Modeling Car Crash Management with KAOS

Antoine Cailliau, Christophe Damas, Bernard Lambeau, and Axel van Lamsweerde
Université catholique de Louvain (UCL) (http://uclouvain.be/)
Louvain-La-Neuve, Belgium
{firstname}.{lastname}@uclouvain.be

Introduction

This document contains a KAOS [Lam09] modeling for a car crash system [Cal12]. It is the "full modeling" companion of [Cai13]. We invite the reader to have a look at [Cai13] to understand the context in which this work took place and to have a first overview of the modeled system and the KAOS method that has been applied to create it.

This document is semi-automatically generated from the model. The latest pdf and html versions are maintained online at the adresses below. We recommend the HTML version which contains hyperlinks for navigating the model. It requires a modern browser and has been tested both under Google Chrome and Firefox.

- HTML version with hyperlinks (http://kaos.info.ucl.ac.be/bcms.html)
- PDF version (http://kaos.info.ucl.ac.be/bcms.pdf)

For any question about the model, available tool support or this document, please contact the authors of [Cai13].

References

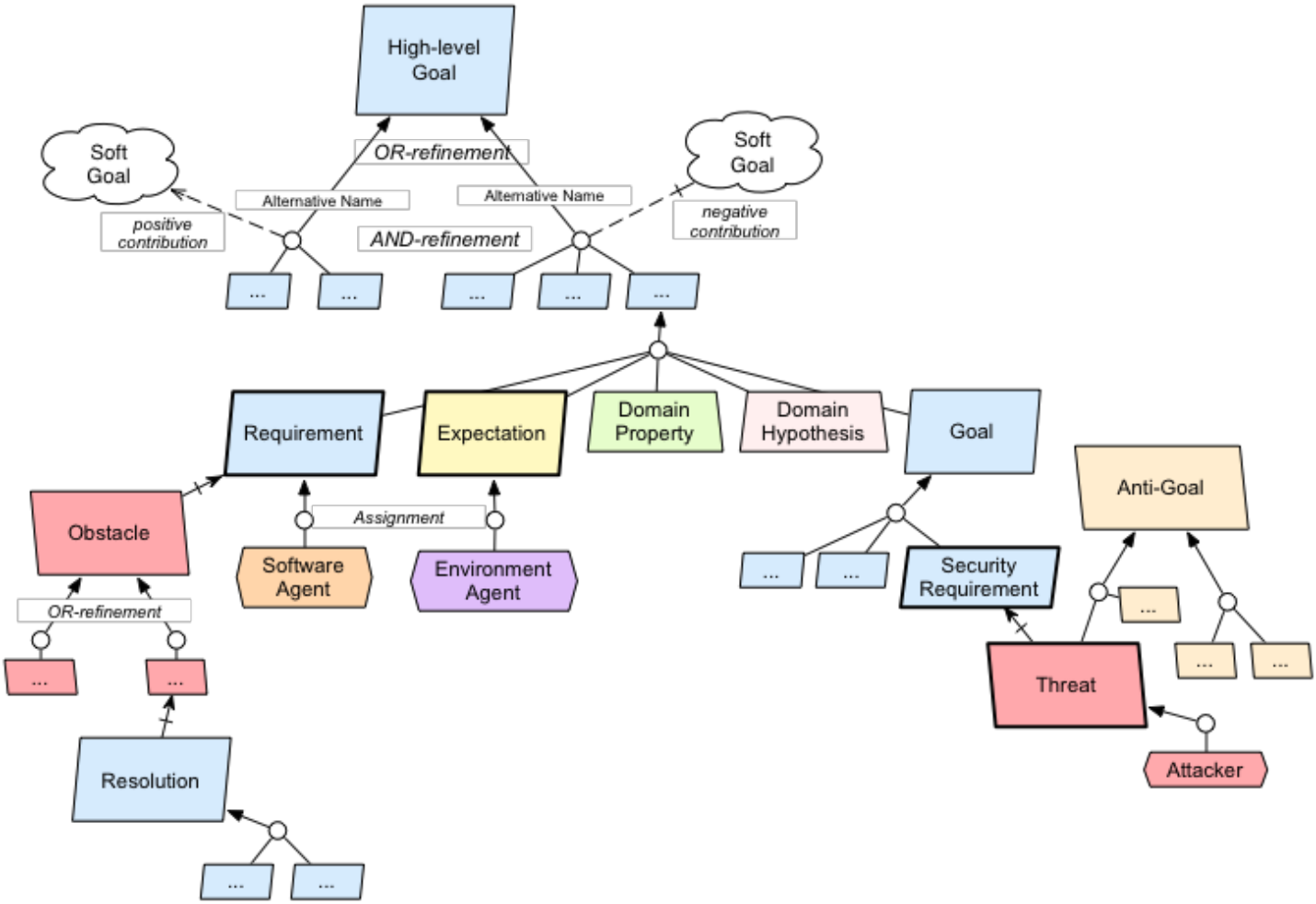
- [Cal12] A. Capozucca, B. H.C. Cheng, G. Georg, N. Guelfi, P. Istoan, G. Mussbacher, *Requirements Definition Document for a software product line of car crash management systems*, May 2012, http://cserg0.site.uottawa.ca/cma2013re/CaseStudy.pdf (http://cserg0.site.uottawa.ca/cma2013re/CaseStudy.pdf)
- [Cai13] A. Cailliau, C. Damas, B. Lambeau, A. van Lamsweerde, *KAOS Modeling for a Car Crash System*, Submitted to "Comparing Requirements Modeling Approaches", Workshop at Requirements Engineering (RE) 2013
- [Lam09] A. van Lamsweerde, *Requirements Engineering: From System Goals to UML Models to Software Specifications*. Wiley, 2009

Outline

Goal Model

This section provides an overview of the main objectives of the bCMS system. High-level goals are successively refined until being assignable to particular agents (see the graphical legend below).

Despite obstacle analysis has already been conducted, the goal model is still idealistic; in particular, it relies on some domain hypotheses whose list can be found in the detailed definition section. Most of those hypotheses should probably be relaxed.

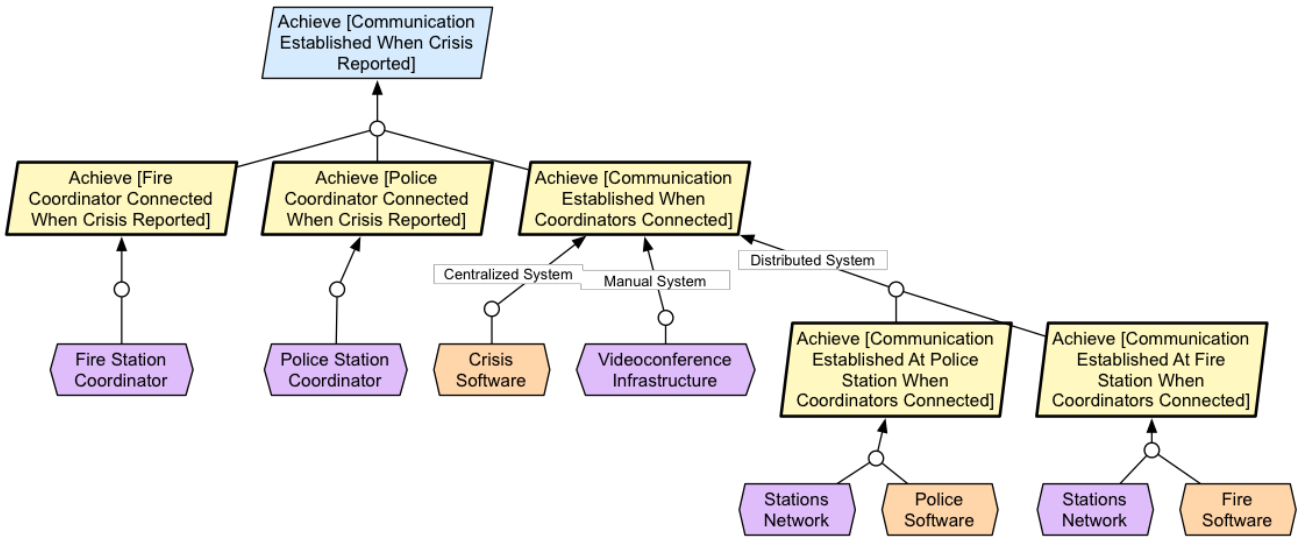


Behavioral goals

Functional goals

Achieve [Communication Established When Crisis Reported]

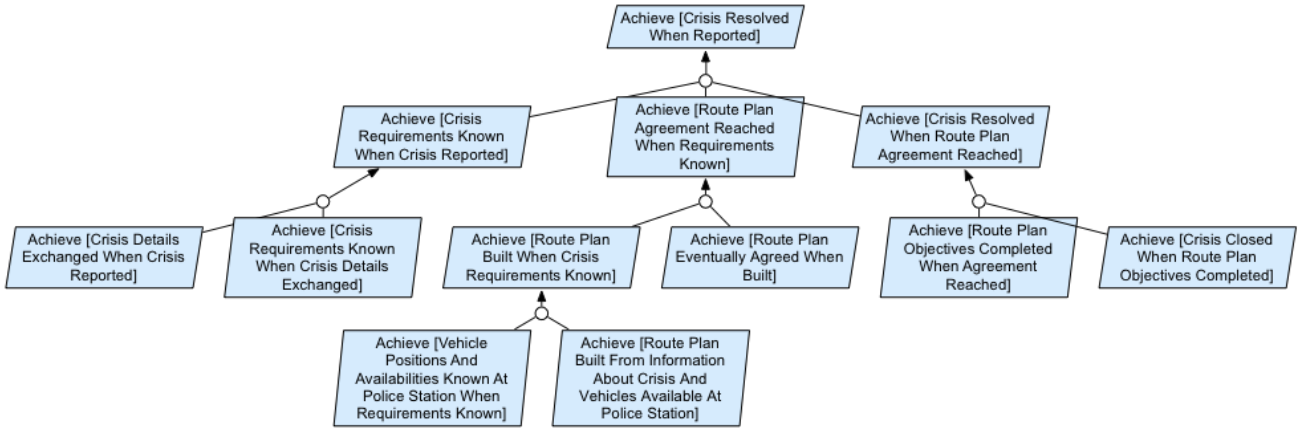
For every reported crisis, communication shall be established between the responsible police and fire coordinators.



Name	Definition
Achieve [Communication Established When Crisis Reported]	For every reported crisis, communication shall be established between the responsible police and fire coordinators.
Achieve [Fire Coordinator Connected When Crisis Reported]	For every reported crisis, the reponsible fire coordinator shall connect to the system as soon as possible.
Achieve [Police Coordinator Connected When Crisis Reported]	For every reported crisis, the reponsible police coordinator shall connect to the system as soon as possible.
Achieve [Communication Established When Coordinators Connected]	For every reported crisis, communication shall be established between the police and fire coordinators as soon as they are connected.
Achieve [Communication Established At Police Station When Coordinators Connected]	For every reported crisis, communication shall be established at police station as soon as fire and police coordinators are connected.
Achieve [Communication Established At Fire Station When Coordinators Connected]	For every reported crisis, communication shall be established at fire station as soon as fire and police coordinators are connected.

Achieve [Crisis Resolved When Reported]

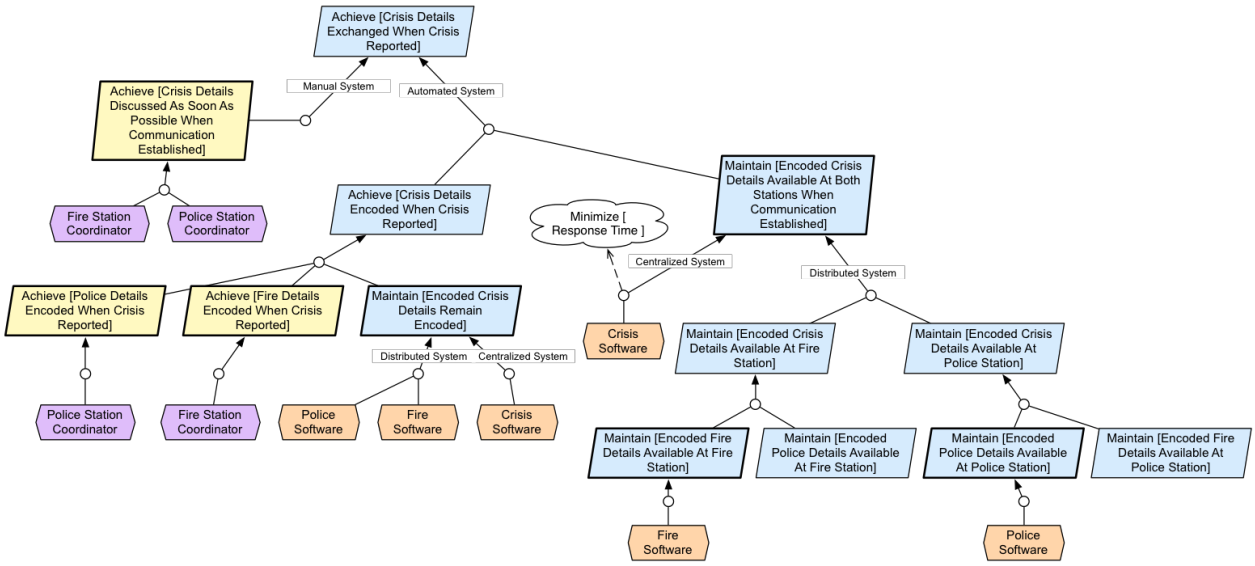
Every crisis shall be eventually resolved when reported.



Name	Definition
Achieve [Crisis Resolved When Reported]	Every crisis shall be eventually resolved when reported.
Achieve [Crisis Requirements Known When Crisis Reported]	For every reported crisis, required resources for handling the crisis shall eventually be known by both coordinators.
Achieve [Route Plan Agreement Reached When Requirements Known]	For every crisis, based on established requirements, the police and fire coordinators shall eventually agree on a route plan to be deployed so as to resolve the crisis.
Achieve [Crisis Resolved When Route Plan Agreement Reached]	For every crisis, when a route plan has been agreed by coordinators then the crisis is eventually resolved.
Achieve [Crisis Details Exchanged When Crisis Reported]	For every reported crisis, all relevant information (e.g. crisis location, number of victims, etc.) shall eventually be exchanged between coordinators.
Achieve [Crisis Requirements Known When Crisis Details Exchanged]	For every reported crisis, when the details have been exchanged between coordinators, the requirements (e.g. the number of required vehicles) shall eventually be known by both of them.
Achieve [Route Plan Built When Crisis Requirements Known]	For every crisis, based on established requirements, a feasible route plan is eventually built by the police coordinator.
Achieve [Route Plan Eventually Agreed When Built]	For every crisis, the route plan built by the police coordinator is eventually agreed by the fire coordinator.
Achieve [Vehicle Positions And Availabilities Known At Police Station When Requirements Known]	For every crisis whose requirements are known, the positions and availabilities of police vehicles and fire trucks shall be known at the police station (so as to allow the PSC to build a route plan).
Achieve [Route Plan Built From Information About Crisis And Vehicles Available At Police Station]	The route plan shall be built from the known crisis requirements and known positions of police vehicle and fire truck. By built, we mean that a route plan draft shall exists with a route for each involved vehicle. The draft shall meet all requirements.
Achieve [Route Plan Objectives Completed When Agreement Reached]	For every crisis, when an agreement has been reached between coordinators on the route plan to deploy, the objective of every vehicle allocated to the crisis is eventually completed.
Achieve [Crisis Closed When Route Plan Objectives Completed]	Every crisis whose all objectives are complete shall eventually be closed.

Achieve [Crisis Details Exchanged When Crisis Reported]

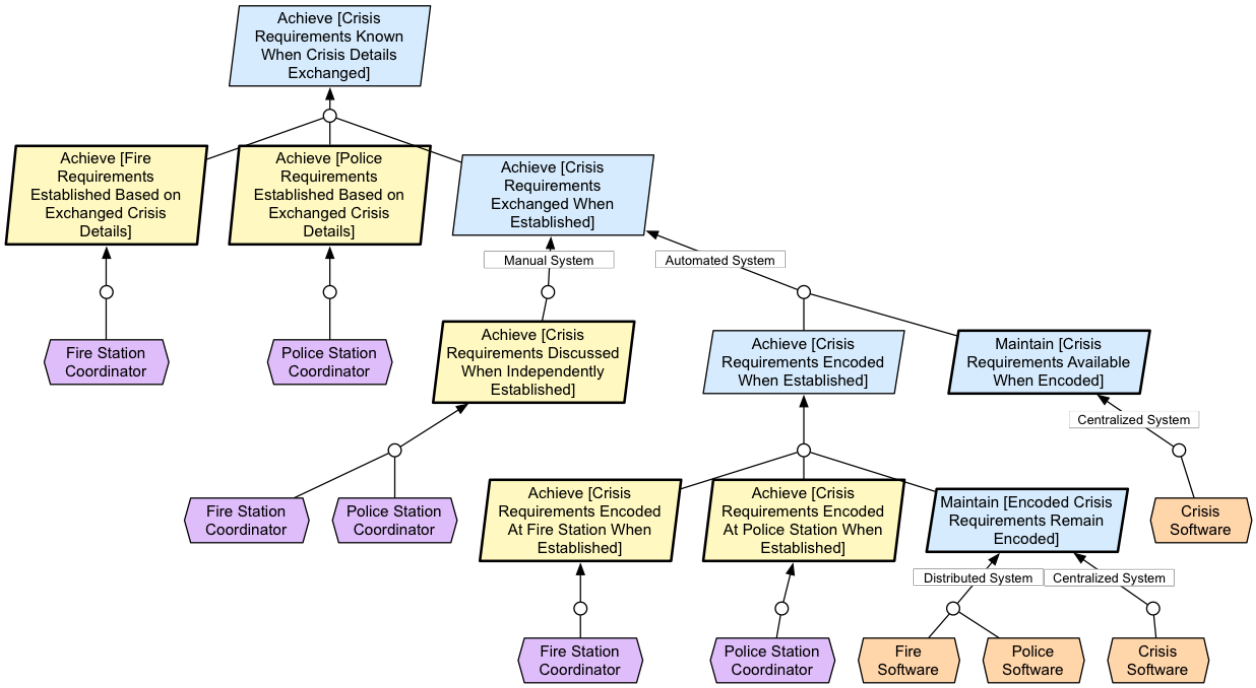
For every reported crisis, all relevant information (e.g. crisis location, number of victims, etc.) shall eventually be exchanged between coordinators.



Name	Definition
Achieve [Crisis Details Exchanged When Crisis Reported]	For every reported crisis, all relevant information (e.g. crisis location, number of victims, etc.) shall eventually be exchanged between coordinators.
Achieve [Crisis Details Discussed As Soon As Possible When Communication Established]	For every reported crisis, as soon as the communication has been established between coordinators, they shall discuss (share and compare) relevant information about the crisis.
Achieve [Crisis Details Encoded When Crisis Reported]	For every crisis, all relevant information shall be independently encoded by coordinators as soon as the crisis is reported.
Maintain [Encoded Crisis Details Available At Both Stations When Communication Established]	For every reported crisis, all encoded details shall be made available both at the fire station and the police station.
Achieve [Police Details Encoded When Crisis Reported]	For every crisis, all relevant information shall be encoded by the police coordinator as soon as the crisis is reported.
Achieve [Fire Details Encoded When Crisis Reported]	For every crisis, all relevant information shall be encoded by the fire coordinator as soon as the crisis is reported.
Maintain [Encoded Crisis Details Remain Encoded]	For every reported crisis, encoded details shall remain encoded until the crisis is resolved.
Maintain [Encoded Crisis Details Available At Fire Station]	The encoded details about the crisis shall be available at fire station. By available, we mean that the information can be known by the fire coordinator (for example, displayed on a screen, printed, etc.).
Maintain [Encoded Crisis Details Available At Police Station]	The encoded details about the crisis shall be available at police station. By available, we mean that the information can be known by the police coordinator (for example, displayed on a screen, printed, etc.).
Maintain [Encoded Fire Details Available At Fire Station]	The encoded fire details about the crisis shall be available at fire station.
Maintain [Encoded Police Details Available At Fire Station]	The encoded police details about the crisis shall be available at fire station.
Maintain [Encoded Police Details Available At Police Station]	The encoded police details about the crisis shall be available at police station.
Maintain [Encoded Fire Details Available At Police Station]	The encoded fire details about the crisis shall be available at police station.

Achieve [Crisis Requirements Known When Crisis Details Exchanged]

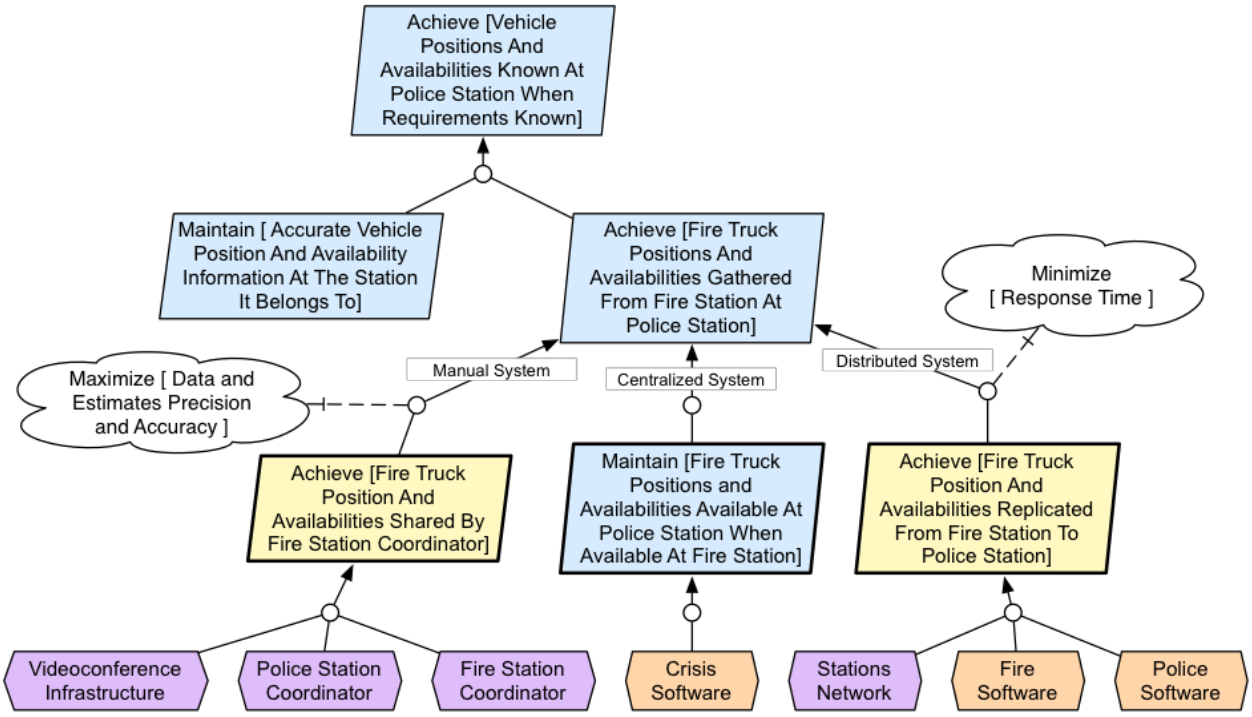
For every reported crisis, when the details have been exchanged between coordinators, the requirements (e.g. the number of required vehicles) shall eventually be known by both of them.



Name	Definition
Achieve [Crisis Requirements Known When Crisis Details Exchanged]	For every reported crisis, when the details have been exchanged between coordinators, the requirements (e.g. the number of required vehicles) shall eventually be known by both of them.
Achieve [Fire Requirements Established Based on Exchanged Crisis Details]	For every crisis, based on exchanged information, the number of fire trucks required shall eventually be established by the fire coordinator.
Achieve [Police Requirements Established Based on Exchanged Crisis Details]	For every crisis, based on exchanged information, the number of police vehicles required shall eventually be established by the police coordinator.
Achieve [Crisis Requirements Exchanged When Established]	For every crisis, when fire and police requirements have been established, they are eventually exchanged with the other coordinator.
Achieve [Crisis Requirements Discussed When Independently Established]	Crisis requirements shall be discussed by both coordinators when crisis has been reported at both station independently.
Achieve [Crisis Requirements Encoded When Established]	Fire and route requirements shall be encoded when crisis has been established at both stations.
Maintain [Crisis Requirements Available When Encoded]	Crisis requirements shall be made available to both coordinators when encoded.
Achieve [Crisis Requirements Encoded At Fire Station When Established]	Fire vehicle requirements shall be encoded at fire station when crisis is established.
Achieve [Crisis Requirements Encoded At Police Station When Established]	Route and police vehicle requirements shall be encoded at police station when crisis is established.
Maintain [Encoded Crisis Requirements Remain Encoded]	When crisis requirements have been encoded in the software they shall remain encoded until the crisis is closed.

Achieve [Vehicle Positions And Availabilities Known At Police Station When Requirements Known]

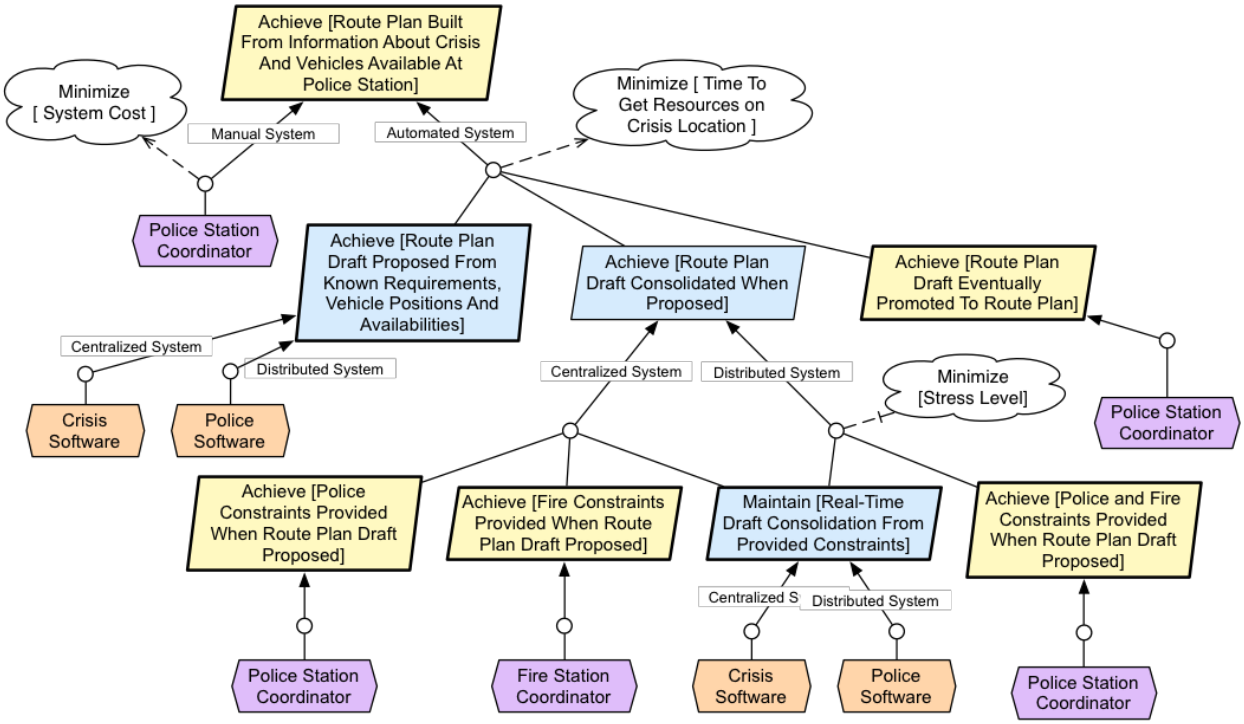
For every crisis whose requirements are known, the positions and availabilities of police vehicles and fire trucks shall be known at the police station (so as to allow the PSC to build a route plan).



Name	Definition
Achieve [Vehicle Positions And Availabilities Known At Police Station When Requirements Known]	For every crisis whose requirements are known, the positions and availabilities of police vehicles and fire trucks shall be known at the police station (so as to allow the PSC to build a route plan).
Maintain [Accurate Vehicle Position And Availability Information At The Station It Belongs To]	The system shall ensure that the information about the positions and availibilities of police vehicles and fire trucks used in critical decisions remains accurate 99,99% of the time at the station to which the vehicle belongs.
Achieve [Fire Truck Positions And Availabilities Gathered From Fire Station At Police Station]	For every crisis whose requirements are known, the positions and availabilities of fire trucks shall be gathered from the fire station so as to be known at police station too.
Achieve [Fire Truck Position And Availabilities Shared By Fire Station Coordinator]	The position and availabilities of each fire truck shall be shared by the fire station coordinator with the police station coordinators.
Maintain [Fire Truck Positions and Availabilities Available At Police Station When Available At Fire Station]	The position and availabilities of each fire truck shall be available at the police station when available at the fire station.
Achieve [Fire Truck Position And Availabilities Replicated From Fire Station To Police Station]	The position and availabilities of each fire truck shall be replicated from the database of the fire station to the database of the police station.

Achieve [Route Plan Built From Information About Crisis And Vehicles Available At Police Station]

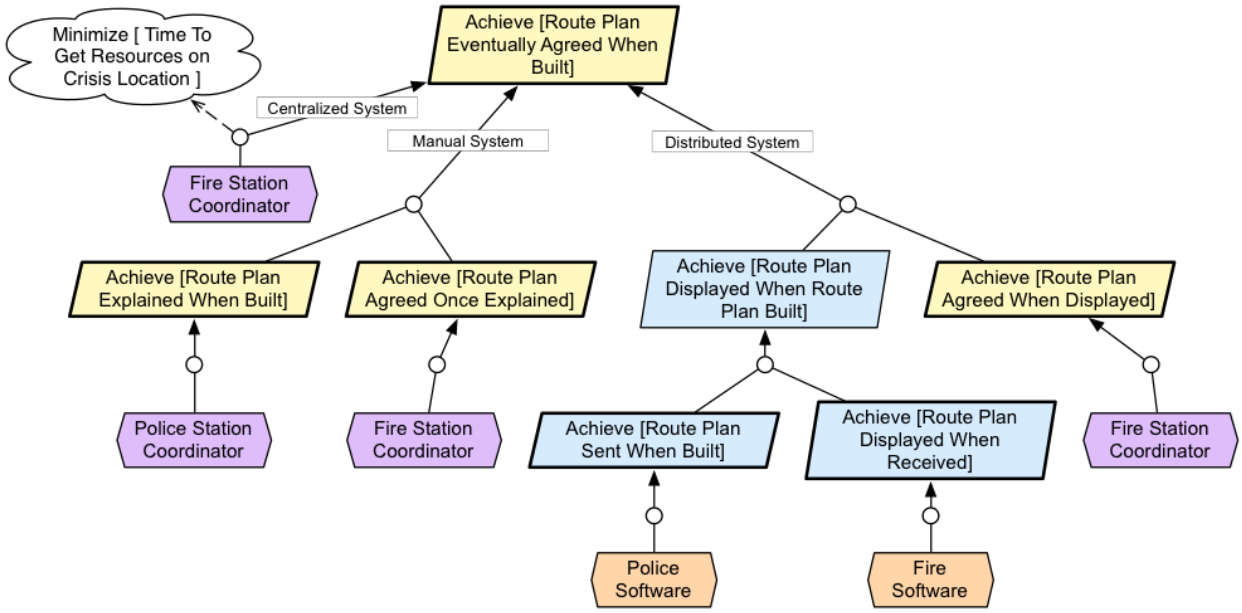
The route plan shall be built from the known crisis requirements and known positions of police vehicle and fire truck. By built, we mean that a route plan draft shall exists with a route for each involved vehicle. The draft shall meet all requirements.



Name	Definition
Achieve [Route Plan Built From Information About Crisis And Vehicles Available At Police Station]	The route plan shall be built from the known crisis requirements and known positions of police vehicle and fire truck. By built, we mean that a route plan draft shall exists with a route for each involved vehicle. The draft shall meet all requirements.
Achieve [Route Plan Draft Proposed From Known Requirements, Vehicle Positions And Availabilities]	When the crisis requirements as well as vehicle positions and availibilities are known a route plan draft is eventually proposed by the software to the coordinators.
Achieve [Route Plan Draft Consolidated When Proposed]	When a route plan draft is proposed, it is eventually consolidated, meaning that necessary constraints known by coordinators are taken into account such that the plan deployment is feasible and such that the crisis is likely to be resolved in a timely manner. Also, for each vehicle its path (from its current position to the crisis scene) and its ETA is computed.
Achieve [Route Plan Draft Eventually Promoted To Route Plan]	The consolidated route plan draft is eventually promoted as a route plan when it all necessary constraints have been taken into account.
Achieve [Police Constraints Provided When Route Plan Draft Proposed]	When a route plan draft is proposed, the police constraints are eventually provided to the software for plan consolidation.
Maintain [Real-Time Draft Consolidation From Provided Constraints]	The software shall consolidate the route plan draft from the known vehicle position and constraints provided by coordinator(s). In particular, the path (from its current position to the crisis scene) and ETA is computed for each vehicle.
Achieve [Fire Constraints Provided When Route Plan Draft Proposed]	When a route plan draft is proposed, the fire constraints are eventually provided to the software for plan consolidation.
Achieve [Police and Fire Constraints Provided When Route Plan Draft Proposed]	When a route plan draft is proposed, the police and fire constraints are eventually provided to the software for plan consolidation.

Achieve [Route Plan Eventually Agreed When Built]

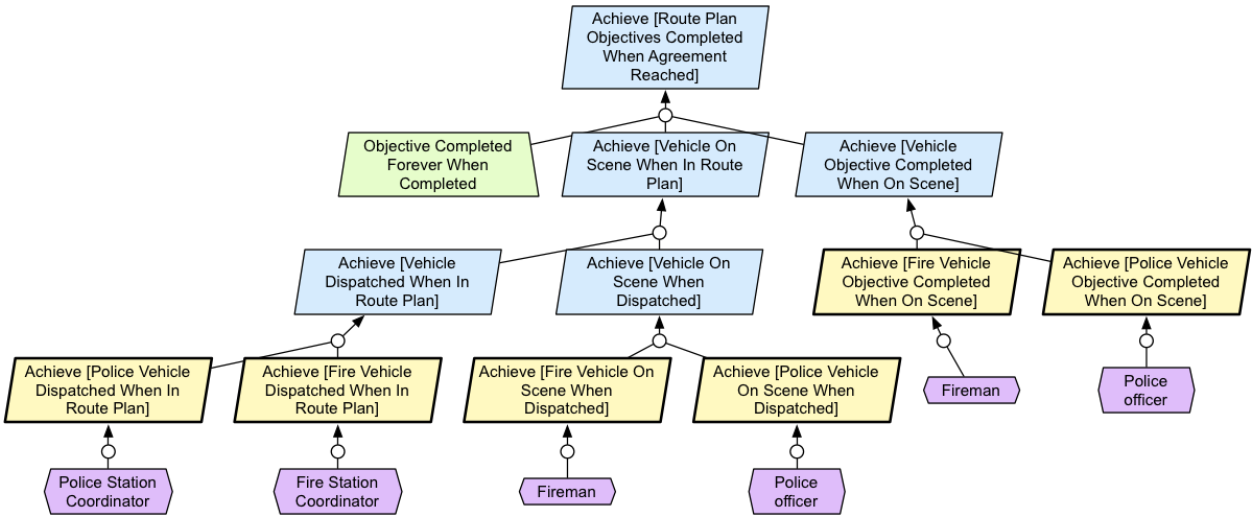
For every crisis, the route plan built by the police coordinator is eventually agreed by the fire coordinator.



Name	Definition
Achieve [Route Plan Eventually Agreed When Built]	For every crisis, the route plan built by the police coordinator is eventually agreed by the fire coordinator.
Achieve [Route Plan Explained When Built]	For every crisis, the route plan built by the police coordinator is eventually explained to the fire coordinator.
Achieve [Route Plan Agreed Once Explained]	For every crisis, the route plan built by the police coordinator is eventually agreed by the fire coordinator when it has been explained.
Achieve [Route Plan Displayed When Route Plan Built]	For every crisis, the route plan built by the police coordinator is eventually displayed at the fire station.
Achieve [Route Plan Agreed When Displayed]	For every crisis, the route plan built by the police coordinator is eventually agreed by the fire coordinator when displayed in the fire station.
Achieve [Route Plan Sent When Built]	For every crisis, the route plan built by the police coordinator is eventually sent at the fire station.
Achieve [Route Plan Displayed When Received]	When received at the fire station, the route plan is eventually displayed.

Achieve [Route Plan Objectives Completed When Agreement Reached]

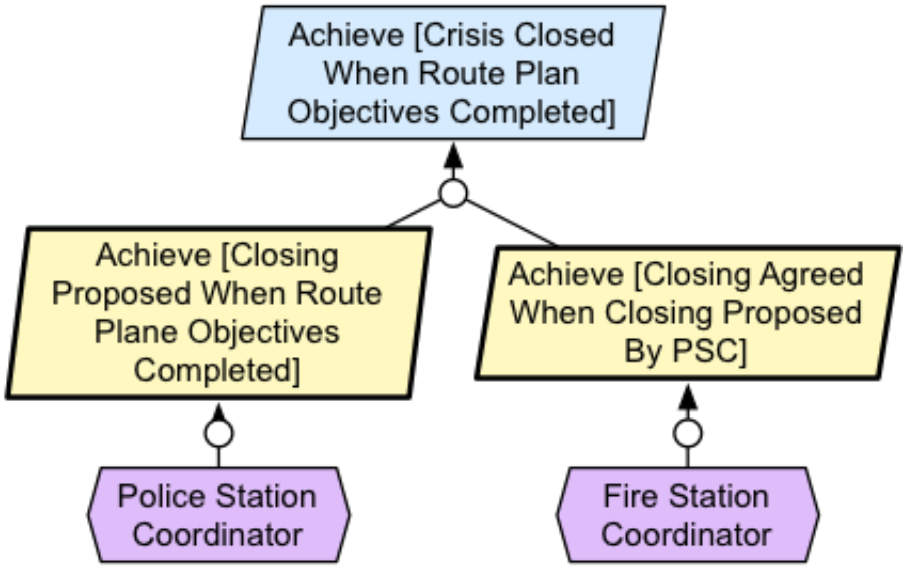
For every crisis, when an agreement has been reached between coordinators on the route plan to deploy, the objective of every vehicle allocated to the crisis is eventually completed.



Name	Definition
Achieve [Route Plan Objectives Completed When Agreement Reached]	For every crisis, when an agreement has been reached between coordinators on the route plan to deploy, the objective of every vehicle allocated to the crisis is eventually completed. $\forall$ c:Crisis · RoutePlanAgreementReached(c) $\Rightarrow$ $\Diamond$ $\forall$ v:Vehicle · VehicleObjectiveCompleted(c, v)
Achieve [Vehicle On Scene When In Route Plan]	Every vehicle involved in a agreed route plan shall be at the crisis location as soon as possible. $\forall$ c:Crisis, v:Vehicle, rp:RoutePlan · Agreed(rp, c) $\wedge$ VehicleInRoutePlan(v, rp) $\Rightarrow$ $\Diamond_{\leq 12m}$ VehicleOnScene(c, v)
Achieve [Vehicle Dispatched When In Route Plan]	Every vehicle involved in a agreed route plan shall be dispatched as soon as possible. $\forall$ c:Crisis, v:Vehicle, rp:RoutePlan · Agreed(rp, c) $\wedge$ VehicleInRoutePlan(v, rp) $\Rightarrow$ $\Diamond_{\leq 2m}$ VehicleDespatched(c, v)
Achieve [Police Vehicle Dispatched When In Route Plan]	Every police vehicle involved in a agreed route plan shall be dispatched as soon as possible. $\forall$ c:Crisis, v:PoliceVehicle, rp:RoutePlan · Agreed(rp, c) $\wedge$ VehicleInRoutePlan(v, rp) $\Rightarrow$ $\Diamond_{\leq 2m}$ VehicleDespatched(c, v)
Achieve [Vehicle On Scene When Dispatched]	Every dispatched vehicle shall reach the crisis location as soon as possible. $\forall$ c:Crisis, v:Vehicle · VehicleDespatched(c, v) $\Rightarrow$ $\Diamond_{\leq 10m}$ VehicleOnScene(c, v)
Achieve [Fire Truck On Scene When Dispatched]	Every dispatched fire truck shall reach the crisis location as soon as possible. $\forall$ c:Crisis, v:FireVehicle · VehicleDespatched(c, v) $\Rightarrow$ $\Diamond_{\leq 10m}$ VehicleOnScene(c, v)
Achieve [Police Vehicle On Scene When Dispatched]	Every dispatched police vehicle shall reach the crisis location as soon as possible. $\forall$ c:Crisis, v:PoliceVehicle · VehicleDespatched(c, v) $\Rightarrow$ $\Diamond_{\leq 10m}$ VehicleOnScene(c, v)
Achieve [Vehicle Objective Completed When On Scene]	Every vehicle at the crisis location shall eventually complete its objective. $\forall$ c:Crisis, v:Vehicle · VehicleDespatched(c, v) $\Rightarrow$ $\Diamond$ VehicleObjectiveCompleted(c, v)
Achieve [Fire Truck Objective Completed When On Scene]	Every fire truck at the crisis location shall eventually complete its objective. $\forall$ c:Crisis, v:FireVehicle · VehicleDespatched(c, v) $\Rightarrow$ $\Diamond$ VehicleObjectiveCompleted(c, v)
Achieve [Police Vehicle Objective Completed When On Scene]	Every police vehicle at the crisis location shall eventually complete its objective. $\forall$ c:Crisis, v:PoliceVehicle · VehicleDespatched(c, v) $\Rightarrow$ $\Diamond$ VehicleObjectiveCompleted(c, v)

Achieve [Crisis Closed When Route Plan Objectives Completed]

Every crisis whose all objectives are complete shall eventually be closed.

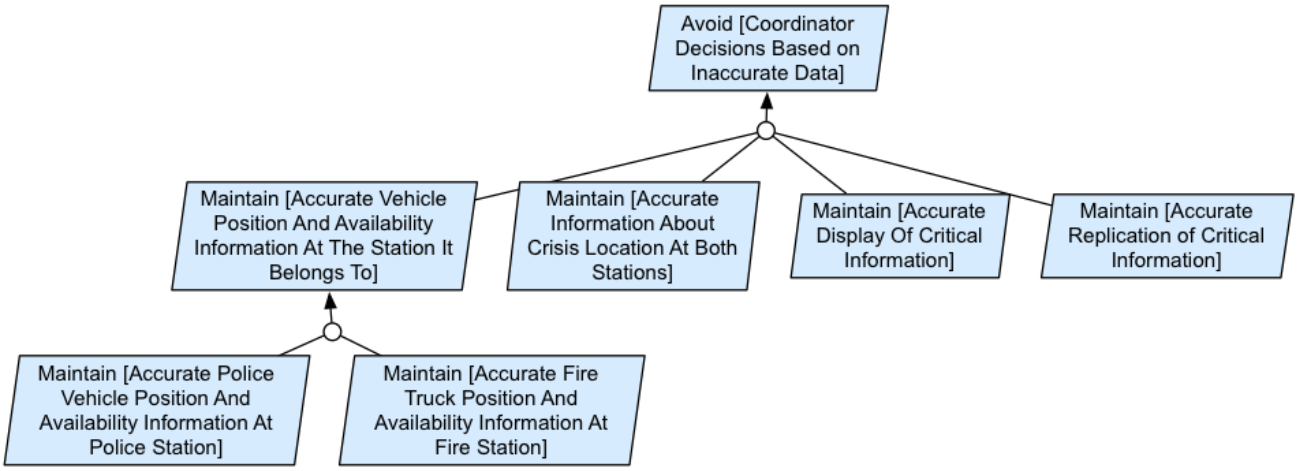


Name	Definition
Achieve [Crisis Closed When Route Plan Objectives Completed]	Every crisis whose all objectives are complete shall eventually be closed. $\forall$ c:Crisis · ($\forall$ v:Vehicle · VehicleObjectiveCompleted(c, v)) $\Rightarrow$ $\Diamond_{\leq 1h}$ CrisisClosed(c)
Achieve [Closing Proposed When Route Plane Objectives Completed]	For every crisis for which all route plan objectives have been completed a closing proposal shall be proposed by the PSC to the FSC. $\forall$ c:Crisis · ($\forall$ v:Vehicle · VehicleObjectiveCompleted(c, v)) $\Rightarrow$ $\Diamond_{\leq 55m}$ ClosingProposed(c)
Achieve [Closing Agreed When Closing Proposed By PSC]	A crisis closing proposal shall eventually be accepted by the FSC when proposed by the PSC. $\forall$ c:Crisis · ClosingProposed(c) $\Rightarrow$ $\Diamond_{\leq 5m}$ CrisisClosed(c)

Non-functional goals

Avoid [Coordinator Decisions Based on Inaccurate Data]

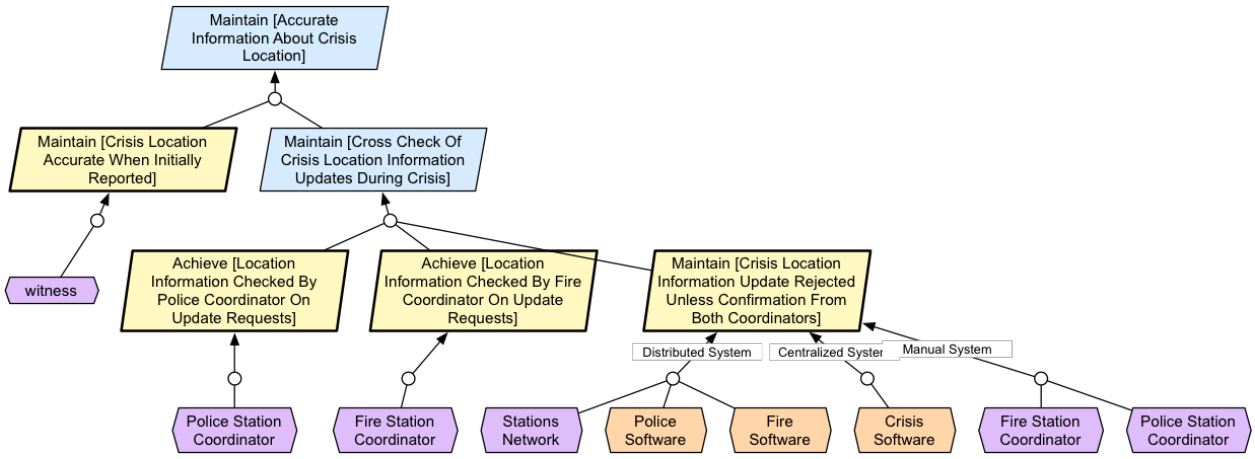
The system shall ensure that every critical decision taken by coordinators shall be based on accurate data 99,99% of the time and 95% of the time for other decisions.



Name	Definition
Avoid [Coordinator Decisions Based on Inaccurate Data]	The system shall ensure that every critical decision taken by coordinators shall be based on accurate data 99,99% of the time and 95% of the time for other decisions.
Maintain [Accurate Vehicle Position And Availability Information At The Station It Belongs To]	The system shall ensure that the information about the positions and availibilities of police vehicles and fire trucks used in critical decisions remains accurate 99,99% of the time at the station to which the vehicle belongs.
Maintain [Accurate Information About Crisis Location At Both Stations]	The system shall ensure that the information about the crisis location is accurate 99,99% of the time as such information is used for critical decisions.
Maintain [Accurate Display Of Critical Information]	The system shall ensure the accuracy of critical information when displayed. In particular, devices diplaying the location of the crisis and vehicles shall be refreshed in less than 3 sec. every time the underlying information changes.
Maintain [Accurate Replication of Critical Information]	Every replication of critical information from one station to the other shall be accurate. In particular, if replicated, vehicle information (position, availability) shall not differ for longer than 1 sec, 99,99% of the time.
Maintain [Accurate Police Vehicle Position And Availability Information At Police Station]	The positions and availabilities of police vehicle shall be accurately known at police station. The refinement of this goal is similar to what happens for fire trucks.
Maintain [Accurate Fire Truck Position And Availability Information At Fire Station]	The position and availabilities of fire truck shall be accurately known at fire station. By accurate, we mean that the position does not differ for more than X meters and the availability are the same within Y seconds.

Maintain [Accurate Information About Crisis Location At Both Stations]

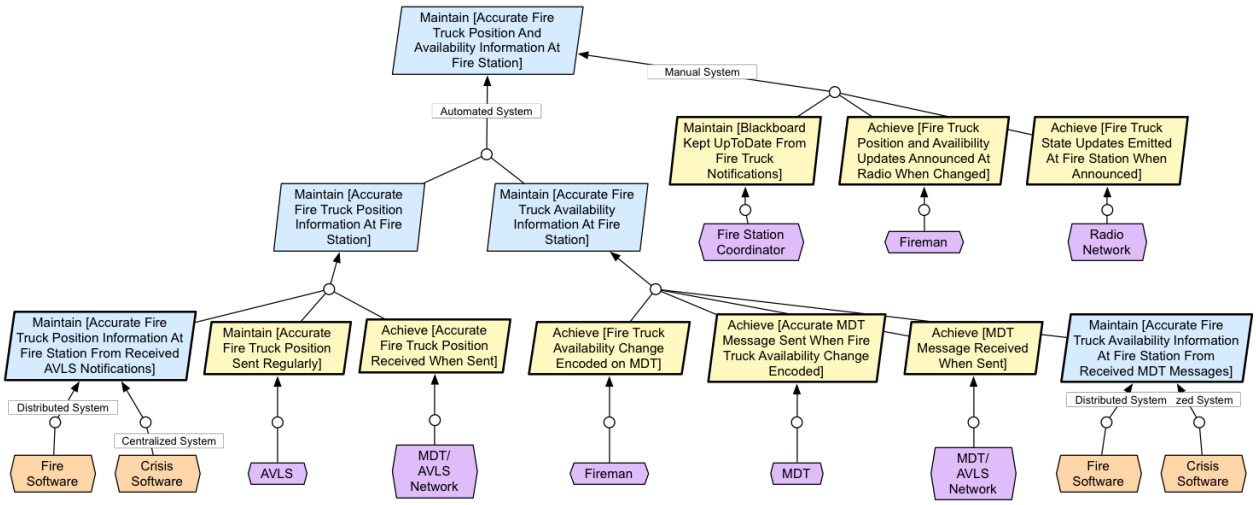
The system shall ensure that the information about the crisis location is accurate 99,99% of the time as such information is used for critical decisions.



Name	Definition
Maintain [Accurate Information About Crisis Location At Both Stations]	The system shall ensure that the information about the crisis location is accurate 99,99% of the time as such information is used for critical decisions.
Maintain [Crisis Location Accurate When Initially Reported]	The crisis location shall be accurately reported by witnesses.
Maintain [Cross Check Of Crisis Location Information Updates During Crisis]	The system shall ensure that updates to the crisis location information at stations shall be cross checked by both coordinators.
Achieve [Location Information Checked By Police Coordinator On Update Requests]	The crisis location shall be explicitely checked by the police coordinator every time an update of the location information is requested to the software.
Achieve [Location Information Checked By Fire Coordinator On Update Requests]	The crisis location shall be explicitely checked by the fire coordinator every time an update of the location information is requested to the software.
Maintain [Crisis Location Information Update Rejected Unless Confirmation From Both Coordinators]	Every request for update of the crisis location information at stations shall be rejected unless a confirmation has been explicitely made by both coordinators.

Maintain [Accurate Fire Truck Position And Availability Information At Fire Station]

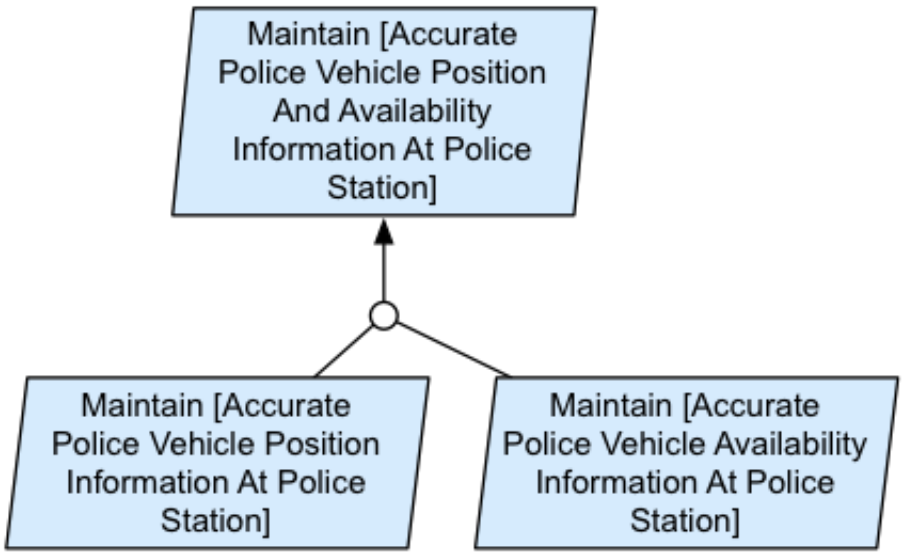
The position and availabilities of fire truck shall be accurately known at fire station. By accurate, we mean that the position does not differ for more than X meters and the availability are the same within Y seconds.



Name	Definition
Maintain [Accurate Fire Truck Position And Availability Information At Fire Station]	The position and availabilities of fire truck shall be accurately known at fire station. By accurate, we mean that the position does not differ for more than X meters and the availability are the same within Y seconds.
Achieve [Fire Truck Position and Availibility Updates Announced At Radio When Changed]	Fireman shall announce at radio state main changes of the fire truck position and availability updates.
Achieve [Fire Truck State Updates Emitted At Fire Station When Announced]	Fire truck, resp. police vehicle, state updates announced by radio shall be emitted at the fire station.
Maintain [Blackboard Kept UpToDate From Fire Truck Notifications]	Accurate information about the position and availability of the fire trucks shall be kept up-to-date and displayed on a blackboard. State shall be updated on update notification.
Maintain [Accurate Fire Truck Position Information At Fire Station]	The position of fire trucks shall be accurately known at fire station.
Maintain [Accurate Fire Truck Availability Information At Fire Station]	The availabilities of fire truck shall be accurately known at fire station.
Maintain [Accurate Fire Truck Position Sent Regularly]	The accurate position of fire truck shall be sent every 30 seconds.
Achieve [Accurate Fire Truck Position Received When Sent]	The accurate position shall be received within 5 seconds when sent.
Maintain [Accurate Fire Truck Position Information At Fire Station From Received AVLS Notifications]	The accurate position of fire truck shall be known at fire station when received.
Achieve [Fire Truck Availability Change Encoded on MDT]	When the availability of the fire vehicle changes, the fireman shall encode that change by pressing rhe right button on its MDT. More specifically, the 'Available' button shall be pressed when the fire truck completed its objectives, 'Dispatched' shall be pressed when the fire vehicle acknowledges its participation to a route plan and 'OnScene' when the fire truck arrives on the crisis scene.
Achieve [Accurate MDT Message Sent When Fire Truck Availability Change Encoded]	Every time the availability of a fire truck is changed through encoding on its MDT, a message shall be sent containing the vehicle ID and information about the new availability.
Achieve [MDT Message Received When Sent]	Sent MDT messages shall be received at corresponding station.
Maintain [Accurate Fire Truck Availability Information At Fire Station From Received MDT Messages]	The accurate availabilities of fire trucks shall be known at fire station based on the received MDT messages.

Maintain [Accurate Police Vehicle Position And Availability Information At Police Station]

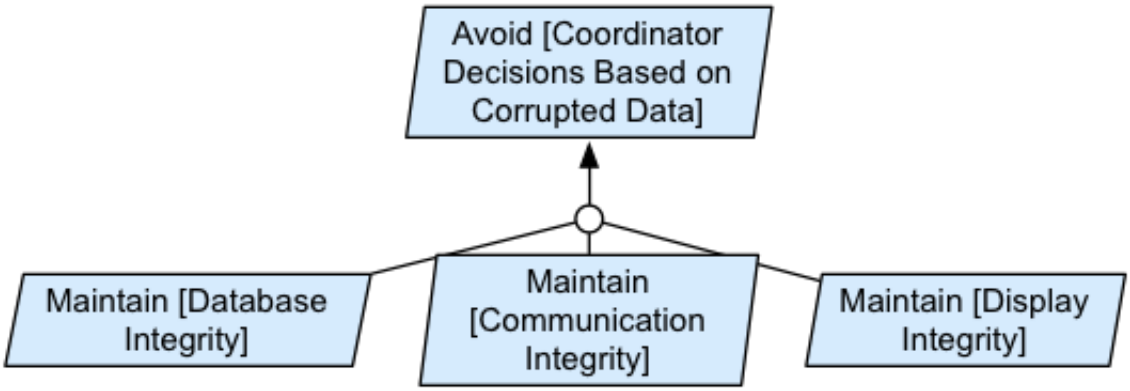
The positions and availabilities of police vehicle shall be accurately known at police station. The refinement of this goal is similar to what happens for fire trucks.



Name	Definition
Maintain [Accurate Police Vehicle Position Information At Police Station]	The positions of police vehicle shall be accurately known at police station. The refinement of this goal is similar to what happens for fire trucks.
Maintain [Accurate Police Vehicle Availability Information At Police Station]	The availabilities of police vehicle shall be accurately known at police station. The refinement of this goal is similar to what happens for fire trucks.

Avoid [Coordinator Decisions Based on Corrupted Data]

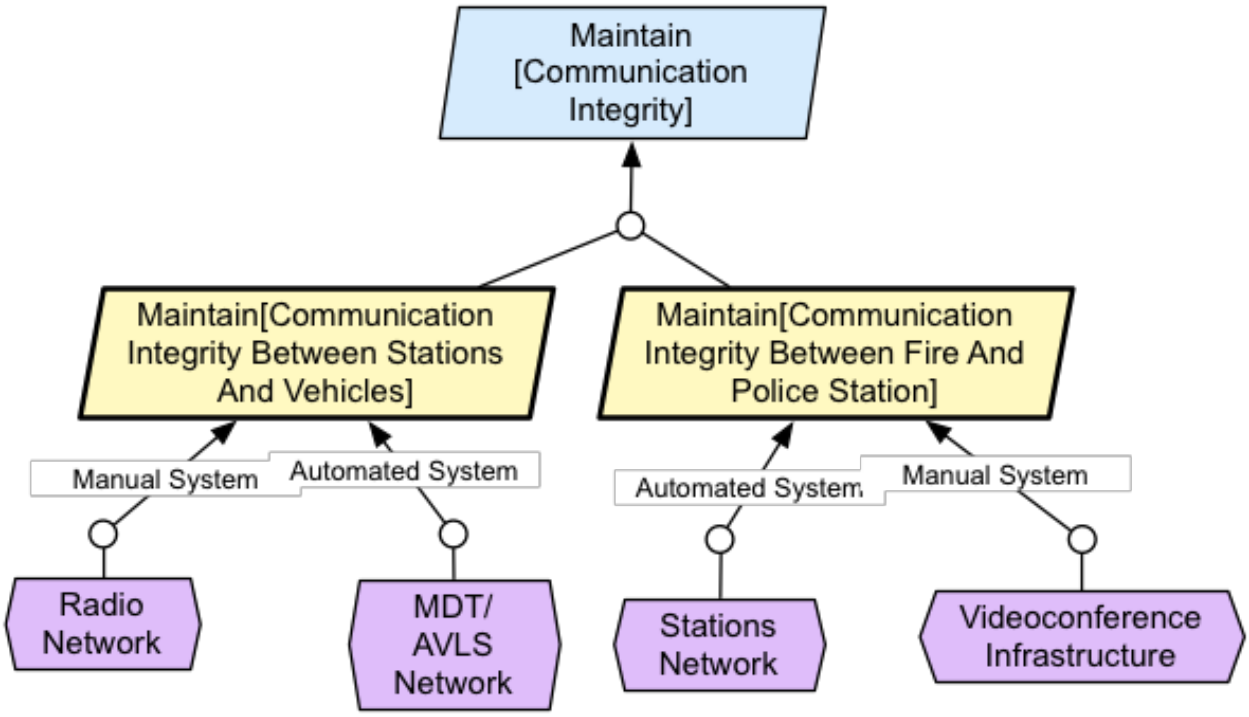
The system shall ensure that the integrity of every data on which critical decisions are taken by coordinators (such as crisis location, vehicle number and vehicle location) is preserved 99,99% of the time and 95% of the time for other data.



Name	Definition
Avoid [Coordinator Decisions Based on Corrupted Data]	The system shall ensure that the integrity of every data on which critical decisions are taken by coordinators (such as crisis location, vehicle number and vehicle location) is preserved 99,99% of the time and 95% of the time for other data.
Maintain [Database Integrity]	The system shall ensure that the integrity of data kept in software databases is preserved 99,99% of the time.
Maintain [Communication Integrity]	The system shall ensure that the integrity of every critical data transmitted to stations (such as crisis location, vehicle number and vehicle location) is preserved 99,99% of the time and 95% of the time for other data.
Maintain [Display Integrity]	The system shall ensure that the integrity of every critical data displayed at stations (such as crisis location, vehicle number and vehicle location) is preserved 99,99% of the time and 95% of the time for other data.

Maintain [Communication Integrity]

The system shall ensure that the integrity of every critical data transmitted to stations (such as crisis location, vehicle number and vehicle location) is preserved 99,99% of the time and 95% of the time for other data.



Name	Definition
Maintain[Communication Integrity Between Fire And Police Station]	The system shall ensure that the integrity of every critical data transmitted between fire and police stations (such as crisis location, vehicle number and vehicle location) is preserved 99,99% of the time and 95% of the time for other data.

Maintain [Database Integrity]

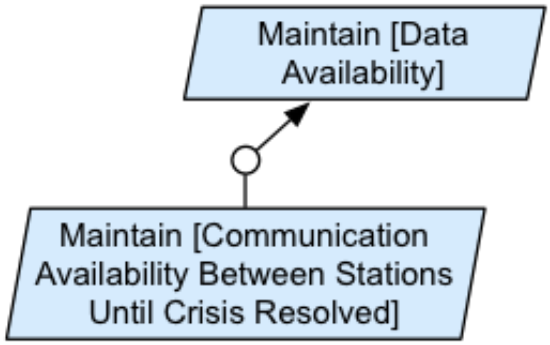
The system shall ensure that the integrity of data kept in software databases is preserved 99,99% of the time.

Maintain [Display Integrity]

The system shall ensure that the integrity of every critical data displayed at stations (such as crisis location, vehicle number and vehicle location) is preserved 99,99% of the time and 95% of the time for other data.

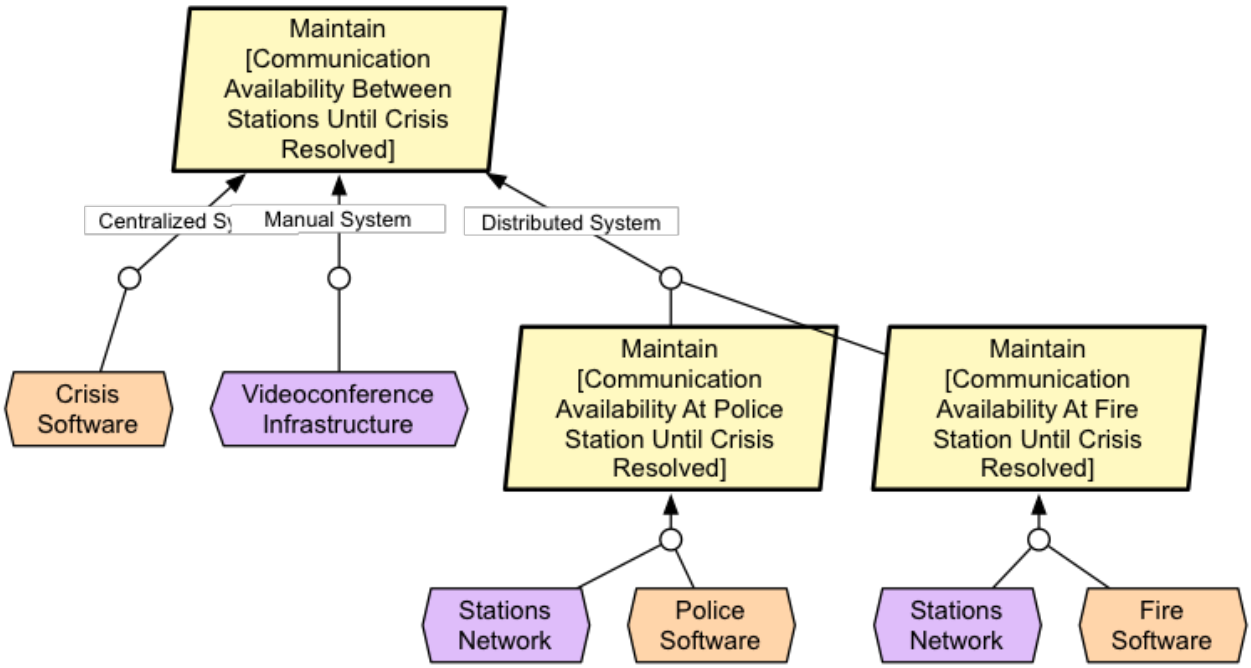
Maintain [Data Availability]

- The crisis details, route plan and information related to the identification of coordinators shall be available with the exception of a total of 5 minutes during the time period when at least one crisis is active.
- The crisis details and route plans should be available with the exception of a total of 30 minutes for every 48 hours when no crisis is active.



Maintain [Communication Availability Between Stations Until Crisis Resolved]

For every crisis, when communication is established between the responsible police and fire coordinators, it shall remain established until the crisis is resolved.



Name	Definition
Maintain [Communication Availability Between Stations Until Crisis Resolved]	For every crisis, when communication is established between the responsible police and fire coordinators, it shall remain established until the crisis is resolved.
Maintain [Communication Availability At Police Station Until Crisis Resolved]	For every crisis, when communication is established at the police station, it shall remain established until the crisis is resolved.
Maintain [Communication Availability At Fire Station Until Crisis Resolved]	For every crisis, when communication is established at the fire station, it shall remain established until the crisis is resolved.

Soft goals

Minimize [Time To Get Resources on Crisis Location]

Getting needed resources on the crisis location, such as police vehicles and fire trucks shall take the shortest possitble amount of time.

Maximize [Data and Estimates Precision and Accuracy]

The estimation of resource needs and time of arrivals for resources shall be as accurate as possible. More generally the accuracy and precision of any non-critical data critical shall be maximized.

Minimize [Stress Level]

The system shall help minimizing the stress level of both coordinators.

Minimize [System Cost]

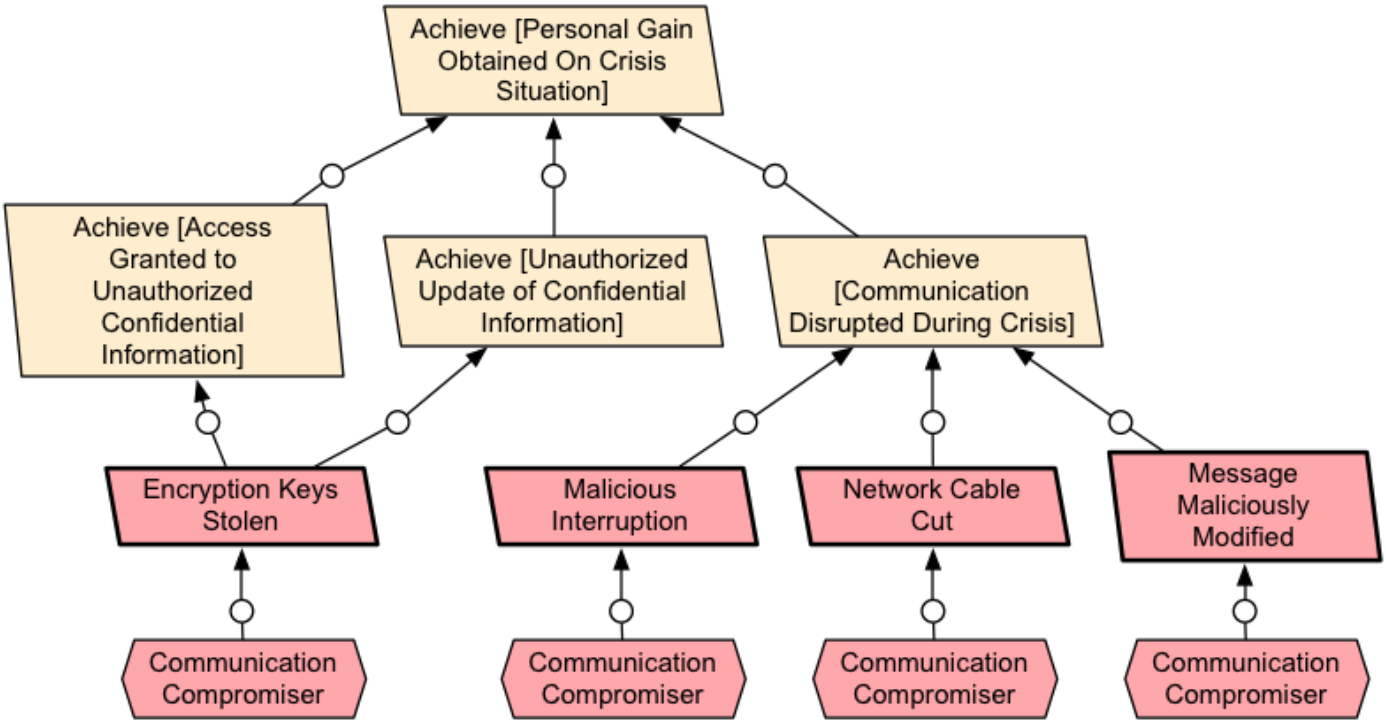
The system shall ensure effective response times with minimal costs.

Minimize [Response Time]

- The system shall respond to user requests within 5 seconds 95% of the time.
- The system shall respond to user requests within 30 seconds 99,99% of the time.

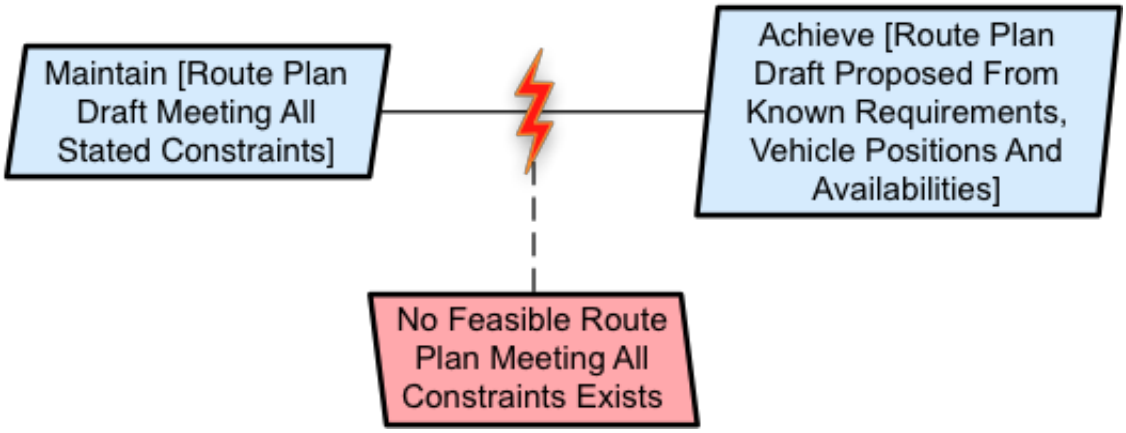
Anti-Goals

The anti-goal model is only preliminary as the domain of the communication compromiser has not been elicited. See the obstacle-analysis section for resolution of security threats identified here.



Conflicts

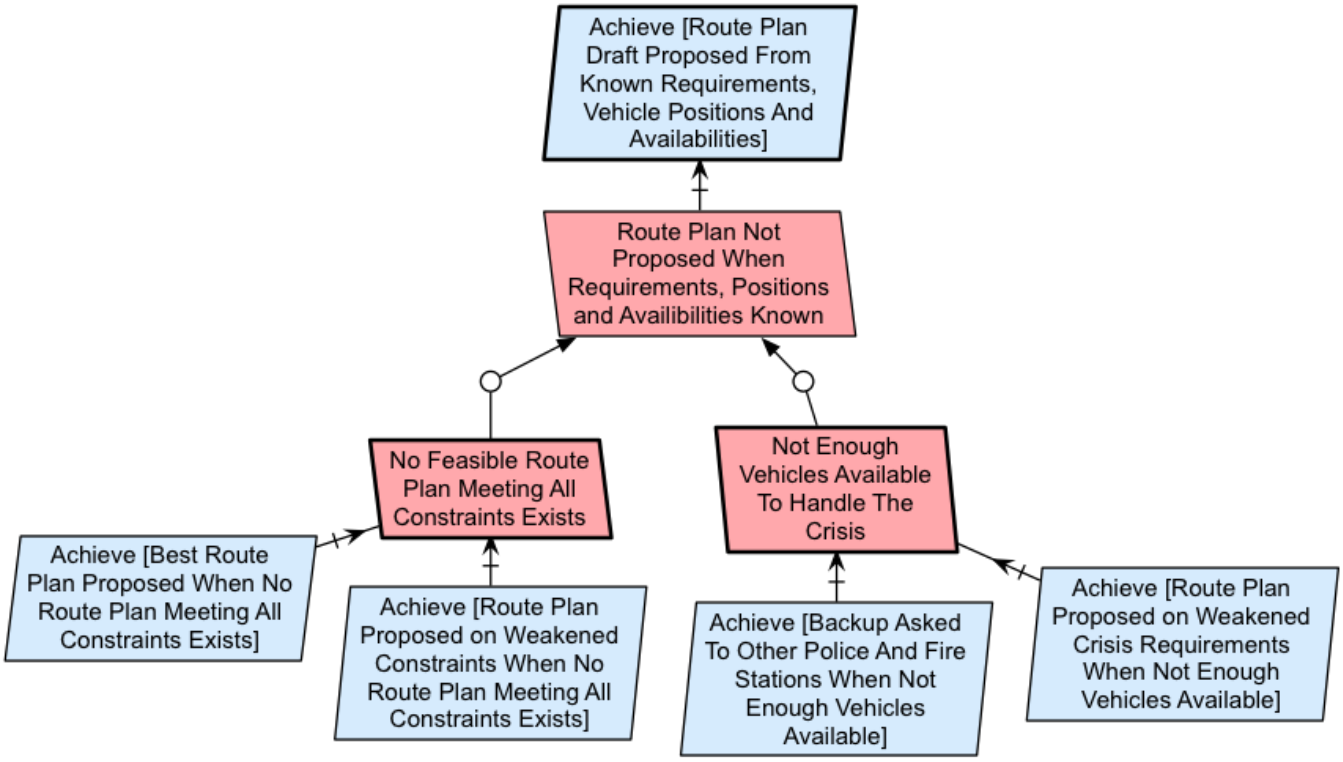
The conflict analysis is only preliminary and provided as an example of how conflicts can be identified and resolved. See the obstacle-analysis section for resolution of the conflict identified here.



Obstacles

Route Plan Not Proposed When Requirements, Positions and Availibilities Known

Despite crisis requirements being known as well as vehicle positions and availibilities, no plan is proposed to the coordinators by the bCMS software.

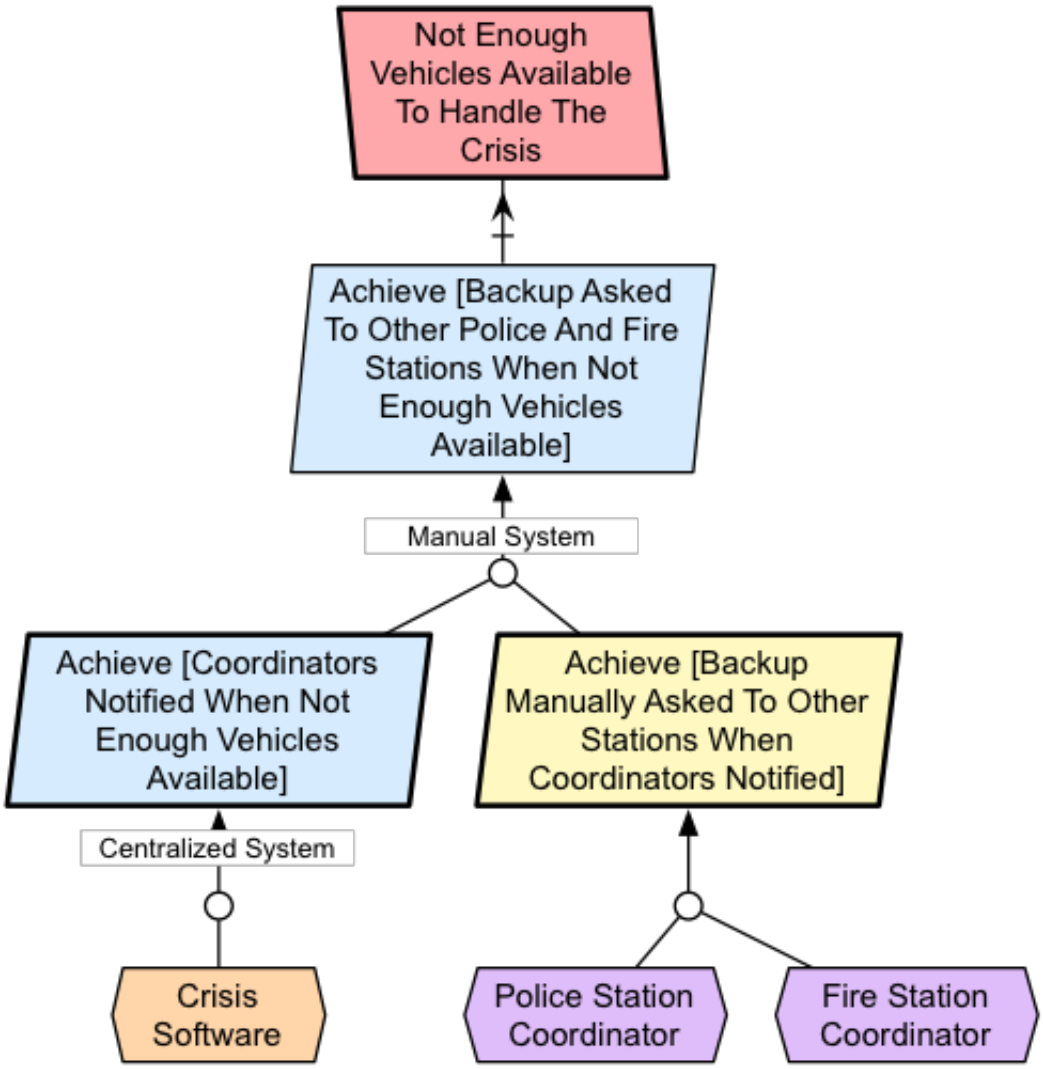


Not Enough Vehicles Available To Handle The Crisis

No sufficient vehicles are available for handling the crisis given the stated requirements.

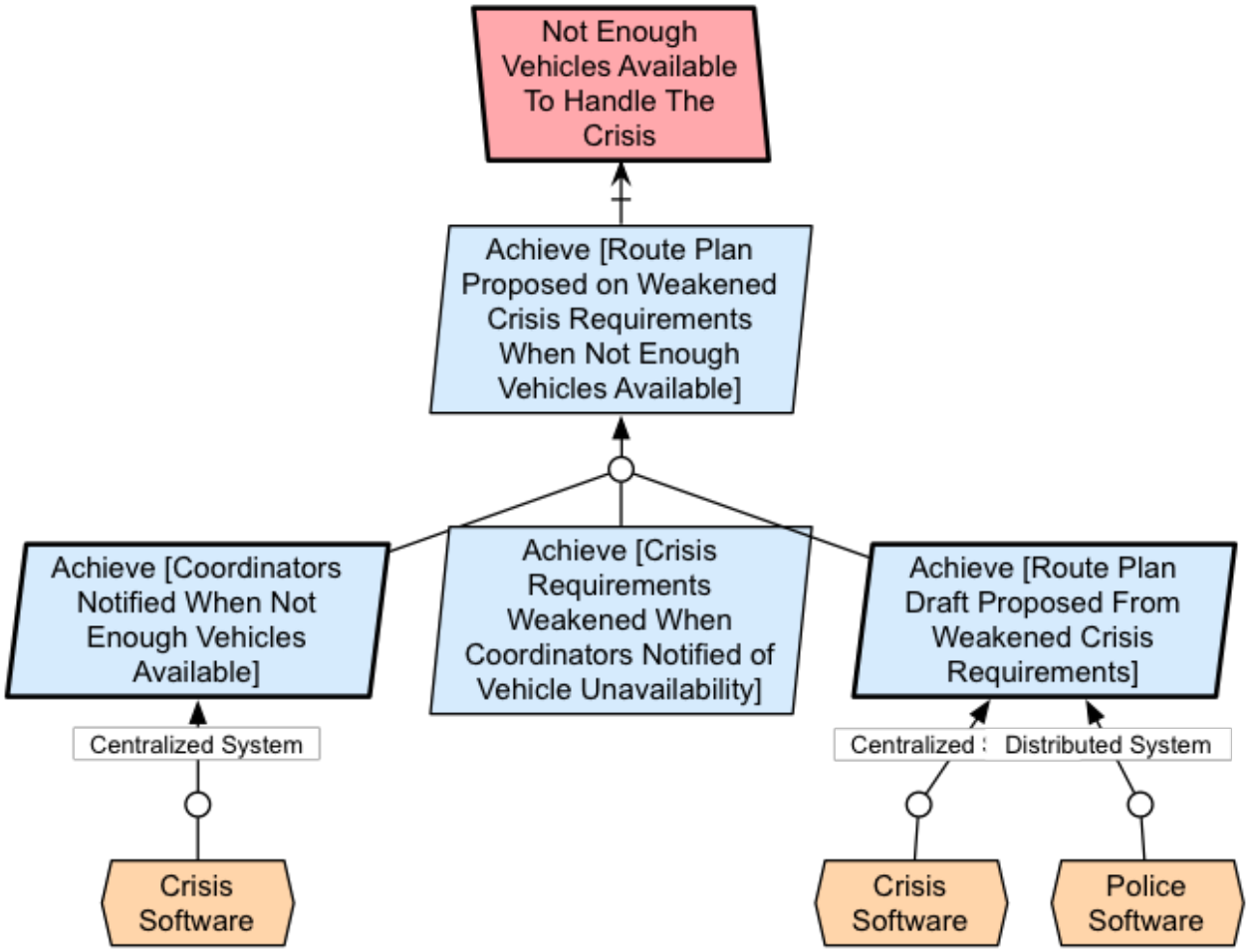
Achieve [Backup Asked To Other Police And Fire Stations When Not Enough Vehicles Available]

When not enough vehicles are available to handle the crisis with respect to the stated requirements then backup shall be asked to other police and fire stations.



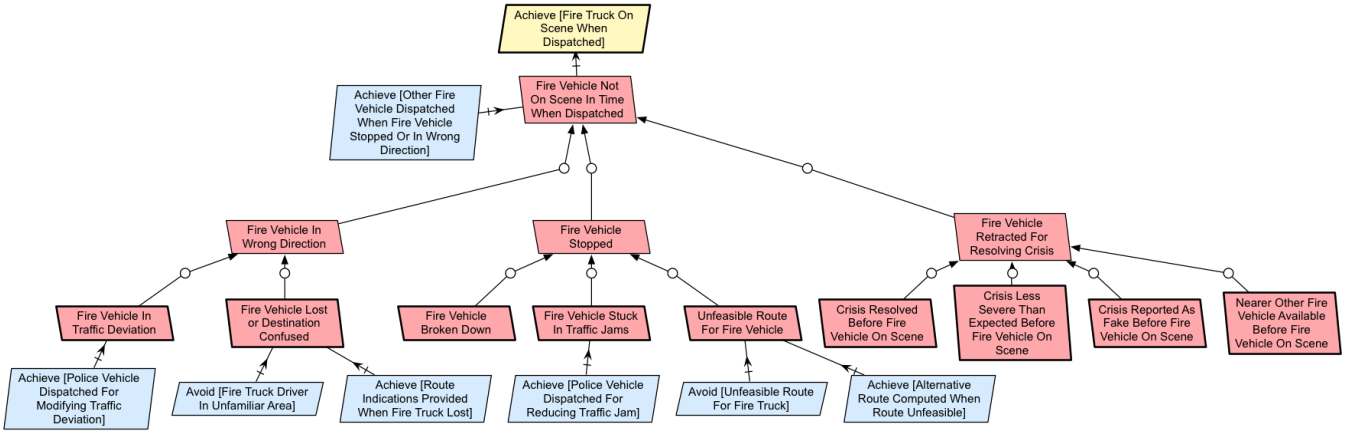
Achieve [Route Plan Proposed on Weakened Crisis Requirements When Not Enough Vehicles Available]

When not enough vehicles are available to handle the crisis with respect to the stated requirements then the crisis requirements shall eventually be weakened by the coordinators



Fire Vehicle Not On Scene In Time When Dispatched

The dispatched fire vehicle is not the crisis scene within the required delays. Similar obstacle analysis can be conducted on police vehicles.

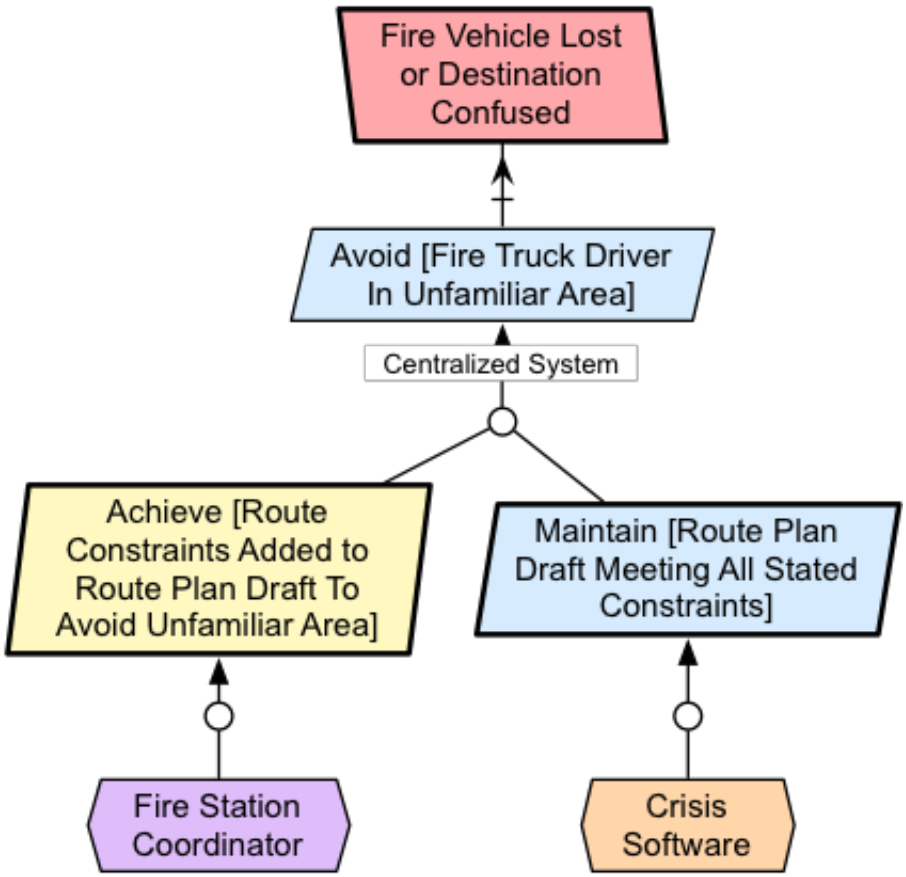


Fire Vehicle Lost or Destination Confused

The fire vehicle driver confused the destination.

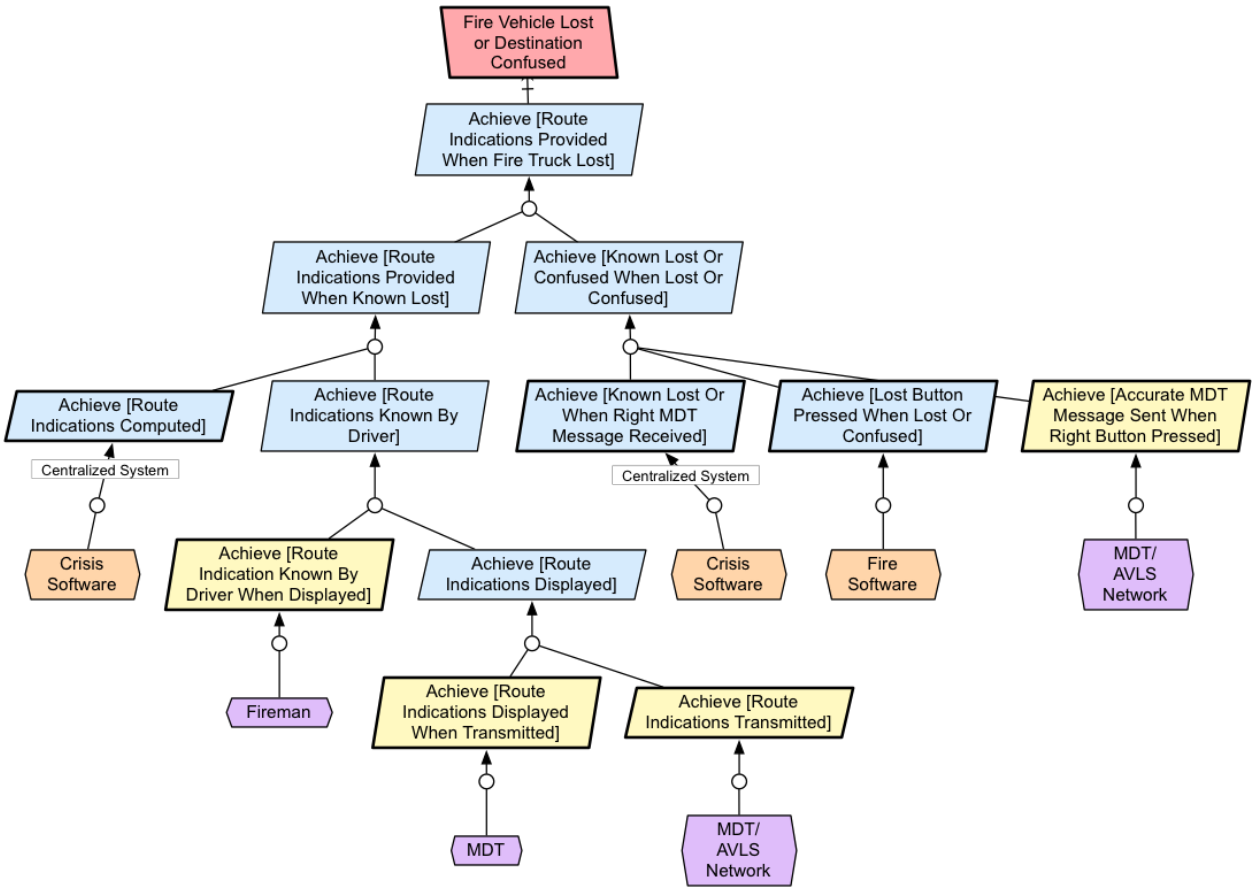
Avoid [Fire Truck Driver In Unfamiliar Area]

The route chosen for every allocated fire truck shall be such that the truck driver won't have to ride in an area unfamiliar to her.



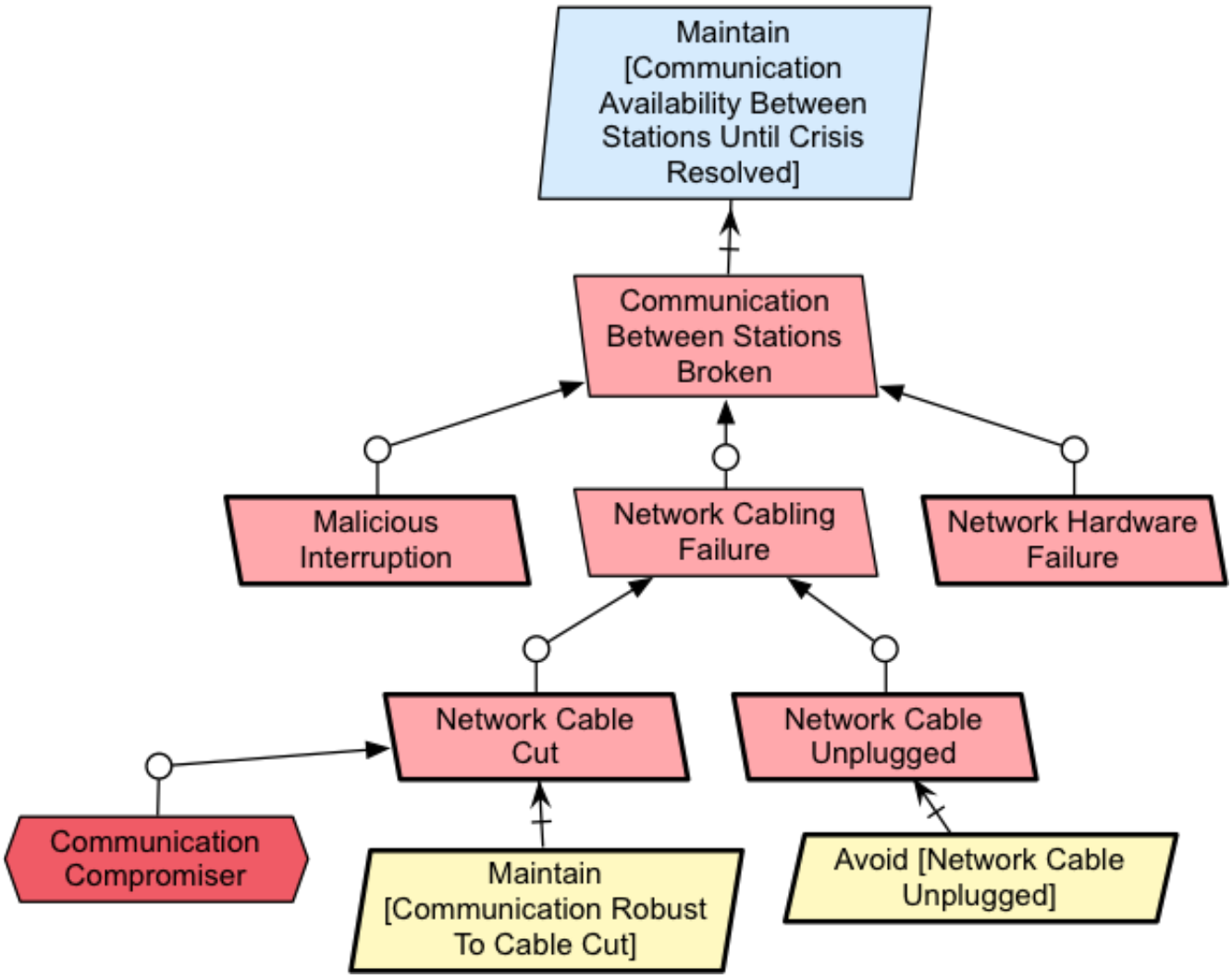
Achieve [Route Indications Provided When Fire Truck Lost]

Every truck driver lost of confused about the crisis location shall received details indications on how to reach the crisis scene from her current location.



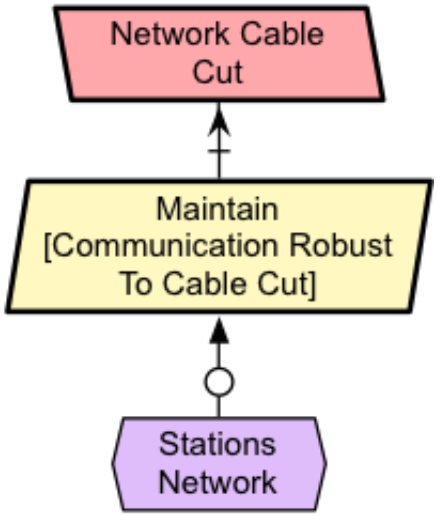
Communication Between Stations Broken

The communication between the fire and police station is completely broken.



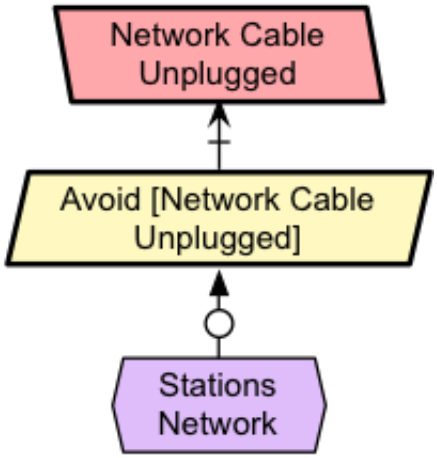
Maintain [Communication Robust To Cable Cut]

The communication system between stations shall be sufficiently robust to support the failures/cuts of a small number of communication lines.



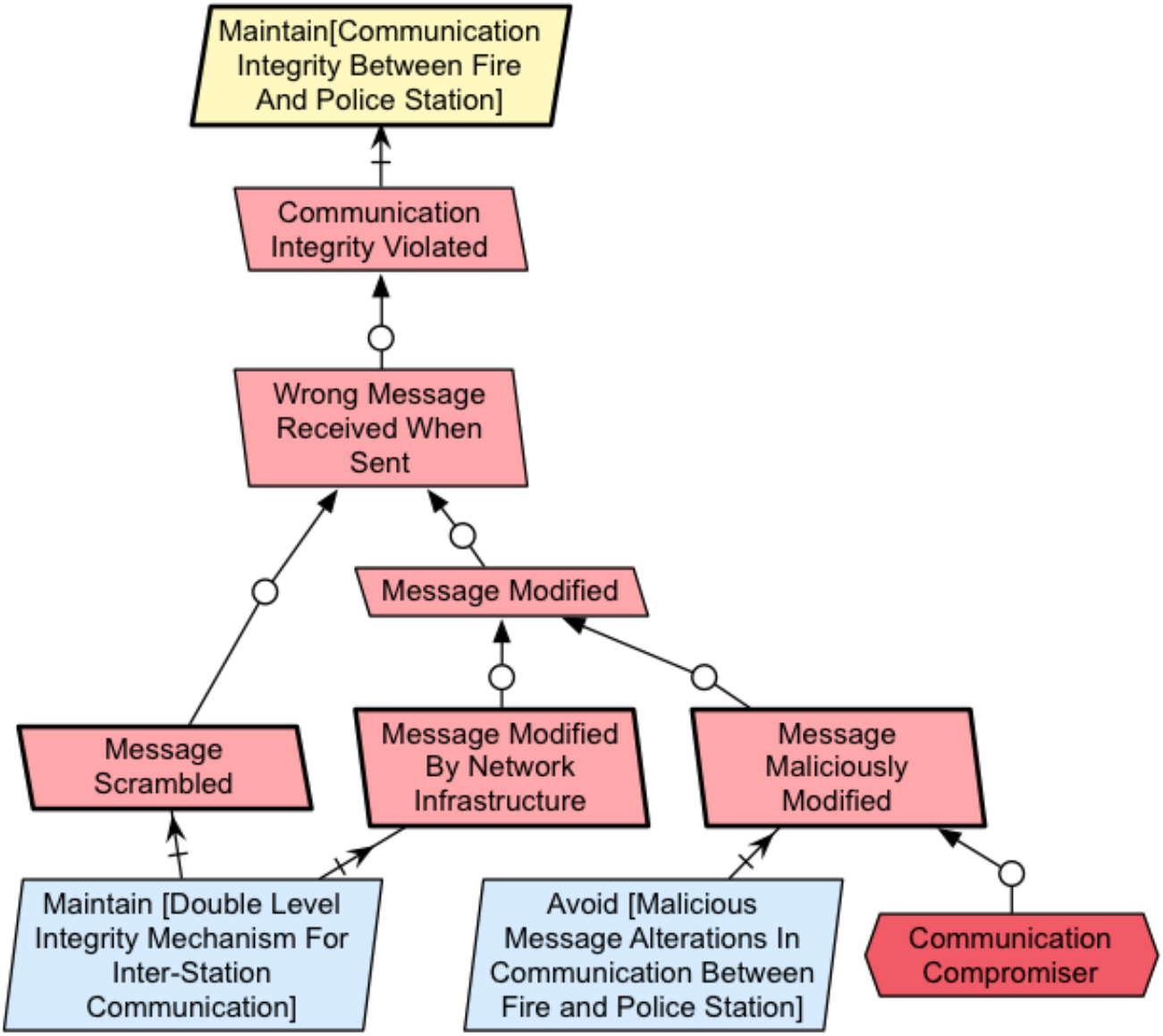
Avoid [Network Cable Unplugged]

The system shall be such that unplugging network cables is as unlikely as possible at fire and police stations.



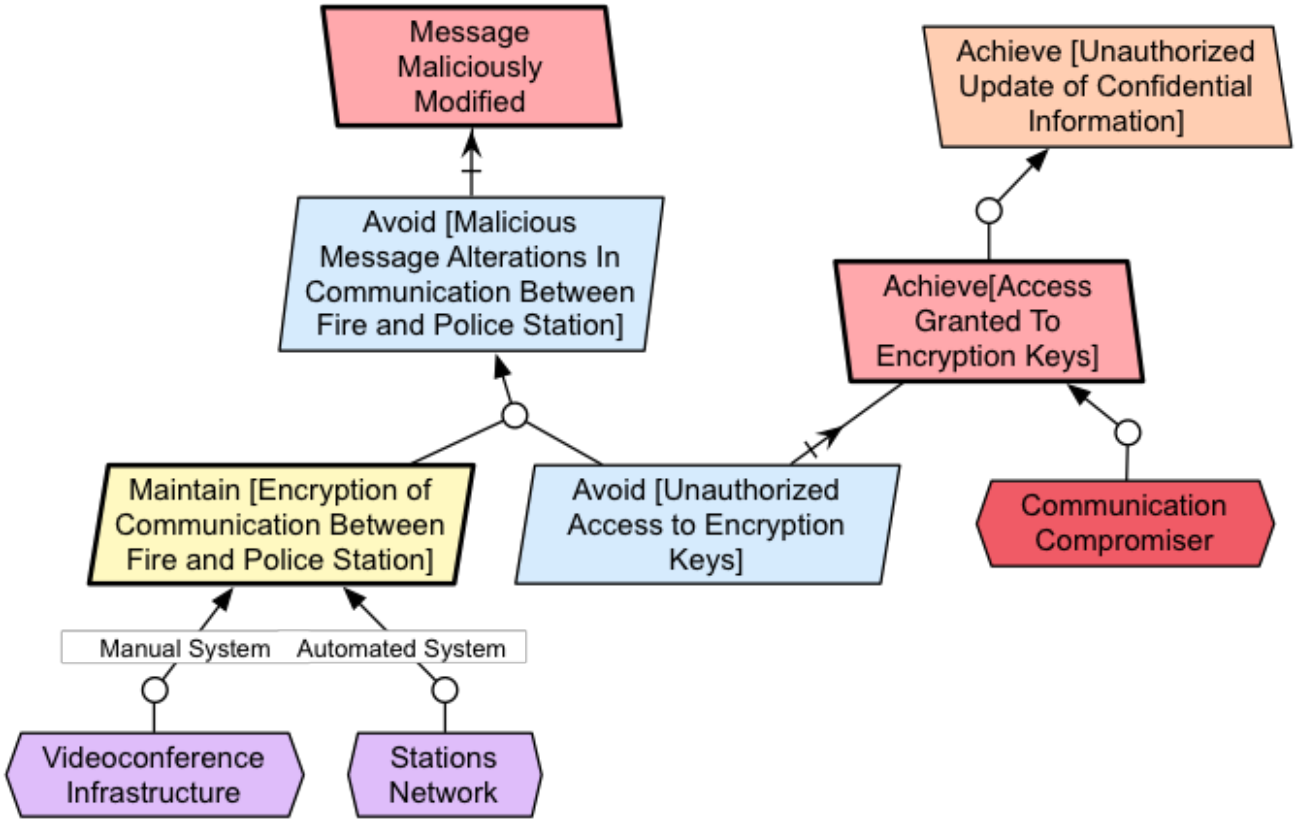
Communication Integrity Violated

Integrity of communication between fire and police station is violated either intentionally (by malicious users) or unintentionally (by network devices or software)



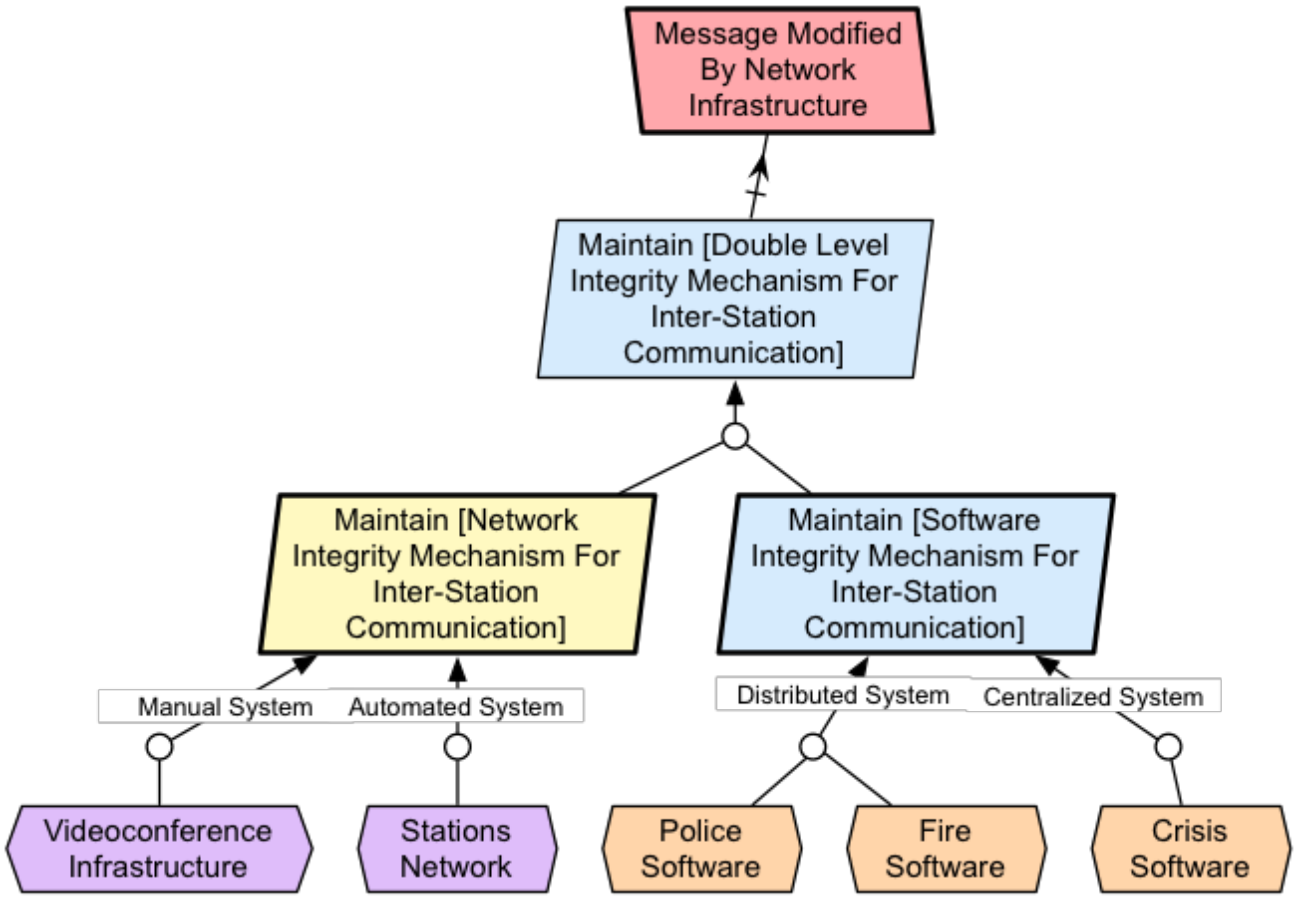
Avoid [Malicious Message Alterations In Communication Between Fire and Police Station]

The system shall ensure that no alteration of messages by malicious users is possible.



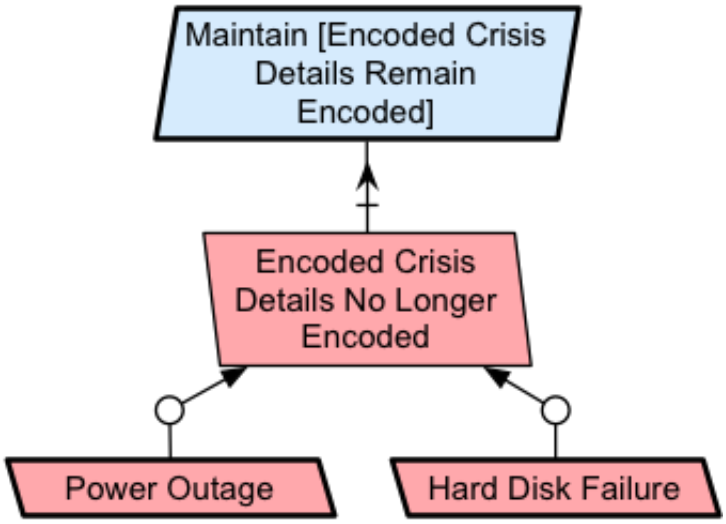
Maintain [Double Level Integrity Mechanism For Inter-Station Communication]

The system shall ensure a double level integrity mechanism for every message exchanged between stations.



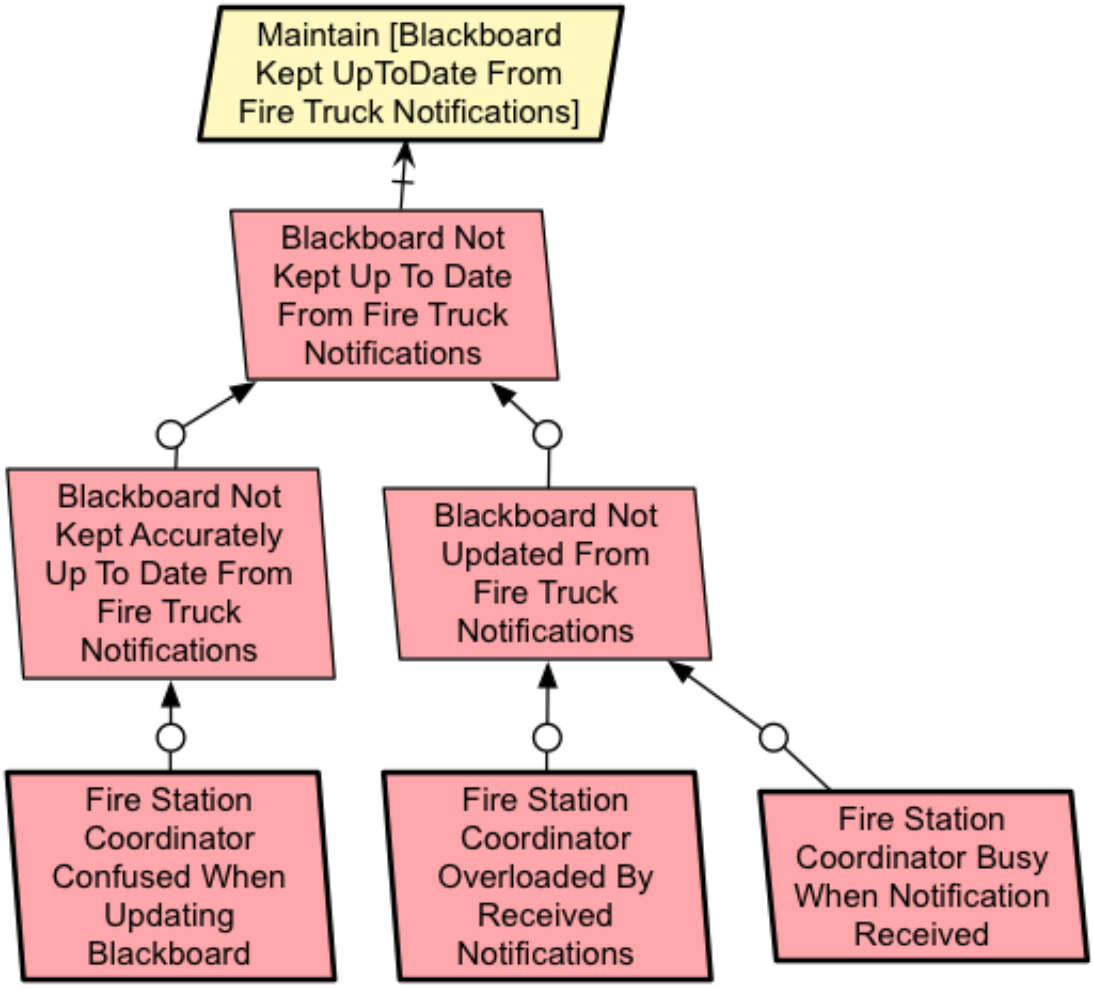
Encoded Crisis Details No Longer Encoded

The encoded crisis details are no longer available.



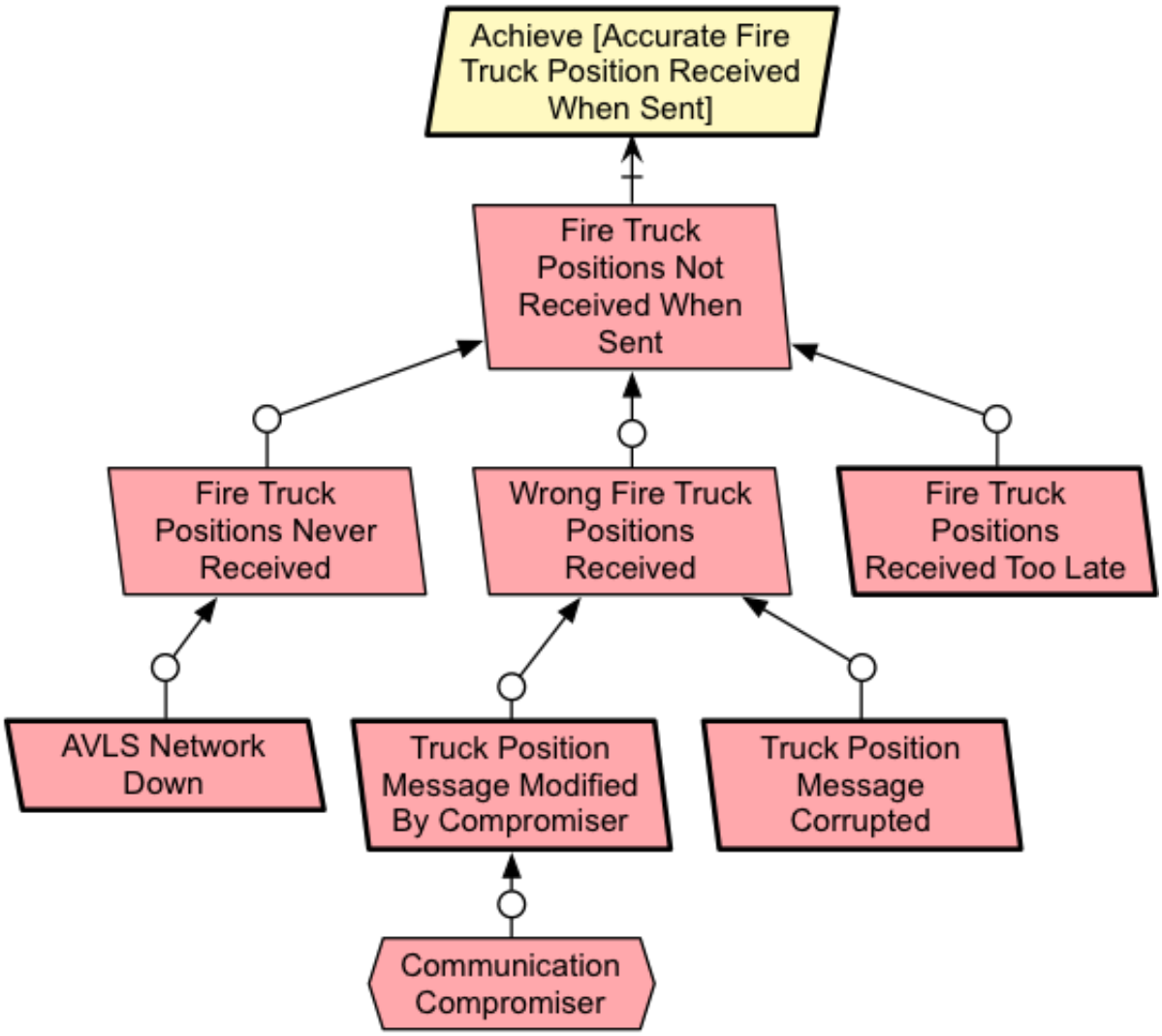
Blackboard Not Kept Up To Date From Fire Truck Notifications

The blackboard is not kept up to date when fire truck notifications.



Fire Truck Positions Not Received When Sent

The fire truck positions are not received in time when sent.

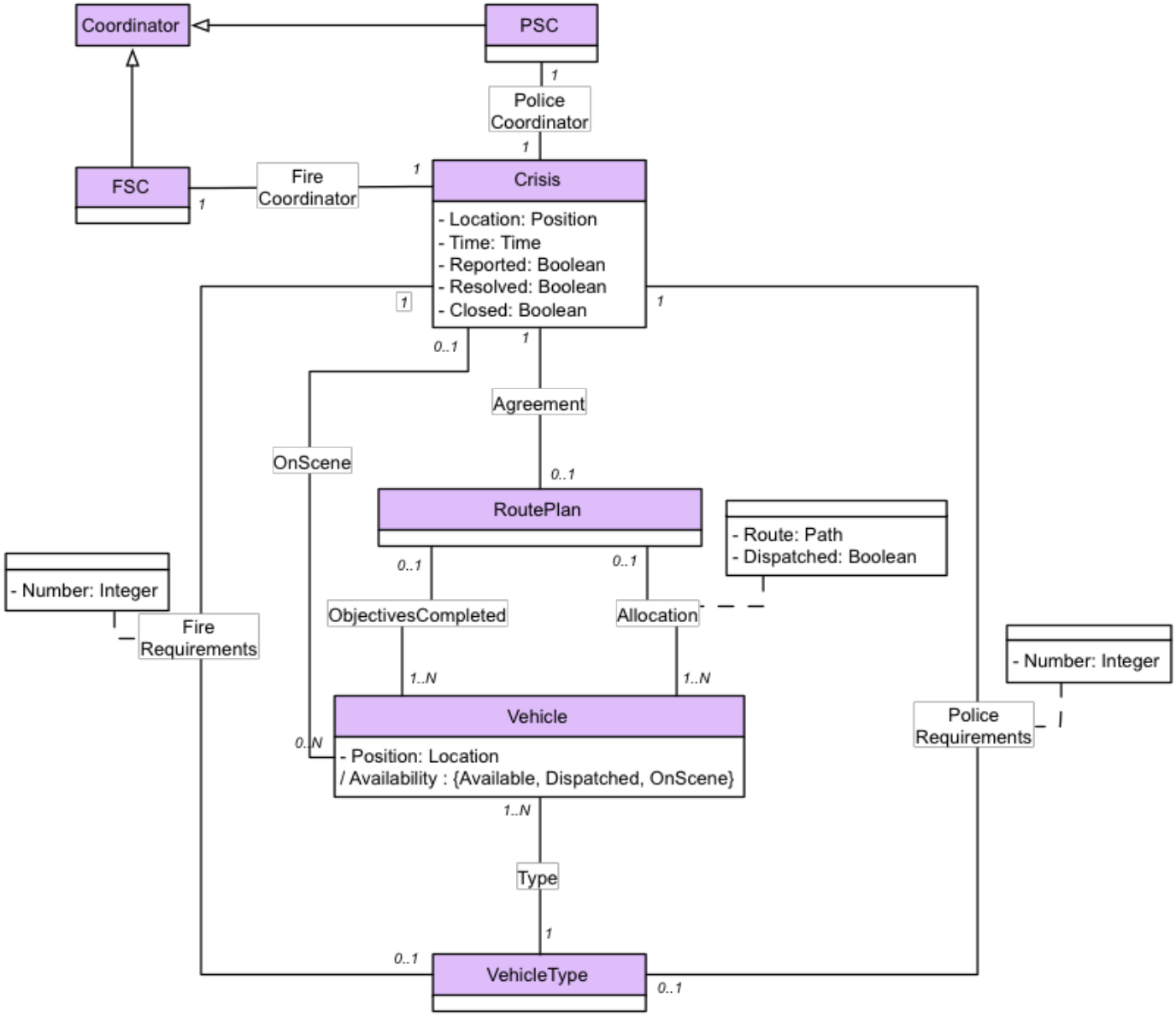


Structural model

The following sections contains various object model fragments. In those diagrams, objects in purple belong to the real world, those in orange belong to the software world (i.e. capture *information* about the real world), and those in green highlight shared phenomena between software components and the environment agents.

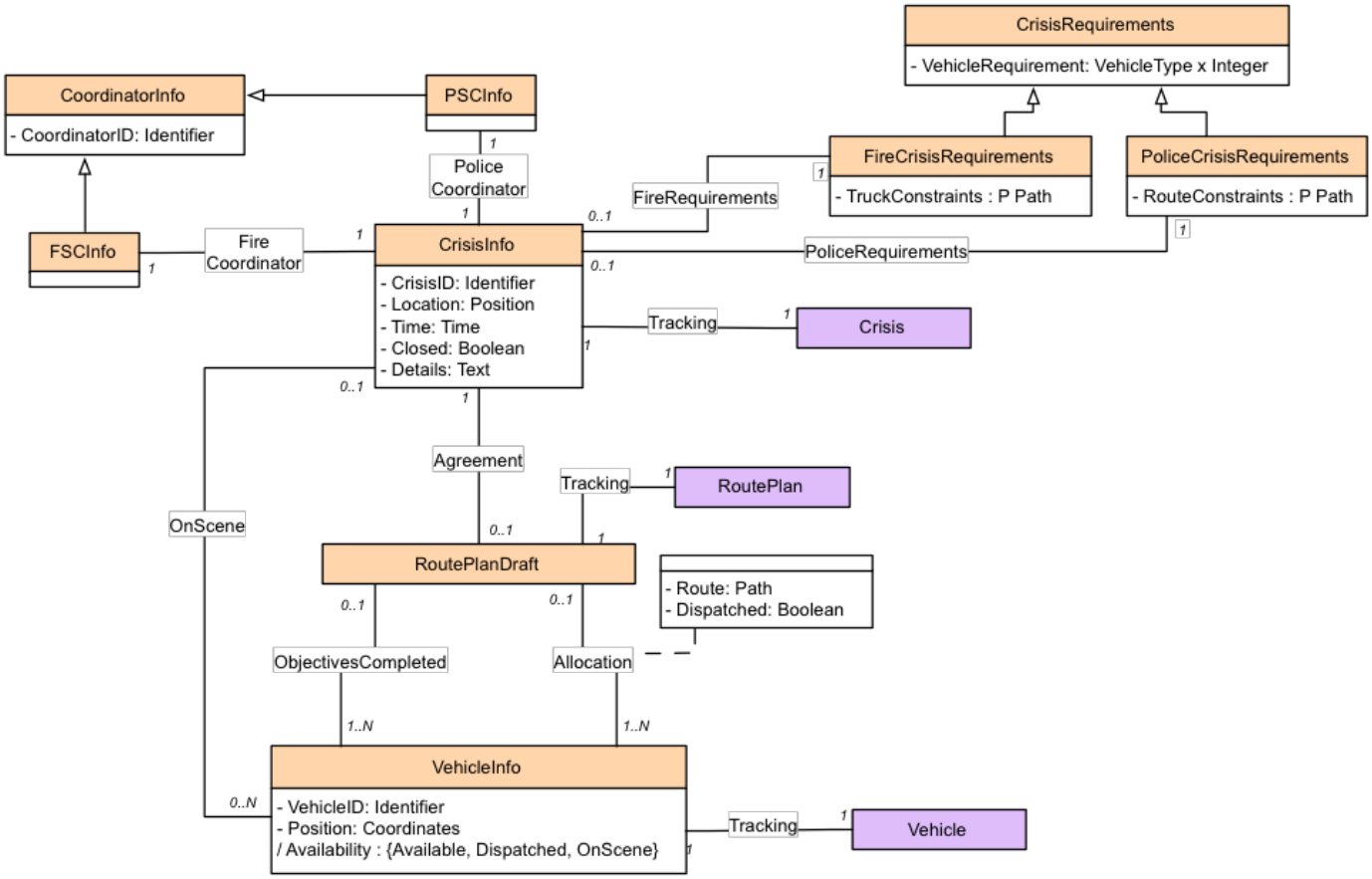
Objects in the environment

Structural model capturing environment objects, i.e. real-world citizens.



Software information about the environment

Structural model capturing the software information about the real-world, in contrast to real-world objects.

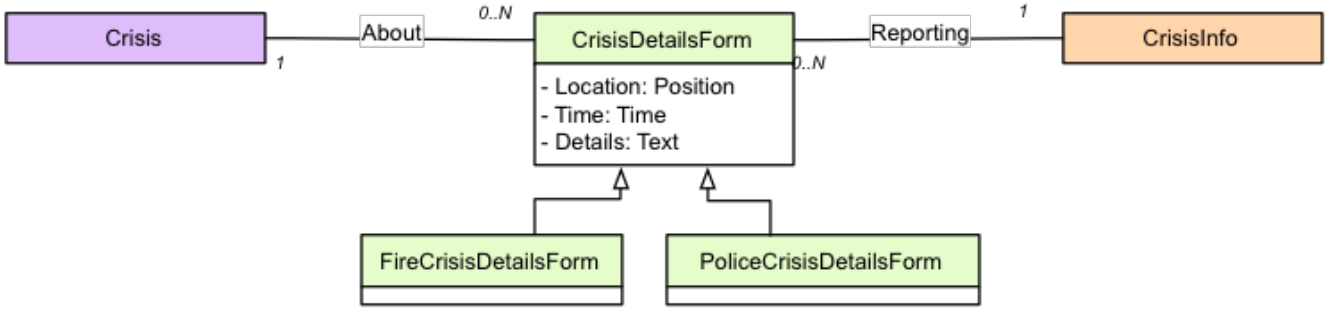


Shared phenomena

Structural models capturing shared phenomena between the software and its environment.

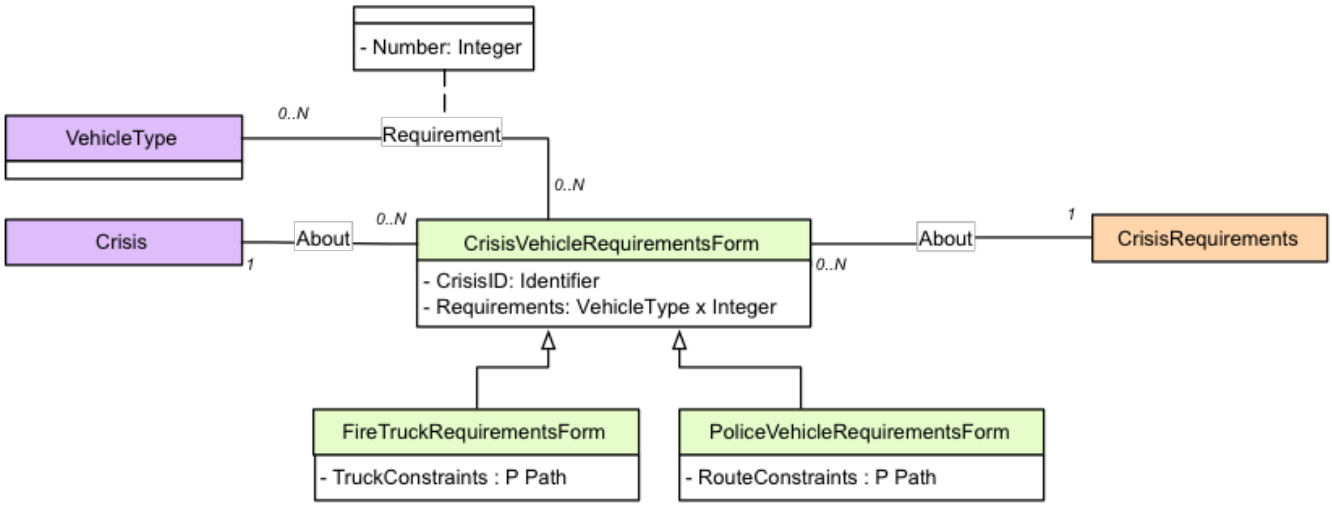
Crisis details exchange

Crisis details exchange as a shared phenomena through the encoding of a software-based form about the crisis.



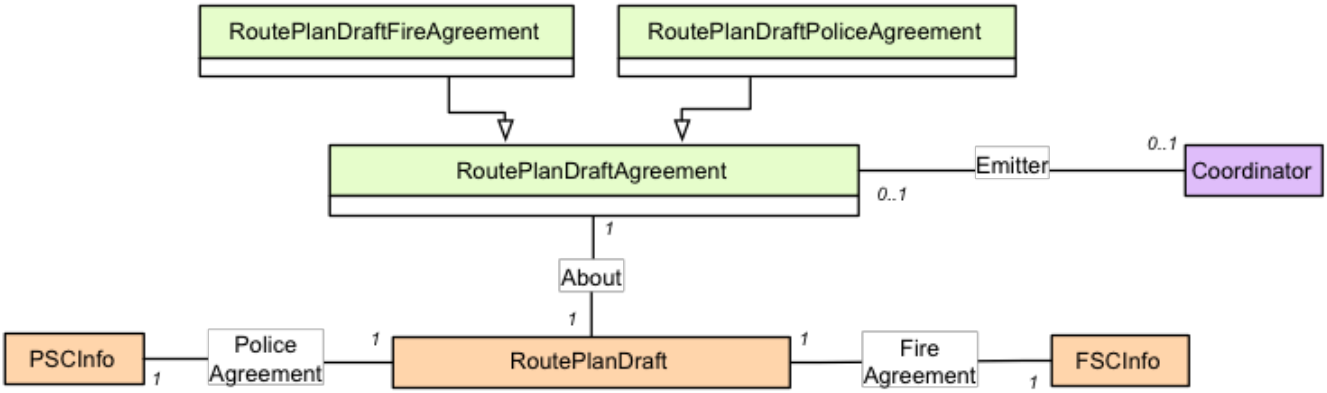
Crisis requirements exchange

Crisis requirements exchange as a shared phenomena through the encoding of a software-based form about the requirements and constraints.



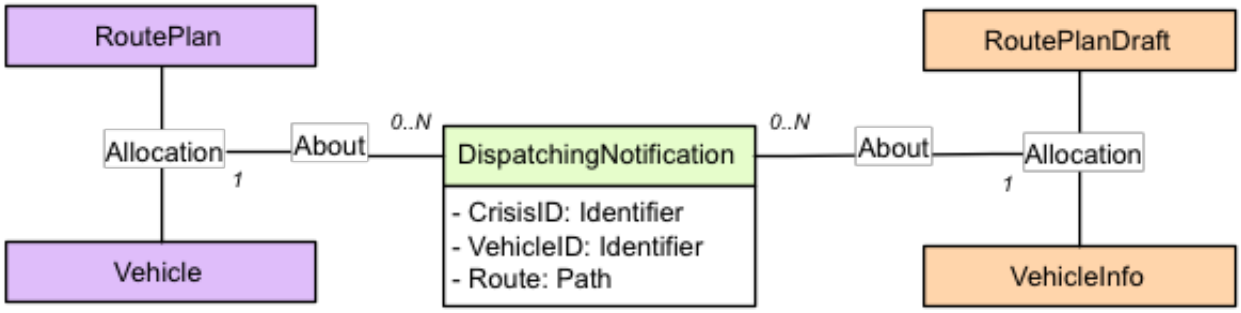
Route plan agreement

Coordinators agreement about a route plan seen as a shared phenomena, in terms of agreement information in the real world about the route plan draft proposed in the software world.



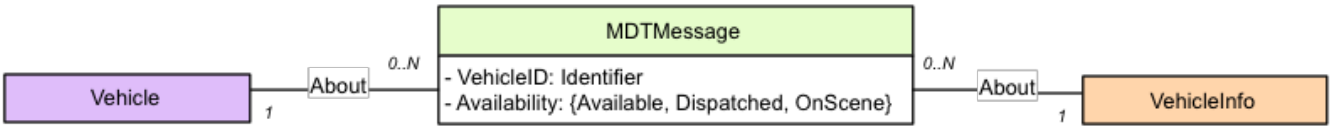
Dispatching notification

Structural models capturing shared phenomena between the software and its environment.



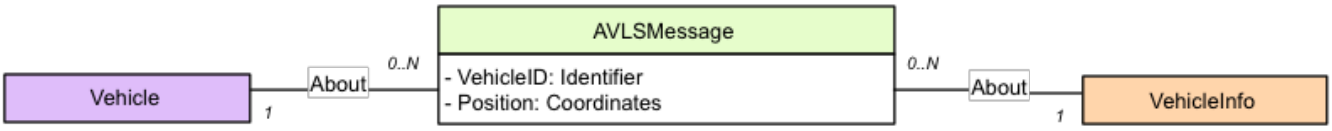
Vehicle availability notification

Notification of vehicle availability changes seen as messages received by the software from the vehicle MDT.



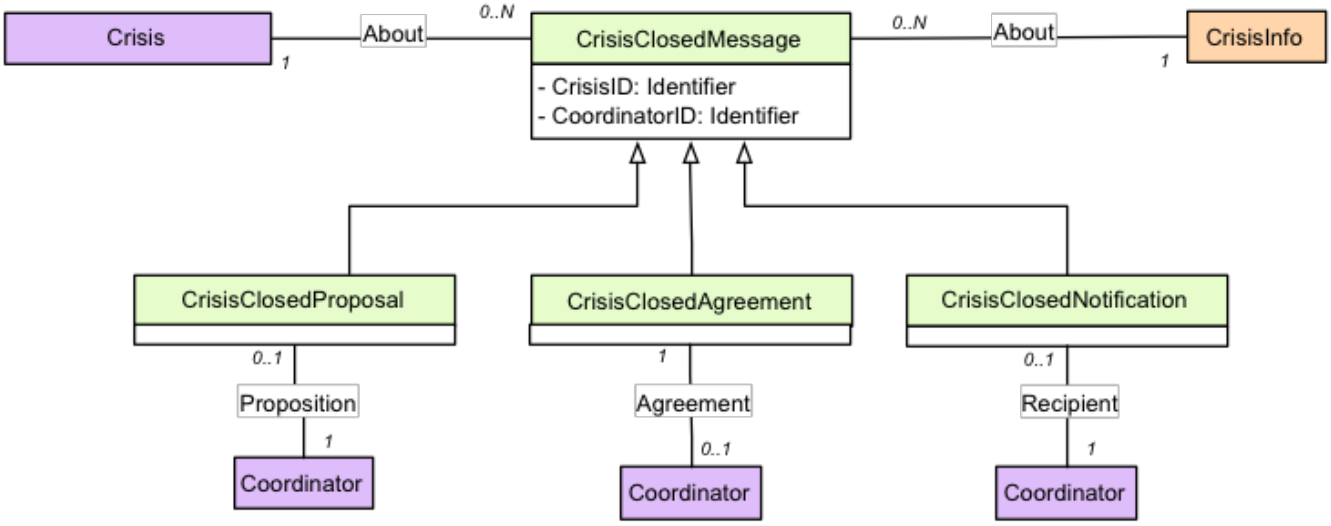
Vehicle position update

Notification of vehicle position changes seen as messages received by the software from the vehicle AVLS.



Crisis closing agreement

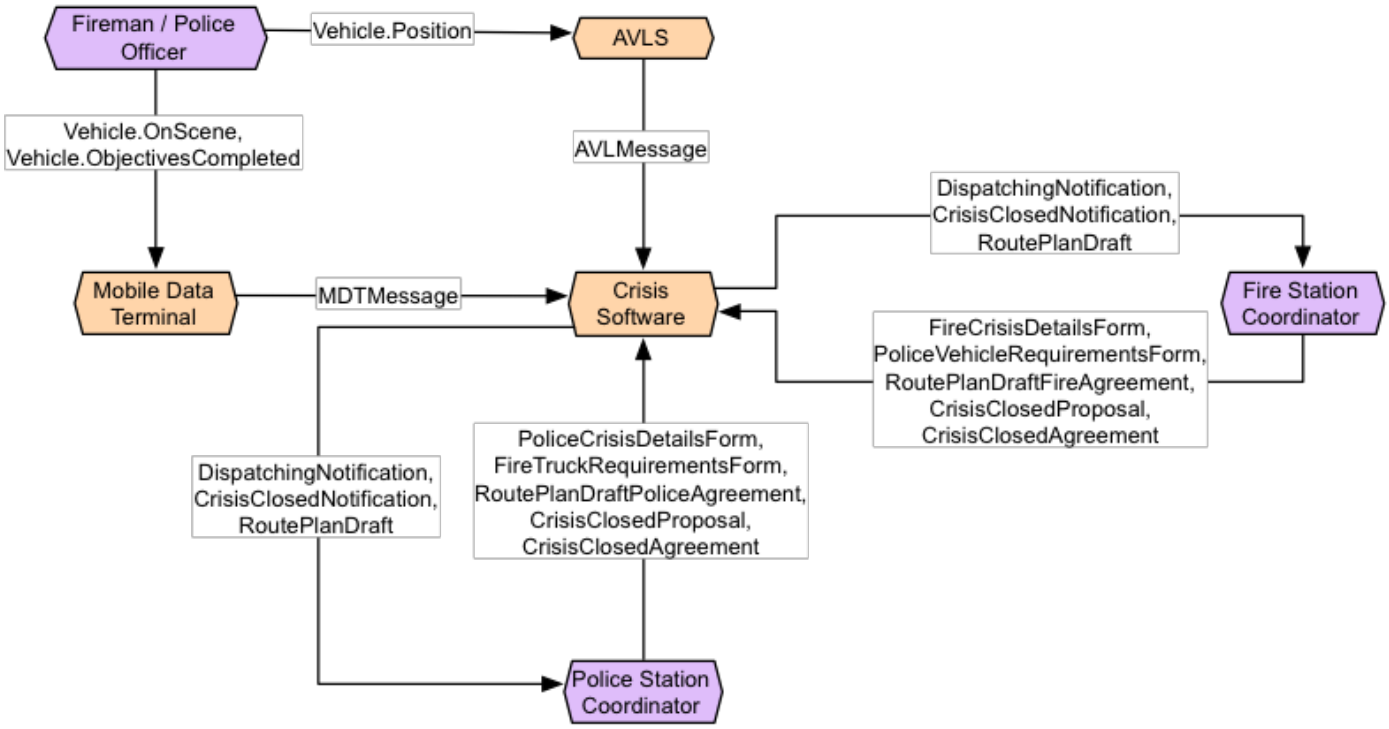
Coordinators agreement for closing a crisis as a notification sent to the software.



Agents

Context diagram

Context diagrams capture agents and their interfaces in terms of monitored and controlled variables. The nodes in such diagram represent involved agents. Edges are labelled with objects, attributes and associations declared in the object model. Semantically, such label means that the source agent controls that object, attribute or association, whereas the target agent monitors it.

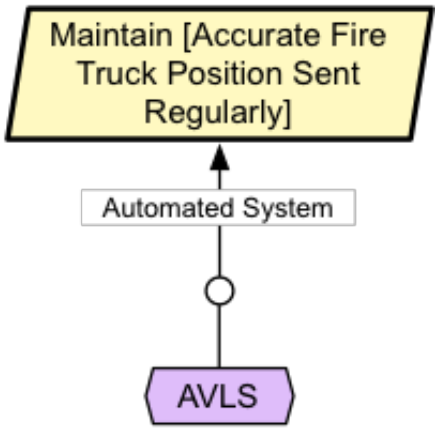


Responsibilities

The following sub-sections show responsibility diagrams for the different agents. Those diagrams provide a nice overview of all expectations and requirements assigned to environment and software agents, respectively. Together with soft goals, responsibility diagrams help comparing and choosing between various system alternatives.

AVLS

The Automated Vehicle Location System is an agent located vehicles and fire trucks that frequently reports the vehicle location to the police and fire stations, respectively.

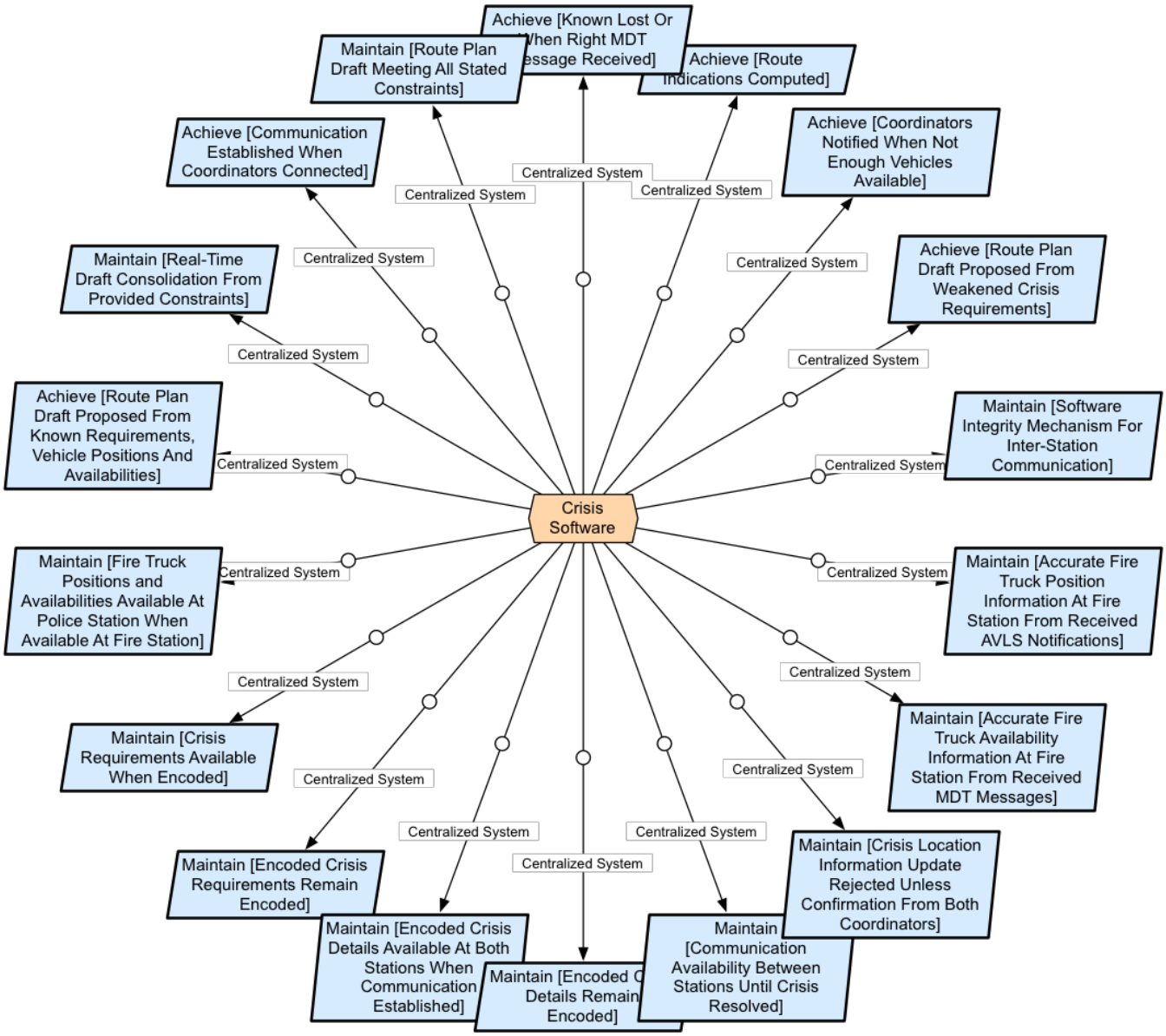


Communication Compromiser

The communication compromiser wants to achieve personal gain during the crisis.

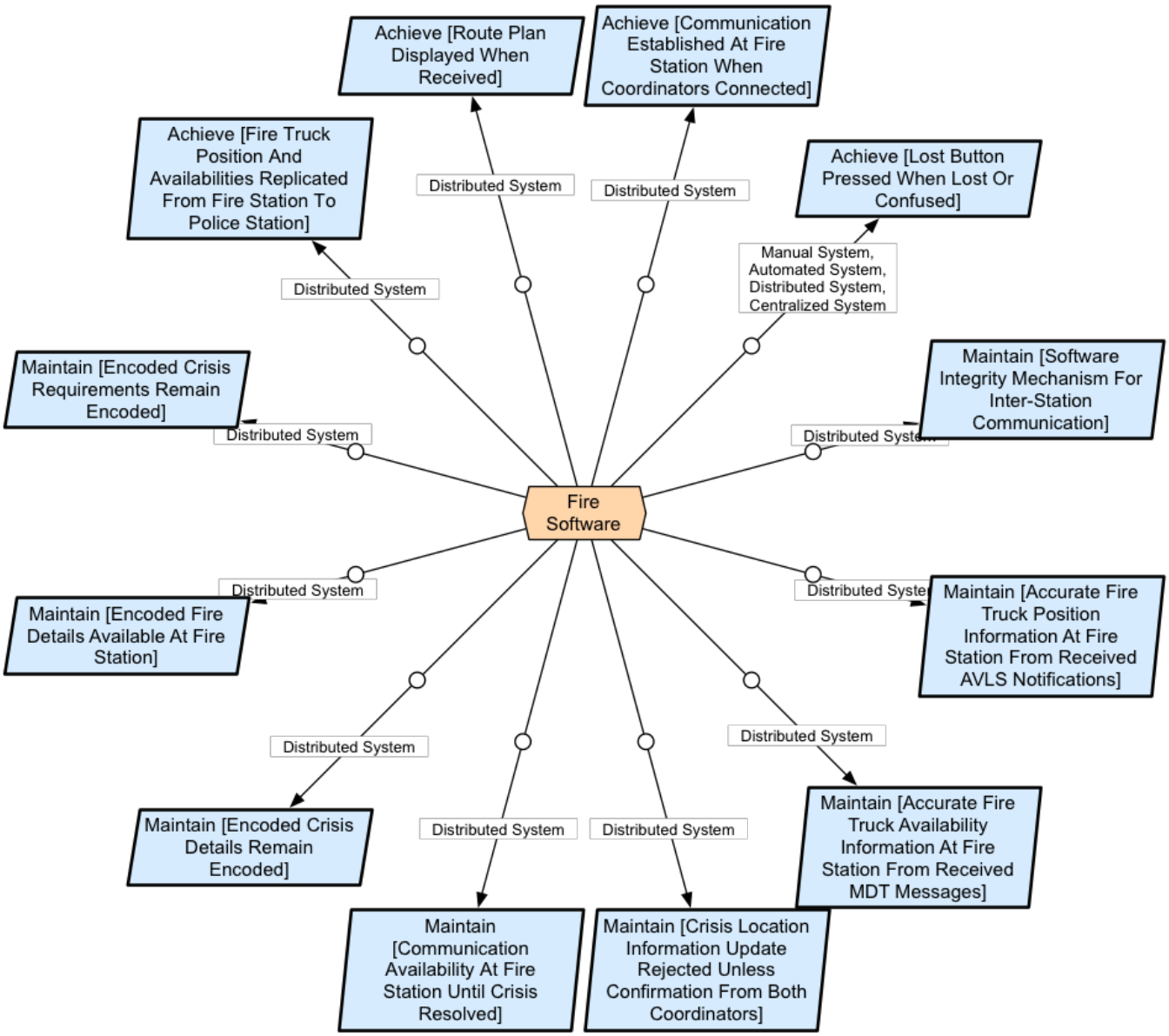
Crisis Software

The Crisis Software is the main software in the centralized system alternative. Among others, it is responsible of maintaining effective communitation between the FSC and PSC and helping them achieving their goals through computing intelligence (real-time feedback, route computing, etc.).



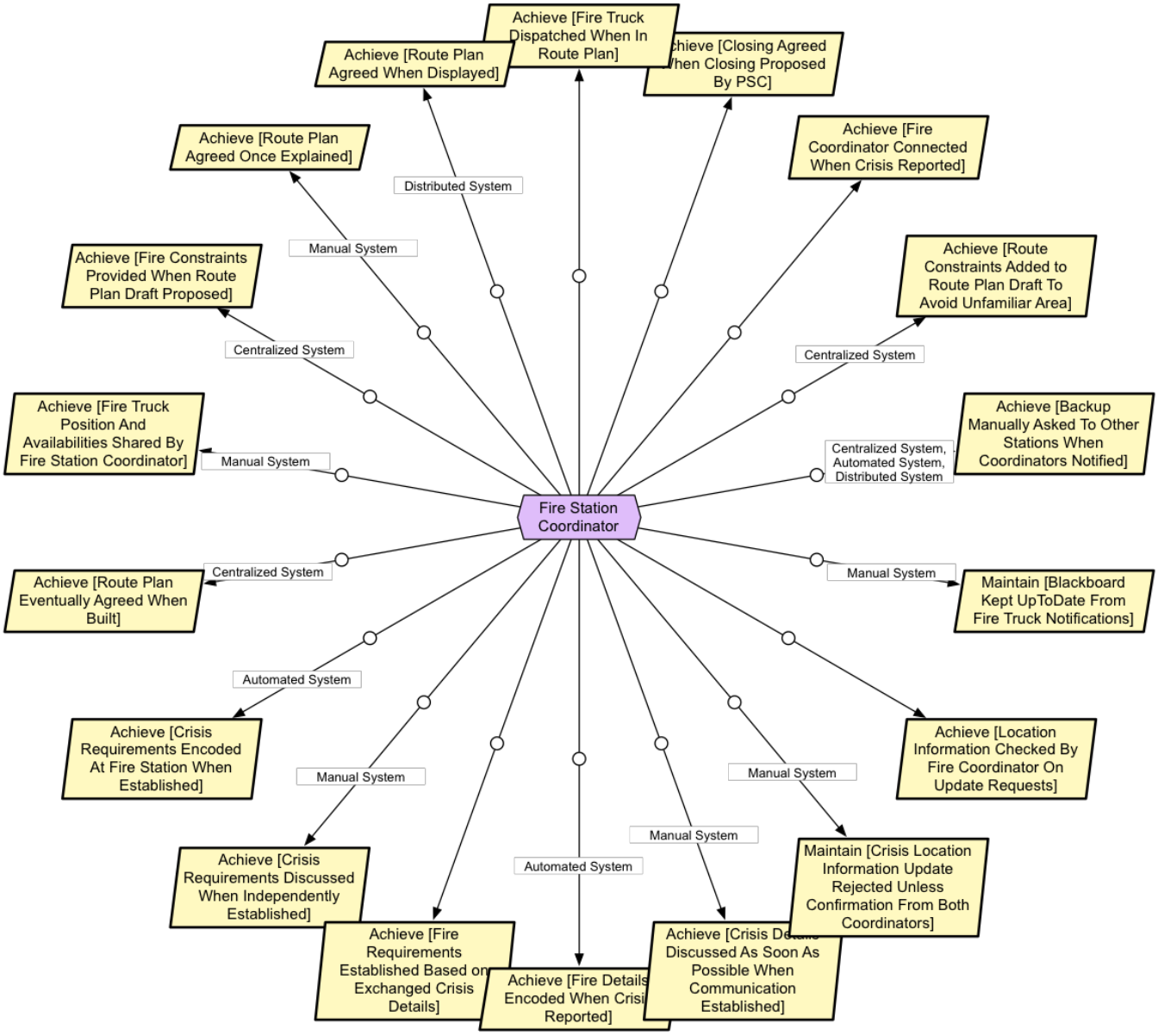
Fire Software

The Fire Software is a software agent in the distributed system alternative. It is responsible of helping the FSC with fireman-related responsibilities as well as guaranteeing that needed information from the police station is available at the fire station.



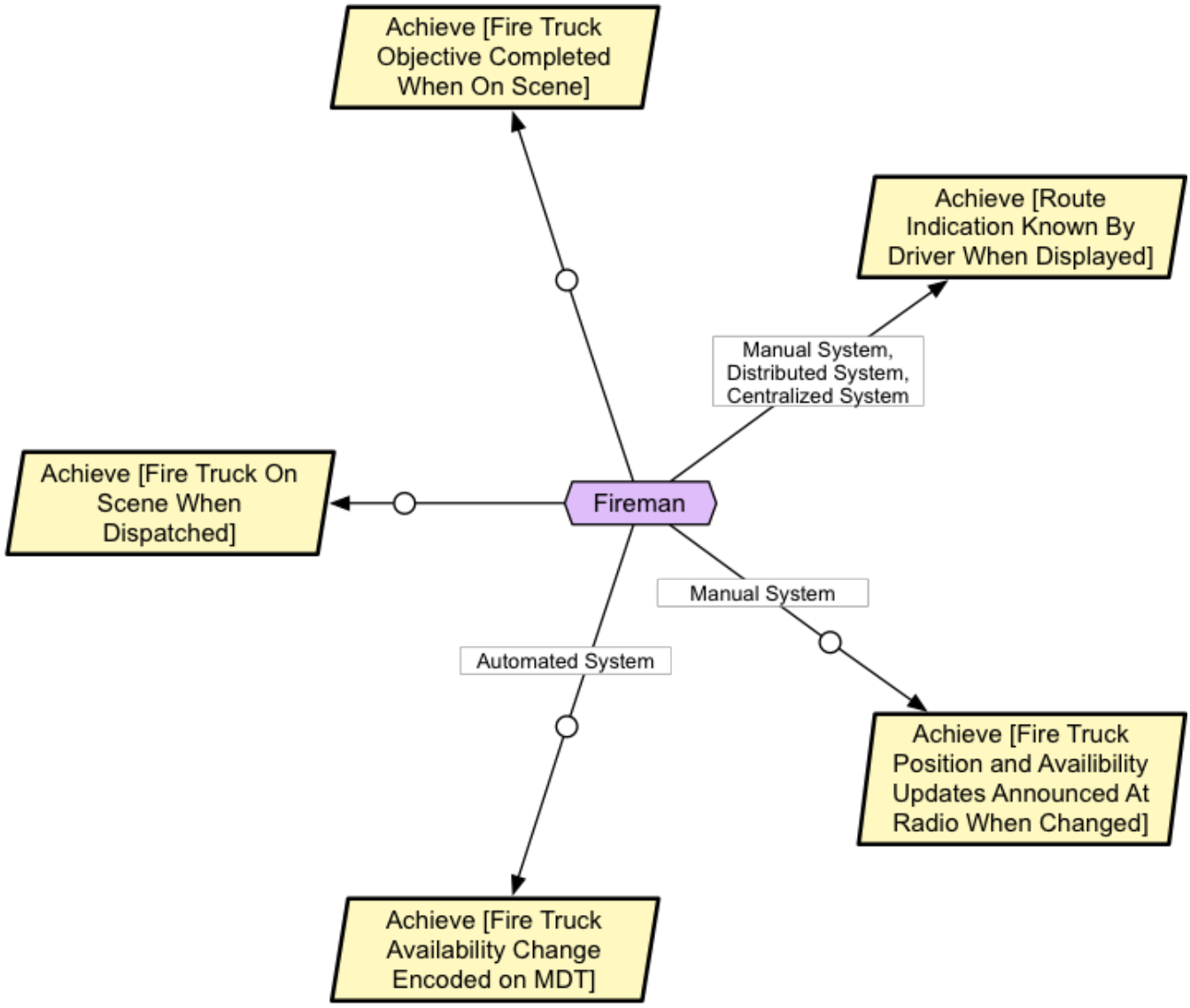
Fire Station Coordinator

A FSC maintains control over a crisis situation by communicating with the police station coordinator (PSC) as well as firemen



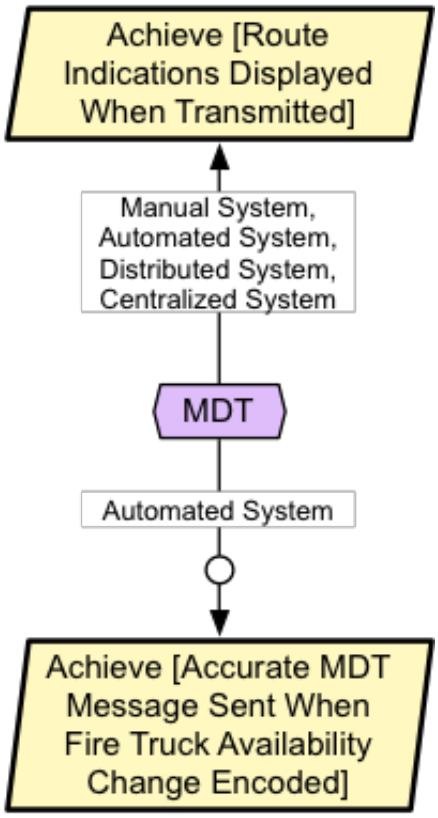
Fireman

A fireman acts on orders received from the FSC and reports crisis-related information back to the FSC. Furthermore, a fireman communicates with other firemen, victims, and witnesses at the crisis location.



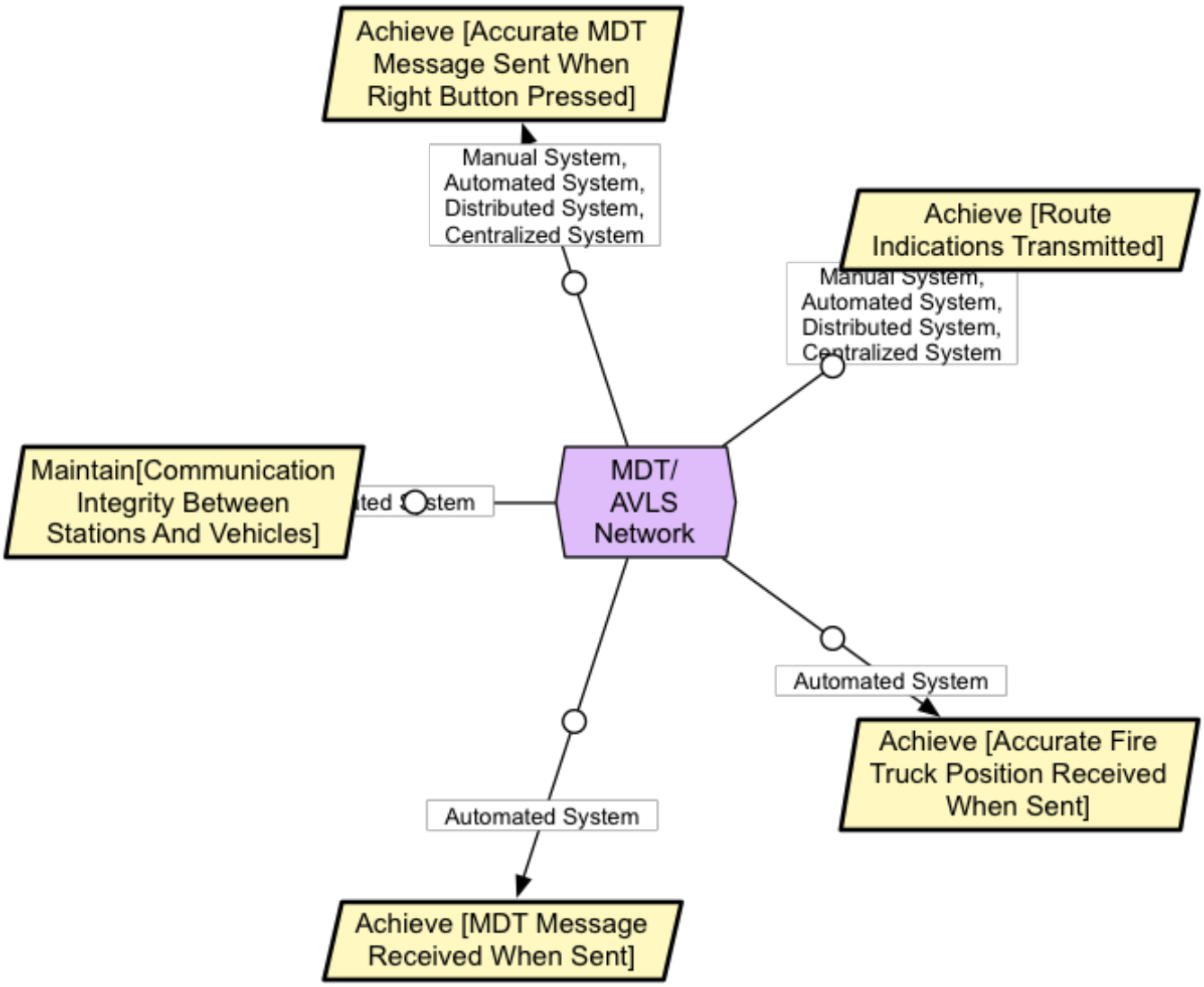
MDT

The Mobile Data Terminal is an agent located inside police vehicles and fire trucks that allows reporting the vehicle availability to the police and fire stations, respectively.



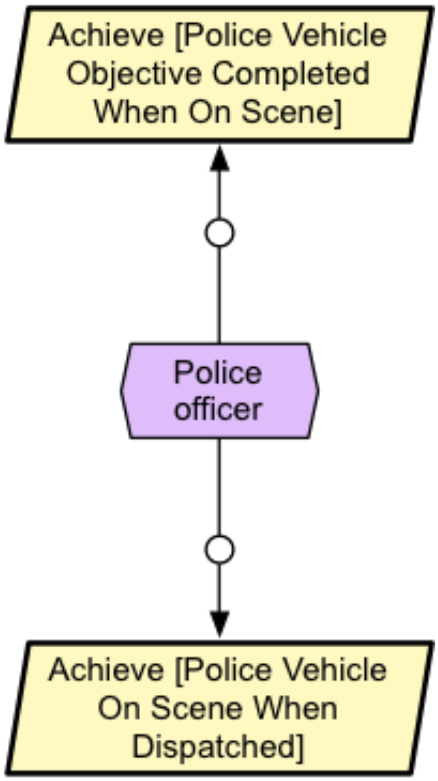
MDT/AVLS Network

The communication infrastructure used by the AVLS and MDT agents to send/receive availability and position notifications with the fire and police stations.



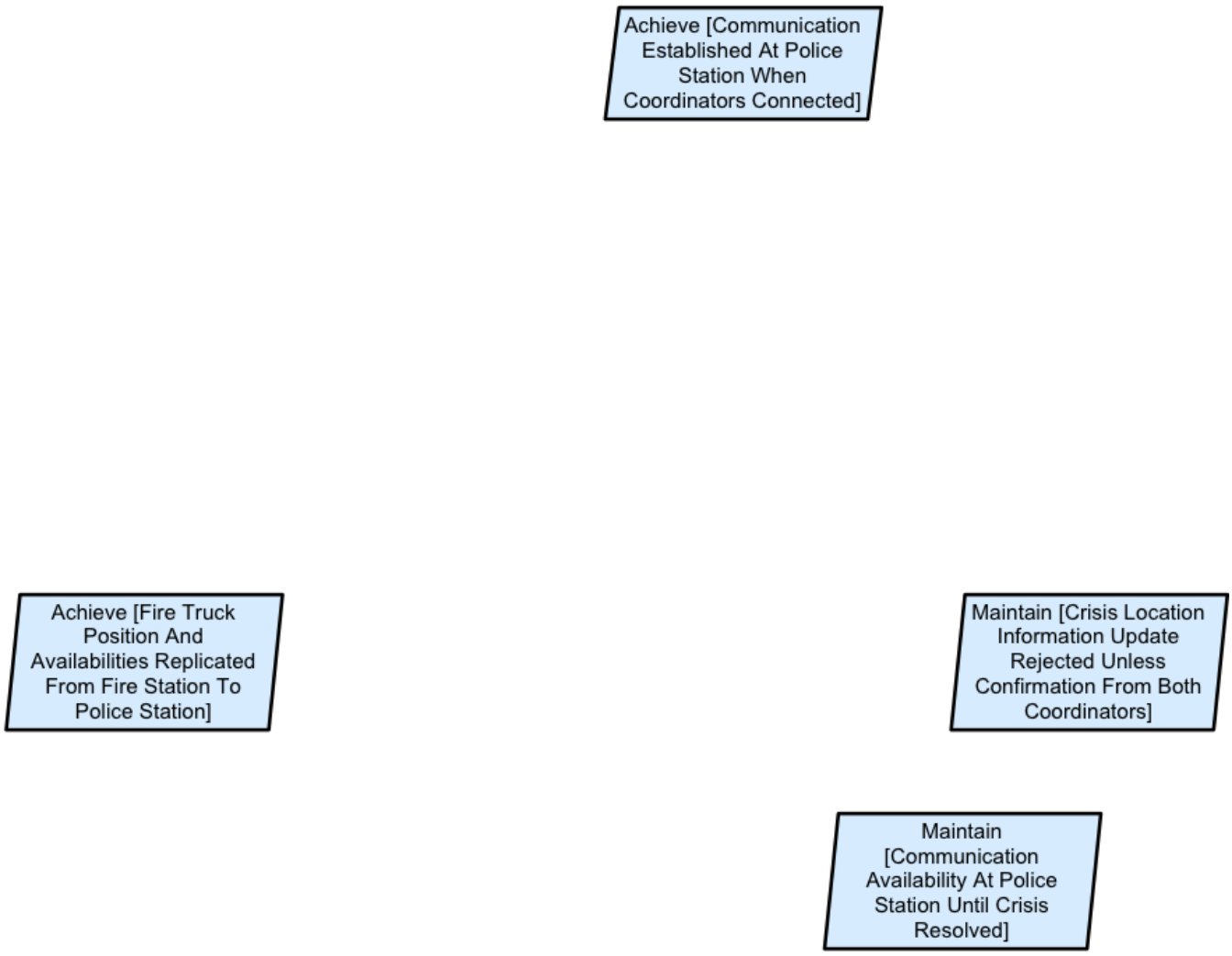
Police officer

A police officer acts on orders received from the PSC and reports crisis-related information back to the PSC. Furthermore, a police officer communicates with other policemen, victims, and witnesses at the crisis location.



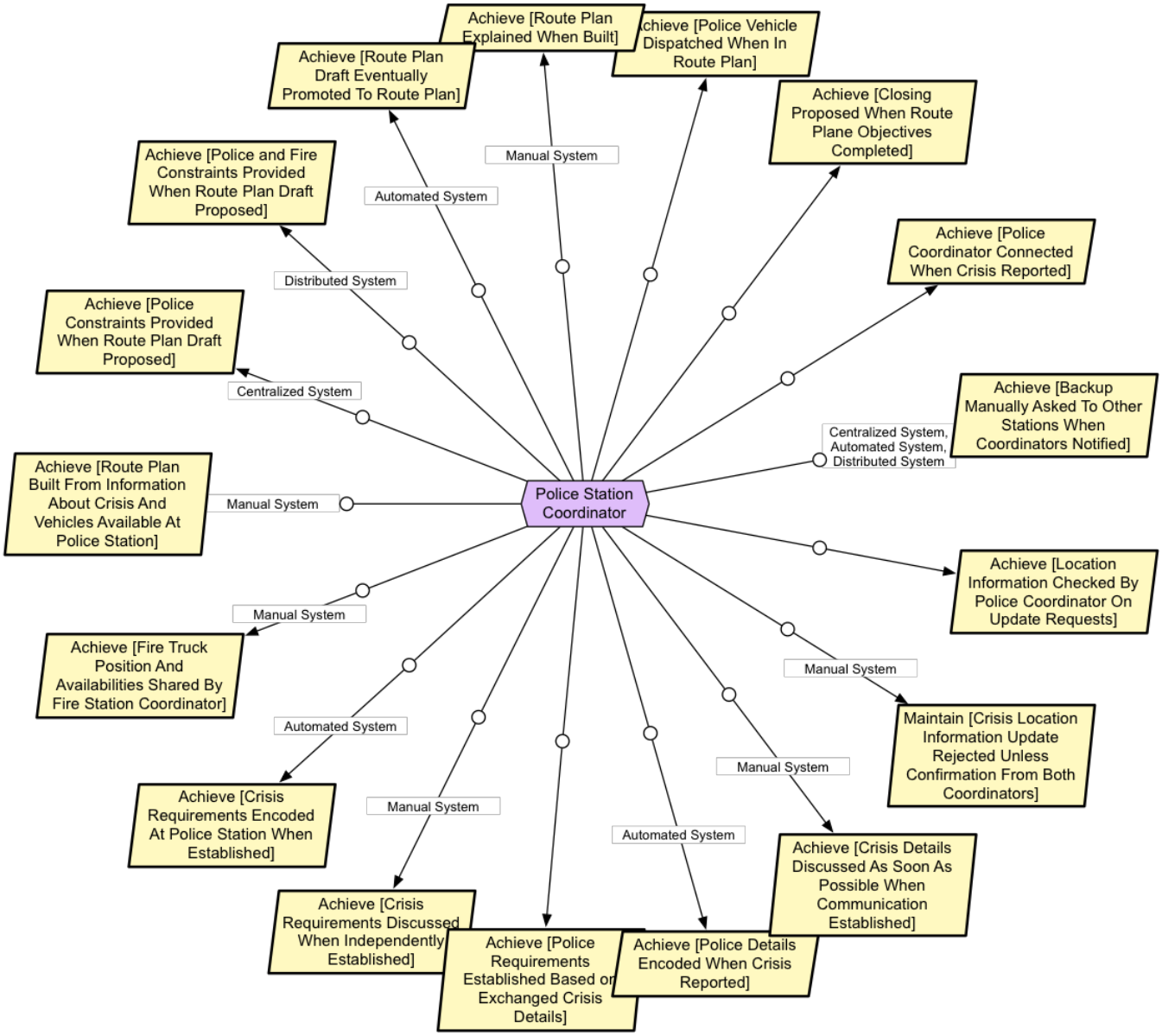
Police Software

The Police Software is a software agent in the distributed system alternative. It is responsible of helping the PSC with police officer-related responsibilities as well as guaranteeing that needed information from the fire station is available at the police station.



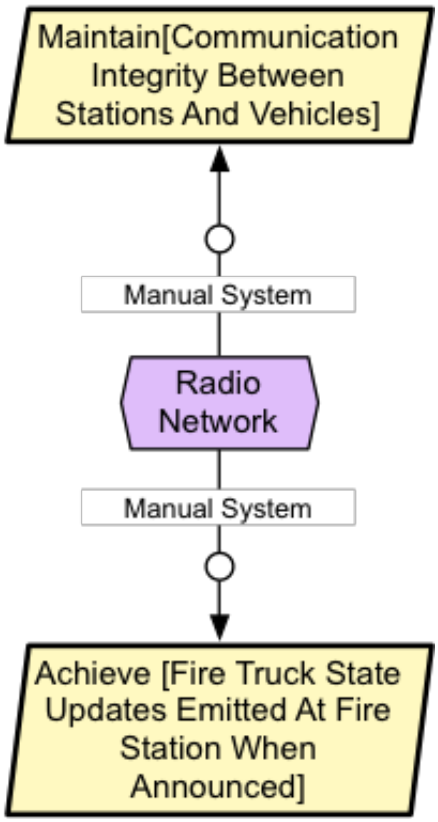
Police Station Coordinator

A PSC maintains control over a crisis situation by communicating with the fire station coordinator (FSC) as well as policemen.



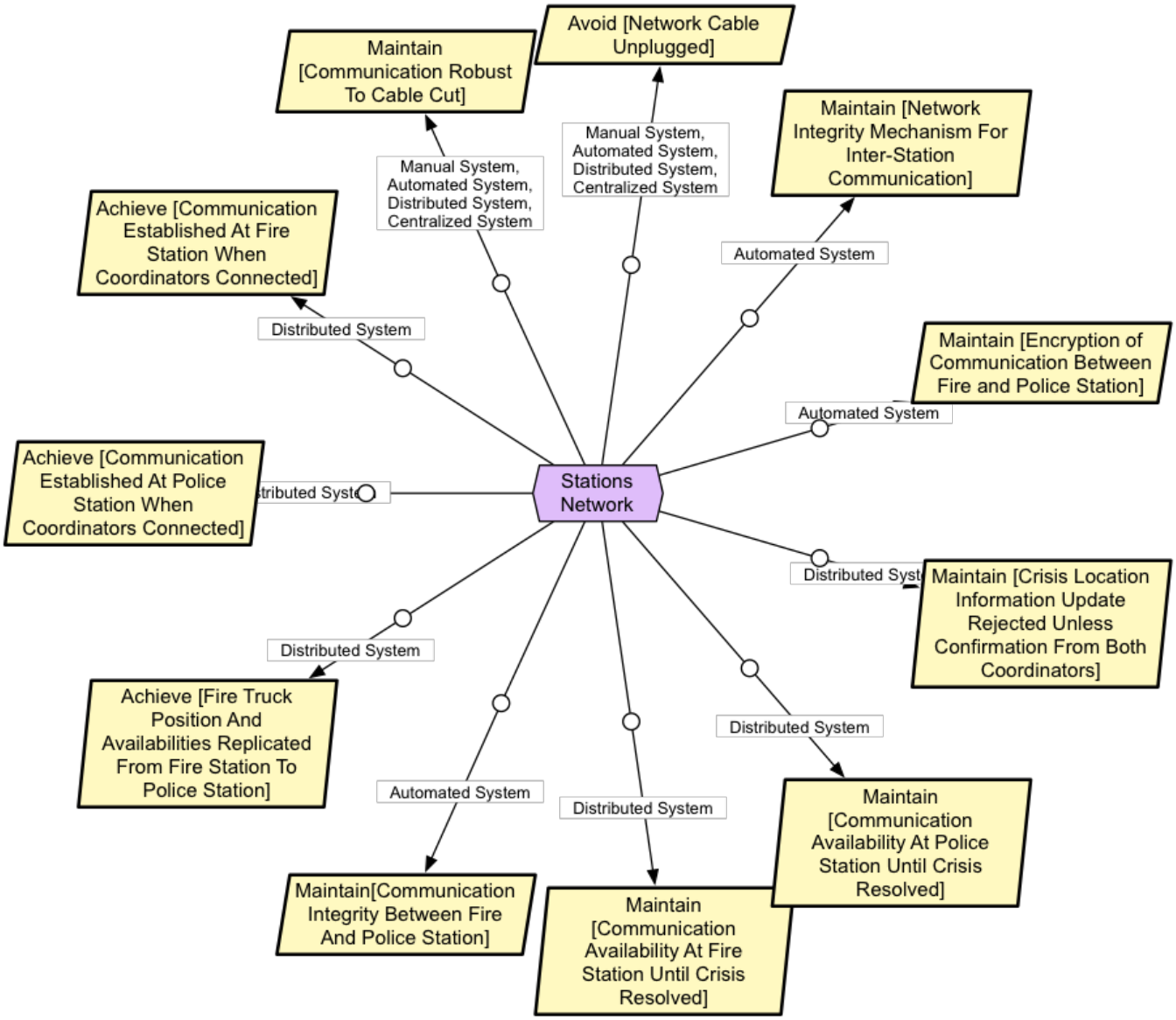
Radio Network

The communication infrastructure between the fire and police stations on one side and police vehicle and fire trucks on other side.



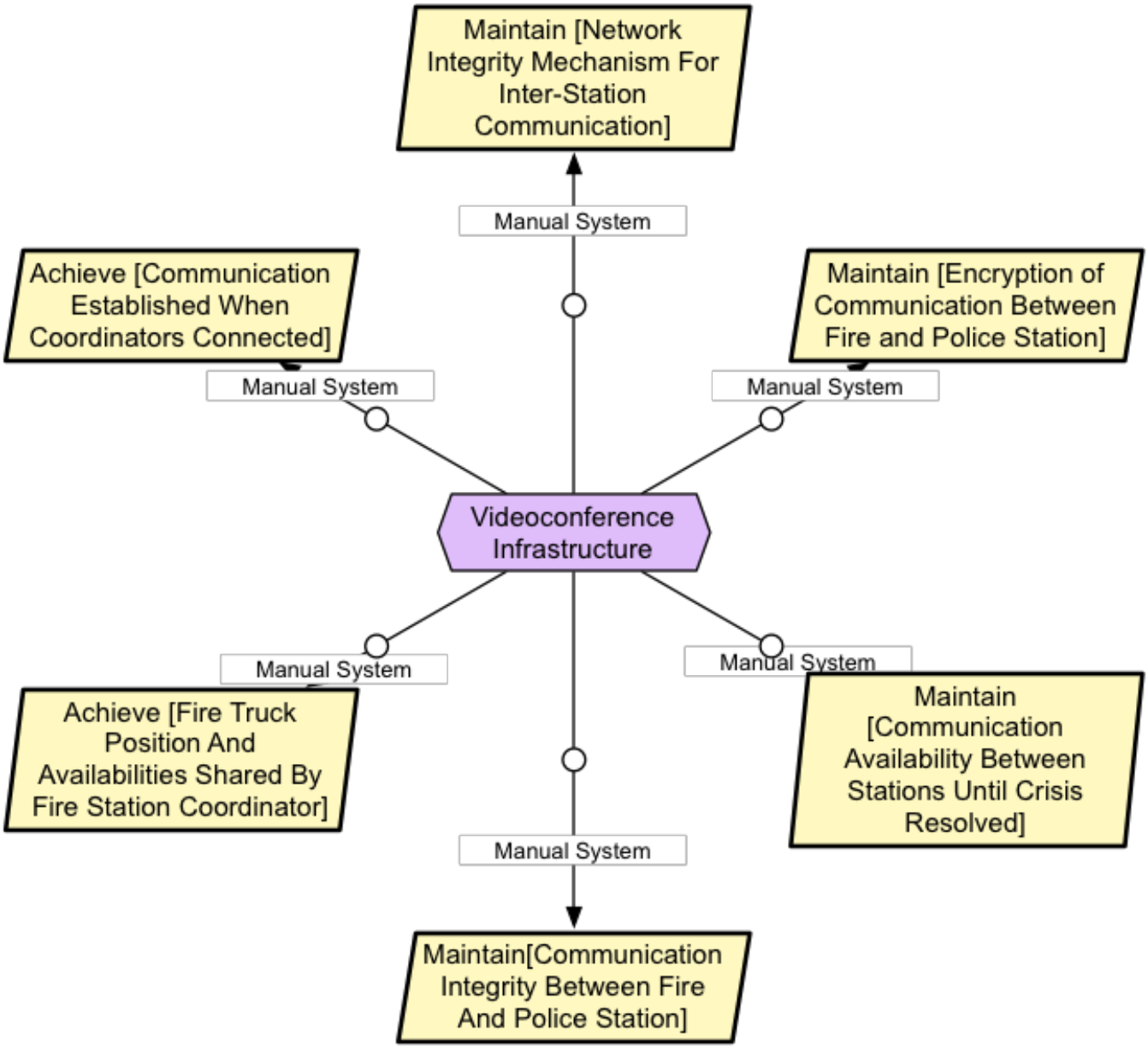
Stations Network

The communication infrastructure between the fire and police stations.



Videoconference Infrastructure

This agent allows the fire and police coordinators communicating effectively through video and sound between physically distant fire and police stations.



Witness

A witness of the crisis.

Behaviors

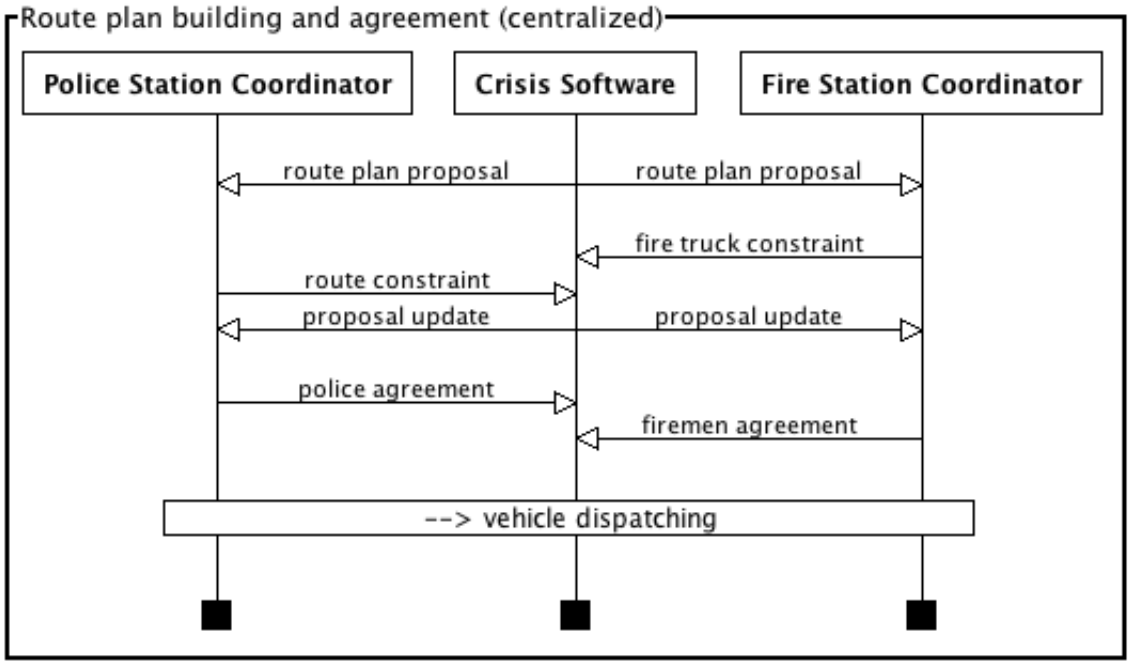
This section provides a few models capuring the behavior of specific agents, mostly in the centralized alternative. We invite the reader to observe the following inter-model consistency rules:

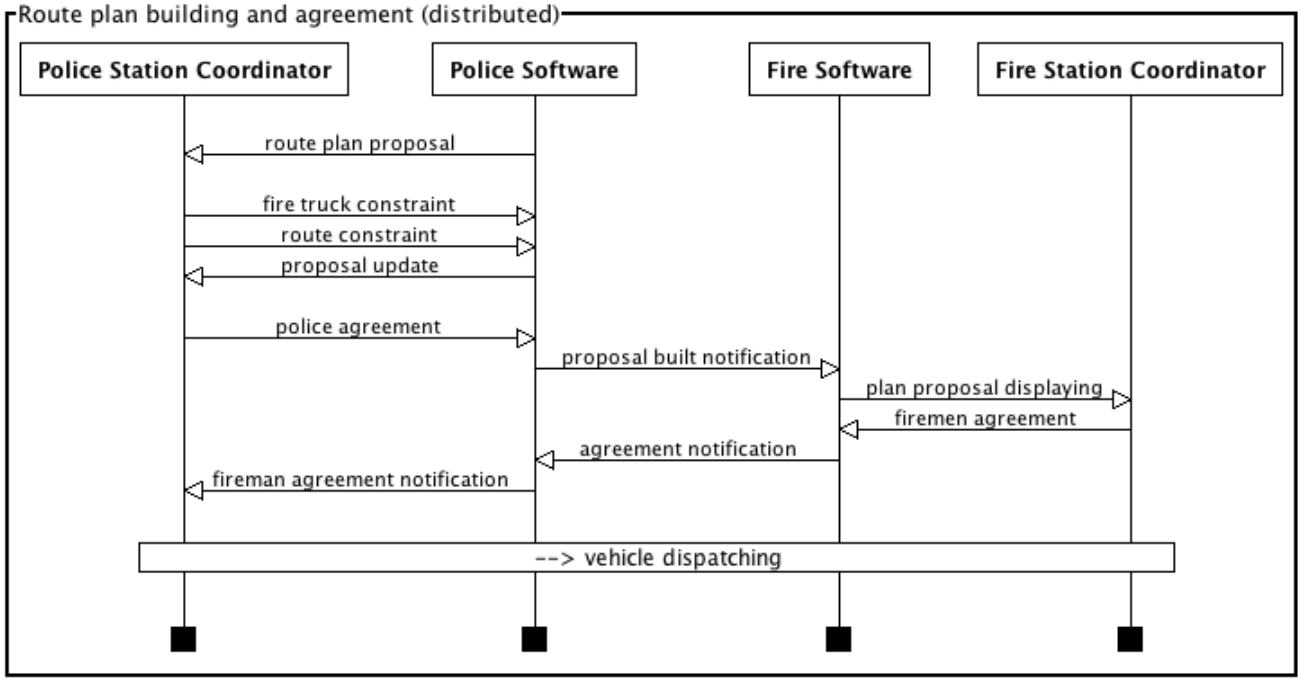
- Timelines correspond to agent instances (cfr. agent model).
- Scenario events correspond to events and/or actions in the state machines, according to whether the event is monitored or controlled by the software.
- Event sequences correspond to admissible paths in the agent's state machines.

Scenarios

Route plan building and agreement

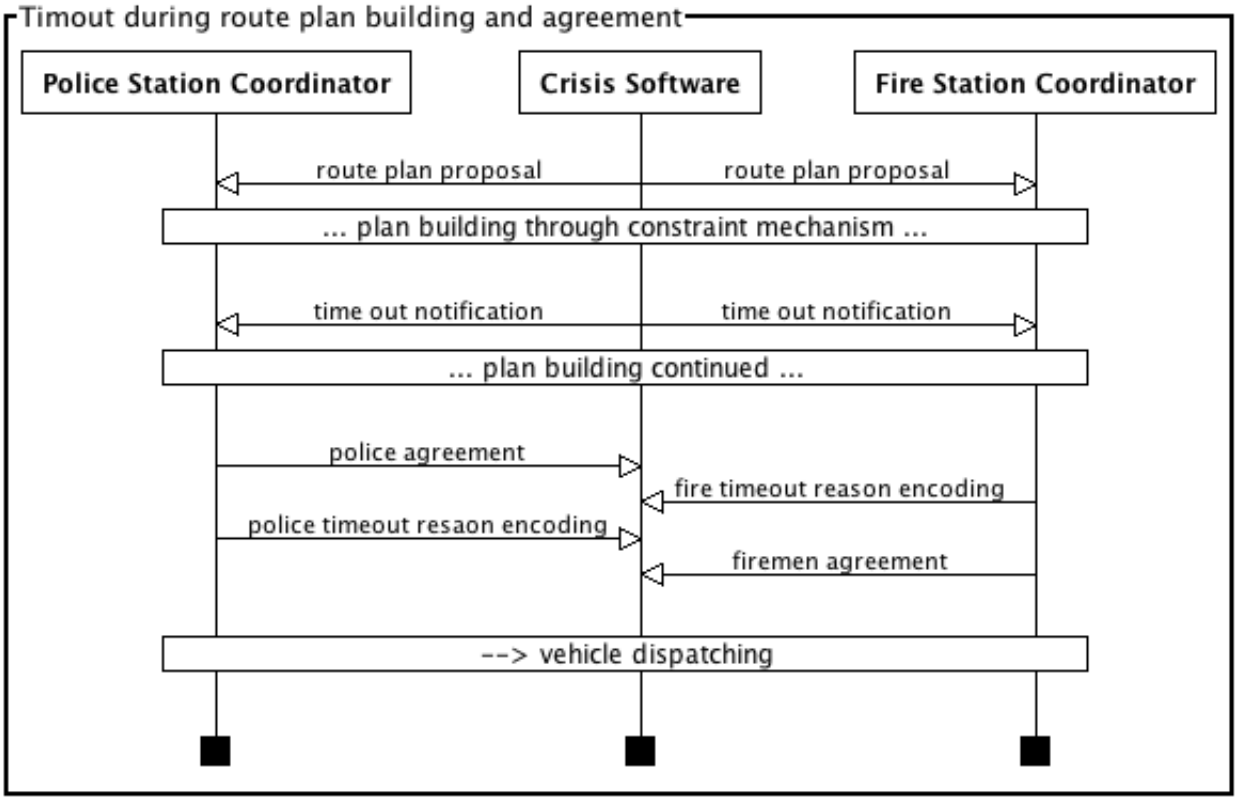
Comparison of the centralized and distributed alternative ways of building and agreeing on a route plan.





Timeout during route plan building

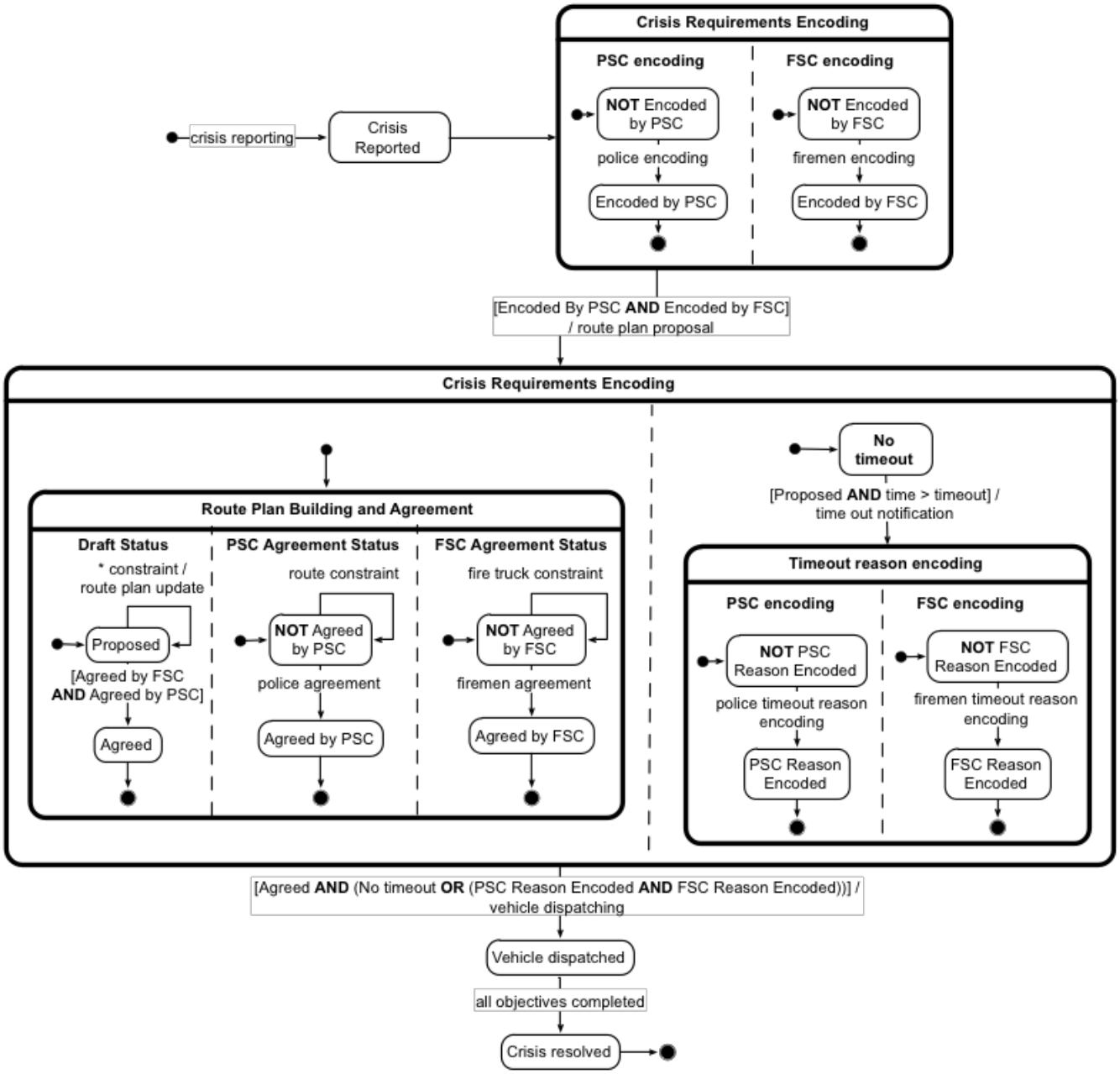
This scenario shows that the coordinators have to explain the reason of a timeout during the route plan building. This can be made in parallel with the agreement of the route plan (cfr. state machines) but before vehicle dispatching.



State machines

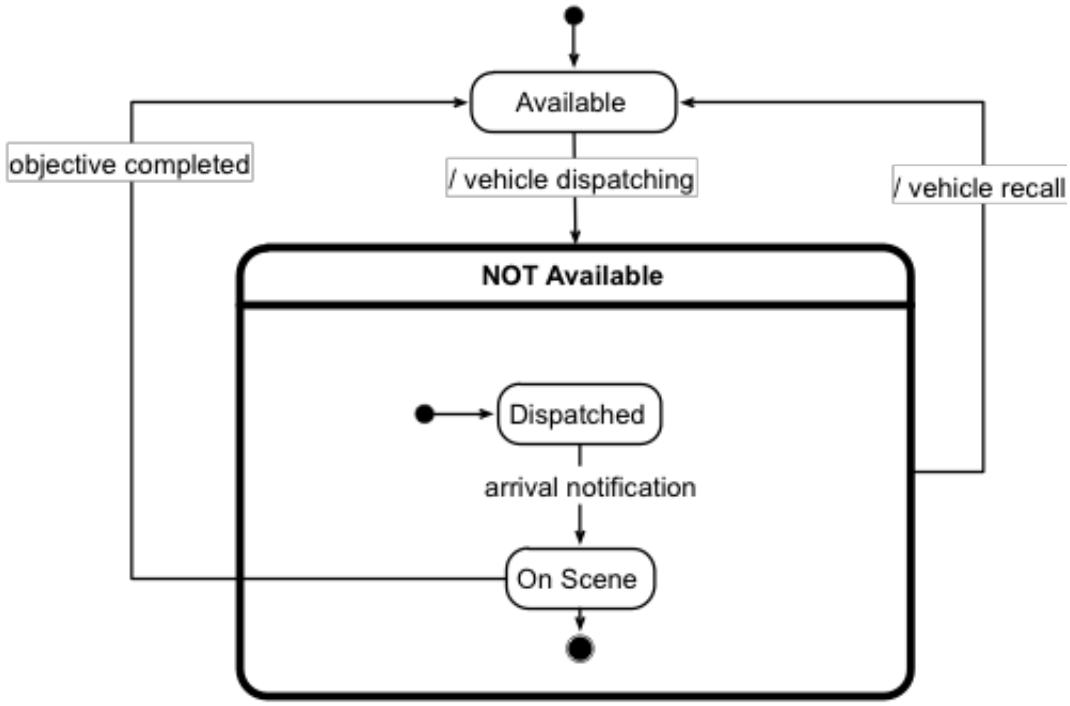
Crisis Software Information

State machine of the `CrisisInfo.Status` attribute, controlled by the `Crisis Software` agent.



Vehicle Availability Information

State machine of the `VehicleInfo.Availability` attribute controlled by the `Crisis Software` agent.

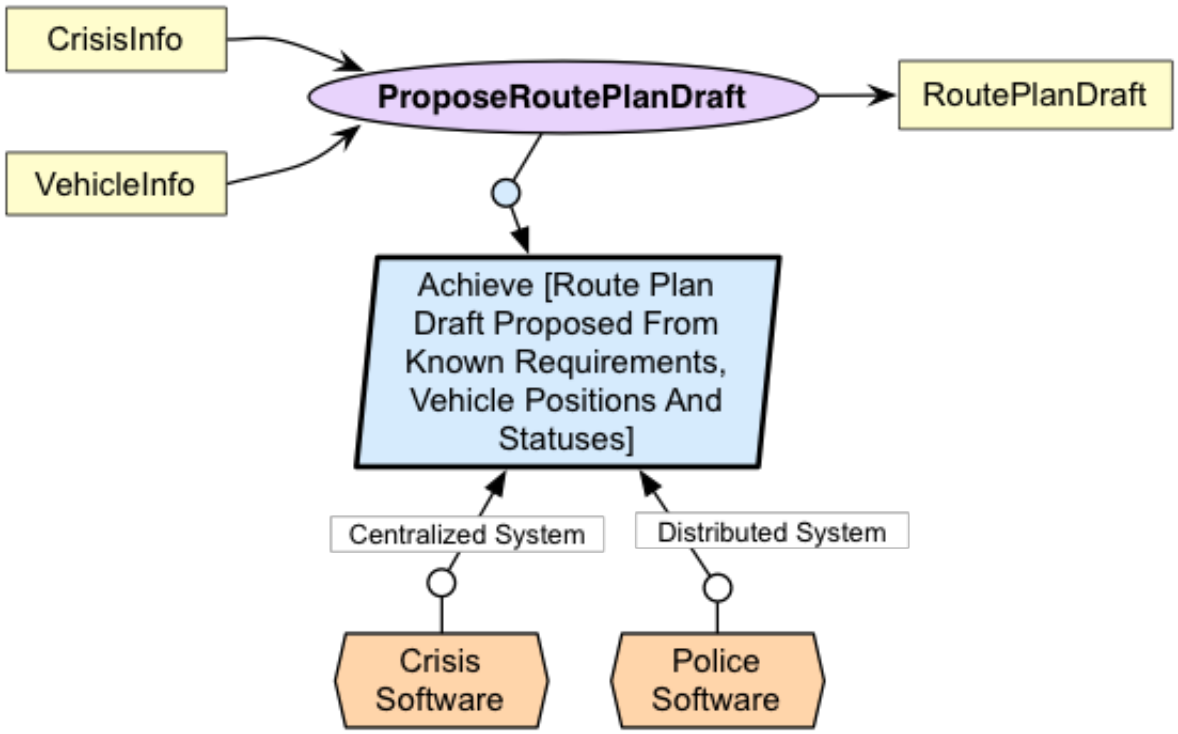


Operations

This section presents the software operations derived from requirements. We focus here on the centralized alternative only.

ProposeRoutePlanDraft

Operation that captures the proposal of a route plan draft to the coordinators.

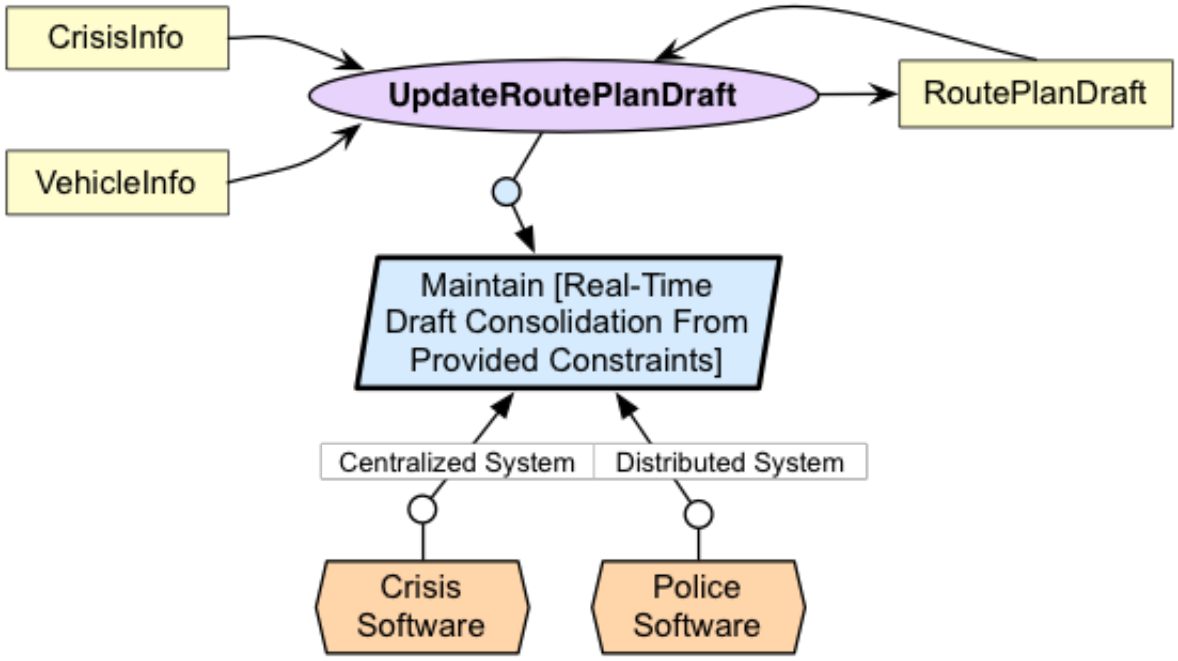


Attribute	Definition
Input	`c: CrisisInfo`, `v1..vn: VehicleInfo`
Output	`rp: RoutePlanDraft`
Associated event	`route plan proposal`
Domain precondition	No route plan draft exists for resolving `c`
Domain postcondition	`rp` is proposed to resolve `c`
Required trigger conditions	For: Achieve [Route Plan Draft Proposed From Known Requirements, Vehicle Positions And Availabilities] Definition: The number of fire trucks and police vehicles needed for handling `c` has just been encoded by coordinators.
Required preconditions	For: Maintain [Route Plan Draft Meeting Crisis Requirements] (*to be defined*) Definition: The are sufficient vehicles available so as to build a route plan meeting the requirements. Note that in the ideal model, this precondition is trivially met in accordance to our domain hypotheses.
Required postconditions	For: Maintain [Route Plan Draft Meeting Crisis Requirements] (*to be defined*)

Definition	rp allocates at least as many fire truck and police vehicles as stated in the fire and police requirements for crisis `c`, respectively.
For	Avoid [Fire Truck Driver In Unfamiliar Area]
Definition	`rp` respects all constraints stated by fire and police coordinators. In particular, it does not allocate vehicles or use routes explicitly stated by them as to be avoided.
For	Maintain [Route Plan Remains Feasible Until Agreed]
Definition	Every vehicle in rp is currently available, the time to reach the crisis location from its current location is below X minutes and its path can be followed easily enough (e.g. streets are large enough for fire trucks to turn, etc.).

UpdateRoutePlanDraft

Operation that captures the update of a route plan draft to stay up to date with all vehicle information, route plan constraints, and crisis requirements.



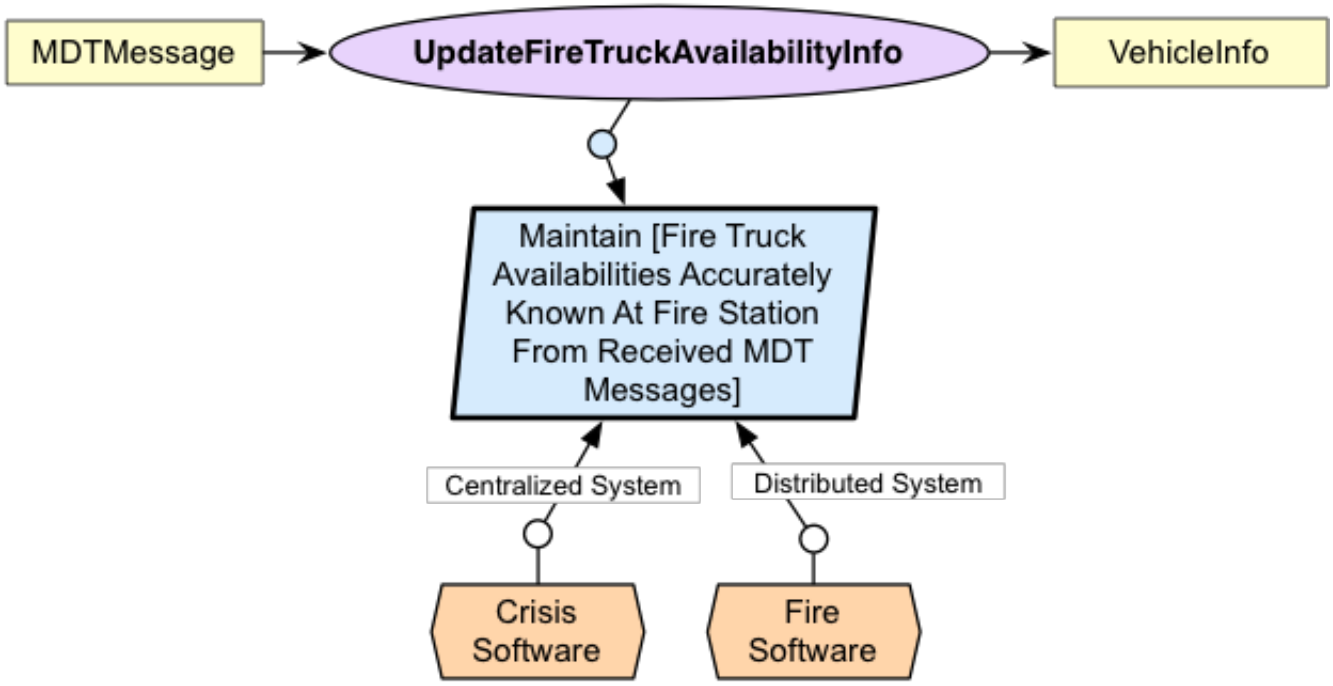
Attribute	Definition
Input	`c: CrisisInfo`, `v1..vn: VehicleInfo`, `rp: RoutePlanDraft`
Output	`rp: RoutePlanDraft`
Associated event	`route plan update`
Domain precondition	The route plan draft `rp` is not up to date
Domain postcondition	`rp` is up to date
Required trigger conditions	For: Maintain [Real-Time Draft Consolidation From Provided Constraints] Definition: The crisis requirements have just been changed. For: Maintain [Real-Time Draft Consolidation From Provided Constraints] Definition: A new route or vehicle constraint has just been added by a coordinator. For: Maintain [Real-Time Draft Consolidation From Provided Constraints] Definition: The information about the position or availability of a vehicle has just been modified.
Required preconditions	For: Maintain [Route Plan Draft Meeting Crisis Requirements] (*to be defined*) Definition:

	The are sufficient vehicles available so as to update the route plan in such a way that it meets the requirements. Note that in the ideal model, this precondition is trivially met in accordance to our domain hypotheses.

Required postconditions		
	For	Maintain [Route Plan Draft Meeting Crisis Requirements] (*to be defined*)
	Definition	rp allocates at least as many fire truck and police vehicles as stated in the fire and police requirements for crisis `c`, respectively.
	For	Avoid [Fire Truck Driver In Unfamiliar Area]
	Definition	`rp` respects all constraints stated by fire and police coordinators. In particular, it does not allocate vehicles or use routes explicitly stated by them as to be avoided.
	For	Maintain [Route Plan Remains Feasible Until Agreed]
	Definition	Every vehicle in rp is currently available, the time to reach the crisis location from its current location is below X minutes and its path can be followed easily enough (e.g. streets are large enough for fire trucks to turn, etc.).

UpdateFireTruckAvailabilityInfo

Operation that captures the update of a fire truck availability as known by the software everytime a MDT message is received.



Attribute	Definition
Input	`m: MDTMessage`
Output	`vi: VehicleInfo`
Associated event	`fire truck availability update`
Domain precondition	the message `m` has not been handled
Domain postcondition	the message `m` has been handled
Required trigger conditions	For: Maintain [Accurate Fire Truck Availability Information At Fire Station From Received MDT Messages] Definition: The message `m` has just been received.
Required preconditions	
Required postconditions	For: Maintain [Accurate Fire Truck Availability Information At Fire Station From Received MDT Messages] Definition: `vi.Availability == m.Availability`

Detailed definitions

Agents

Name	Definition
AVLS	The Automated Vehicle Location System is an agent located vehicles and fire trucks that frequently reports the vehicle location to the police and fire stations, respectively.
Communication Compromiser	The communication compromiser wants to achieve personal gain during the crisis.
Crisis Software	The Crisis Software is the main software in the centralized system alternative. Among others, it is responsible of maintaining effective communitation between the FSC and PSC and helping them achieving their goals through computing intelligence (real-time feedback, route computing, etc.).
Fire Software	The Fire Software is a software agent in the distributed system alternative. It is responsible of helping the FSC with fireman-related responsibilities as well as guaranteeing that needed information from the police station is available at the fire station.
Fire Station Coordinator	A FSC maintains control over a crisis situation by communicating with the police station coordinator (PSC) as well as firemen
Fireman	A fireman acts on orders received from the FSC and reports crisis-related information back to the FSC. Furthermore, a fireman communicates with other firemen, victims, and witnesses at the crisis location.
MDT	The Mobile Data Terminal is an agent located inside police vehicles and fire trucks that allows reporting the vehicle availability to the police and fire stations, respectively.
MDT/AVLS Network	The communication infrastructure used by the AVLS and MDT agents to send/receive availability and position notifications with the fire and police stations.
Police officer	A police officer acts on orders received from the PSC and reports crisis-related information back to the PSC. Furthermore, a police officer communicates with other policemen, victims, and witnesses at the crisis location.
Police Software	The Police Software is a software agent in the distributed system alternative. It is responsible of helping the PSC with police officer-related responsibilities as well as guaranteeing that needed information from the fire station is available at the police station.
Police Station Coordinator	A PSC maintains control over a crisis situation by communicating with the fire station coordinator (FSC) as well as policemen.
Radio Network	The communication infrastructure between the fire and police stations on one side and police vehicle and fire trucks on other side.
Stations Network	The communication infrastructure between the fire and police stations.
Videoconference Infrastructure	This agent allows the fire and police coordinators communicating effectively through video and sound between physically distant fire and police stations.
Witness	A witness of the crisis.

Goals

Name	Definition
	to be defined
Achieve [Accurate Fire Truck Position Received When Sent]	The accurate position shall be received within 5 seconds when sent.
Achieve [Accurate MDT Message Sent When Fire Truck Availability Change Encoded]	Every time the availability of a fire truck is changed through encoding on its MDT, a message shall be sent containing the vehicle ID and information about the new availability.
Achieve [Accurate MDT Message Sent When Right Button Pressed]	*to be defined*
Achieve [Alternative Route Computed When Route Unfeasible]	*to be defined*
Achieve [Backup Asked To Other Police And Fire Stations When Not Enough Vehicles Available]	When not enough vehicles are available to handle the crisis with respect to the stated requirements then backup shall be asked to other police and fire stations.
Achieve [Backup Manually Asked To Other Stations When Coordinators Notified]	When coordinators are notified that not enough vehicles are available to handle the crisis with respect to the stated requirements then they shall call for backup to other police and fire stations.
Achieve [Best Route Plan Proposed When No Route Plan Meeting All Constraints Exists]	When no route plan exists that meet all stated constraints then a route plan draft is eventually proposed that violates the minimum of stated constraints.
Achieve [Closing Agreed When Closing Proposed By PSC]	A crisis closing proposal shall eventually be accepted by the FSC when proposed by the PSC.
Achieve [Closing Proposed When Route Plane Objectives Completed]	For every crisis for which all route plan objectives have been completed a closing proposal shall be proposed by the PSC to the FSC.
Achieve [Communication Established At Fire Station When Coordinators Connected]	For every reported crisis, communication shall be established at fire station as soon as fire and police coordinators are connected.
Achieve [Communication Established At Police Station When Coordinators Connected]	For every reported crisis, communication shall be established at police station as soon as fire and police coordinators are connected.
Achieve [Communication	

Established When Coordinators Connected]	For every reported crisis, communication shall be established between the police and fire coordinators as soon as they are connected.
Achieve [Communication Established When Crisis Reported]	For every reported crisis, communication shall be established between the responsible police and fire coordinators.
Achieve [Coordinators Notified When Not Enough Vehicles Available]	The coordinators shall be notified by the software when not enough vehicles are available to handle the crisis with respect to the stated crisis requirements.
Achieve [Crisis Closed When Route Plan Objectives Completed]	Every crisis whose all objectives are complete shall eventually be closed.
Achieve [Crisis Details Discussed As Soon As Possible When Communication Established]	For every reported crisis, as soon as the communication has been established between coordinators, they shall discuss (share and compare) relevant information about the crisis.
Achieve [Crisis Details Encoded When Crisis Reported]	For every crisis, all relevant information shall be independently encoded by coordinators as soon as the crisis is reported.
Achieve [Crisis Details Exchanged When Crisis Reported]	For every reported crisis, all relevant information (e.g. crisis location, number of victims, etc.) shall eventually be exchanged between coordinators.
Achieve [Crisis Requirements Discussed When Independently Established]	Crisis requirements shall be discussed by both coordinators when crisis has been reported at both station independently.
Achieve [Crisis Requirements Encoded At Fire Station When Established]	Fire vehicle requirements shall be encoded at fire station when crisis is established.
Achieve [Crisis Requirements Encoded At Police Station When Established]	Route and police vehicle requirements shall be encoded at police station when crisis is established.
Achieve [Crisis Requirements Encoded When Established]	Fire and route requirements shall be encoded when crisis has been established at both stations.
Achieve [Crisis Requirements Exchanged When Established]	For every crisis, when fire and police requirements have been established, they are eventually exchanged with the other coordinator.
Achieve [Crisis Requirements Known When Crisis Details Exchanged]	For every reported crisis, when the details have been exchanged between coordinators, the requirements (e.g. the number of required vehicles) shall eventually be known by both of them.

Achieve [Crisis Requirements Known When Crisis Reported]	For every reported crisis, required resources for handling the crisis shall eventually be known by both coordinators.
Achieve [Crisis Requirements Weakened When Coordinators Notified of Vehicle Unavailability]	When notified of the non availability of enough vehicles to handle the crisis, the coordinators shall weaken the crisis requirements.
Achieve [Crisis Resolved When Reported]	Every crisis shall be eventually resolved when reported.
Achieve [Crisis Resolved When Route Plan Agreement Reached]	For every crisis, when a route plan has been agreed by coordinators then the crisis is eventually resolved.
Achieve [Fire Constraints Provided When Route Plan Draft Proposed]	When a route plan draft is proposed, the fire constraints are eventually provided to the software for plan consolidation.
Achieve [Fire Coordinator Connected When Crisis Reported]	For every reported crisis, the reponsible fire coordinator shall connect to the system as soon as possible.
Achieve [Fire Details Encoded When Crisis Reported]	For every crisis, all relevant information shall be encoded by the fire coordinator as soon as the crisis is reported.
Achieve [Fire Requirements Established Based on Exchanged Crisis Details]	For every crisis, based on exchanged information, the number of fire trucks required shall eventually be established by the fire coordinator.
Achieve [Fire Truck Availability Change Encoded on MDT]	When the availability of the fire vehicle changes, the fireman shall encode that change by pressing rhe right button on its MDT. More specifically, the 'Available' button shall be pressed when the fire truck completed its objectives, 'Dispatched' shall be pressed when the fire vehicle acknowledges its participation to a route plan and 'OnScene' when the fire truck arrives on the crisis scene.
Achieve [Fire Truck Dispatched When In Route Plan]	Every fire truck involved in a agreed route plan shall be dispatched as soon as possible.
Achieve [Fire Truck Objective Completed When On Scene]	Every fire truck at the crisis location shall eventually complete its objective.
Achieve [Fire Truck On Scene When Dispatched]	Every dispatched fire truck shall reach the crisis location as soon as possible.
Achieve [Fire Truck Position And Availabilities Replicated From Fire Station To Police Station]	The position and availabilities of each fire truck shall be replicated from the database of the fire station to the database of the police station.
Achieve [Fire Truck Position And Availabilities	The position and availabilities of each fire truck shall be shared by the fire station coordinator with the police station coordinators.

Shared By Fire Station Coordinator]	
Achieve [Fire Truck Position and Availibility Updates Announced At Radio When Changed]	Fireman shall announce at radio state main changes of the fire truck position and availability updates.
Achieve [Fire Truck Positions And Availabilities Gathered From Fire Station At Police Station]	For every crisis whose requirements are known, the positions and availabilities of fire trucks shall be gathered from the fire station so as to be known at police station too.
Achieve [Fire Truck State Updates Emitted At Fire Station When Announced]	Fire truck, resp. police vehicle, state updates announced by radio shall be emitted at the fire station.
Achieve [Known Lost Or Confused When Lost Or Confused]	*to be defined*
Achieve [Known Lost Or When Right MDT Message Received]	*to be defined*
Achieve [Location Information Checked By Fire Coordinator On Update Requests]	The crisis location shall be explicitely checked by the fire coordinator every time an update of the location information is requested to the software.
Achieve [Location Information Checked By Police Coordinator On Update Requests]	The crisis location shall be explicitely checked by the police coordinator every time an update of the location information is requested to the software.
Achieve [Lost Button Pressed When Lost Or Confused]	*to be defined*
Achieve [MDT Message Received When Sent]	Sent MDT messages shall be received at corresponding station.
Achieve [Other Fire Vehicle Dispatched When Fire Vehicle Stopped Or In Wrong Direction]	*to be defined*
Achieve [Police and Fire Constraints Provided When Route Plan Draft Proposed]	When a route plan draft is proposed, the police and fire constraints are eventually provided to the software for plan consolidation.
Achieve [Police Constraints Provided When Route Plan Draft Proposed]	When a route plan draft is proposed, the police constraints are eventually provided to the software for plan consolidation.
Achieve [Police	

Coordinator Connected When Crisis Reported]	For every reported crisis, the reponsible police coordinator shall connect to the system as soon as possible.
Achieve [Police Details Encoded When Crisis Reported]	For every crisis, all relevant information shall be encoded by the police coordinator as soon as the crisis is reported.
Achieve [Police Requirements Established Based on Exchanged Crisis Details]	For every crisis, based on exchanged information, the number of police vehicles required shall eventually be established by the police coordinator.
Achieve [Police Vehicle Dispatched For Modifying Traffic Deviation]	*to be defined*
Achieve [Police Vehicle Dispatched For Reducing Traffic Jam]	*to be defined*
Achieve [Police Vehicle Dispatched When In Route Plan]	Every police vehicle involved in a agreed route plan shall be dispatched as soon as possible.
Achieve [Police Vehicle Objective Completed When On Scene]	Every police vehicle at the crisis location shall eventually complete its objective.
Achieve [Police Vehicle On Scene When Dispatched]	Every dispatched police vehicle shall reach the crisis location as soon as possible.
Achieve [Route Constraints Added to Route Plan Draft To Avoid Unfamiliar Area]	*to be defined*
Achieve [Route Indication Known By Driver When Displayed]	*to be defined*
Achieve [Route Indications Computed]	*to be defined*
Achieve [Route Indications Displayed When Transmitted]	*to be defined*
Achieve [Route Indications Displayed]	*to be defined*
Achieve [Route Indications Known By Driver]	*to be defined*
Achieve [Route Indications Provided When Fire Truck Lost]	Every truck driver lost of confused about the crisis location shall received details indications on how to reach the crisis scene from her current location.
Achieve [Route Indications	*to be defined*

Provided When Known Lost]	
Achieve [Route Indications Transmitted]	*to be defined*
Achieve [Route Plan Agreed Once Explained]	For every crisis, the route plan built by the police coordinator is eventually agreed by the fire coordinator when it has been explained.
Achieve [Route Plan Agreed When Displayed]	For every crisis, the route plan built by the police coordinator is eventually agreed by the fire coordinator when displayed in the fire station.
Achieve [Route Plan Agreement Reached When Requirements Known]	For every crisis, based on established requirements, the police and fire coordinators shall eventually agree on a route plan to be deployed so as to resolve the crisis.
Achieve [Route Plan Built From Information About Crisis And Vehicles Available At Police Station]	The route plan shall be built from the known crisis requirements and known positions of police vehicle and fire truck. By built, we mean that a route plan draft shall exists with a route for each involved vehicle. The draft shall meet all requirements.
Achieve [Route Plan Built When Crisis Requirements Known]	For every crisis, based on established requirements, a feasible route plan is eventually built by the police coordinator.
Achieve [Route Plan Displayed When Received]	When received at the fire station, the route plan is eventually displayed.
Achieve [Route Plan Displayed When Route Plan Built]	For every crisis, the route plan built by the police coordinator is eventually displayed at the fire station.
Achieve [Route Plan Draft Consolidated When Proposed]	When a route plan draft is proposed, it is eventually consolidated, meaning that necessary constraints known by coordinators are taken into account such that the plan deployment is feasible and such that the crisis is likely to be resolved in a timely manner. Also, for each vehicle its path (from its current position to the crisis scene) and its ETA is computed.
Achieve [Route Plan Draft Eventually Promoted To Route Plan]	The consolidated route plan draft is eventually promoted as a route plan when it all necessary constraints have been taken into account.
Achieve [Route Plan Draft Proposed From Known Requirements, Vehicle Positions And Availabilities]	When the crisis requirements as well as vehicle positions and availibilities are known a route plan draft is eventually proposed by the software to the coordinators.
Achieve [Route Plan Draft Proposed From Weakened Crisis Requirements]	When the crisis requirements have been weakened by the coordinators a route plan draft is eventually proposed by the software to the coordinators.
Achieve [Route Plan Eventually Agreed When Built]	For every crisis, the route plan built by the police coordinator is eventually agreed by the fire coordinator.
Achieve [Route Plan	

Explained When Built]	For every crisis, the route plan built by the police coordinator is eventually explained to the fire coordinator.
Achieve [Route Plan Objectives Completed When Agreement Reached]	For every crisis, when an agreement has been reached between coordinators on the route plan to deploy, the objective of every vehicle allocated to the crisis is eventually completed.
Achieve [Route Plan Proposed on Weakened Constraints When No Route Plan Meeting All Constraints Exists]	When no route plan exists that meet all stated constraints then a route plan draft is eventually proposed after constraints having been weakened by coordinators.
Achieve [Route Plan Proposed on Weakened Crisis Requirements When Not Enough Vehicles Available]	When not enough vehicles are available to handle the crisis with respect to the stated requirements then the crisis requirements shall eventually be weakened by the coordinators
Achieve [Route Plan Sent When Built]	For every crisis, the route plan built by the police coordinator is eventually sent at the fire station.
Achieve [Vehicle Dispatched When In Route Plan]	Every vehicle involved in a agreed route plan shall be dispatched as soon as possible.
Achieve [Vehicle Objective Completed When On Scene]	Every vehicle at the crisis location shall eventually complete its objective.
Achieve [Vehicle On Scene When Dispatched]	Every dispatched vehicle shall reach the crisis location as soon as possible.
Achieve [Vehicle On Scene When In Route Plan]	Every vehicle involved in a agreed route plan shall be at the crisis location as soon as possible.
Achieve [Vehicle Positions And Availabilities Known At Police Station When Requirements Known]	For every crisis whose requirements are known, the positions and availabilities of police vehicles and fire trucks shall be known at the police station (so as to allow the PSC to build a route plan).
Avoid [Coordinator Decisions Based on Corrupted Data]	The system shall ensure that the integrity of every data on which critical decisions are taken by coordinators (such as crisis location, vehicle number and vehicle location) is preserved 99,99% of the time and 95% of the time for other data.
Avoid [Coordinator Decisions Based on Inaccurate Data]	The system shall ensure that every critical decision taken by coordinators shall be based on accurate data 99,99% of the time and 95% of the time for other decisions.
Avoid [Fire Truck Driver In Unfamiliar Area]	The route chosen for every allocated fire truck shall be such that the truck driver won't have to ride in an area unfamiliar to her.
Avoid [Malicious Message Alterations In Communication Between	The system shall ensure that no alteration of messages by malicious users is possible.

Fire and Police Station]	
Avoid [Network Cable Unplugged]	The system shall be such that unplugging network cables is as unlikely as possible at fire and police stations.
Avoid [Unauthorized Access to Encryption Keys]	The bcms system/organization shall ensure that encryption keys used to secure the communication between stations cannot not be accessed by unauthorized users.
Avoid [Unecessary Communication Between Stations]	*to be defined*
Avoid [Unfeasible Route For Fire Truck]	*to be defined*
Maintain [Accurate Display Of Critical Information]	The system shall ensure the accuracy of critical information when displayed. In particular, devices diplaying the location of the crisis and vehicles shall be refreshed in less than 3 sec. every time the underlying information changes.
Maintain [Accurate Fire Truck Availability Information At Fire Station From Received MDT Messages]	The accurate availabilities of fire trucks shall be known at fire station based on the received MDT messages.
Maintain [Accurate Fire Truck Availability Information At Fire Station]	The availabilities of fire truck shall be accurately known at fire station.
Maintain [Accurate Fire Truck Position And Availability Information At Fire Station]	The position and availabilities of fire truck shall be accurately known at fire station. By accurate, we mean that the position does not differ for more than X meters and the availability are the same within Y seconds.
Maintain [Accurate Fire Truck Position Information At Fire Station From Received AVLS Notifications]	The accurate position of fire truck shall be known at fire station when received.
Maintain [Accurate Fire Truck Position Information At Fire Station]	The position of fire trucks shall be accurately known at fire station.
Maintain [Accurate Fire Truck Position Sent Regularly]	The accurate position of fire truck shall be sent every 30 seconds.
Maintain [Accurate Information About Crisis Location At Both Stations]	The system shall ensure that the information about the crisis location is accurate 99,99% of the time as such information is used for critical decisions.
Maintain [Accurate Police Vehicle Availability	The availabilities of police vehicle shall be accurately known at police station. The refinement of this goal is similar to what happens for fire trucks.

Information At Police Station]	
Maintain [Accurate Police Vehicle Position And Availability Information At Police Station]	The positions and availabilities of police vehicle shall be accurately known at police station. The refinement of this goal is similar to what happens for fire trucks.
Maintain [Accurate Police Vehicle Position Information At Police Station]	The positions of police vehicle shall be accurately known at police station. The refinement of this goal is similar to what happens for fire trucks.
Maintain [Accurate Replication of Critical Information]	Every replication of critical information from one station to the other shall be accurate. In particular, if replicated, vehicle information (position, availability) shall not differ for longer than 1 sec, 99,99% of the time.
Maintain [Accurate Vehicle Position And Availability Information At The Station It Belongs To]	The system shall ensure that the information about the positions and availibilities of police vehicles and fire trucks used in critical decisions remains accurate 99,99% of the time at the station to which the vehicle belongs.
Maintain [Blackboard Kept UpToDate From Fire Truck Notifications]	Accurate information about the position and availability of the fire trucks shall be kept up-to-date and displayed on a blackboard. State shall be updated on update notification.
Maintain [Communication Availability At Fire Station Until Crisis Resolved]	For every crisis, when communication is established at the fire station, it shall remain established until the crisis is resolved.
Maintain [Communication Availability At Police Station Until Crisis Resolved]	For every crisis, when communication is established at the police station, it shall remain established until the crisis is resolved.
Maintain [Communication Availability Between Stations Until Crisis Resolved]	For every crisis, when communication is established between the responsible police and fire coordinators, it shall remain established until the crisis is resolved.
Maintain [Communication Integrity]	The system shall ensure that the integrity of every critical data transmitted to stations (such as crisis location, vehicle number and vehicle location) is preserved 99,99% of the time and 95% of the time for other data.
Maintain [Communication Robust To Cable Cut]	The communication system between stations shall be sufficiently robust to support the failures/cuts of a small number of communication lines.
Maintain [Crisis Communication High Quality-of-service Priority]	*to be defined*
Maintain [Crisis Location Accurate When Initially Reported]	The crisis location shall be accurately reported by witnesses.
Maintain [Crisis Location	

Information Update Rejected Unless Confirmation From Both Coordinators]	Every request for update of the crisis location information at stations shall be rejected unless a confirmation has been explicitely made by both coordinators.
Maintain [Crisis Requirements Available When Encoded]	Crisis requirements shall be made available to both coordinators when encoded.
Maintain [Cross Check Of Crisis Location Information Updates During Crisis]	The system shall ensure that updates to the crisis location information at stations shall be cross checked by both coordinators.
Maintain [Data Availability]	• The crisis details, route plan and information related to the identification of coordinators shall be available with the exception of a total of 5 minutes during the time period when at least one crisis is active. • The crisis details and route plans should be available with the exception of a total of 30 minutes for every 48 hours when no crisis is active.
Maintain [Database Integrity]	The system shall ensure that the integrity of data kept in software databases is preserved 99,99% of the time.
Maintain [Display Integrity]	The system shall ensure that the integrity of every critical data displayed at stations (such as crisis location, vehicle number and vehicle location) is preserved 99,99% of the time and 95% of the time for other data.
Maintain [Double Level Integrity Mechanism For Inter-Station Communication]	The system shall ensure a double level integrity mechanism for every message exchanged between stations.
Maintain [Encoded Crisis Details Available At Both Stations When Communication Established]	For every reported crisis, all encoded details shall be made available both at the fire station and the police station.
Maintain [Encoded Crisis Details Available At Fire Station]	The encoded details about the crisis shall be available at fire station. By available, we mean that the information can be known by the fire coordinator (for example, displayed on a screen, printed, etc.).
Maintain [Encoded Crisis Details Available At Police Station]	The encoded details about the crisis shall be available at police station. By available, we mean that the information can be known by the police coordinator (for example, displayed on a screen, printed, etc.).
Maintain [Encoded Crisis Details Remain Encoded]	For every reported crisis, encoded details shall remain encoded until the crisis is resolved.
Maintain [Encoded Crisis Requirements Remain Encoded]	When crisis requirements have been encoded in the software they shall remain encoded until the crisis is closed.
Maintain [Encoded Fire	The encoded fire details about the crisis shall be available at fire station.

Details Available At Fire Station]	
Maintain [Encoded Fire Details Available At Police Station]	The encoded fire details about the crisis shall be available at police station.
Maintain [Encoded Police Details Available At Fire Station]	The encoded police details about the crisis shall be available at fire station.
Maintain [Encoded Police Details Available At Police Station]	The encoded police details about the crisis shall be available at police station.
Maintain [Encryption of Communication Between Fire and Police Station]	The system shall use state-of-the-art cryptography techniques to encrypt the coommunication between stations.
Maintain [Fast Response From Software]	The software shall respond quickly to user queries and quickly perform required tasks. What 'quickly' precisely mean shall be further defined with stackholders.
Maintain [Fire Truck Positions and Availabilities Available At Police Station When Available At Fire Station]	The position and availabilities of each fire truck shall be available at the police station when available at the fire station.
Maintain [Network Integrity Mechanism For Inter-Station Communication]	The integrity of all messages exchanged between fire and police station shall be ensured by the network hardward devices and protocols.
Maintain [Real-Time Draft Consolidation From Provided Constraints]	The software shall consolidate the route plan draft from the known vehicle position and constraints provided by coordinator(s). In particular, the path (from its current position to the crisis scene) and ETA is computed for each vehicle.
Maintain [Route Plan Draft Meeting All Stated Constraints]	A route plan draft shall meet all constraints stated by the coordinators.
Maintain [Route Plan Remains Feasible Until Agreed]	For every crisis, the route plan built by the police coordinator shall remain feasible until being agreed by the fire coordinator.
Maintain [Software Integrity Mechanism For Inter-Station Communication]	The integrity of all messages exchanged between fire and police station shall be ensured by software composants using state-of-the-art cryptography mechanisms.
Maintain[Communication Integrity Between Fire And Police Station]	The system shall ensure that the integrity of every critical data transmitted between fire and police stations (such as crisis location, vehicle number and vehicle location) is preserved 99,99% of the time and 95% of the time for other data.
Maintain[Communication Integrity Between Stations	The system shall ensure that the integrity of every data transmitted from vehicle to stations (e.g. number and location) is preserved 99,99% of the time.

And Vehicles]

Soft goals

Name	Definition
Minimize [Time To Get Resources on Crisis Location]	Getting needed resources on the crisis location, such as police vehicles and fire trucks shall take the shortest possitble amount of time.
Maximize [Data and Estimates Precision and Accuracy]	The estimation of resource needs and time of arrivals for resources shall be as accurate as possible. More generally the accuracy and precision of any non-critical data critical shall be maximized.
Minimize [Stress Level]	The system shall help minimizing the stress level of both coordinators.
Minimize [System Cost]	The system shall ensure effective response times with minimal costs.
Minimize [Response Time]	• The system shall respond to user requests within 5 seconds 95% of the time. • The system shall respond to user requests within 30 seconds 99,99% of the time.

Domain properties

Name	Definition
Objective Completed Forever When Completed	The objective of a police vehicle or a fire truck remains completed once completed. The resurgence of an emergency situation, such as a fire, is modeled as a new objective to which some vehicle needs to be allocated.

Domain hypotheses

Name	Definition
Allocated Vehicles Stay Immobile Until Route Plan Agreed	The location of each vehicle allocated in a route plan does not significantly change from the moment the plan has been built until it is agreed by the fire coordinator.
No Obstacle Appearance on Routes Choosen for Allocated Vehicles	No significant change of route conditions (obstacles, congestion, etc.) appear between the moment where the route has been computed for a vehicle allocated in a route plan until the vehicle actually reaches the crisis location.

Obstacles

Name	Definition
AVLS Network Congestion	*to be defined*
AVLS Network Down	*to be defined*
Blackboard Not Kept Accurately Up To Date From Fire Truck Notifications	The blackboard is innaccurately updated from fire truck notifications.
Blackboard Not Kept Up To Date From Fire Truck Notifications	The blackboard is not kept up to date when fire truck notifications.
Blackboard Not Updated From Fire Truck Notifications	The blackboard is not updated from fire truck notifications.
Communication Between Stations Broken	The communication between the fire and police station is completely broken.
Communication Integrity Violated	Integrity of communication between fire and police station is violated either intentionally (by malicious users) or unintentionally (by network devices or software)
Crisis Less Severe Than Expected Before Fire Vehicle On Scene	Before the vehicle reached the crisis scene, crisis have been reported as less severe than expected, the fire vehicle is no longer required for handling the crisis.
Crisis Reported As Fake Before Fire Vehicle On Scene	Crisis have been reported as fake before the fire vehicle reached the crisis scene.
Crisis Resolved Before Fire Vehicle On Scene	Before the vehicle reached the crisis scene, crisis have been reported as resolved, the fire vehicle is therefore no longer required for handling the crisis.
Encoded Crisis Details No Longer Encoded	The encoded crisis details are no longer available.
Encryption Keys Stolen	*to be defined*
Fire Station Coordinator Busy When Notification Received	The fire station coordinator is too busy when a notification is received.
Fire Station Coordinator Confused When Updating Blackboard	The fire station coordinator is confused when updating the blackboard.
Fire Station Coordinator Overloaded By Received Notifications	The fire station coordinator is overloaded by the received notifications.
Fire Truck Positions Never Received	The fire truck position is never received at station.
Fire Truck Positions Not Received When Sent	The fire truck positions are not received in time when sent.
Fire Truck Positions Received Too Late	The fire truck positions are received too late.
Fire Vehicle Broken Down	The fire vehicle is broken down.
Fire Vehicle In Traffic Deviation	The fire vehicle is deviated from its initial route such that it will not be able to reach the incident scene within the prescribed delay.

Fire Vehicle In Wrong Direction	The fire vehicle toke a wrong direction such that it will not be able to reach the crisis scene within prescribed delays.
Fire Vehicle Lost or Destination Confused	The fire vehicle driver confused the destination.
Fire Vehicle Not On Scene In Time When Dispatched	The dispatched fire vehicle is not the crisis scene within the required delays. Similar obstacle analysis can be conducted on police vehicles.
Fire Vehicle Retracted For Resolving Crisis	The fire vehicle is retracted by the fire station coordinator.
Fire Vehicle Stopped	The fire vehicle stopped before arriving on the crisis scene.
Fire Vehicle Stuck In Traffic Jams	The fire vehicle is stuck in traffic jams such that it will not be able to reach the crisis scene within prescribed delays.
Flooding Attack	Malicious user attemps to perform a denial-of-service attack by flooding the network with a large number of fake message.
Hard Disk Failure	The hard disk storing the encoded crisis details have an hardware failure.
Large Traffic Peak	Large traffic peak slow down the communication between the two stations.
Malicious Communication Delay	Malicious user slows down the communication between the two stations.
Malicious Interruption	Malicious user drops messages sent.
Message Maliciously Modified	Malicious user modified the message.
Message Modified	Message has been modified, but is still intelligible for the receiver.
Message Modified By Network Infrastructure	Message has been altered by the network infrastructure (by middlebox for example) so that it is not the same as the one sent.
Message Received Too Late When Sent	Sent message is received too late.
Message Scrambled	Message is unintelligible by the receiver.
Nearer Other Fire Vehicle Available Before Fire Vehicle On Scene	A fire vehicle nearer the crisis scene is available and sent in place of the already dispatched fire vehicle.
Network Cable Cut	Network cable joining the two station has been cut by some external event.
Network Cable Unplugged	Network cable has been inadvertently unplugged at one of the station.
Network Cabling Deficiency	Network cabling fails to deliver some parts of the sent message.
Network Cabling Failure	Network cable fails to conduct the message from one station to the other.
Network Devices Deficiency	Network devices fails to deliver some parts of the sent message.

Network Devices Saturated	The network devices composing the network infrastructure abnormaly delays the communication.
Network Hardware Failure	Network hardware fails to conduct the message from one station to the other.
No Feasible Route Plan Meeting All Constraints Exists	There exists no feasible route plan to handle the crisis that meets all stated route and vehicle constraints.
Not Enough Vehicles Available To Handle The Crisis	No sufficient vehicles are available for handling the crisis given the stated requirements.
Power Outage	Power required for the data server to run is no longer available.
Route Plan Not Proposed When Requirements, Positions and Availibilities Known	Despite crisis requirements being known as well as vehicle positions and availibilities, no plan is proposed to the coordinators by the bCMS software.
Too Many Fire Truck Positions Sent	*to be defined*
Truck Position Message Corrupted	*to be defined*
Truck Position Message Modified By Compromiser	*to be defined*
Unfeasible Route For Fire Vehicle	The fire vehicle cannot reach the crisis scene due to an unpracticable route (road too small, impassable, muddy, snowy, flooded, do not support weight, etc.)
Wrong Fire Truck Positions Received	The fire truck positions received is not the same as the one sent.
Wrong Message Received When Sent	Message received is not the same as the message sent.

Predicates

Name	Definition
CommunicationEstablished	The communication between the PSC `p` and FSC `f` has been established through the system, that is, each of them knows who is the other and they can exchange any relevant information about the crisis `c`.
CrisisClosed	The fire and police coordinators agreed to consider the crisis as closed.
ClosingProposed	It has been proposed to close the crisis `c`.
Reported	A crisis is reported when it has been detected and declared both at the fire station and the police station, possibly independently.
CrisisRequirementsKnown	The fire and police coordinators both know what resources are required to resolve the crisis, in particular, the number of fire trucks and police vehicles needed.
Resolved	A crisis is resolved when all route plan objectives are completed and an agreement for closing the crisis has been reached between the fire and police station coordinators.
Accurate	For every vehicle allocated in the route plan `rp`, the departure point of its path to the crisis location corresponds to its real current position (with a tolerance of X meters); the destination point corresponds to the crisis location.
Agreed	The route plan `rp` has been explicitely agreed by the coordinators in charge of the crisis crisis `c`.
RoutePlanAgreementReached	The police and fire coordinators agree on a route plan to deploy for resolving the crisis. Such route plan describes all police and fire vehicles allocated to the crisis together with the route to be followed for each of them from its current position to the crisis location. In addition, the route plan meets established requirements, is accurate and feasible.
Feasible	Every vehicle in the route plan fleet is currently available, the time to reach the crisis location from its current location is below Y minutes and its path can be followed easily enough (e.g. streets are large enough for fire trucks to turn, etc.).
MeetsRequirements	The route plan `rp` allocates at least as many fire truck and police vehicles as stated in the fire and police requirements for crisis `c`, respectively.
VehicleDespatched	The vehicle `v` is considered as despatched when the team in the vehicle has confirmed that they will go to the crisis scene.
VehicleInRoutePlan	The vehicle is involved in the route plan.
VehicleObjectiveCompleted	Vehicle objectives are considered as completed when the team in the corresponding vehicle fullfiled their respective mission, e.g. extinguish fire, moving vehicles, rescuing victims, enforcing law, etc. Description of respective objectives to complete is outside the scope of this document.
VehicleOnScene	

The vehicle `v` is considered on scene when the team in the vehicle has confirmed that are, physically, on the crisis scene.
