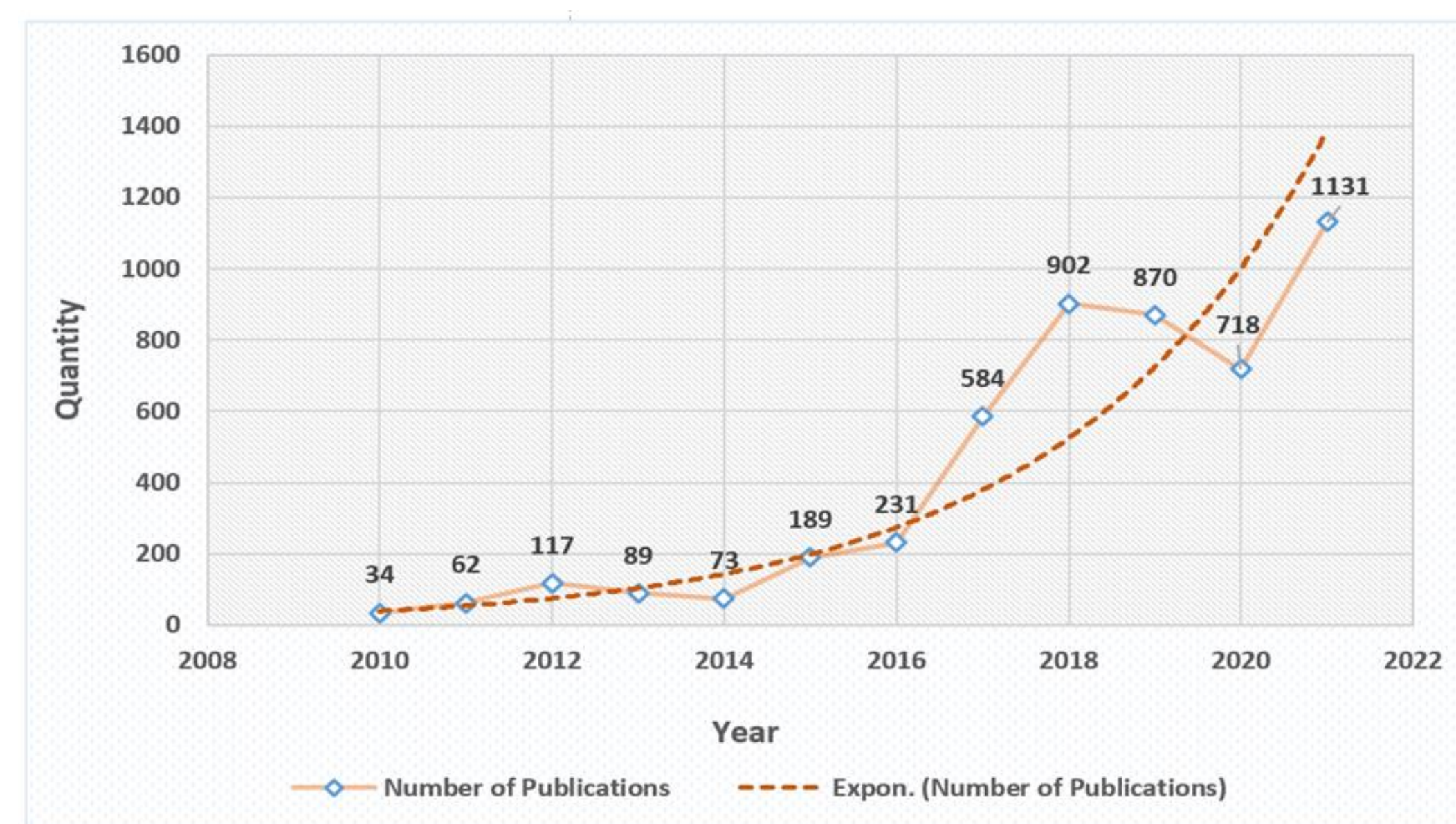
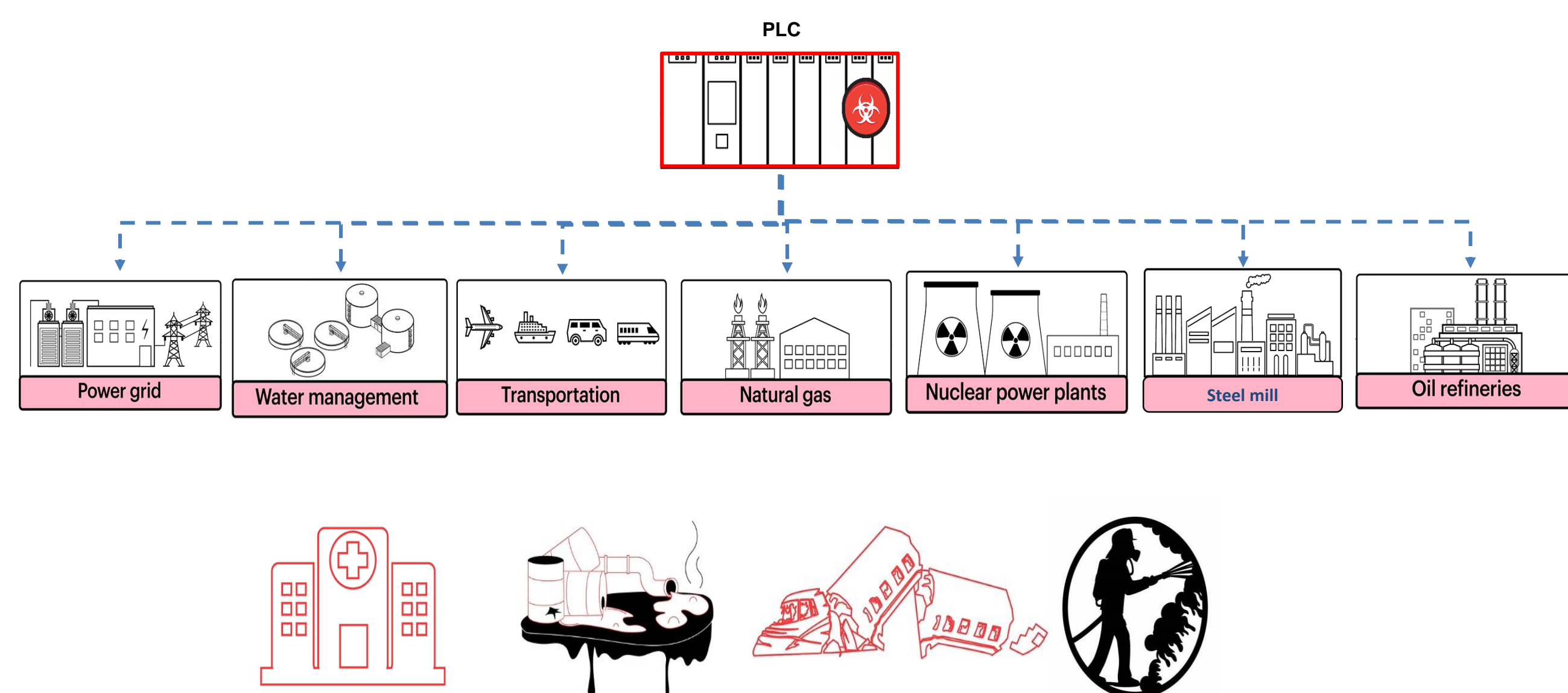


Problem Statement

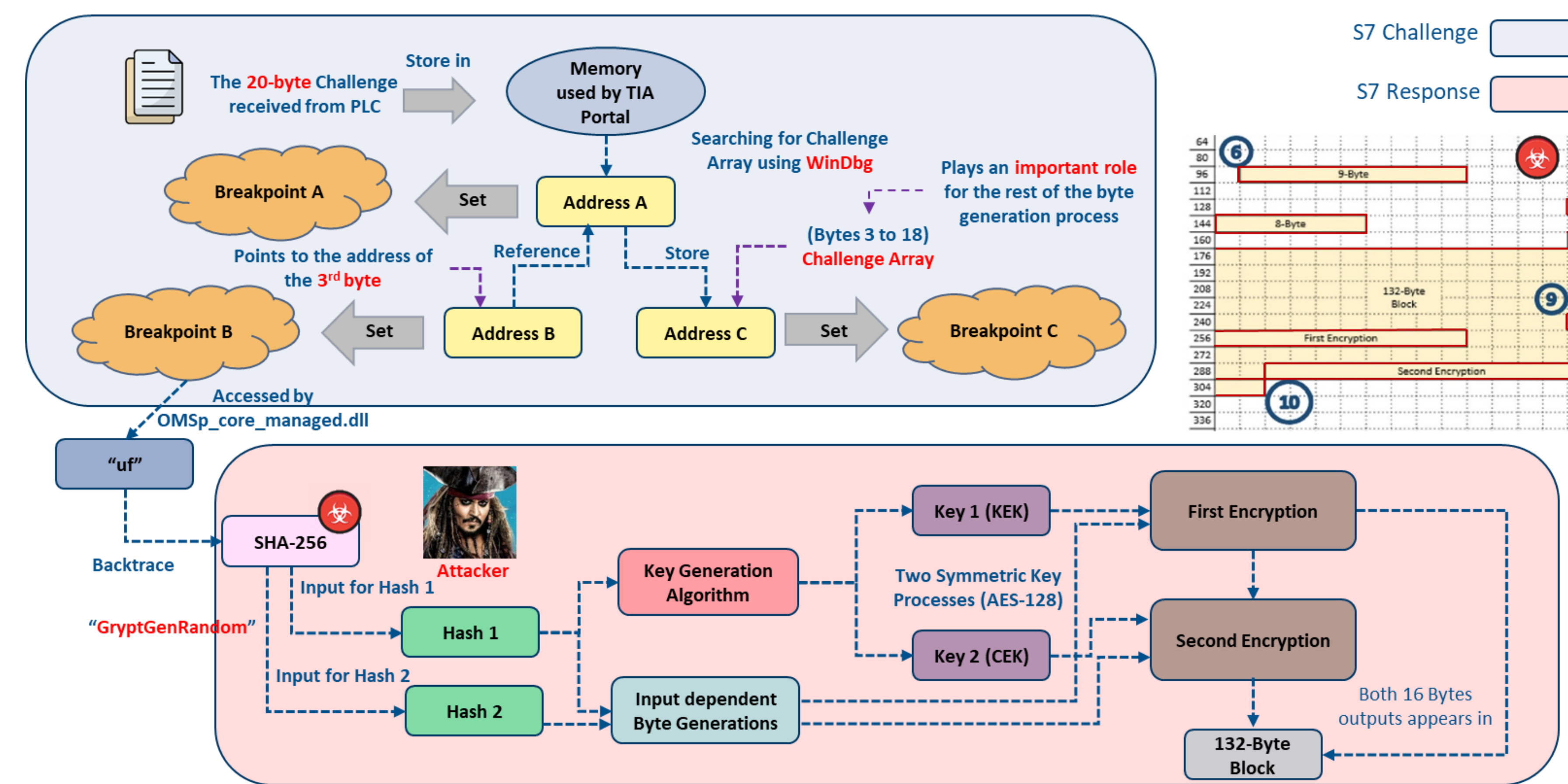


↑ Fig 1. The number of Attacks reported in scientific papers per year

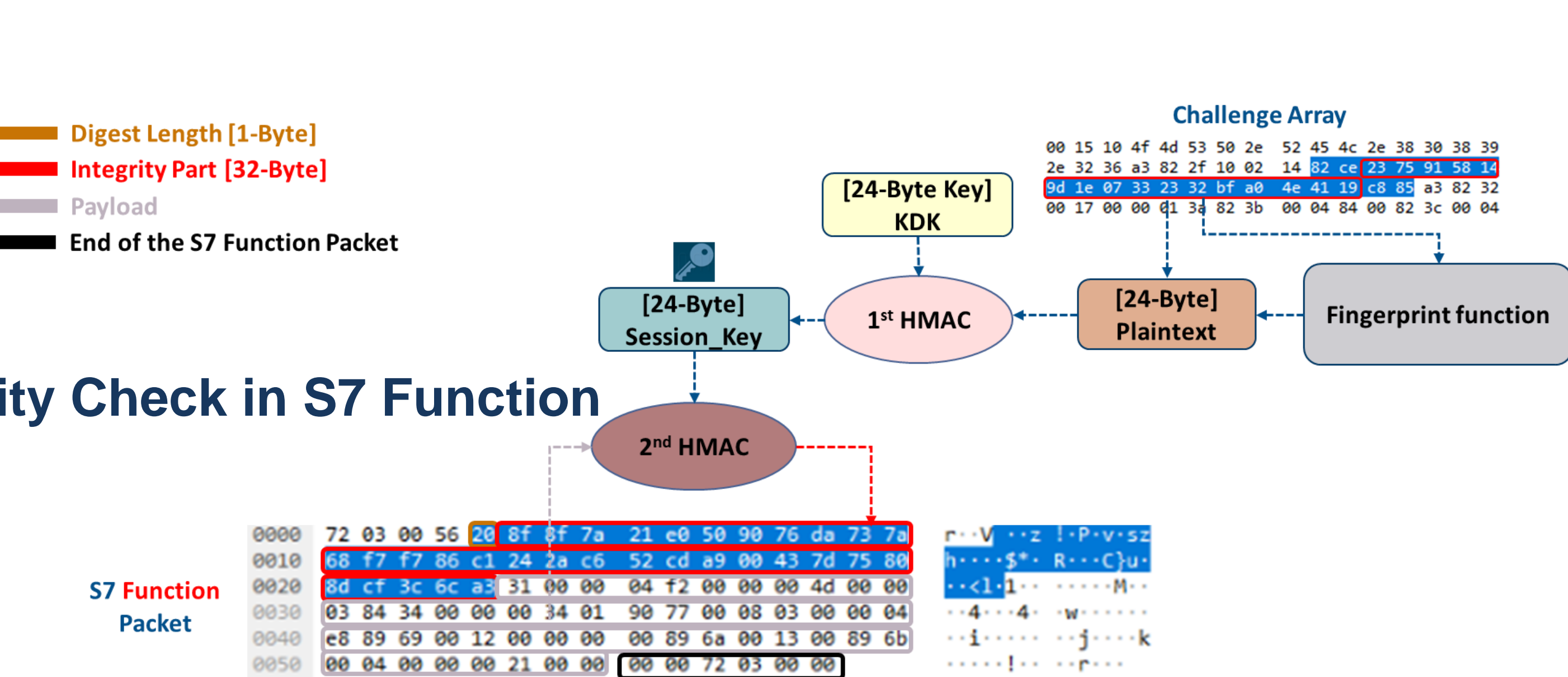
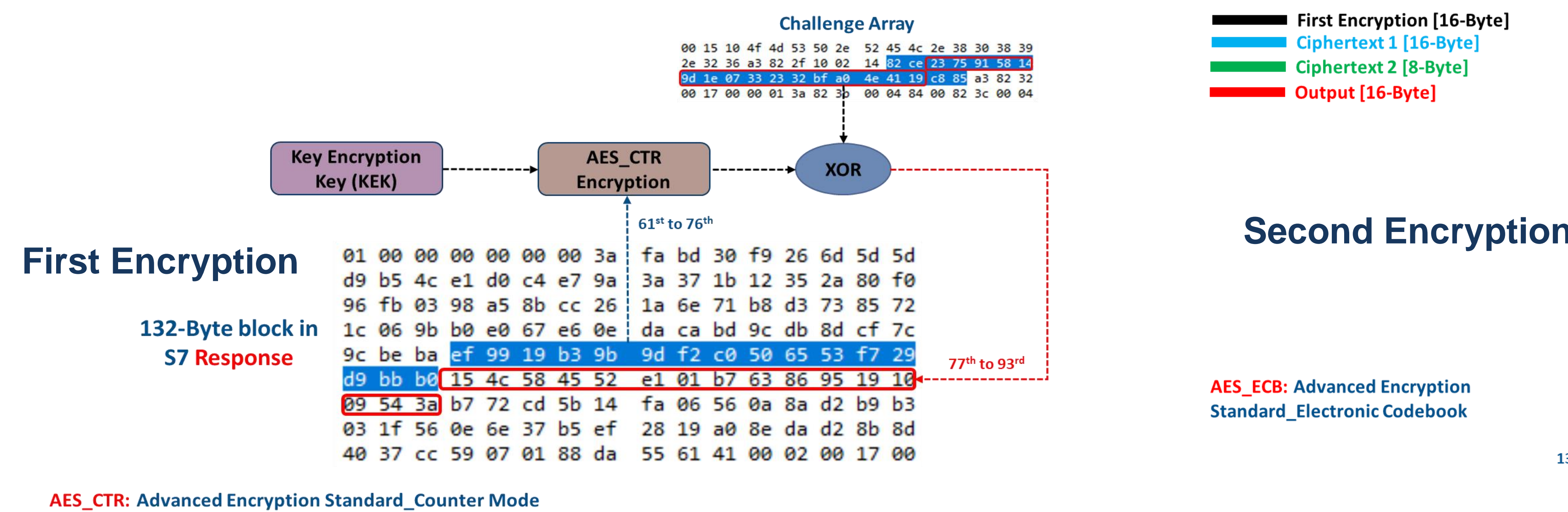
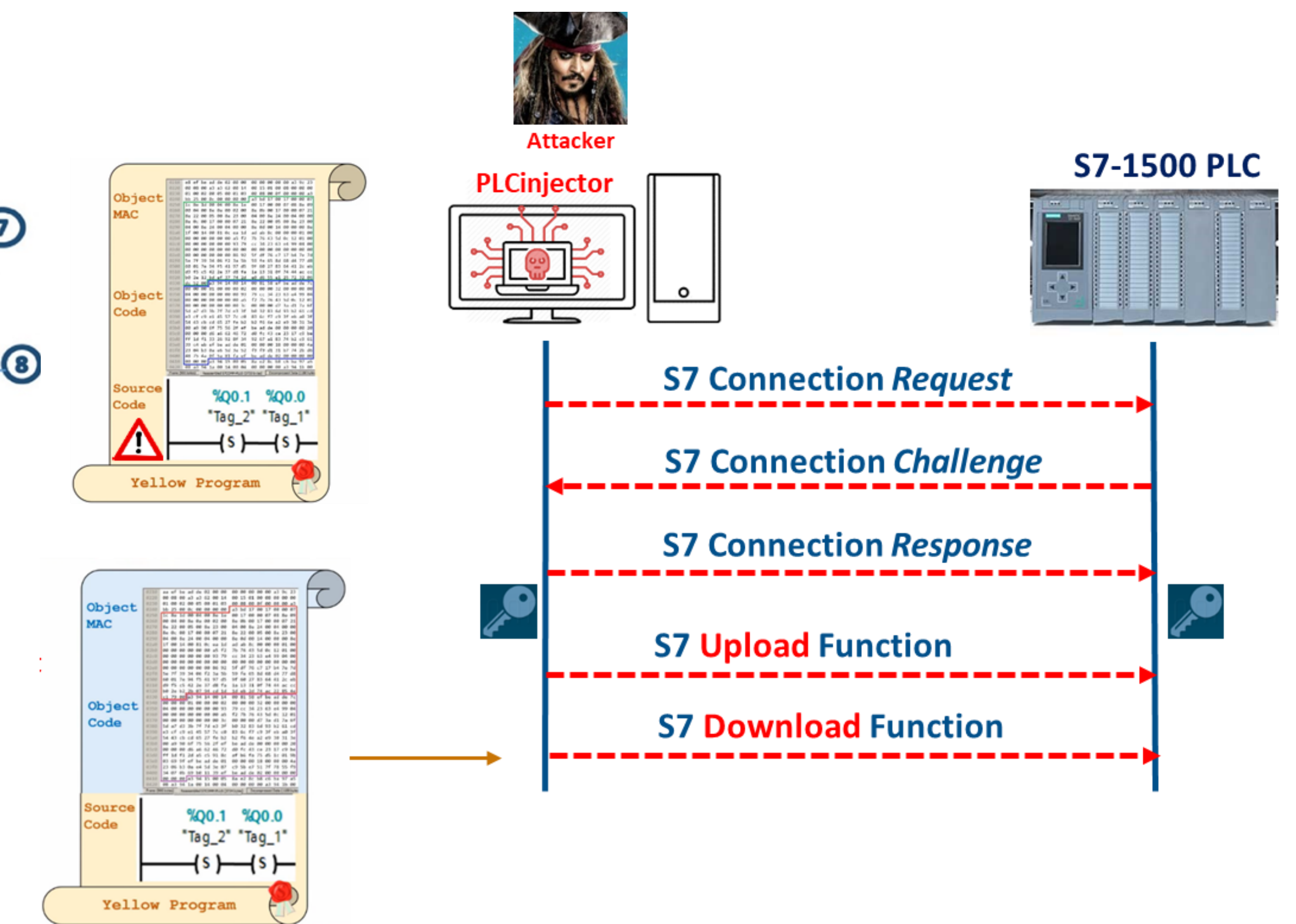
Protocol	Port	Censys	Shodan	ZoomEye	Ditetecting
Modbus	502/TCP	35,018	61,902	31,706	14,173
Siemens S7	102/TCP	6,804	56,010	40,099	2464
DNP3	20000/TCP	597	962,297	14,750,352	367
BACnet	47808/TCP	15,514	31,157	56,767	11,750
Niagara Fox	1911/TCP	25,398	80,902	262,111	26,634
Ethernet/IP	44818/TCP	Not Available	65,402	27,637	1971
Phonix/PCWorx	1962/TCP	Not Available	48,924	316,365	168
Codesys	2455/TCP	Not Available	37,099	241,809	1298

↑ Table 1. The number of Internet-accessible PLCs on March 22, 2023

S7CommPlusV3 Vulnerabilities Analysis



Attack Scenario



Evaluation

