

FAQ – Systematic Case

Where is the COP device supposed to be deployed?

Are there automatic updates regarding position from the associated units to the mobile SitaWare system?

Do we have to consider security levels in the system?

Do we have to provide any kind of security mechanism like login control in order to use the SitaWare solution?

Could you provide us some additional details about the legacy systems that are used with the new SitaWare solution?

Do we have to fulfill any kind of standard in order to handle the information exchange?

Should network setup be automatically done? Where is the COP device supposed to be deployed?

Where is the COP device supposed to be deployed? Urban areas? Low developed environments with no communication infrastructure? In the case a communication infrastructure is not already deployed the connection can be easily lost between the mobileHQ and the fixed one, or between the mobileHQ and the mobile units.

It is assumed that the solution will be usable nationally as well as internationally. If this has any implications on the solution you're devising please document this. You must describe the requirements for your solution, the choice of what you provide and what you require is yours as long as you document it.

Are there automatic updates regarding position from the associated units to the mobile SitaWare system? For example: a police team enters the operations theatre, is the commander supposed to register them manually on his system or they will automatically appear on the screen? Maybe the police team is using a handheld device that reports the commander automatically the position.

Again this is a design decision you must make, just remember to describe and justify your decisions so that I can see that you have considered the various options.

Do we have to consider security levels in the system? Do we have to consider different permissions depending on the information layer we want to access? For instance: the army forces are able to trace police movements but the ambulances are not allowed to do so.

Definitely – We need to be able to control access to the information accumulated in the system.

Should network setup be automatically done? In the case of an emergence we suppose that setting up the communication should be automated to some extent, since there are more important issues to solve. We would like to have a little bit more of information regarding this process.

In case of a major disaster you cannot expect infrastructure to remain fully functional. Your solution should be self-contained. Please remember that any part of the problem that you are aware of, but does not address, must be stated.

Do we have to fulfill any kind of standard in order to handle the information exchange? Since it is a military system may be we have to apply some kind of special technique to protect how the communication is done or how the data is stored in the system.

You can expect SitaWare to handle the information in a safe way. Your communication should be secured using commercially available techniques.

Could you provide us some additional details about the legacy systems that are used with the new SitaWare solution? If we have to design our system in order to be compatible with them (as it is explained in the SOW), we would like to get a more detailed insight on this matter.

The static and dynamic information is available from public databases and web-services such as gis.aarhus.dk and dmi.dk. On a suitable level of abstraction you must describe how you intent to integrate these information.

Do we have to provide any kind of security mechanism like login control in order to use the SitaWare solution? For example: the commander is the only one allowed to use the terminal and he is logs in with a digital certificate.

Yes, we need access control. Please describe which technology you choose to use to authenticate the users.