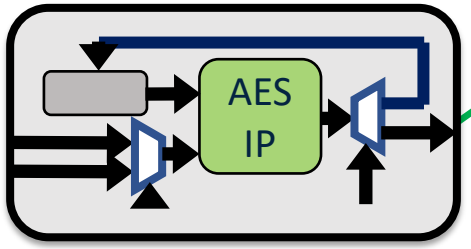
SA-EDI Use case: Find CWEs related to Asset

- Determine which CWEs are related to asset
  - Use information in Asset Definition Data Object
  - Create Element Data Object, requires Weakness Reference

Asset Definition	
Name	user_key
Description	Keys for AES
Family	Security
Type	Cryptographic
Database_ID	CWE



RTL Design

EDA Tool

Element	
Asset Name	user_key
Direction	input
Weakness Reference	???
Ports	clk, reset, Mode, Valid_In, Key_or_Data, Encrypted_Data, Encrypted_Key

Example: Use SA-EDI Family to find CWEs

- The table lists SA-EDI “Family” attribute values
- Use “Family” to query CWE fields: “Applicable Platforms | Technologies | Class “
  - Audio/Video, Clock/Counter, Communications, Controllers, Memories, Microcontroller, Network-on-Chip, Processors, Security, Test/Debug, Interface IP, Bus IP, Analog & Mixed-Signal IP, Management, Sensors

#	Name	Definition	Examples
1	Accelerator	IP dedicated to offload a specific workload to enhance performance	DSP, TPU, packet processing, mathematical, compression
2	Analog & Mixed-Signal	IP that controls or senses the electricals for communication, which receives or transmits signals conditioned outside of a system’s digital domain	PHY, ADC, DAC
3	Audio/Video	IP designed to manipulate audio/video data	Coders/Decoders, speech recognition, format converters
4	Bus/Interface	IP implementing an interconnect among elements in a computing system	I2C, PCIe, DDR, MMC, USB, GPIO
5	Communications	IP designed to transmit/receive information	Modulator/Demodulator, 802.11, Bluetooth, CDMA/GSM
6	Controllers	A circuit hard-wired (e.g. Finite State Machine) to react in a closed-loop control system or other limited context, to control another entity	Arbiter, APIC, USB, Peripheral, Memory, Storage
7	Counter/Timer	IP reflecting the passage of time in oscillations or human units	Real Time Clock, Watchdog, Monotonic Counter
8	Memories	Volatile (transient) data storage	DRAM, SRAM
9	Microcontroller	A specialized processor acting as a programmable controller	8051, Nios
10	Power Management	IP which controls and/or monitors the power state of a system	Voltage regulators, power controllers or monitors
11	Processors	A programmable computing engine	CPU, GPU, TPU
12	Security	IP designed to protect assets	Cryptography, authorization, tamper detection, access controls, RNG
13	Storage	non-volatile (permanent) data storage	EEPROM, eFuse, flash, ROM, OTP, NVRAM
14	Test/Debug	IP designed to verify functionality and identify root cause of defects	JTAG, BIST, boundary scan, pattern generator
15	Transducers	IP which converts energy from one form to another, such as physical to electrical	sensors, actuators
16	<User Defined>	This type is used to accommodate families that have not been defined in this table (e.g. proprietary IP). To add a family, the value should have the prefix “UD:”.	UD: *CustomIP*

Database Queries

- Return all matching database entries for query, all fields of CWEs
- Query Architectures?, match SA-EDI Family?
- Query Name, Description, Extended Description
  - Match SA-EDI Type?
  - Is this three calls or one API call?
- Search for specified keyword(s) in Description and Extended Description fields.
  - Require all keywords if multiple are given e.g. search for “key” and “boot” in Description.

Use case: Select from list of all HW CWEs

- Tool has pull down menu of all HW CWEs and user selects CWE entries that are relevant for a specific security requirement
- The tool will use the API to get an up to date list of CWE number and description
- The tool may keep a cached list and call the API to update it at a regular interval or when the user searches the list
- Know what version is used and which is the latest
- Get only HW, SW or all CWEs for example