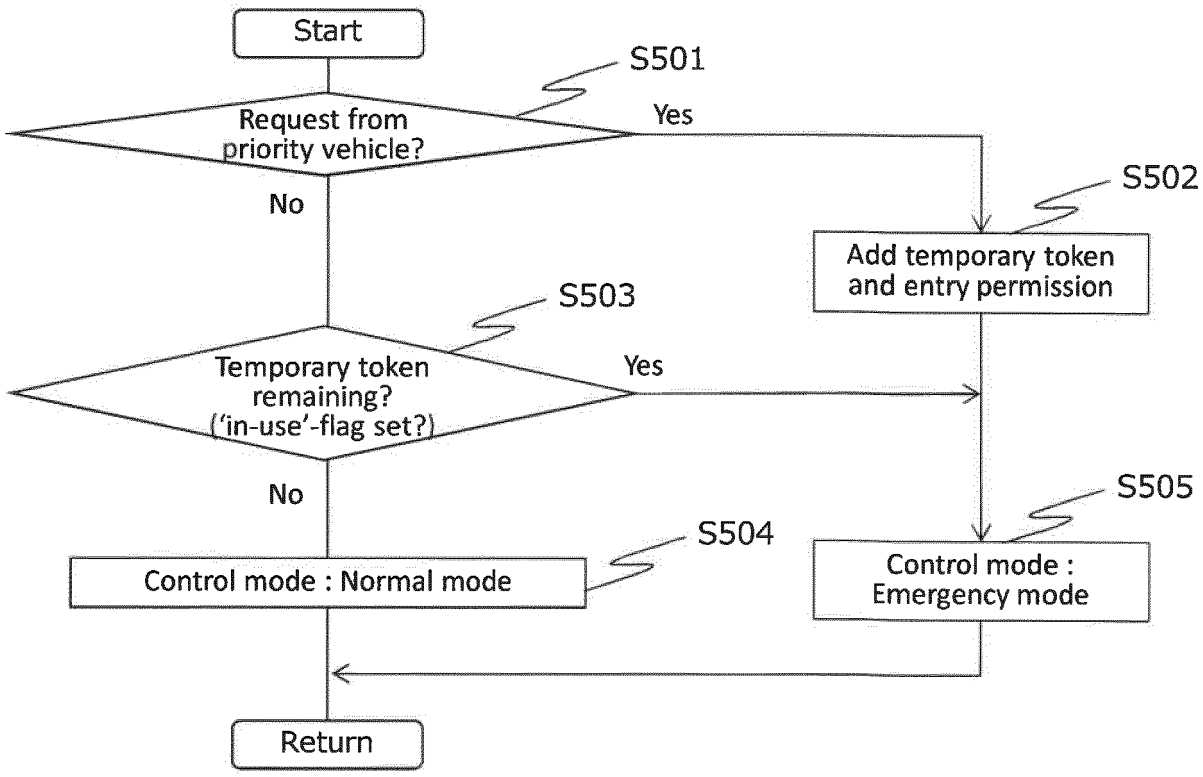

Start
S501
Request from priority vehicle?
Yes
No
S502
Add temporary token and entry permission
S503
Temporary token remaining? ('in-use'-flag set?)
Yes
No
S505
S504
Control mode : Normal mode
Control mode : Emergency mode
Return

Fig. 25

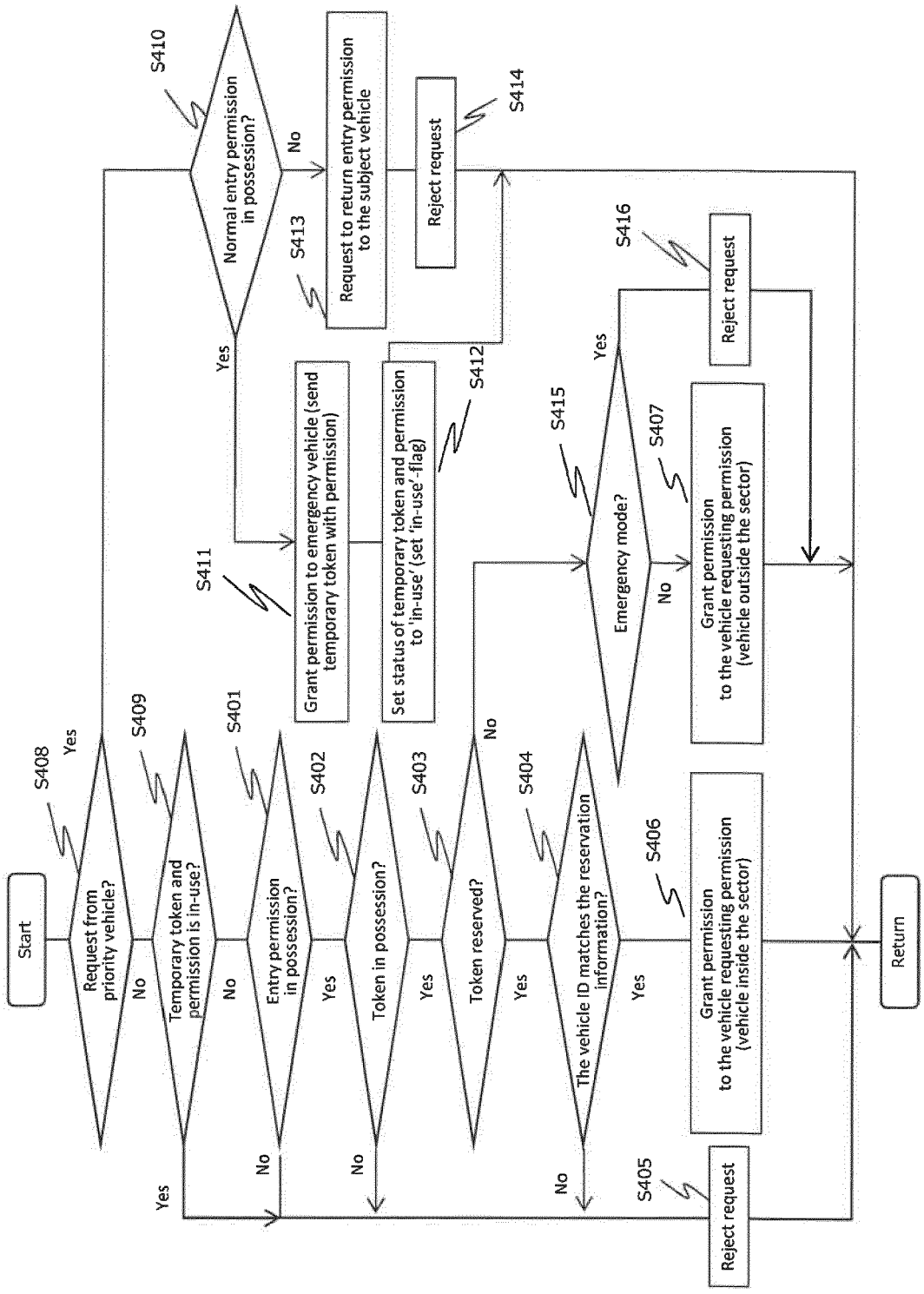

Start
Request from priority vehicle?
Yes
No
S408
Temporary token and permission is in-use?
Yes
No
S409
Entry permission in possession?
Yes
No
S401
Token in possession?
Yes
No
S402
Token reserved?
Yes
No
S403
The vehicle ID matches the reservation information?
Yes
No
S404
Emergency mode?
Yes
No
S415
Normal entry permission in possession?
Yes
No
S410
Grant permission to emergency vehicle (send temporary token with permission)
S411
Set status of temporary token and permission to 'in-use' (set 'in-use'-flag)
S412
Request to return entry permission to the subject vehicle
S413
Reject request
S414
Grant permission to the vehicle requesting permission (vehicle inside the sector)
S406
Grant permission to the vehicle requesting permission (vehicle outside the sector)
S407
Reject request
S405
Reject request
S416
Return

Fig. 26

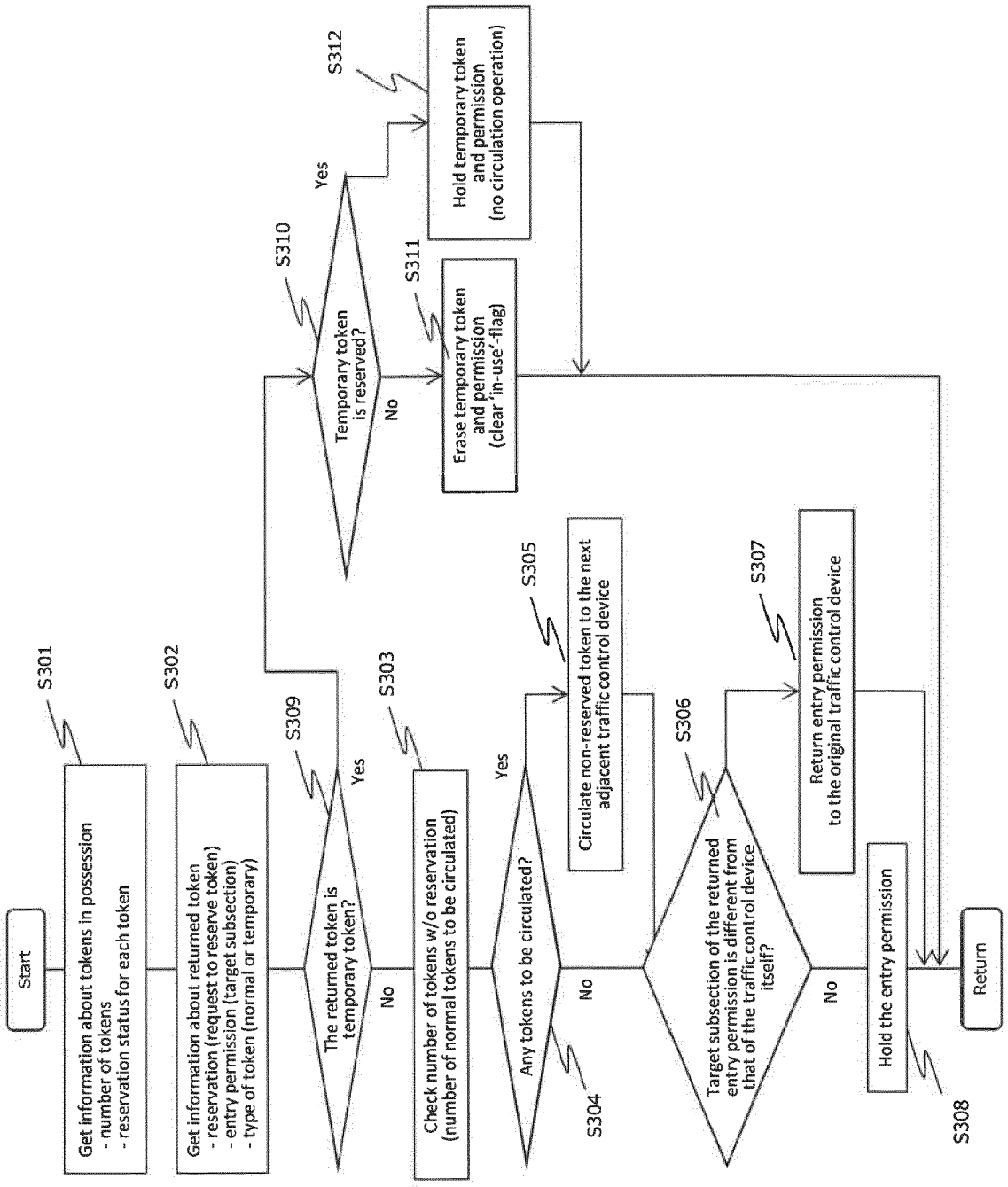

Start
S301
Get information about tokens in possession
- number of tokens
- reservation status for each token
S302
Get information about returned token
- reservation (request to reserve token)
- entry permission (target subsection)
- type of token (normal or temporary)
S309
The returned token is temporary token?
Yes
No
S303
Check number of tokens w/o reservation (number of normal tokens to be circulated)
Yes
S305
Circulate non-reserved token to the next adjacent traffic control device
Any tokens to be circulated?
No
S304
S306
Target subsection of the returned entry permission is different from that of the traffic control device itself?
S307
Return entry permission to the original traffic control device
No
Hold the entry permission
S308
Return
S310
Temporary token is reserved?
Yes
S312
Hold temporary token and permission (no circulation operation)
No
S311
Erase temporary token and permission (clear 'in-use'-flag)

Fig. 27

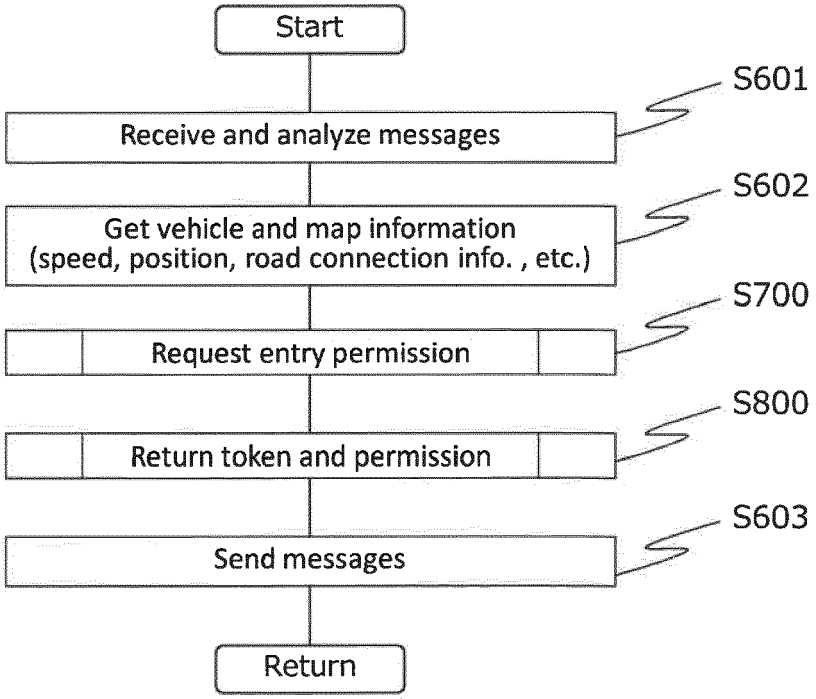

Start
S601
Receive and analyze messages
S602
Get vehicle and map information
(speed, position, road connection info. , etc.)
S700
Request entry permission
S800
Return token and permission
S603
Send messages
Return

Fig. 28

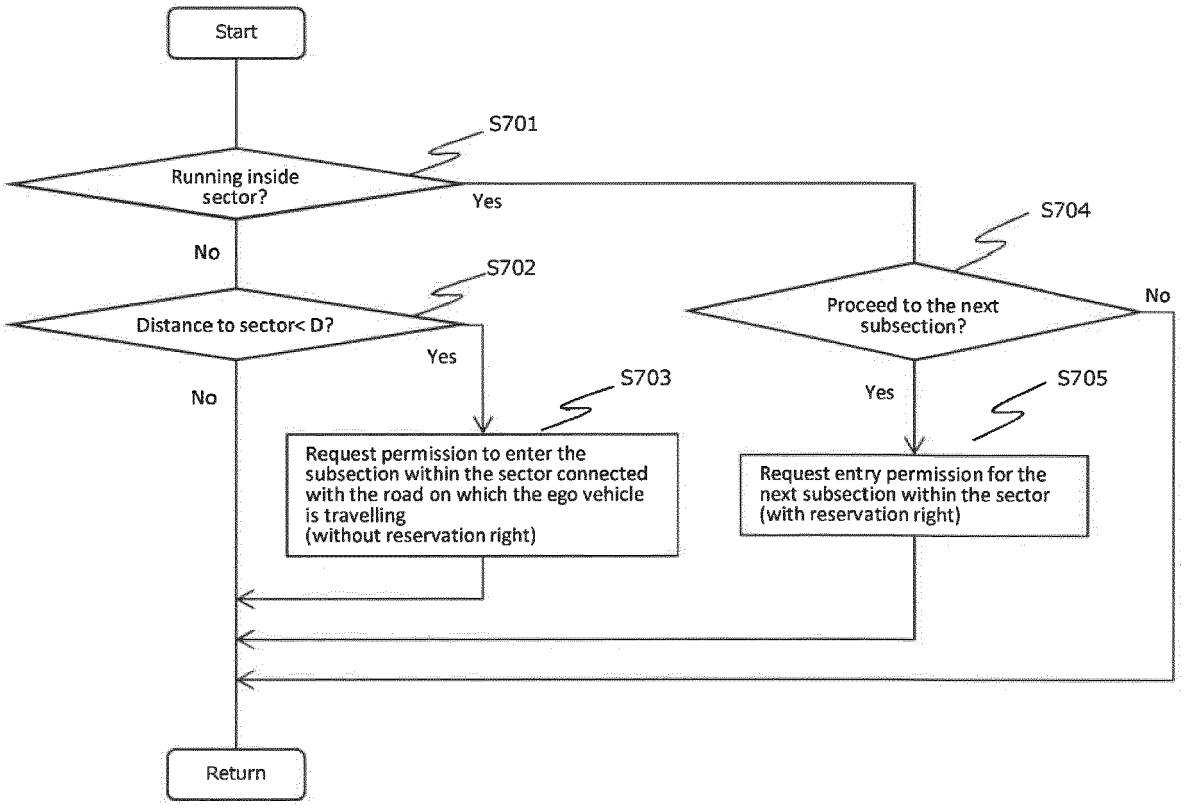

Start
S701
Running inside sector?
Yes
No
S702
Distance to sector< D?
Yes
No
S703
Request permission to enter the subsection within the sector connected with the road on which the ego vehicle is travelling
(without reservation right)
S704
Proceed to the next subsection?
No
Yes
S705
Request entry permission for the next subsection within the sector
(with reservation right)
Return

Fig. 29

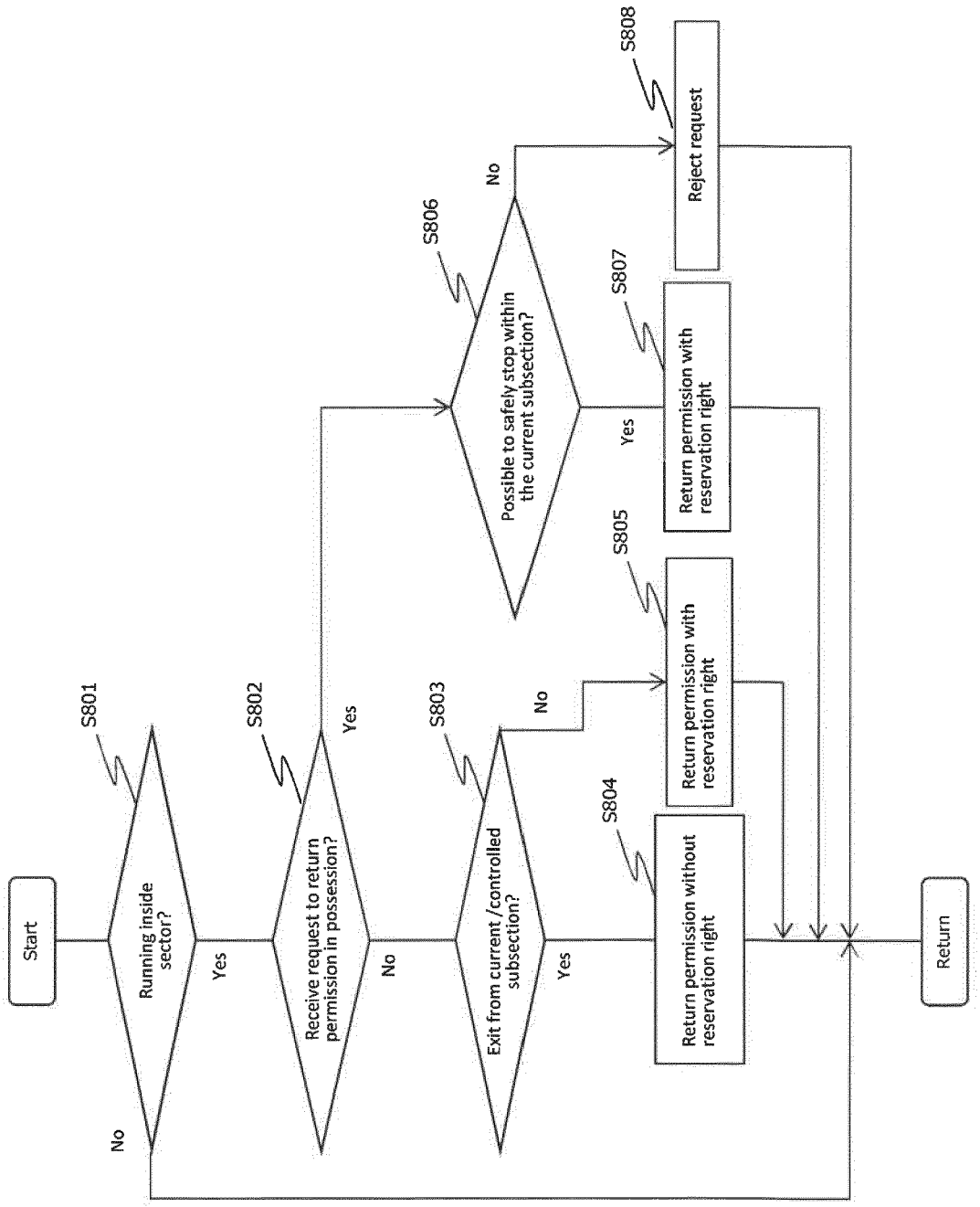

Start
S801
Running inside sector?
Yes
No
S802
Receive request to return permission in possession?
Yes
No
S803
Exit from current /controlled subsection?
Yes
No
S804
Return permission without reservation right
S805
Return permission with reservation right
S806
Possible to safely stop within the current subsection?
Yes
No
S807
Return permission with reservation right
S808
Reject request
Return

Fig. 30

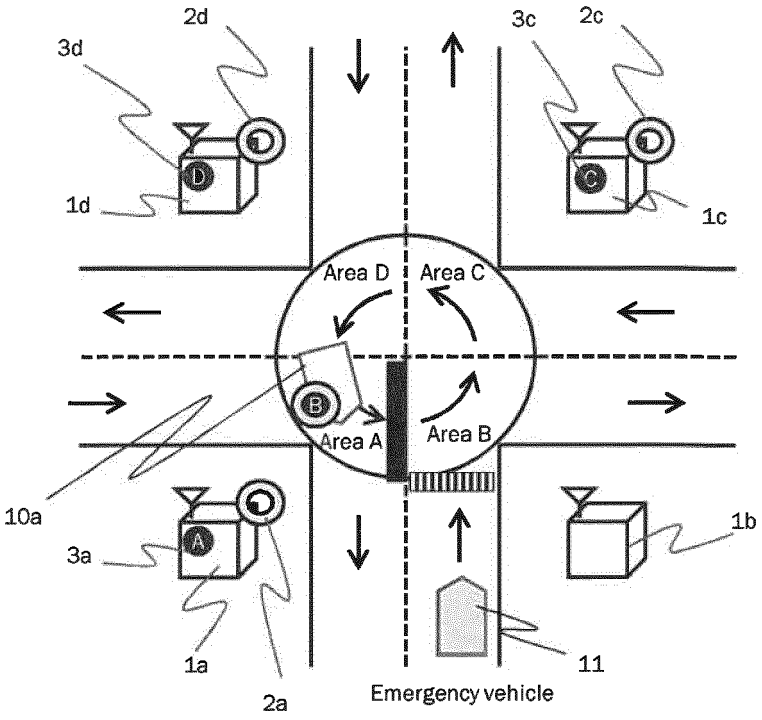

2d
3d
3c
2c
1d
1c
Area D
Area C
Area A
Area B
10a
3a
1b
1a
11
2a
Emergency vehicle

Fig. 31

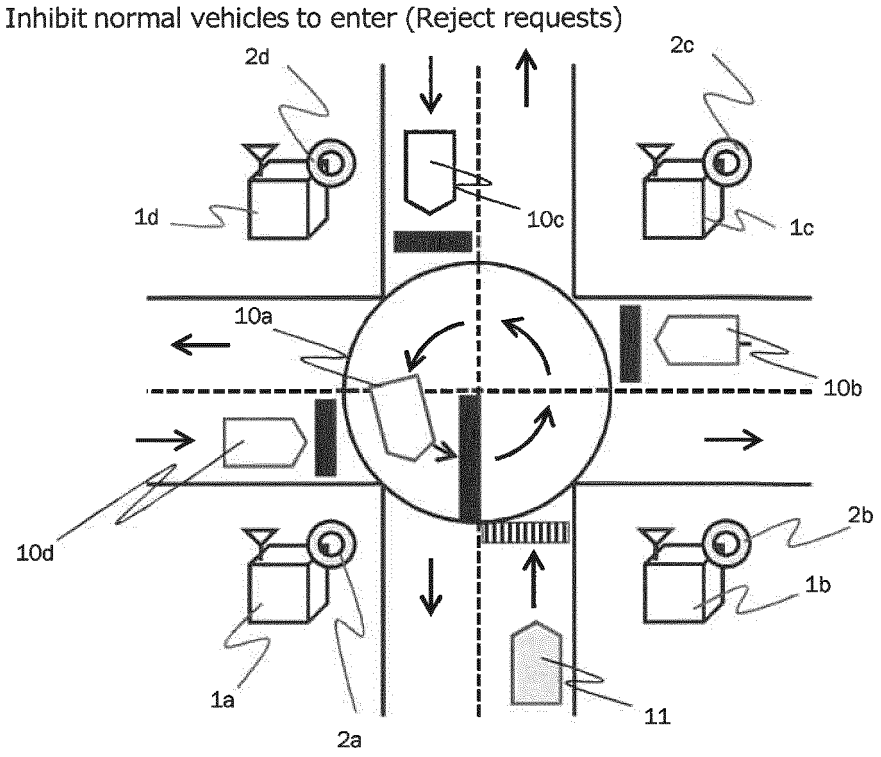

Inhibit normal vehicles to enter (Reject requests)
2d
2c
1d
10c
1c
10a
10b
10d
2b
1b
1a
11
2a

Fig. 32

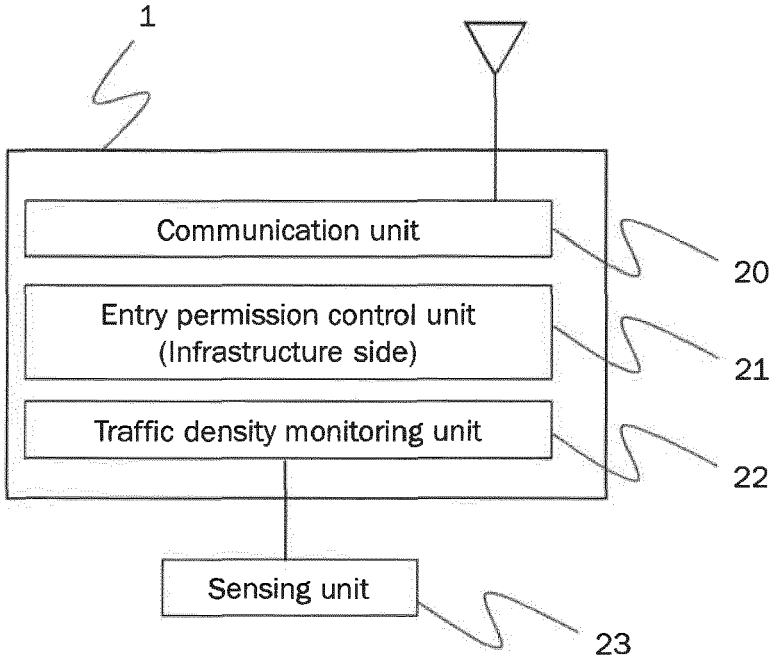

1
Communication unit
20
Entry permission control unit
(Infrastructure side)
21
Traffic density monitoring unit
22
Sensing unit
23

Fig. 33

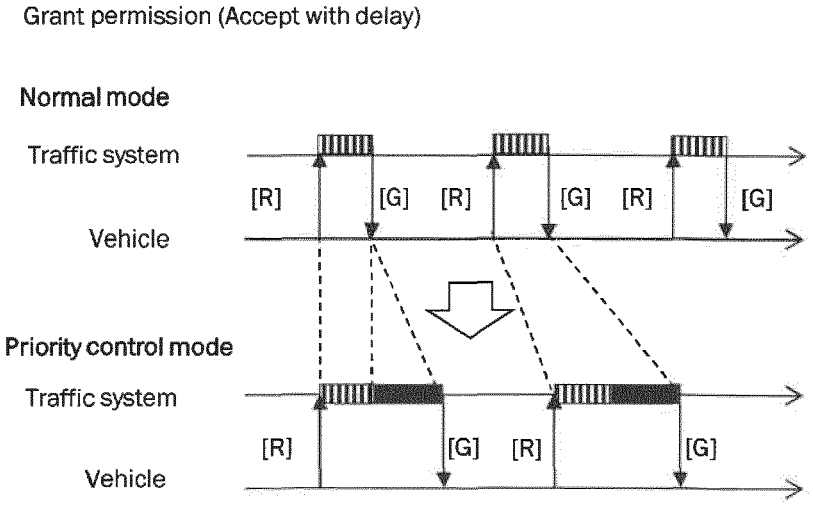
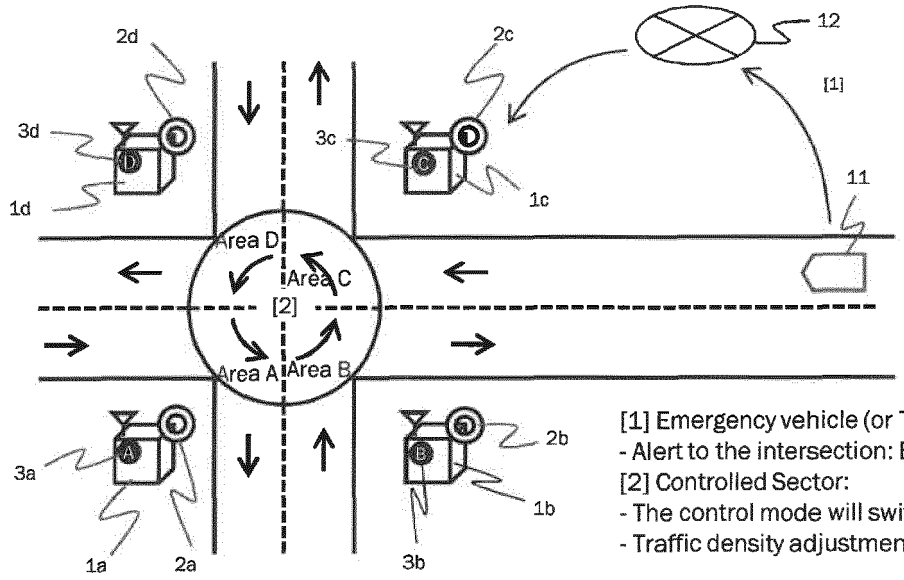
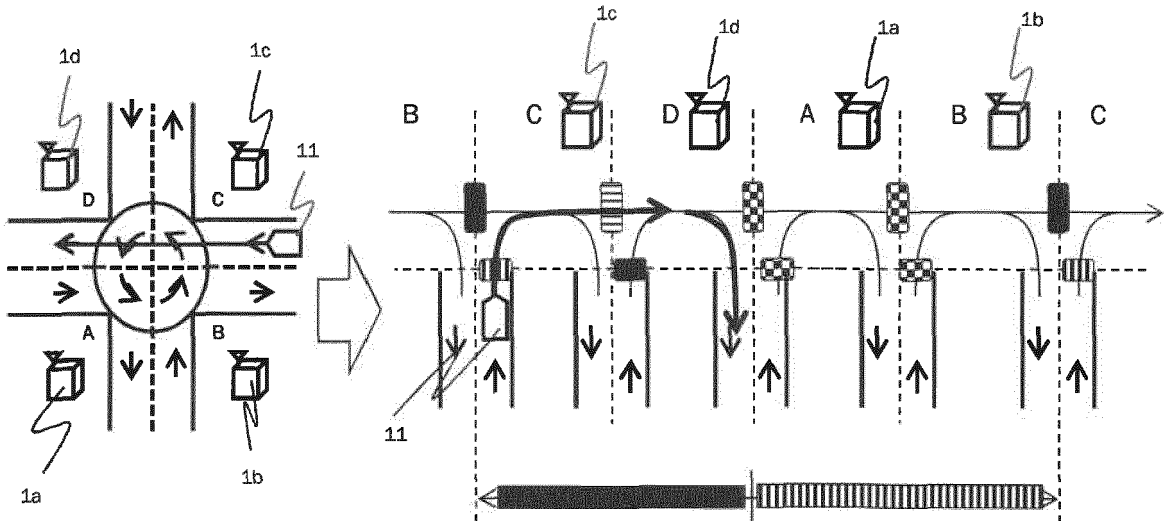

Grant permission (Accept with delay)
Normal mode
Traffic system
[R]
[G]
[R]
[G]
[R]
[G]
Vehicle
Priority control mode
Traffic system
[R]
[G]
[R]
[G]
Vehicle

Fig. 34




[1] Emergency vehicle (or Traffic management center):
- Alert to the intersection: Emergency vehicle is closing
[2] Controlled Sector:
- The control mode will switch to the emergency mode
- Traffic density adjustment will be activated

Fig. 35




Occupancy should be less than X% so that the priority vehicle can smoothly pass the intersection through Areas C to D.

Adjust occupancy of normal vehicles based on how many areas the priority vehicle needs to pass.

Fig. 36

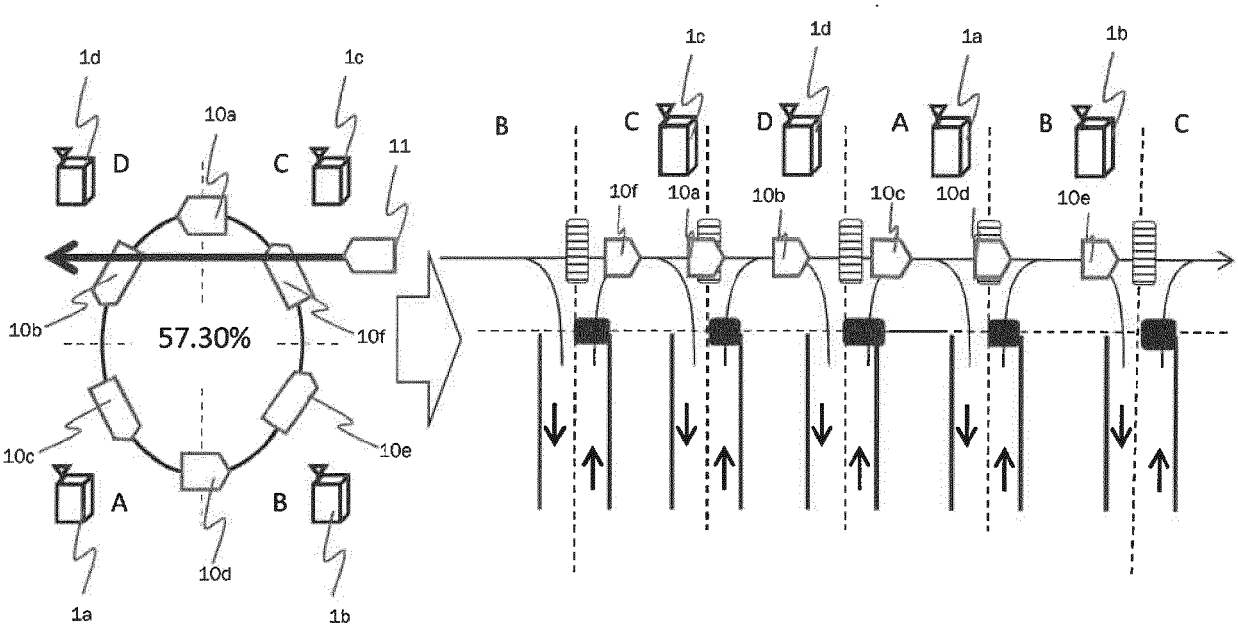

1d
1c
10a
D
C
11
10b
57.30%
10f
10c
10e
A
B
10d
1a
1b
B
C
1c
1d
D
A
1a
B
1b
C
10f
10a
10b
10c
10d
10e

Fig. 37

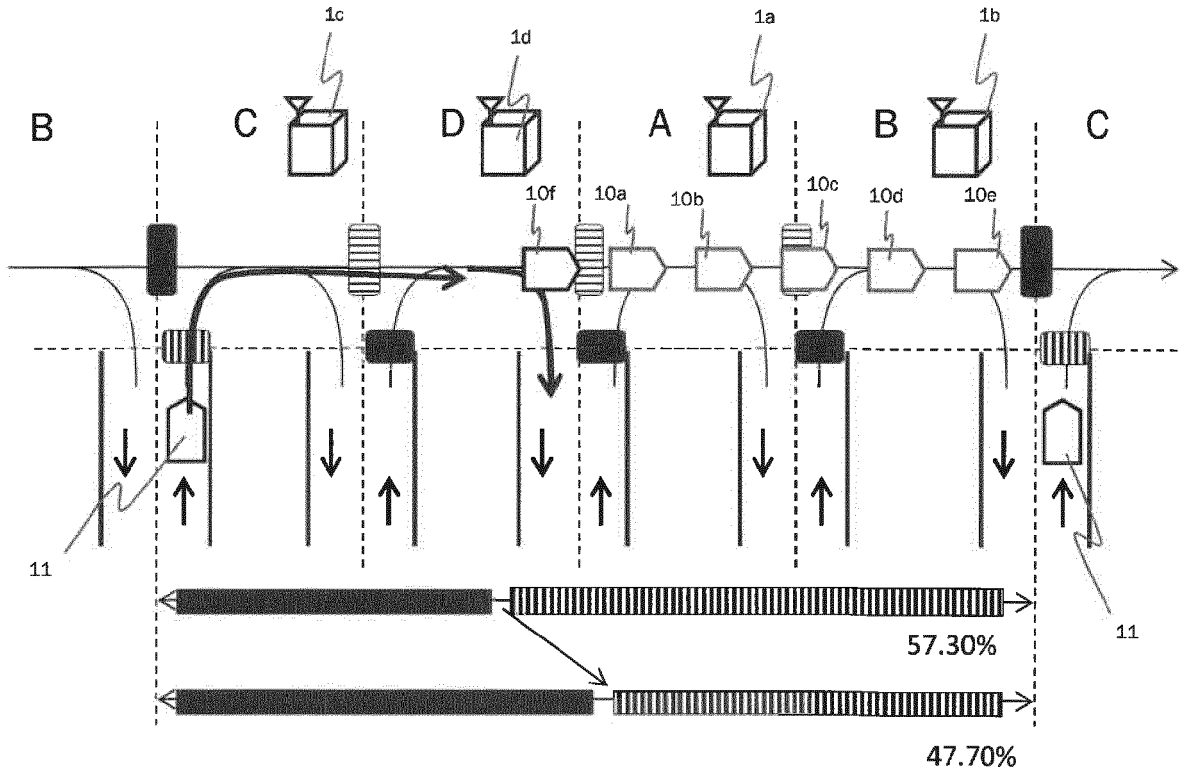

1c
1d
1a
1b
B
C
D
A
B
C
10f
10a
10b
10c
10d
10e
11
57.30%
11
47.70%

Fig. 38

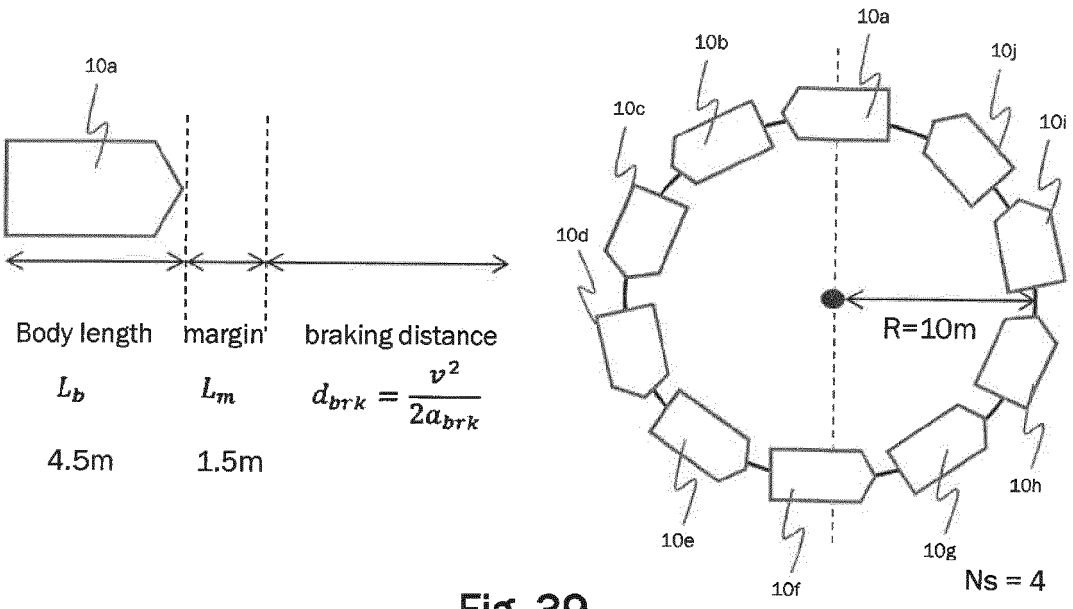



Fig. 39

| | Formula | Example |
|---|---|---|
| Average vehicle speed [m/s] | $v$ | 18kph(5m/s) |
| Braking deceleration [m/s2] | $a_{brk}$ | -0.306G(3.0m/s2) |
| Braking distance[m] | $d_{brk} = \frac{v^2}{2a_{brk}}$ | 4.170m |
| Length of circle[m] | $L_c = 2\pi R$ | 62.832m (in case of R=17m) |
| Required length for each vehicle[m] | $D = L_b + L_m + d_{brk}$ | 6.0m (if v = 0; standstill) |
| Max capacity (Number of vehicles) | $N_{Max} = \frac{L_c}{D}$ | 10.472 vehicle can run at the same time |
| Max capacity / area (Ns: Number of areas) | $\frac{N_{Max}}{Ns}$ | 2.618 vehicle (if Ns=4) |
| Occupancy[%] | $C = \frac{N}{N_{Max}}$ | 38.197% (if N=Ns=4) |

Fig. 40

Europäisches Patentamt
European Patent Office
Office européen des brevets

# EUROPEAN SEARCH REPORT

Application Number
EP 20 18 2410

## DOCUMENTS CONSIDERED TO BE RELEVANT

| Category | Citation of document with indication, where appropriate, of relevant passages | Relevant to claim | CLASSIFICATION OF THE APPLICATION (IPC) |
|---|---|---|---|
| X | DE 10 2013 108034 B3 (DEUTSCHES ZENTRUM FÜR LUFT UND RAUMFAHRT E V [DE]) 8 January 2015 (2015-01-08) | 1,8,17 | INV. G08G1/065 G08G1/0965 G08G1/0967 G07B15/06 |
| A | * paragraph [0007] - paragraph [0012] * * paragraph [0017] * * paragraph [0020] * * paragraph [0043] - paragraph [0044] * * paragraph [0050] - paragraph [0051] * * paragraph [0058] - paragraph [0067] * | 2-7,9-16 | |
| A | US 2019/287396 A1 (SAYIN MUHAMMED O [US] ET AL) 19 September 2019 (2019-09-19) * paragraph [0051] - paragraph [0061] * * paragraph [0090] - paragraph [0111] * | 1-17 | |
| A | US 2019/051166 A1 (BRONK MATEUSZ [PL]) 14 February 2019 (2019-02-14) * paragraph [0038] - paragraph [0048] * * paragraph [0085] - paragraph [0087] * | 1-17 | |
| A | US 2019/311617 A1 (KARAOGUZ CEM [FR]) 10 October 2019 (2019-10-10) * paragraph [0056] - paragraph [0072] * | 1-17 | TECHNICAL FIELDS SEARCHED (IPC) G08G G07B |

The present search report has been drawn up for all claims

| Place of search | Date of completion of the search | Examiner |
|---|---|---|
| The Hague | 22 January 2021 | Nanos, Alexander |

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

## ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 20 18 2410

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

22-01-2021

| Patent document cited in search report | Publication date | Patent family member(s) | Publication date |
|---|---|---|---|
| DE 102013108034 B3 | 08-01-2015 | NONE | |
| US 2019287396 A1 | 19-09-2019 | NONE | |
| US 2019051166 A1 | 14-02-2019 | CN 110660230 A | 07-01-2020 |
| | | DE 102019104309 A1 | 02-01-2020 |
| | | US 2019051166 A1 | 14-02-2019 |
| US 2019311617 A1 | 10-10-2019 | AU 2019202500 A1 | 24-10-2019 |
| | | CA 3039874 A1 | 10-10-2019 |
| | | EP 3553762 A1 | 16-10-2019 |
| | | FR 3079956 A1 | 11-10-2019 |
| | | US 2019311617 A1 | 10-10-2019 |

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82

## REFERENCES CITED IN THE DESCRIPTION

*This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.*

### Patent documents cited in the description


- US 2019130739 A1 **[0002]**
- US 2019302781 A1 **[0002]**