**UC2 Manual Analysis Outcomes**

|  |  |  |  |
| --- | --- | --- | --- |
| **Function (F)** | **GW:** Not being Executed Causes Vulnerabilities (NECV) | **GW:** being Executed Causes Vulnerabilities (ECV) | **GW:** Timing Issues (TI) |
| P/S/D\_F1: Plain data process | / | P/S/D\_F1\_IFB1, P/S/D\_F1\_IFB2 | P/S/D\_F1\_IFB3 |
| P/S/D\_F2: Data transmission | P/S/D\_F2\_IFB1 | P/S/D\_F2\_IFB2 | P/S/D\_F2\_IFB3 |
| P/S/D\_F3: Data encryption | P/S/D\_F3\_IFB1 | P/S/D\_F3\_IFB2, P/S/D\_F3\_IFB3 | P/S/D\_F3\_IFB4 |
| P/S/D\_F4: Data decryption | P/S/D\_F4\_IFB1 | P/S/D\_F4\_IFB2, P/S/D\_F4\_IFB3 | P/S/D\_F4\_IFB4 |
| P/S\_F5: Signature calculation | P/S\_F5\_IBF1 | P/S\_F5\_IBF2 | P/S\_F5\_IBF3 |
| P/S\_F6: Signature verification | P/S\_F6\_IFB1 | P/S\_F6\_IFB2 | P/S\_F6\_IBF3 |
| U/M\_F7: human operation | / | U/M\_F7\_IFB1,  U/M\_F7\_IFB2 | / |
| **IFBs Description** | | | |
| P/S/D\_F1\_IFB1: The plain data process function is executed with unexpected behaviors (e.g. reject or modify valid data). [V-1/2]  P/S/D\_F1\_IFB2: The plain data process function is executed with data leakage risks (e.g. user password). [V-3]  P/S/D\_F2\_IFB1: The required data fail to be transmitted. [V-1/2]  P/S/D\_F2\_IFB2: The data is attacked (e.g. eavesdrop, tamper) during the transmission. [V-1/2/3]  P/S/D\_F3\_IFB1: The data encryption function fails to execute correctly. [V-2]  P/S/D\_F3\_IFB2: The data encryption function is executed with a fake key. [V-1/2/3]  P/S/D\_F3\_IFB3: The data encryption function is executed with an incorrect algorithm. [V-1/2/3]  P/S/D\_F4\_IFB1: The data decryption function fails to execute correctly. [V-2]  P/S/D\_F4\_IFB2: The data decryption function is executed with a fake key. [V-1/2]  P/S/D\_F4\_IFB3: The data decryption function is executed with an incorrect algorithm. [V-1/2]  P/S\_F5\_IBF1: The signature calculation function fails to execute correctly. [V-2]  P/S\_F5\_IBF2: The signature calculation function is executed with an incorrect algorithm. [V-1/2]  P/S\_F6\_IBF1: The signature verification function fails to executed correctly. [V-2]  P/S\_F6\_IBF2: The signature verification function is executed with an incorrect algorithm. [V-1/2]  P/S/D\_F1\_IFB3, P/S/D\_F2\_IFB3, P/S/D\_F3\_IFB4, P/S/D\_F4\_IFB4, P/S\_F5\_IBF3, P/S\_F6\_IBF3: Function execution violates the timing limits. [V-2] (This set of IFBs is call P/S/D\_Fc\_IFB1)  U/M\_F7\_IFB1: The invalid entity operates with valid data. [V-1/2]  U/M\_F7\_IFB2: The valid entity operates with invalid or incorrect data. [V-1/2] | | | |

|  |  |  |
| --- | --- | --- |
| **IFBs** | **GW:** Function Itself | **GW:** Environment (Env) |
| P/S/D\_F1\_IFB1 | P/S/D\_F1\_IFB1\_LS1 | / |
| P/S/D\_F1\_IFB2 | P/S/D\_F1\_IFB2\_LS1 | / |
| P/S/D\_F2\_IFB1 | / | P/S/D\_F2\_IFB1\_LS1 |
| P/S/D\_F2\_IFB2 | / | P/S/D\_F2\_IFB2\_LS1 |
| P/S/D\_F3\_IFB1 | P/S/D\_F3\_IFB1\_LS1 | P/S/D\_F3\_IFB1\_LS2, P/S/D\_F3\_IFB1\_LS3 |
| P/S/D\_F3\_IFB2 | P/S/D\_F3\_IFB2\_LS1 | / |
| P/S/D\_F3\_IFB3 | P/S/D\_F3\_IFB3\_LS1 | / |
| P/S/D\_F4\_IFB1 | P/S/D\_F4\_IFB1\_LS1 | P/S/D\_F4\_IFB1\_LS2, P/S/D\_F4\_IFB1\_LS3 |
| P/S/D\_F4\_IFB2 | P/S/D\_F4\_IFB2\_LS1 | / |
| P/S/D\_F4\_IFB3 | P/S/D\_F4\_IFB3\_LS1 | / |
| P/S\_F5\_IBF1 | P/S\_F5\_IBF1\_LS1 | P/S\_F5\_IBF1\_LS2 |
| P/S\_F5\_IBF2 | P/S\_F5\_IBF2\_LS1 | / |
| P/S\_F6\_IBF1 | P/S\_F6\_IBF1\_LS1 | P/S\_F6\_IBF1\_LS2 |
| P/S\_F6\_IBF2 | P/S\_F6\_IBF2\_LS1 | / |
| P/S/D\_Fc\_IFB1 | P/S/D\_Fc\_IFB1\_LS1 | P/S/D\_Fc\_IFB1\_LS2, P/S/D\_Fc\_IFB1\_LS3, P/S/D\_Fc\_IFB1\_LS4 |
| U/M\_F7\_IFB1 | U/M\_F7\_IFB1\_LS1 | / |
| U/M\_F7\_IFB2 | U/M\_F7\_IFB2\_LS1 | / |
| **LS Descriptions** | | |
| P/S/D\_F1\_IFB1\_LS1/ P/S/D\_F3\_IFB1\_LS1/ P/S/D\_F3\_IFB3\_LS1/ P/S/D\_F4\_IFB1\_LS1/ P/S/D\_F4\_IFB3\_LS1/ P/S\_F5\_IBF1\_LS1/ P/S\_F5\_IBF2\_LS1/ P/S\_F6\_IBF1\_LS1/ P/S\_F6\_IBF2\_LS1/ P/S/D\_Fc\_IFB1\_LS1: The function algorithm is modified to cause corresponding insecure function behaviors. (Function itself)  P/S/D\_F1\_IFB2\_LS1: The malicious software is installed to eavesdrop the plain data. (Function itself)  P/S/D\_F2\_IFB1\_LS1: The data is blocked on links or routed to an unexpected destination. (Env-Links)  P/S/D\_F2\_IFB2\_LS1: The data is eavesdropped or tampered on links. (Env -Links)  P/S/D\_F3\_IFB1\_LS2: The input data is tampered and violates the input requirements. (Env -Function Inputs)  P/S/D\_F3\_IFB1\_LS3/ P/S/D\_F4\_IFB1\_LS3/ P/S\_F5\_IBF1\_LS2/ P/S\_F6\_IBF1\_LS2: The function is bypassed but fake correct outputs. (Env -Calling Behaviors)  P/S/D\_F3\_IFB2\_LS1/ P/S/D\_F4\_IFB2\_LS1: The valid key is replaced by a fake one. (Function itself)  P/S/D\_F4\_IFB1\_LS2: The input data is tampered and cannot be decrypted as expected. (Env -Function Inputs)  P/S/D\_Fc\_IFB1\_LS2: The input data size is modified, which requires more time to compute. (Env -Function Inputs)  P/S/D\_Fc\_IFB1\_LS3: Computing resource is occupied to cause violation of execution timing limitations. (Env -Computing Resources)  P/S/D\_Fc\_IFB1\_LS4: Transmission is slowed down by additional mechanisms on links (e.g. additional switches). (Only for transmit-related functions) (Env -Links)  U/M\_F7\_IFB1\_LS1: The invalid entity obtains the valid data and pretend to be valid. (Function itself)  U/M\_F7\_IFB2\_LS1: The valid entity is fooled intendedly to use invalid or incorrect data. (Function itself) | | |