Annex A. Checklists for Generic Attack Probability Trees

Introduction to checklist:

As stated in 4.1, for simple instruments, for all generic threats with high-level attack vectors that correspond to an acceptable solution or are not applicable, no point score need to be provided for the attack vectors. Instead this checklist can be used. For the generic threats with high-level attack vectors, gereric AtPTs are found in 3.4.1. These correspond to the following checklists.

In the column "Break down threat", an explication is required on how the attack could be performed. Each threat defined shall correspond to a counter measure, which can be either an acceptable solution from Welmec 7.2 or an explanation to why it is not applicable. The Notified Body is later responsible for assessing for every countermeasure that it is acceptable.

Document history

Version: Date: Instrument: Authors and roles:

1.1 Software protection

This point correspond to chapter **3.4.1.1** of this Guide and includes all three child nodes in the AtPT; (Identification, Evidence of an Intervention and Adequate Protection).

1.1.1 Through other software

Threat nr.	Asset nr.	Asset	Countermeasure	Break down threat	Passed / Failed	Remarks
T.1	1	**Legally relevant software**				
T.1.1	**Extension S**	Inadmissible influence **Through other software**				
T.1.1.1	**P2, U2**	**Identification**				
T.1.1.1.1		Availability				
T.1.1.1.2		Integrity				
T.1.1.1.3		Authenticity				
T.1.1.2		**Evidence of an intervention**				
T.1.1.2.1		Availability				
T.1.1.2.2		Integrity				
T.1.1.2.3		Authenticity				
T.1.1.3		**Adequate protection with respect to**				
T.1.1.3.1		Availability				
T.1.1.4		**Combined evaluation (T.1.1.1-T.1.1.3)**				

1.1.2 Through user interface

Threat nr.	Asset nr.	Asset	Countermeasure	Break down threat	Passed / Failed	Remarks
T.1	1	**Legally relevant software**				
T.1.2	**P3, U3**	Inadmissible influence **Through the User Interface**				
T.1.2.1	**P2, U3**	**Identification**				
T.1.2.1.1		Availability				
T.1.2.1.2		Integrity				
T.1.2.1.3		Authenticity				
T.1.2.2		**Evidence of an intervention**				
T.1.2.2.1		Availability				
T.1.2.2.2		Integrity				
T.1.2.2.3		Authenticity				
T.1.2.3		**Adequate protection**				
T.1.2.3.1		Availability				
T.1.2.4		**Combined evaluation (T.1.2.1-T.1.2.3)**				

1.1.3 Through communication interface

1.1.3.1 Directly through the communication interface

Threat nr.	Asset nr.	Asset	Countermeasure	Break down threat	Passed / Failed	Remarks
T.1	1	**Legally relevant software**				
T.1.3	**P4, U4**	Inadmissible influence **Through the communication interface**				
T.1.3.1		Directly through the communication interface				
T.1.3.1.1	**P2, U2**	**Identification**				
T.1.3.1.1.1		Availability				
T.1.3.1.1.2		Integrity				
T.1.3.1.1.3		Authenticity				
T.1.3.1.2		**Evidence of an intervention**				
T.1.3.1.2.1		Availability				
T.1.3.1.2.2		Integrity				
T.1.3.1.2.3		Authenticity				
T.1.3.1.3		**Adequate protection**				
T.1.3.1.3.1		Availability				
T.1.3.1.4		**Combined evaluation (T.1.3.1.1-T.1.3.1.3)**				

1.1.3.2 Through software download

Threat nr.	Asset nr.	Asset	Countermeasure	Break down threat	Passed / Failed	Remarks
T.1	1	**Legally relevant software**				
T.1.3	**P4, U4**	Inadmissible influence **Through the communication interface**				
T.1.3.2	**Extension D**	Through **Software download**				
T.1.3.2.1	**P2, U2**	**Identification**				
T.1.3.2.1.1		Availability				
T.1.3.2.1.2		Integrity				
T.1.3.2.1.3		Authenticity				
T.1.3.2.2		**Evidence of an intervention**				
T.1.3.2.2.1		Availability				
T.1.3.2.2.2		Integrity				
T.1.3.2.2.3		Authenticity				
T.1.3.2.3		**Adequate protection**				
T.1.3.2.3.1		Availability				
T.1.3.2.4		**Combined evaluation (T.1.3.2.1-T.1.3.2.3)**				

1.1.4 Through exchanging hardware

1.1.4.1 Through replacing parts

Threat nr.	Asset nr.	Asset	Countermeasure	Break down threat	Passed / Failed	Remarks
T.1	1	**Legally relevant software**				
T.1.4	**P4, U4**	Inadmissible influence **Through replacing hardware**				
T.1.4.1		By replacing **complete parts**				
T.1.4.1.1	**P2, U2**	**Identification**				
T.1.4.1.1.1		Availability				
T.1.4.1.1.2		Integrity				
T.1.4.1.1.3		Authenticity				
T.1.4.1.2		**Evidence of an intervention**				
T.1.4.1.2.1		Availability				
T.1.4.1.2.2		Integrity				
T.1.4.1.2.3		Authenticity				
T.1.4.1.3		**Adequate protection**				
T.1.4.1.3.1		Availability				
T.1.4.1.4		**Combined evaluation (T.1.4.1.1-T.1.4.1.4)**				

1.1.4.2 Through replacing components

Threat nr.	Asset nr.	Asset	Countermeasure	Break down threat	Passed / Failed	Remarks
T.1	1	**Legally relevant software**				
T.1.4		Inadmissible influence **Through replacing hardware**				
T.1.4.2		By replacing **memory chips**				
T.1.4.2.1	**P2, U2**	**Identification**				
T.1.4.2.1.1		Availability				
T.1.4.2.1.2		Integrity				
T.1.4.2.1.3		Authenticity				
T.1.4.2.2		**Evidence of an intervention**				
T.1.4.2.2.1		Availability				
T.1.4.2.2.2		Integrity				
T.1.4.2.2.3		Authenticity				
T.1.4.2.3		**Adequate protection**				
T.1.4.2.3.1		Availability				
T.1.4.2.4		**Combined evaluation (T.1.4.2.1-T.1.4.2.3)**				

1.2 Parameter protection

This point correspond to chapter **3.4.1.2** of this Guide. (Adequate protection and attack on Evidence of an Intervention are the child nodes).

1.2.1 Through other software

Threat nr.	Asset nr.	Asset	Countermeasure	Break down threat	Passed / Failed	Remarks
T.2	2	**Legally relevant parameters**				
T.2.1	**Extension S**	Inadmissible influence **Through other software**				
T.2.1.1		**Adequate protection with respect to**				
T.2.1.1.1		Availability				
T.2.1.1.2		Integrity				
T.2.1.1.3		Authenticity				
T.2.1.2		**Evidence of an intervention**				Although evidence of an intervention is not required in the case of parameter protection it is a typical form of protection so this needs to be considered when evaluating the integrity of the parameters.
T.2.1.2.1		Availability				
T.2.1.2.2		Integrity				
T.2.1.2.3		Authenticity				
T.2.1.3		**Combined evaluation (T.2.1.1-T.2.1.2)**				

1.2.2 Through user interface

Threat nr.	Asset nr.	Asset	Countermeasure	Break down threat	Passed / Failed	Remarks
T.2	2	**Legally relevant parameters**				
T.2.2	**P3, U3**	Inadmissible influence **Through the User Interface**				
T.2.2.1		**Adequate protection with respect to**				
T.2.2.1.1		Availability				
T.2.2.1.2		Integrity				
T.2.2.1.3		Authenticity				
T.2.2.2		**Evidence of an intervention**				
T.2.2.2.1		Availability				
T.2.2.2.2		Integrity				
T.2.2.2.3		Authenticity				
T.2.2.3		**Combined evaluation (T.2.2.1-T.2.2.2)**				

1.2.3 Through communication interface

1.2.3.1 Directly through the communication interface

Threat nr.	Asset nr.	Asset	Countermeasure	Break down threat	Passed / Failed	Remarks
T.2	2	**Legally relevant parameters**				
T.2.3		Inadmissible influence **Through the communication interface**				
T.2.3.1		Directly through the communication interface				
T.2.3.1.1		**Adequate protection with respect to**				
T.2.3.1.1.1		Availability				
T.2.3.1.1.2		Integrity				
T.2.3.1.1.3		Authenticity				
T.2.3.1.2		**Evidence of an intervention**				
T.2.3.1.2.1		Availability				
T.2.3.1.2.2		Integrity				
T.2.3.1.2.3		Authenticity				
T.2.3.1.3		**Combined evaluation (T.2.3.1.1-T.2.3.1.2)**				

1.2.3.2 Through transmission of parameters

Threat nr.	Asset nr.	Asset	Countermeasure	Break down threat	Passed / Failed	Remarks
T.2	2	**Legally relevant parameters**				
T.2.3		Inadmissible influence **Through the communication interface**				

T.2.3.2	**Extension D**	Through **Transmission of parameters**				
T.2.3.2.1		**Adequate protection with respect to**				
T.2.3.2.1.1		Availability				
T.2.3.2.1.2		Integrity				
T.2.3.2.1.3		Authenticity				
T.2.3.2.2		**Evidence of an intervention**				
T.2.3.2.2.1		Availability				
T.2.3.2.2.2		Integrity				
T.2.3.2.2.3		Authenticity				
T.2.3.2.3		**Combined evaluation (T.2.3.2.1-T.2.3.2.2)**				

1.2.4 Through exchanging hardware

1.2.4.1 By replacing complete parts

Threat nr.	Asset nr.	Asset	Countermeasure	Break down threat	Passed / Failed	Remarks
T.2	2	**Legally relevant parameters**				
T.2.4		Inadmissible influence **Through replacing hardware**				
T.2.4.1		By replacing complete parts				
T.2.4.1.1		**Adequate protection with respect to**				
T.2.4.1.1.1		Availability				
T.2.4.1.1.2		Integrity				
T.2.4.1.1.3		Authenticity				
T.2.4.1.2		**Evidence of an intervention**				
T.2.4.1.2.1		Availability				
T.2.4.1.2.2		Integrity				
T.2.4.1.2.3		Authenticity				
T.2.4.1.3		**Combined evaluation (T.2.4.1.1-T.2.4.1.2)**				

1.2.4.2 Through replacing components

Threat nr.	Asset nr.	Asset	Countermeasure	Break down threat	Passed / Failed	Remarks
T.2	2	**Legally relevant parameters**				
T.2.4		Inadmissible influence **Through replacing hardware**				
T.2.4.2		**By replacing memory chips**				
T.2.4.2.1		**Adequate protection with respect to**				
T.2.4.2.1		Availability				
T.2.4.2.1.2		Integrity				
T.2.4.2.1.3		Authenticity				

T.2.4.2.2		**Evidence of an intervention**				
T.2.4.2.2.1		Availability				
T.2.4.2.2.2		Integrity				
T.2.4.2.2.3		Authenticity				
T.2.4.2.3		**Combined evaluation (T.2.4.2.1-T.2.4.2.2)**				

1.3 Protection of measurement results during processing

This point correspond to chapter **3.4.1.3** of this Guide. (Adequate protection is the only child node).

1.3.1 Through other software

Threat nr.	Asset nr.	Asset	Countermeasure	Break down threat	Passed / Failed	Remarks
T.3	3	**Measurement result relevant data**				
T.3.1		Inadmissible influence **Through other software**				
T.3.1.1		**Adequate protection with respect to**				
T.3.1.1.1		Availability				
T.3.1.1.2		Integrity				
T.3.1.1.3		Authenticity				

1.3.2 Through user interface

Threat nr.	Asset nr.	Asset	Countermeasure	Break down threat	Passed / Failed	Remarks
T.3	3	**Measurement result relevant data**				
T.3.2		Inadmissible influence **Through the User Interface**				
T.3.2.1		**Adequate protection with respect to**				
T.3.2.1.1		Availability				
T.3.2.1.2		Integrity				
T.3.2.1.3		Authenticity				

1.3.3 Through communication interface

1.3.3.1 Directly through the communication interface

Threat nr.	Asset nr.	Asset	Countermeasure	Break down threat	Passed / Failed	Remarks
T.3	3	**Measurement result relevant data**				
T.3.3		Inadmissible influence **Through the communication interface**				
T.3.3.1		Directly through the communication interface				

T.3.3.1.1		**Adequate protection with respect to**				
T.3.3.1.1.1		Availability				
T.3.3.1.1.2		Integrity				
T.3.3.1.1.3		Authenticity				

1.3.3.2 Through transmission of results

Threat nr.	Asset nr.	Asset	Countermeasure	Break down threat	Passed / Failed	Remarks
T.3	3	**Measurement result relevant data**				
T.3.3		Inadmissible influence **Through the communication interface**				
T.3.3.2		Through **Transmission of measurement results**				
T.3.3.2.1		**Adequate protection with respect to**				
T.3.3.2.1.1		Availability				
T.3.3.2.1.2		Integrity				
T.3.3.2.1.3		Authenticity				

1.3.4 Through exchanging hardware

1.3.4.1 By replacing complete parts

Threat nr.	Asset nr.	Asset	Countermeasure	Break down threat	Passed / Failed	Remarks
T.3	3	**Measurement result relevant data**				
T.3.4		Inadmissible influence **Through replacing hardware**				
T.3.4.1		By replacing complete parts				
T.3.4.1.1		**Adequate protection with respect to**				
T.3.4.1.1.1		Availability				
T.3.4.1.1.2		Integrity				
T.3.4.1.1.3		Authenticity				

1.3.4.2 Through replacing components

Threat nr.	Asset nr.	Asset	Countermeasure	Break down threat	Passed / Failed	Remarks
T.3	3	**Measurement result relevant data**				
T.3.4		Inadmissible influence **Through replacing hardware**				
T.3.4.2		By replacing memory chips				
T.3.4.2.1		**Adequate protection with respect to**				
T.3.4.2.1.1		Availability				
T.3.4.2.1.2		Integrity				
T.3.4.2.1.3		Authenticity				

1.4 Protection of stored measurement result

This point correspond to chapter **3.4.1.4** of this Guide.

1.4.1 Through other software

Threat nr.	Asset nr.	Asset	Countermeasure	Break down threat	Passed / Failed	Remarks
T.4	4	**Stored measurement result**				
T.4.1		Inadmissible influence **Through other software**				
T.4.1.1		**Adequate protection with respect to**				
T.4.1.1.1		Availability				
T.4.1.1.2		Integrity				
T.2.4.1.1.3		Authenticity				
T.4.1.2		**Evidence of an intervention**				
T.4.1.2.1		Availability				
T.4.1.2.2		Integrity				
T.4.1.2.3		Authenticity				
T.4.1.3		**Combined evaluation (T.4.2.1-T.4.2.2)**				

1.4.2 Through user interface

Threat nr.	Asset nr.	Asset	Countermeasure	Break down threat	Passed / Failed	Remarks
T.4	4	**Stored measurement result**				
T.4.2		Inadmissible influence **Through the User Interface**				
T.4.2.1		**Adequate protection with respect to**				
T.4.2.1.1		Availability				
T.4.2.1.2		Integrity				
T.4.2.1.3		Authenticity				
T.4.2.2		**Evidence of an intervention**				
T.4.2.2.1		Availability				
T.4.2.2.2		Integrity				
T.4.2.2.3		Authenticity				
T.4.2.3		**Combined evaluation (T.4.2.1-T.4.2.2)**				

1.4.3 Through communication interface

1.4.3.1 Directly through the communication interface

Threat nr.	Asset nr.	Asset	Countermeasure	Break down threat	Passed / Failed	Remarks
T.4	4	**Stored measurement result**				
T.4.3		Inadmissible influence **Through the communication interface**				
T.4.3.1		Directly through the communication interface				
T.4.3.1.1		**Adequate protection with respect to**				
T.4.3.1.1.1		Availability				
T.4.3.1.1.2		Integrity				
T.4.3.1.1.3		Authenticity				
T.4.3.1.2		**Evidence of an intervention**				
T.4.3.1.2.1		Availability				
T.4.3.1.2.2		Integrity				
T.4.3.1.2.3		Authenticity				
T.4.3.1.3		**Combined evaluation (T.4.3.1.1-T.4.3.1.2)**				

1.4.3.2 Through transmission of measurement results

Threat nr.	Asset nr.	Asset	Countermeasure	Break down threat	Passed / Failed	Remarks
T.4	4	**Stored measurement result**				
T.4.3		Inadmissible influence **Through the communication interface**				
T.4.3.2		Through **Transmission of measurement results**				
T.4.3.2.1		**Adequate protection with respect to**				
T.4.3.2.1.1		Availability				
T.4.3.2.1.2		Integrity				
T.4.3.2.1.3		Authenticity				
T.4.3.2.2		**Evidence of an intervention**				
T.4.3.2.2.1		Availability				
T.4.3.2.2.2		Integrity				
T.4.3.2.2.3		Authenticity				
T.4.3.2.3		**Combined evaluation (T.4.3.2.1-T.4.3.2.2)**				

1.4.4 Through exchanging hardware

1.4.4.1 By replacing complete parts

Threat nr.	Asset nr.	Asset	Countermeasure	Break down threat	Passed / Failed	Remarks
T.4	4	**Stored measurement result**				
T.4.4		Inadmissible influence **Through replacing hardware**				
T.4.4.1		By replacing complete parts				
T.4.4.1.1		**Adequate protection with respect to**				
T.4.4.1.1.1		Availability				
T.4.4.1.1.2		Integrity				
T.4.4.1.1.3		Authenticity				
T.4.4.1.2		**Evidence of an intervention**				
T.4.4.1.2.1		Availability				
T.4.4.1.2.2		Integrity				
T.4.4.1.2.3		Authenticity				
T.4.4.1.3		**Combined evaluation (T.4.4.1.1-T.4.4.1.2)**				

1.4.4.2 Through replacing components

Threat nr.	Asset nr.	Asset	Countermeasure	Break down threat	Passed / Failed	Remarks
T.4	4	**Stored measurement result**				
T.4.4		Inadmissible influence **Through replacing hardware**				
T.4.4.2		**By replacing memory chips**				
T.4.4.2.1		**Adequate protection with respect to**				
T.4.4.2.1.1		Availability				
T.4.4.2.1.2		Integrity				
T.4.4.2.1.3		Authenticity				
T.4.4.2.2		**Evidence of an intervention**				
T.4.4.2.2.1		Availability				
T.4.4.2.2.2		Integrity				
T.4.4.2.2.3		Authenticity				
T.4.4.2.3		**Combined evaluation (T.4.4.2.1-T.4.4.2.2)**				

1.5 Protection of indication of the measurement result

This point correspond to chapter **3.4.1.5** of this Guide. (Adequate protection is the only child node).

1.5.1 Through other software

Threat nr.	Asset nr.	Asset	Countermeasure	Break down threat	Passed / Failed	Remarks
T.5	5	**Indication**				
T.5.1		Inadmissible influence **Through other software**				
T.5.1.1		**Adequate protection with respect to**				
T.5.1.1.1		Availability				
T.5.1.1.2		Integrity				
T.5.1.1.3		Authenticity				

1.5.2 Through user interface

Threat nr.	Asset nr.	Asset	Countermeasure	Break down threat	Passed / Failed	Remarks
T.5	5	**Indication**				
T.5.2		Inadmissible influence **Through the User Interface**				
T.5.2.1		**Adequate protection with respect to**				
T.5.2.1.1		Availability				
T.5.2.1.2		Integrity				
T.5.2.1.3		Authenticity				

1.5.3 Through communication interface

1.5.3.1 Directly through the communication interface

Threat nr.	Asset nr.	Asset	Countermeasure	Break down threat	Passed / Failed	Remarks
T.5	5	**Indication**				
T.5.3		Inadmissible influence **Through the communication interface**				
T.5.3.1		Directly through the communication interface				
T.5.3.1.1		**Adequate protection with respect to**				
T.5.3.1.1.1		Availability				
T.5.3.1.1.2		Integrity				
T.5.3.1.1.3		Authenticity				

1.5.3.2 Through transmission of indication values

Threat nr.	Asset nr.	Asset	Countermeasure	Break down threat	Passed / Failed	Remarks
T.5	5	**Indication**				
T.5.3		Inadmissible influence **Through the communication interface**				
T.5.3.2		Through **Transmission of measurement results**				
T.5.3.2.1		**Adequate protection with respect to**				
T.5.3.2.1.1		Availability				
T.5.3.2.1.2		Integrity				
T.5.3.2.1.3		Authenticity				

1.5.4 Through exchanging hardware

1.5.4.1 By replacing complete parts

Threat nr.	Asset nr.	Asset	Countermeasure	Break down threat	Passed / Failed	Remarks
T.5	5	**Indication**				
T.5.4		Inadmissible influence **Through replacing hardware**				
T.5.4.1		By replacing complete parts				
T.5.4.1.1		**Adequate protection with respect to**				
T.5.4.1.1.1		Availability				
T.5.4.1.1.2		Integrity				
T.5.4.1.1.3		Authenticity				

1.5.4.2 Through replacing components

Threat nr.	Asset nr.	Asset	Countermeasure	Break down threat	Passed / Failed	Remarks
T.5	5	**Indication**				
T.5.4		Inadmissible influence **Through replacing hardware**				
T.5.4.2		**By replacing memory chips**				
T.5.4.2.1		**Adequate protection with respect to**				
T.5.4.2.1.1		Availability				
T.5.4.2.1.2		Integrity				
T.5.4.2.1.3		Authenticity				