Since July 1, 2004 C2000 replaced the analog communication networks of Dutch emergency services. Nowadays the police forces, fire departments, ambulances and the Koninklijke Marechaussee (a force providing military police and civil police duties) all use the C2000 system for their communication. Recently, this system caused quite some unrest in the Netherlands, due to some possible failures of the system during some major events. In this article the concerns that are associated with C2000, will be pointed out.

Before we look at the issues that arose with C2000, we first address the reasons for the transfer to C2000. After that a brief technical analysis of the C2000 system will be given. Finally, the problems that arose in using C2000 will be pointed out.

**From analog to digital**

In the mid nineties there were several developments, which caused an understanding among the Dutch emergency services that it was necessary to replace the old analog communications networks. Besides the general tendency towards the digital era, one of the main developments was the insight that the analog system was not providing enough capacity and lacked in security. Besides that, the analog system did not provide the possibility for the different emergency services, like the police, fire squad and ambulances, to communicate with each other. Both the evaluation from the fire at Volendam during the turn of the year 2000 to 2001 and the evaluation of the fireworks explosion...
in Enschede, confirmed these issues some years later.

In September 2004 the C2000 was introduced. It took three years before the last police squad, the one of the region Amsterdam-Amstelland, shut their analog network down and switched to C2000. This completed the nationwide migration towards the digital C2000. C2000 belongs to the class of Private Mobile Radio (PMR) systems, which have different requirements than the public communication networks. The specific demands of users of PMR systems will be addressed later. These demands cannot be satisfied by conventional system like GSM, GSM-R and DECT. Therefore a standard, especially suitable for PMR systems, like C2000, is developed.

**TETRA**

The C2000 communication network makes use of the standard TETRA, which is an abbreviation for TErrestrial Trunked Radio. Trunking is a word borrowed from the telephone system to describe a system, in which a large number of users share a much smaller number of communication paths. Traditionally, this was related to a wire (the trunk) that was assigned to a telephone user upon making a call. In the case of terrestrial radio the scarce resource is bandwidth. If we relate this for example to the police in a certain region, where there are at a given time quite a number of police officers on duty, who all need to stay in contact with a dispatcher. If each officer would use an exclusive channel, the available frequency band would soon run out of possible channels. Moreover, this is not a very efficient way to assign radio channels, since each channel would be idle most of the time.

In a trunked radio system the total numbers of users are divided into groups. Imagine waiting with a group of friends for a table at a crowded restaurant. You go up to the hostess and give her your name, and she puts it on a list with a bunch of other names. If all the tables already have people at them, you wait. When a table is ready the hostess announces your name over the speaker and you and your friends follow her to the table she selected for you (probably the first one that became available). This principle is also applicable to the kind of trunking used in TETRA. When a user of one group wants to talk to a user of another group, he has to request a channel assignment from a controller first. The controller will check if there is a channel free. If all the channels are occupied, the controller makes you wait until a channel is free, and then publicly announces your talk group and the assigned channel. User A and the intended receiving users then switch to that channel and can communicate with each other.

Trunking can be applied to both a part of the conversation or to the entire conversation. The first is implemented in TETRA. In this case a conversation that takes place over several transmissions may actually occur on several different radio channels because the controller may assign a new channel every time someone presses their push-to-talk button. This is the most efficient way to share radio channels, since other people can use the channel during pauses in the conversation, but it is also what makes it more difficult for a normal scanner to listen in.

At this point, one can wonder why use a complete different standard instead of proven technology like GSM. The reason for this is the specific requirements that communication networks for emergency services demand. The traditional techniques, like GSM, have certain issues, discussed here, which are solved in C2000.

- GSM limits the amount of subscribers in a group to 1024 and the amount of dispatchers to 5. In TETRA no restrictions on group size are defined, but a group can deal with at most 30 dispatchers. Especially the relative small number of possible dispatchers in GSM is a limitation, since one of the objectives of the network is to enable different emergency services to communicate with each other. This requires many dispatchers. A very effective way of informing members of a group in case of an emergency is trough sending a short data message to each member of the group. This function is defined in TETRA, but is not available in GSM. Of course it is possible to send a SMS in GSM to each member of the group individually. However, this is significantly slower than the service TETRA provides. Besides that, since SMS data files run over the signaling channel of GSM, this will put a significant additional load on the signaling channel, when used extensively.

- Another rather important difference origins in the way how both handle call priorities. Call priorities are specified for both TETRA and GSM. However, TETRA is more flexible in this case, because it can provide different priorities to a user or group. Furthermore, in TETRA more priority classes are specified. Another rather important feature of TETRA that is not incorporated in GSM is the speech item priority. In for example emergency situations it can be important that a group leader can get a speech item and force the other subscribers in the group to listen. This feature can be important to achieve organized communications, which can be critical in an emergency situation.

- When designing a communication network for the emergency service the call set-up time is of huge importance. In C2000 it is required that a call can be set-up within 0.5 seconds. With some efforts the call set-up time in GSM can only be reduced to one second.
The security of the network is of extreme importance for the intended users of C2000. The security should ensure that someone not belonging to a certain group is unable to listen to the communication, but also is unable to disturb the communication. In TETRA three types of security measures are implemented. First, authentication ensures that only users with a valid key can use the network. Moreover, the call information, the control information and the identity of the users is encrypted, by a so-called Air Interface Encryption (AIE) protocol. This ensures that a user can be tracked by following the signaling messages on the control channel. Last, encryption between the endpoints of communication is provided. End-to-end encryption (e2ee) prevents eavesdropping by encrypting the information on the traffic channel. The difference with AIE is that the information on the control channel isn’t encrypted.

Issues
In 2009 there were several incidents, which caused some distrust in the C2000 system. In February a passenger flight of Turkish Airlines crashed near Schiphol Airport. During the rescue the system had signs of overloading. For example many people couldn’t get a proper connection using their radio. Afterwards, the Inspection for Public Order and Safety concluded that the available 11 groups were too little for the vast number of emergency services on site. Another, and maybe one of the most well-known, example of the disfunctioning of C2000 is during the riots on the beach of Hoek van Holland. When the situation escalated, again, the system showed signs of overloading. The police men on site couldn’t communicate with each other for some time.

As a result of these incident, the Department of Interior Affairs has investigated the operation of C2000. One of the outcomes of this investigation is that there are some locations in the Netherlands, where the coverage of C2000 is not sufficient. At these locations the link tends to switch between two different base stations, hence drastically deteriorating the connection. These locations are collected in a so-called DIPP list (Dekkings Issue Prioritering Procedure, in short this means a collection of the important locations, where coverage problems arise). This DIPP list also includes Pernis, where the Dutch petrochemical industry is concentrated, Borssele, the location of a nuclear power plant and Vught, the location of an extra secure prison. Recently was announced the coverage of 60 high-risk locations like these will be optimized within two years.

Although some of the technical shortcomings of C2000 are recognized, the influence of the user on the proper functioning of C2000 also has to be taken into account. For example when evaluating the problems that arose during the plane crash in February, it was concluded emergency people were using their radio for non-essential communication too. If the radio was only used for the important messages, the overloading of the network could have been prevented. The failures of the system, during the riots at Hoek van Holland, but also during the attack on Queen’s Day 2009 were ascribed to the fact that there were too many users in the same group. The director of the region Rotterdam-Rijnmond, Don Berghuis, who was appointed for the research, states that many emergency service people all use the same group. Therefore the system seems overloaded. In fact this isn’t the case, but because there are many users in one group, individual users need to wait longer before they can speak. When in critical situations people tend to speak at the same time, this gives problems. Berghuis also added that this isn’t a specific telecommunications problem.

If ten people are talking to each other in person, communication also won’t work if they talk at the same time. To solve this problem, the users of C2000 are trained again to work properly with the system.

Conclusion
More than a decade ago the Dutch emergency services switched from an analog communication network to a digital one: C2000. Theoretically, this new communication network provides the emergency services with state-of-the-art communication, providing in all their specific demands. However, when using C2000 some issues arose. Especially during major incidents, the system showed signs of overloading. Investigations showed that there exist both technical as user related reasons for these issues. To overcome the technical problem of too little base stations at critical locations, the coming years these base stations will be installed. The users of C2000 are once again trained, in order for them to work properly with the system. Maybe, these two actions will finally enable the emergency services to use their life saving communication system.

References: