FAR and FRR

security level versus user convenience

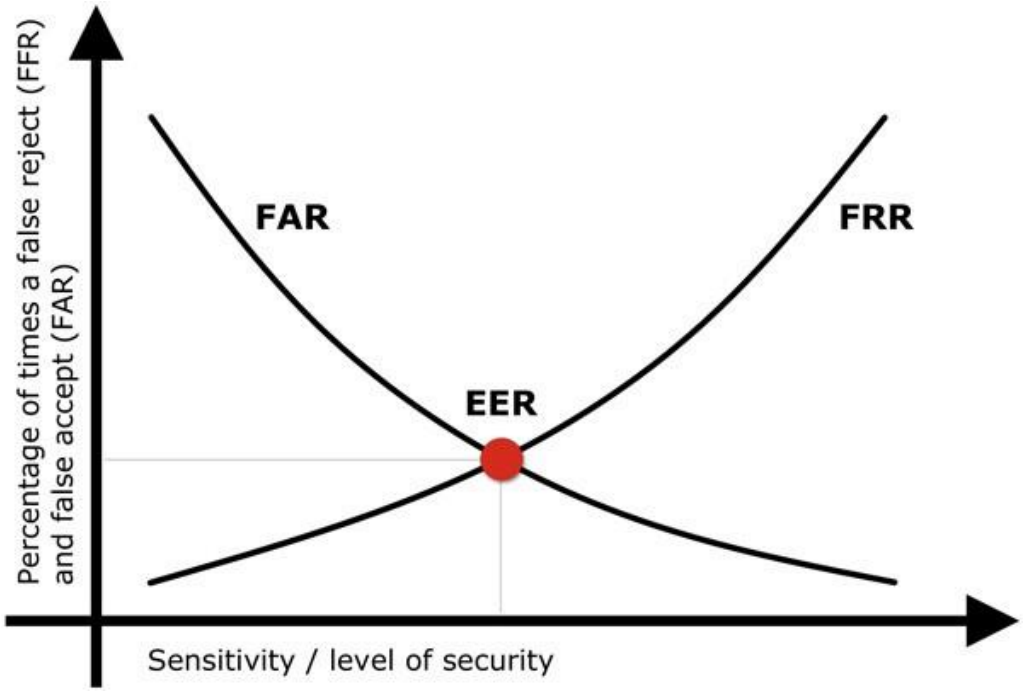
FAR and FRR. Anyone who wants to assess or compare the performance of biometric security systems cannot ignore these terms. In this article we explain what FAR and FRR mean, how they impact on each other and how they affect a system's security level and user convenience.

Let's start with the definitions. The performance of biometric systems is expressed on the basis of the following error rates:

- **False Acceptance Rate (FAR):** the percentage of identification instances in which unauthorized persons are incorrectly accepted.
- **False Rejection Rate (FRR):** the percentage of identification instances in which authorized persons are incorrectly rejected.

How do the FAR and FRR impact on each other?

As the number of false acceptances (FAR) goes down, the number of false rejections (FRR) will go up and vice versa (see the figure below). The point at which the lines intersect also has a name: the Equal Error Rate (EER). This is where the percentage of false acceptances and false rejections is the same.



How does this affect the security level and user convenience?

If you try to reduce the FAR to the lowest possible level, the FRR is likely to rise sharply. In other words, the more secure your access control, the less convenient it will be, as users are falsely rejected by the system. The same also applies the other way round. Do you want to increase user convenience by reducing the FRR? In this case the system is likely to be less secure (higher FAR).

Configuring the FAR and FRR in the software...

The FAR and FRR can usually be configured in a security system's software by adjusting the appropriate criteria so that they are more or less strict. We can conclude from the information above that this will result in a system that is more secure (but less user-friendly) or less secure (but more user-friendly).

... and the problem linked to this

There are only a few systems on the market that allow a high level of security to be achieved in combination with user-friendly access control. If an organization does not opt for such a system, it will often prioritize user convenience over security.

You can imagine the thinking behind this: “We don’t want people to have to queue up at the door because the system is not working properly. They may already have spent all morning stuck in traffic and not yet had a coffee...”

In some situations, of course, prioritizing convenience in this way may be acceptable to users. However, that is clearly not the case in situations where they expect a high level of security. And that is the problem: often the user has no insight into exactly how the software has been configured. This can create a false sense of security.

Something to bear in mind: visibility of the FAR and FRR

Like many security experts, we take the view that the FAR and FRR should not be changed invisibly. We believe that the visibility of these aspects should be part of a system’s configuration. In any case, this is something to bear in mind when selecting your access security system!