

CWEs Mapped to Security Verification Section of Aker Paper

Count	CWE	IP Level	Firmware Level	System Level
1	CWE-276: Incorrect Default Permissions		~	~
2	CWE-441: Unintended Proxy or Intermediary ('Confused Deputy')			X
3	CWE-1189: Improper Isolation of Shared Resources on System-on-Chip (SoC)			X
4	CWE-1191: Exposed Chip Debug and Test Interface With Insufficient or Missing Authorization		~	~
5	CWE-1193: Power-On of Untrusted Execution Core Before Enabling Fabric Access Control		~	~
6	CWE-1220: Insufficient Granularity of Access Control	X	X	X
7	CWE-1221: Incorrect Register Defaults or Module Parameters	X	X	X
8	CWE-1243: Sensitive Non-Volatile Information Not Protected During Debug			
9	CWE-1244: Improper Access to Sensitive Information Using Debug and Test Interfaces	X	X	X
10	CWE-1257: Improper Access Control Applied to Mirrored or Aliased Memory Regions			
11	CWE-1258: Exposure of Sensitive System Information Due to Uncleared Debug Information	X	X	X
12	CWE-1259: Improper Restriction of Security Token Assignment	X	X	X
13	CWE-1260: Improper Handling of Overlap Between Protected Memory Ranges			X
14	CWE-1262: Register Interface Allows Software Access to Sensitive Data or Security Settings		X	X
15	CWE-1264: Hardware Logic with Insecure De-Synchronization between Control and Data Channels	X	X	X
16	CWE-1266: Improper Scrubbing of Sensitive Data from Decommissioned Device	X	X	X
17	CWE-1267: Policy Uses Obsolete Encoding	X	X	X

18	CWE-1268: Policy Privileges are not Assigned Consistently Between Control and Data Agents	X	X	X
19	CWE-1269: Product Released in Non-Release Configuration	X	X	X
20	CWE-1270: Generation of Incorrect Security Tokens	X	X	X
21	CWE-1271: Uninitialized Value on Reset for Registers Holding Security Settings	X	X	X
22	CWE-1272: Sensitive Information Uncleared Before Debug/Power State Transition	X	X	X
23	CWE-1273: Device Unlock Credential Sharing			
24	CWE-1274: Insufficient Protections on the Volatile Memory Containing Boot Code	X	X	X
25	CWE-1280: Access Control Check Implemented After Asset is Accessed	X	X	X
26	CWE-1282: Assumed-Immutable Data is Stored in Writable Memory	X		
27	CWE-1283: Mutable Attestation or Measurement Reporting Data		X	X
28	CWE-1290: Incorrect Decoding of Security Identifiers		X	X
29	CWE-1292: Incorrect Conversion of Security Identifiers		X	X
30	CWE-1326: Missing Immutable Root of Trust in Hardware	X		

Aker Security Property Templates and Relevant CWE Mappings

SP ID	Related CWEs	SP Requirement	SP Specification Template	SP Type	Total SPs After Expanding	Verification Level
01	1258, 1266, 1270, 1271, 1272, 1280	C cannot receive data from P which originates while the ACW is actively being reset.	//# of Generic Signals to Replace = 2 SP01_RECEIVE_GENERIC: assert iflow(`signal_from_P` when (ARESETN == 0) ==> `signal_to_C`);	IFT	11	IP
02	1258, 1266, 1270, 1271, 1272, 1280	C cannot send data to P which originates while the ACW is actively being reset.	//# of Generic Signals to Replace = 2 SP02_SEND_GENERIC: assert iflow(`signal_from_C` when (ARESETN == 0) ==> `signal_to_P`);	IFT	27	IP
03	1221, 1258, 1266, 1269, 1271, 1280	C receives the default AXI signals while the ACW is actively being reset.	//# of Generic Signals to Replace = 2 SP03_DEFAULT_GENERIC: assert iflow(`signal_to_C` == `default_AXI_value` unless (ARESETN != 0));	Trace	11	IP
04	1221, 1258, 1266, 1269, 1271, 1280	The ACW outputs the default AXI signals to P while the ACW is actively being reset.	//# of Generic Signals to Replace = 2 SP04_DEFAULT_GENERIC: assert iflow(`signal_to_P` == `default_AXI_value` unless (ARESETN != 0));	Trace	27	IP
05	1221, 1258, 1259, 1266, 1267, 1269, 1271, 1274, 1280, 1282	The configuration/anomaly registers are cleared and set to contain the default values while the ACW is actively being reset.	//# of Generic Signals to Replace = 2 SP05_DEFAULT_GENERIC: assert iflow(`reg` == `default_value` unless (ARESETN != 0 && `acw_w/r_state` != 2'b00));	Trace	38	IP
06	1269, 1272, 1280	The TE can read from but not write to anomaly registers.	//# of Generic Signals to Replace = 3	IFT	4	Firmware

			<pre> SP06_RONLY_GENERIC: assert iflow(`signal_from_TE` when (S_AXI_CTRL_AWADDR == `reg_addr`) ==> `anomaly_reg`); </pre>			
07	1258, 1270, 1272, 1280	C cannot receive data from P which originates while the ACW is in reset mode.	<pre> //# of Generic Signals to Replace = 3 SP07_RECEIVE_GENERIC: assert iflow(`signal_from_P` when (`acw_w/r_state` == 2'b00) ==> `signal_to_C`); </pre>	IFT	11	IP
08	1258, 1270, 1272, 1280	C cannot send data to P which originates while the ACW is in reset mode.	<pre> //# of Generic Signals to Replace = 3 SP08_SEND_GENERIC: assert iflow(`signal_from_C` when (`acw_w/r_state` == 2'b00) ==> `signal_to_P`); </pre>	IFT	27	IP
09	1221, 1258, 1269, 1272, 1280	C receives the default AXI signals while the ACW is in reset mode.	<pre> //# of Generic Signals to Replace = 3 SP09_DEFAULT_GENERIC: assert iflow(`signal_to_C` == `default_AXI_value` unless (`acw_w/r_state` != 2'b00)); </pre>	Trace	11	IP
10	1221, 1258, 1269, 1272, 1280	The ACW outputs the default AXI signals to P while the ACW is in reset mode.	<pre> //# of Generic Signals to Replace = 3 SP10_DEFAULT_GENERIC: assert iflow(`signal_to_P` == `default_AXI_value` unless (`acw_w/r_state` != 2'b00)); </pre>	Trace	27	IP
11	1221, 1258, 1259, 1267, 1269, 1271, 1272, 1274, 1280, 1282	The configuration/anomaly registers contain the default values until they are modified by the TE (config.) and/or ACW (illegal req. metadata tracking).	<pre> //# of Generic Signals to Replace = 3 SP11_DEFAULT_GENERIC: assert iflow(`unauthorized_signal` when (`reg` == `default_value`) ==> </pre>	IFT	8,768 (all 231 unauthorized sigs) 2,876 (76 non-acw sigs) 1,432 (38 sigs from C)	Firmware

			<code>`reg` unless (`reg` == `default_value`));</code>			
12	1270, 1272, 1280	C cannot receive data associated with an illegal address from P which originates while the ACW is in supervising mode.	<code>/// # of Generic Signals to Replace = 4 SP12_RECEIVE_GENERIC: assert iflow(`signal_from_P` when (`acw_w/r_state` == 2'b01) && (`AR/AW_ADDR_VALID_FLAG` == 0) ==> `signal_to_C`);</code>	IFT	11	IP
13	1270, 1272, 1280	C cannot send data associated with an illegal address to P which originates while the ACW is in supervising mode.	<code>/// # of Generic Signals to Replace = 4 SP13_SEND_GENERIC: assert iflow(`signal_from_C` when (`acw_w/r_state` == 2'b01) && (`AR/AW_ADDR_VALID_FLAG` == 0) ==> `signal_to_P`);</code>	IFT	27	IP
14	1270, 1272, 1280	C cannot receive data from P which originates while the ACW is in decouple mode.	<code>/// # of Generic Signals to Replace = 3 SP14_RECEIVE_GENERIC: assert iflow(`signal_from_P` when (`acw_w/r_state` == 2'b10) ==> `signal_to_C`);</code>	IFT	11	IP
15	1270, 1272, 1280	C cannot send data to P which originates while the ACW is in decouple mode.	<code>/// # of Generic Signals to Replace = 3 SP15_SEND_GENERIC: assert iflow(`signal_from_C` when (`acw_w/r_state` == 2'b10) ==> `signal_to_P`);</code>	IFT	27	IP
16	1221, 1269, 1272, 1280	C receives the default AXI signals while the ACW is in decouple mode.	<code>/// # of Generic Signals to Replace = 3 SP16_DEFAULT_GENERIC: assert iflow(`signal_to_C` == `default_AXI_value`</code>	Trace	11	IP

			unless (`acw_w/r_state` != 2'b10));			
17	1221, 1269, 1272, 1280	The ACW outputs the default AXI signals to the P while the ACW is in decouple mode.	//# of Generic Signals to Replace = 3 SP17_DEFAULT_GENERIC: assert iflow(`signal_to_P` == `default_AXI_value` unless (`acw_w/r_state` != 2'b10));	Trace	27	IP
18	1272, 1280, 1283	The anomaly registers are updated with illegal request metadata after the ACW detects an illegal request.	//# of Generic Signals to Replace = 3 SP18_DEFAULT_GENERIC: assert iflow(`authorized_signal` when (`acw_w/r_state` == 2'b01) ==> `anomaly_reg` unless (`acw_w/r_state` == 2'b10));	IFT	12	IP
19	1221, 1272, 1280	An interrupt to TE is generated after the ACW detects an illegal request.	//# of Generic Signals to Replace = 2 SP19_INTERRUPT_GENERIC: assert iflow(`INTR_LINE_W/R` == 1 unless (`acw_w/r_state` != 2'b10));	Trace	2	Firmware
20	441, 1189, 1260	Any C cannot receive data from any region not contained within its ACW's LACP.	//# of Generic Signals to Replace = 2 SP20_RECEIVE_GENERIC: assert iflow(`unauthorized` ==> `sig_to_C`);	IFT	22	System
21	441, 1189, 1260	Any C cannot send data to any region not contained within its ACW's LACP.	//# of Generic Signals to Replace = 2 SP21_SEND_GENERIC: assert iflow(`sig_from_C` ==> `unauthorized`);	IFT	54	System