2.10. DISASTER RECOVERY

EMSA's Business Continuity Facility (BCF) is hosted in Porto in the premises of a commercial hosting provider. The BCF is a fully equipped replica of the main site in terms of servers, network equipment, internet connectivity, storage and middleware, and as such it may function as either the main production site for an application, or as back-up site. This choice may be made on a per application basis and depends on the EMSA needs, the application's replication design and capabilities, and the desired SL.

Any new system or application must conform by design to one of the business continuity approaches foreseen so far:

1) **ON/OFF model**:
   The servers and services that constitute the system or application are active and visible on the network only in the main site. They are kept in sync in the secondary site with some middleware or low level replica technology like Dataguard for backends, or virtual machine cloning or storage array based replication for front ends. But the replicated systems are always inactive on the secondary site in an off-state and not visible on the network unless the recovery procedure is executed. Taking over in that case means executing a procedure to stop the systems in the main site (if possible), execute a last synchronisation (if possible), stop the synchronisation flows, then restart the replicated systems in the secondary site changing all the parameters that differ in the two sites like network configuration, internal DNS entries, pointers to database or cartographic servers or to any other horizontal service platform always available in both sites like LDAP, Single Sign On, DNS etc…. Eventually, the external DNS entry should be changed to point external Internet users to the public IP of the system or application in the new site.

   According to this model, it is still possible to have the same internal FQDN for the application servers in both sites, as servers are active and visible on the network only in one site at a time, and when taking over, the A records of the internal DNS can be changed to reflect the different IP address space in the new site.

2) **ON/ON model**:
   The servers and services that constitute the system or application are active and ready to take over at any time in both sites. Synchronisation rely on the features of the application or middleware used rather than on a low-level cloning and transferring of the virtual machines, offering either a fully multi-master active/active approach like Active Directory, or some type of distributed geo-cluster, or anyway an autonomous system which keeps data and configuration in sync between the two legs in the two sites. Taking over in that case is a simpler procedure like activating some built-in system or application feature to switch to the other site, possibly requiring some internal and external DNS changes, or can be even fully transparent.

   According to this model, different FQDNs and IPs for the application servers in the two sites must be chosen, as servers are active and visible on the network in both sites at any time.

Note: it is not accepted to design ON/ON systems where the virtual machines on the two sides have the same internal DNS FQDN.

The ON/ON model, when supported by the application or middleware, might guarantee faster and seamless fail-over procedure, hence it is the preferred approach.

The following figure exemplifies how the interconnection of current EMSA's production environment with the BCF is envisaged and also points to the use of several replication/back-up systems at different levels of the infrastructure: