| **STN** | **Elektronické systémy pre byty a budovy (HBES) Časť 3-4: Zabezpečenie na aplikačnej vrstve, servis zabezpečenia, konfigurácia zabezpečenia a bezpečnostné zdroje Oprava AC** | **STN EN 50090-3-4/AC** |
| | | 36 8051 |

Home and Building Electronic Systems (HBES) - Part 3-4: Secure Application Layer, Secure Service, Secure configuration and security Resources

Táto norma obsahuje anglickú verziu európskej normy.
This standard includes the English version of the European Standard.

Táto norma bola oznámená vo Vestníku ÚNMS SR č. 09/18

Obsahuje: EN 50090-3-4:2017/AC May:2018

127211

CENELEC

Corrigendum to EN 50090-3-4:2017

English version

_____

In 5.1.1.2.1.2, insert the following missing figures and tables:

Figure 12

b_7	b_6	b_5	b_4	b_3	b_2	b_1	b_0	Algorithm	Service	Authentication	Confidentiality
T	SAI			SBC	S-AL service						
	0	0	0		0	0	0	CCM	S-A_Data-PDU	yes	no
	0	0	1		0	0	0	CCM	S-A_Data-PDU	yes	yes
	0	0	1		0	1	0	CCM	S-A_Sync_Req-PDU	yes	yes
	0	0	1		0	1	1	CCM	S-A_Sync_Res-PDU	yes	yes

Figure 13

b_5	Tool Access
0	Not using the specific tool entry
1	Using the specific tool entry

Table 2

b_6	b_5	b_4	Security algorithm and operation mode
0	0	0	CCM (AES CTR for confidentiality and AES CBC for authentication) with authentication only.
0	0	1	CCM with authentication and confidentiality

Table 3

SBC	Name	Definition
0	by service	The communication mode is defined by the used Transport Layer service.
1	system broadcast	The communication mode shall be System Broadcast.

_____

May 2018