Security Aspects

With regard to AJAX, you have to keep in mind the following security risks:

1. **Code Injection**
   The main risk is the so-called "code injection".

   To prevent code injection, all data needs to be checked on the server side. For this purpose, Application Designer offers the `IRequestDataConverter` interface. This filter enables you to convert values coming from the user interface client: each data request contains values of changed properties. Each property value that is transferred into the Application Designer server may be passed through an instance of this interface.

   Background: in certain scenarios you may want to make sure that certain values are not passed into your application system. For example, for reasons of security, you do not want to enable inline scripting or inline SQL statements; therefore, you want to make sure that a user cannot input JavaScript statements or SQL statements. The *cisconfig.xml* file contains the parameter `requestdataconverter`. In order to make use of your data converter, specify the name of your data converter with this parameter. Example:

   ```
   <cisconfig .. requestdataconverter="com.your.RequestDataConverter" />
   ```

2. **Faked Client**
   The second risk is a so-called "faked client" which sends bad HTTP sequences, hoping that there is no server-side validation.

   In this case, the responsibility is on the developer’s side. Application Designer offers a client-side validation: the regular expression `/d/d/d/d` as the validation for a field; the field expects 4 decimal digits which will be validated on the client side. A faked client does not provide any validation. Thus, it depends on the developer to implement a server-side validation as well. One approach is to assume that all data that arrives from the client side might be wrong, even the data that is returned from a combo box. Therefore, if data might be wrong, it is important to double-check it on the server side.