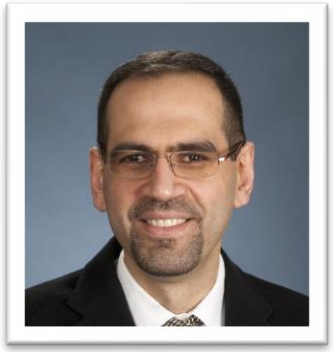
Hardware Assurance Survey

August 2021

All Rights Reserved

Contributors

Dr. Mark Tehranipoor



Dr. Waleed Khalil

Dr. Navid Asadi

Dr. Nima Maghari

Dr. Farimah Farahmandi

Dr. Eslam Tawfik

All Rights Reserved

Participants

Participants:

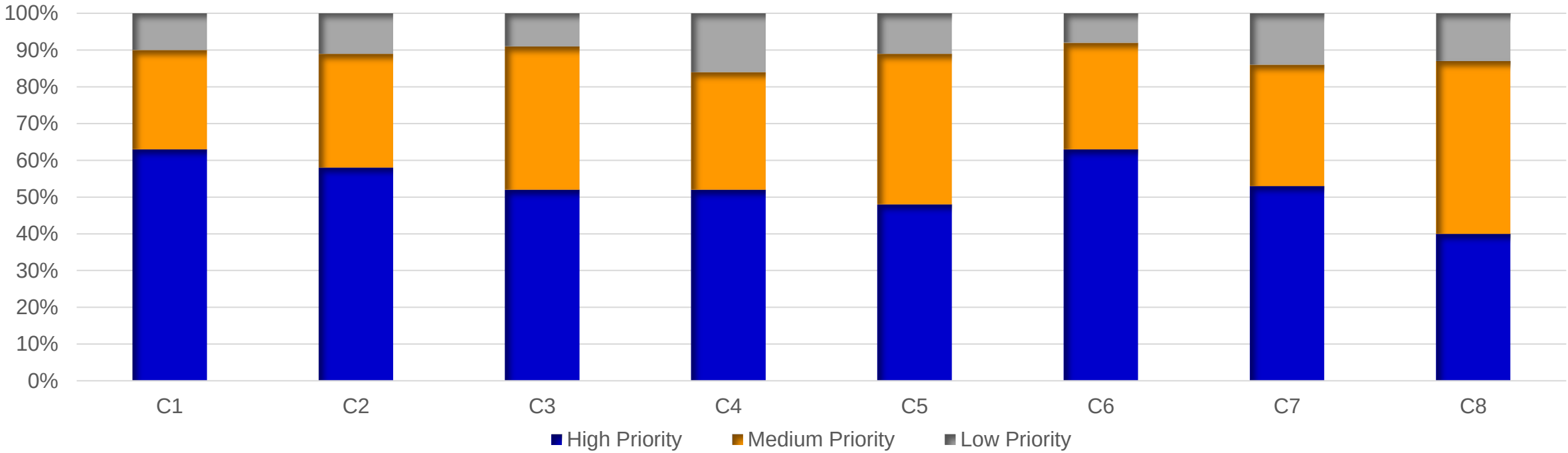
- **Industry/Defense:** 50
- **Government:** 9
- **Academia:** 117
- **Total**: 176

Industry/Defense	Academia
Synopsys	U of Florida
IEEE	U of Auburn
Intel	U of Ohio
Hyperion Gray	Yale
Arm	Clemson U
MITRE	Fullerton
Edaptive	Polimi
Security Compass	U of Michigan
Fox Crypto	Simon Fraser U
Aerocyonics	Eastern Michigan U
LCIS - Grenoble INP	UNC Charlotte
Secure Foundry	Wayne State U
ProtonMail	National U of Singapore
ACM	Purdue U
PQShield	UNTL
Microchip Technology	U of Tehran
Niobium Microsystems	NUST
Garrison	Carnegie Mellon U
Lattice Semi	North South U
Microsoft	KU Leuven
Tescan	U of Applied Sciences of Eastern Switzerland
American Semiconductor	Indian Institute of Technology Madras
Mentor (Siemens)	U of South Florida
Nimbis Services	Indiana U of Pennsylvania
Atlantic Broadband	
Analog	
Raytheon	
Radiance Tech	
Tortuga Logic	
Aero	
SRC	
LMCO	
Battelle	
Boeing	
GLC Squared	
Alion Science	

All Rights Reserved

Counterfeit Electronics Components and Supply Chain

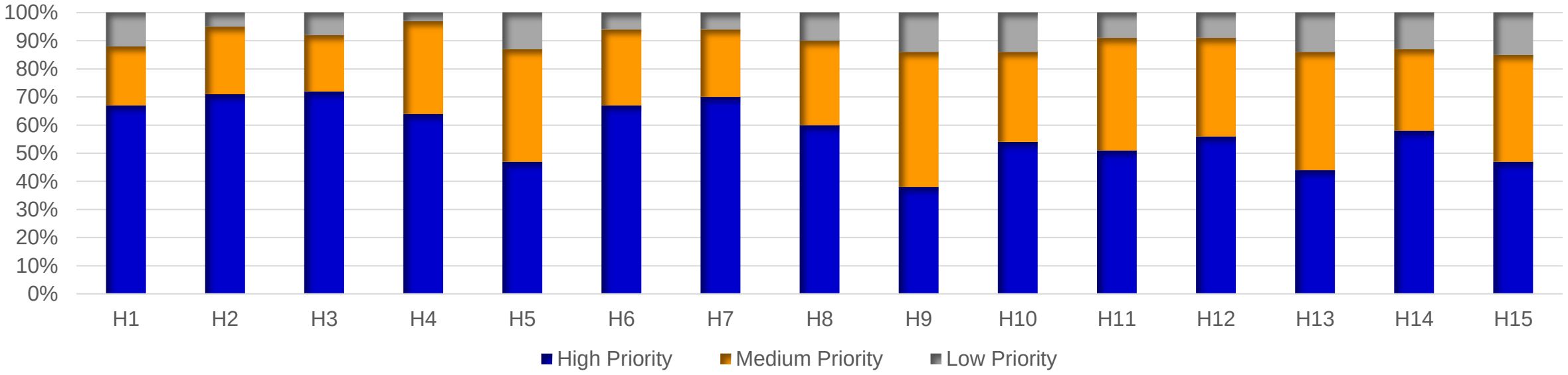
C1	Development of low-cost anti-counterfeiting techniques (E.g., Unique package and chip ID generation for all part types (analog and digital parts, small and large ICs, passive and active components)
C2	Development of low-cost counterfeit detection techniques (E.g., electrical tests; Visual inspection; Spec tests, and more)
C3	Counterfeit detection technology assessment (E.g., Define quantitative metrics; Collect and review historical test data; Test confidence analysis;)
C4	Working with policy makers to mitigate counterfeiting and improving supply chain security
C5	Risk-based analysis for counterfeit detection and prevention
C6	Investigating emerging technologies used by counterfeiters and development of new detection techniques
C7	Establish an adaptive approach to continuously monitor and validate the state of the art in counterfeit detection
C8	Electronic part (IC, PCB, and System) track & trace



All Rights Reserved

Hardware Security and Trust

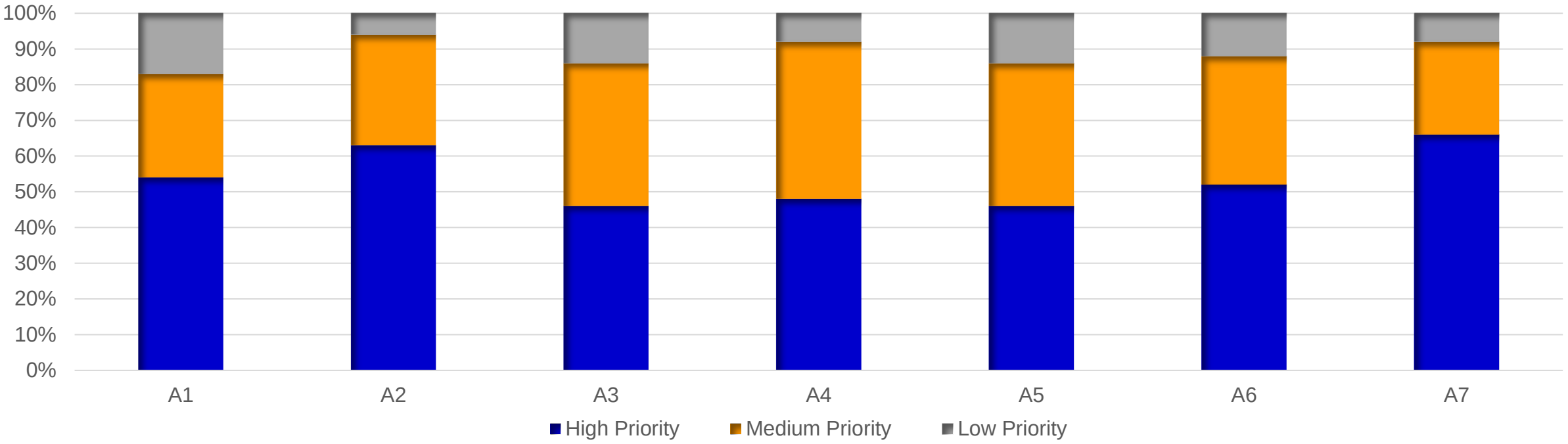
H1	Hardware Trojan detection and prevention
H2	Protection against IP piracy
H3	SoC vulnerability assessment against info leakage, Trojan, side-channel leakage, fault injection, and more
H4	System-level risk and vulnerability analysis, Risk analysis considering hardware-software issues
H5	Reverse engineering and anti-reserve engineering
H6	Run-time security analysis, authentication, and verification
H7	Secure and reliable computing (Data integrity; Code protection and verification; Security of multi-core system: Secure human computer interface)
H8	Post-silicon vulnerability assessment and countermeasures
H9	Hardware security auditing
H10	Light-weight secure cryptographic hardware
H11	Hardware accelerators for secure computation (FHE, FE, encrypted DB)
H12	Hardware interface for managing the security of cloud storage (integrity, freshness, privacy, obfuscation of access patterns, access control policy)
H13	Hardware for verifying security properties (e.g., remote auditing, geolocation of data, network traffic patterns)
H14	Secure CAD tools
H15	Benchmarking



All Rights Reserved

CAD for Assurance

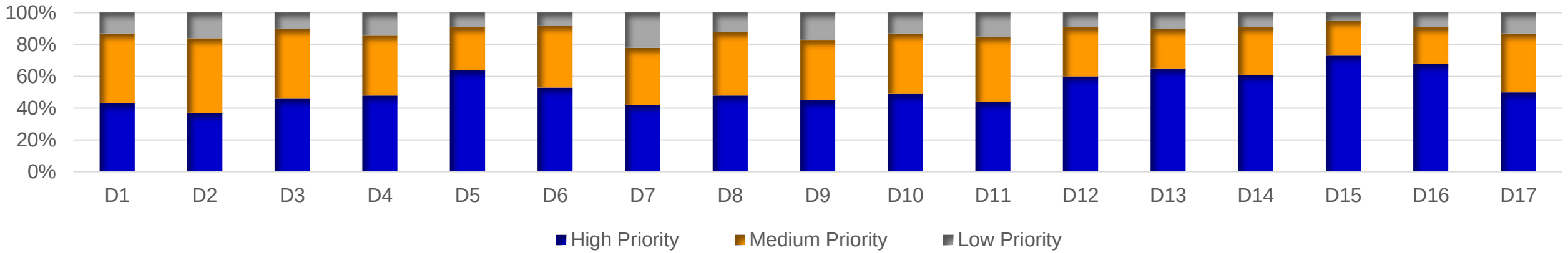
A1	Open-source CAD tools for security verification
A2	Creating metrics for security verification and validation coverage analysis
A3	Developing test chips for cross validation security metrics
A4	Using formal methods to create security and trust proofs
A5	Vulnerability assessment of High-level synthesis flow
A6	Analysis of unintentional security vulnerabilities introduced by EDA tool
A7	Security IP development



All Rights Reserved

Digital and Programmable Devices

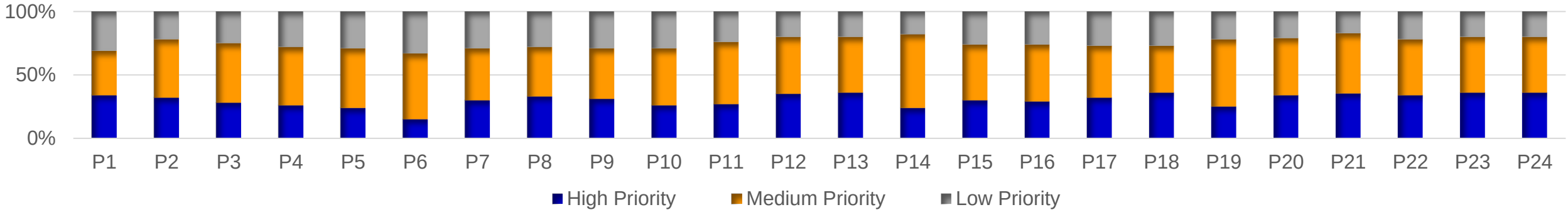
D1	Trojan/Malware insertion
D2	Cloning and Overbuilding
D3	Reverse engineering
D4	FPGA tool chain security (opensource vs proprietary tools)
D5 **D6** **D7** **D8**	Side-Channel attacks on FPGAs (DPA, EMI, FA) Security policies and assets management (key management, HW-RoT, encrypted memory) Over-the-air FPGA programming Security in cloud-based FPGAs
D9	Counterfeited FPGAs
D10	eFPGA implications on the SoCs security (security policy, access rights, testing/programing ports vulnerabilities)
D11 **D12**	Speculative attacks (Meltdown, Spectre, etc.) Side-Channel attacks in processors
D13 **D14** **D15** **D16**	HW security (information leakage, side-channel attacks) in special purpose processors and accelerators: GPUs DSPs Crypto-accelerators AI accelerators
D17	HW-Security and Chain-of-Trust in PLC and SCADA systems (infrastructure monitoring and control, industrial control)



All Rights Reserved

Physical Inspection

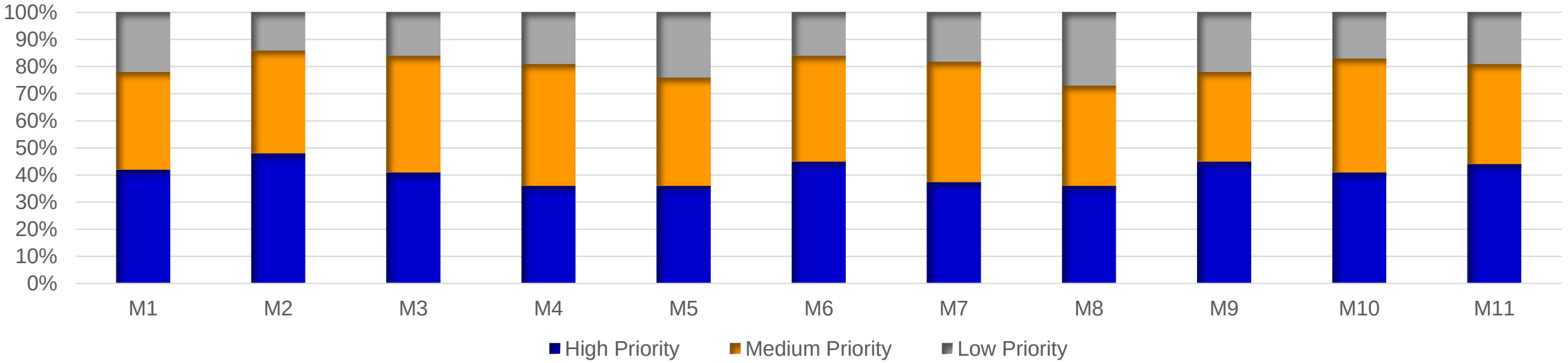
P1 **P2**	Bill of material extraction Defect detection
P3	Optical Inspection for components defect inspection
P4 **P5**	2D X-ray for PCB board internal structure inspection 2D X-ray for PCB surface mounted components inspection
P6 **P7**	3D X-ray for PCB board internal structure inspection 3D X-ray for PCB surface mounted components inspection
P8	Destructive PCB reverse engineering
P9	2D and 3D X-ray for die level inspection
P10	Acoustic imaging for components package integrity
P11	Electro Optical probing and imaging for data extraction
P12	IR and Thermal imaging for IC inspection
P13	Scanning Electron Microscopy (SEM) for IC decomposition or Trojan detection
P14	He Ion imaging for IC decomposition or Trojan detection
P15	THz imaging and spectroscopy for PCB reverse engineering
P16	THz imaging and spectroscopy for components fingerprinting
P17	Focused Ion Beam (FIB) for circuit edit, reroute and asset extraction
P18	Micro/Nano/Pico Probing for asset extraction
P19	Scanning Microwave Impedance Microscopy (sMIM) for asset extraction (floating gates)
P20	Electron Beam Probing for asset extraction (cache activity)
P21	Fault injection using laser/X-ray beam/Electron beam
P22	Packaging encapsulant security and reliability
P23	Packaging interposer security and reliability
P24	3D package structure security and reliability



All Rights Reserved

Analog/Mixed-Signal

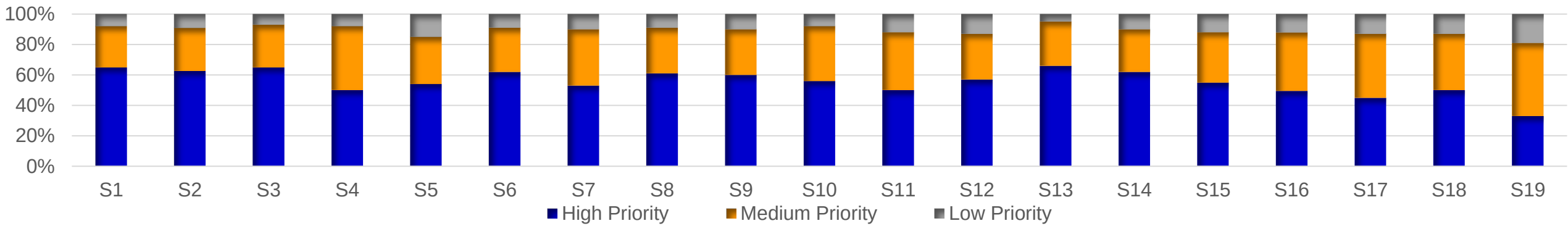
M1	Circuit level reverse engineering and IP piracy
M2	Analog enhanced security IPs including PUFs, CDIR, TRNG, etc.
M3	Side-Channel protection of wireline and wireless receivers
M4	Functional probing and tampering of RF and Mixed-Signal
M5	Camouflaged Analog/RF/Mixed-Signal circuits and systems
M6	Tamper-proof circuits (detection of imaging such as X-RAY, SEM, etc to disable active operation)
M7	Analog signaling and encryption (i.e., modulation analog signal via key or sequences)
M8	Layout-centric IP reverse engineering protection (metallization, dummy circuits, etc)
M9	Post fabrication processing for IP protection
M10	Lifetime/aging analysis for counterfeit detection
M11	Interface security



All Rights Reserved

System Security

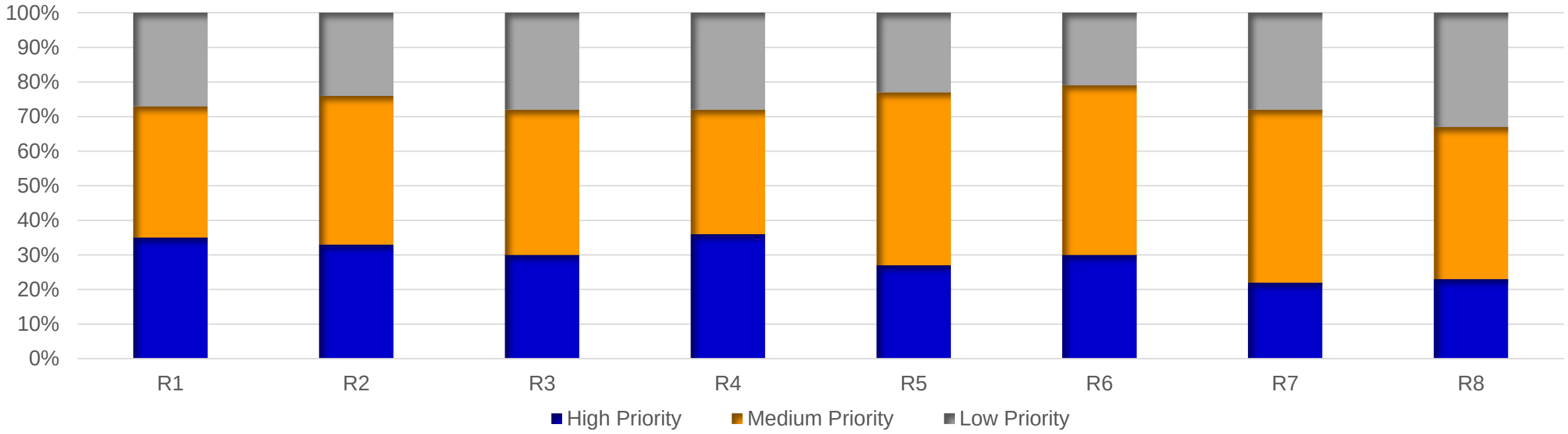
S1 **S2** **S3**	**Security and assurance as a design constraint on system level:** Quantification metrics of security and assurance CAD for security (assessment and countermeasures implementation) End-to-end security and assurance framework (from specification to deployment and retirement)
S4 **S5**	**3PIP security and assurance:** Trojan detection IP protection, overproduction, reverse engineering
S6 **S7** **S8** **S9** **S10** **S11** **S12**	**Security on the SoC level:** Security policies, asset management, and access control Secure enclaves and encrypted/secure memories Integration of untrusted IPs Test structure vulnerabilities and countermeasures Information leakage through SoC interfaces (JTAG, SPI, UART, GPIO, etc) Reverse engineering and IP piracy System stability and fault tolerance
S13 **S14** **S15** **S16**	**SoC HW/SW stack integration:** Hardware Root-of-Trust (HW RoT), and Chain-of-Trust Secure Boot Formally verified secure operating systems Over-the-Air SW updates/patches
S17 **S18** **S19**	**Board level security:** PCB side-channel leakage (EMI and near field information leakage) Supply-chain assurance and malicious components (big-hack like threats) RF/AMS modules security



All Rights Reserved

Reliability

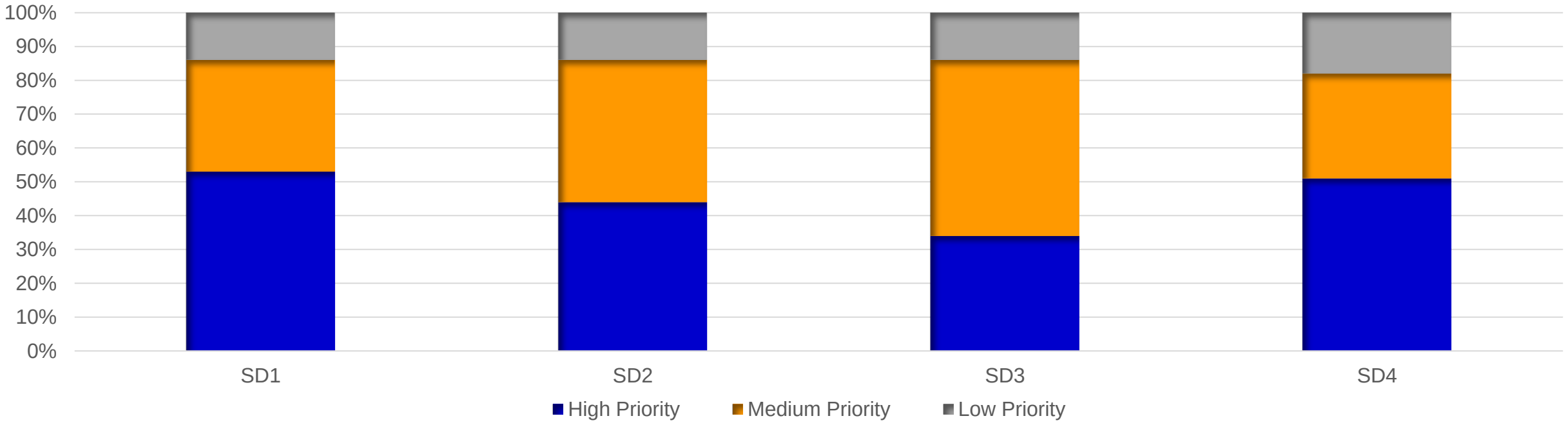
R1	System resiliency and self calibration (ABB and ASV)
R2	Performance degradation and analysis & efficient guardbanding
R3	In-field system repair
R4	Lifetime degradation analysis (MTTF)
R5	Soft-error mitigation
R6	Analyzing reliability challenges in lower technology nodes (TDDB, Electromigration, BTI, and HCI)
R7	Reliable storage that allows proofs of retrievability
R8	ESD analysis and protection



All Rights Reserved

Standard Development

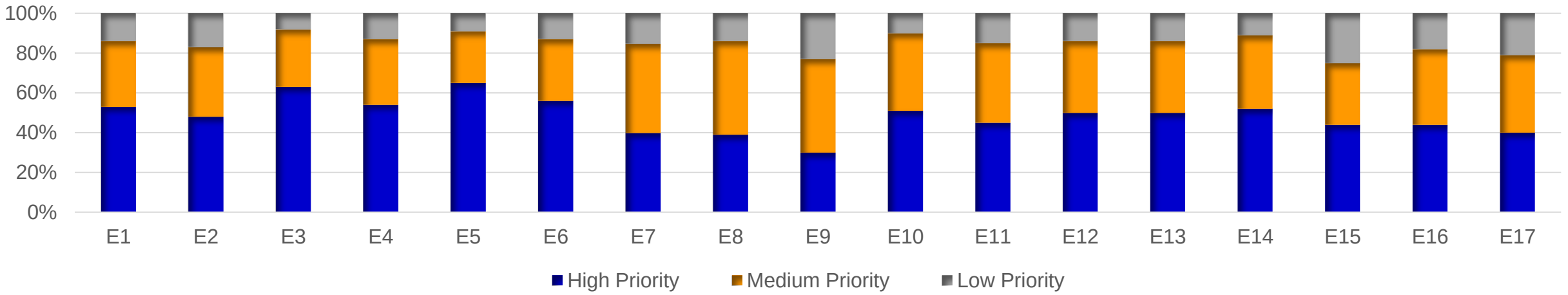
SD1	Development of standard tests or design methods to detect or prevent IC tampering. (Hardware Trojans; Reverse engineering; Side-channel attack; Probing)
SD2	Development of standard for counterfeit IC detection and avoidance.(Technology readiness and cost analysis; Cost/benefit analysis for counterfeit detection using existing techniques;…
SD3	Hardware security auditing
SD4	Development of standards for preventing ICs cloning. (Unique reliable chip ID; Active hardware; metering; Application of DNA marking/Nano rods/Nano particles)



All Rights Reserved

Emerging Threats

E1	Monitoring trends in counterfeiting
E2	New counterfeit types
E3	Automotive security
E4	Introducing new attack vectors
E5	Attacks security features through machine learning and AI
E6	New side-channel attacks (e.g., Cache)
E7	Attacking virtual rootkits
E8	Corrupting devices
E9	Backside imaging techniques without decapping
E10	Security analysis of Post-quantum crypto modules
E11	Neuromorphic Computing
E12	Privacy preserving computing
E13	Homomorphic encryption
E14	Security concerns created by AI accelerators
E15	Blockchain for checking the authenticity of microelectronics and FPGA designs
E16	Digital Twin for secure microelectronics
E17	Secure packaging



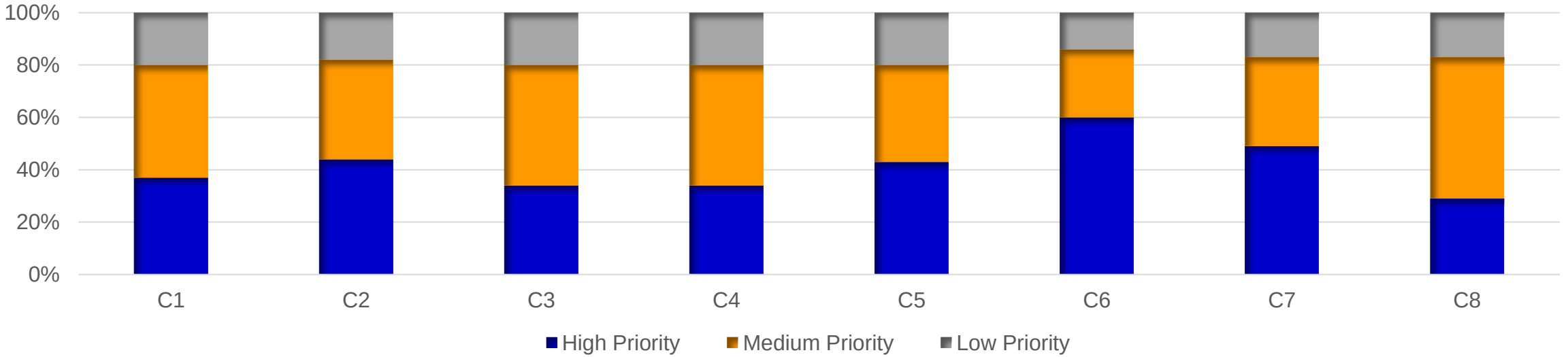
All Rights Reserved

Industry Response

All Rights Reserved

Counterfeit Electronics Components and Supply Chain

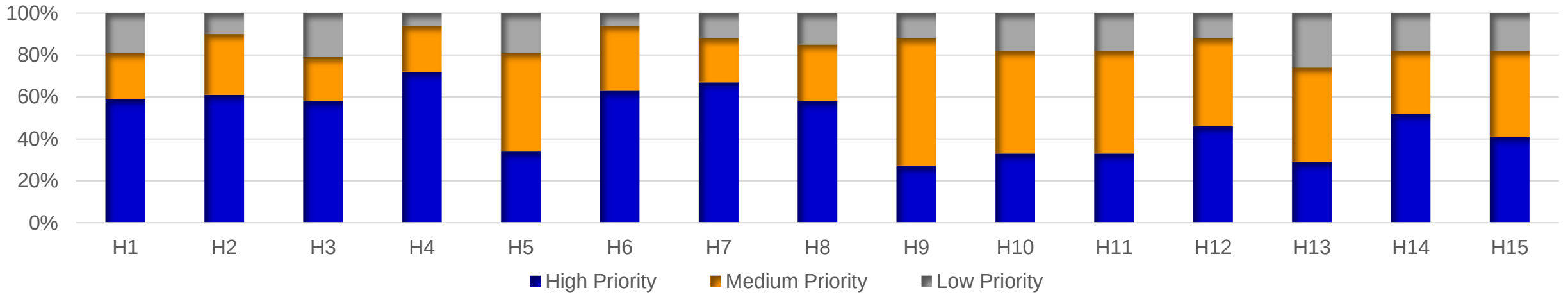
C1	Development of low-cost anti-counterfeiting techniques (E.g., Unique package and chip ID generation for all part types (analog and digital parts, small and large ICs, passive and active components)
C2	Development of low-cost counterfeit detection techniques (E.g., electrical tests; Visual inspection; Spec tests, and more)
C3	Counterfeit detection technology assessment (E.g., Define quantitative metrics; Collect and review historical test data; Test confidence analysis;)
C4	Working with policy makers to mitigate counterfeiting and improving supply chain security
C5	Risk-based analysis for counterfeit detection and prevention
C6	Investigating emerging technologies used by counterfeiters and development of new detection techniques
C7	Establish an adaptive approach to continuously monitor and validate the state of the art in counterfeit detection
C8	Electronic part (IC, PCB, and System) track & trace



All Rights Reserved

Hardware Security and Trust

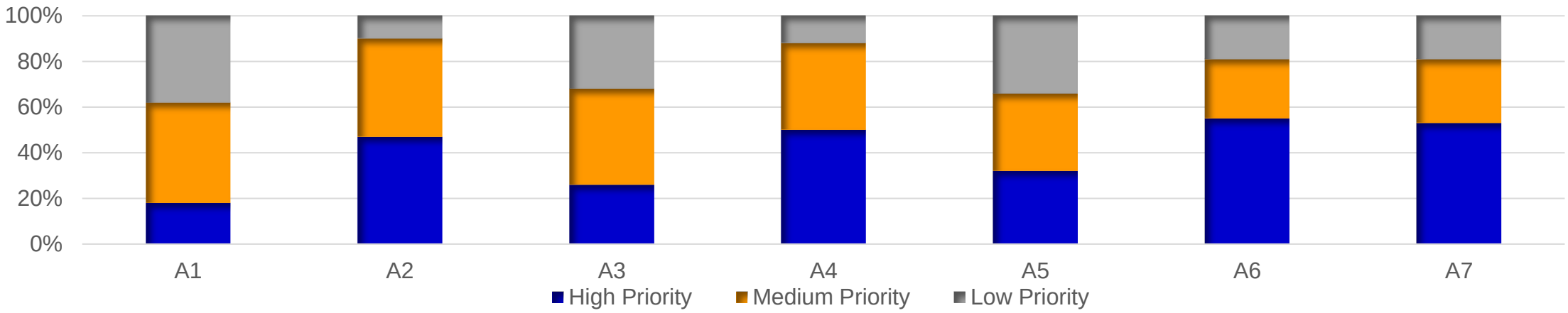
H1	Hardware Trojan detection and prevention
H2	Protection against IP piracy
H3	SoC vulnerability assessment against info leakage, Trojan, side-channel leakage, fault injection, and more
H4	System-level risk and vulnerability analysis, Risk analysis considering hardware-software issues
H5	Reverse engineering and anti-reserve engineering
H6	Run-time security analysis, authentication, and verification
H7	Secure and reliable computing (Data integrity; Code protection and verification; Security of multi-core system: Secure human computer interface)
H8	Post-silicon vulnerability assessment and countermeasures
H9	Hardware security auditing
H10	Light-weight secure cryptographic hardware
H11	Hardware accelerators for secure computation (FHE, FE, encrypted DB)
H12	Hardware interface for managing the security of cloud storage (integrity, freshness, privacy, obfuscation of access patterns, access control policy)
H13	Hardware for verifying security properties (e.g., remote auditing, geolocation of data, network traffic patterns)
H14	Secure CAD tools
H15	Benchmarking



All Rights Reserved

CAD for Assurance

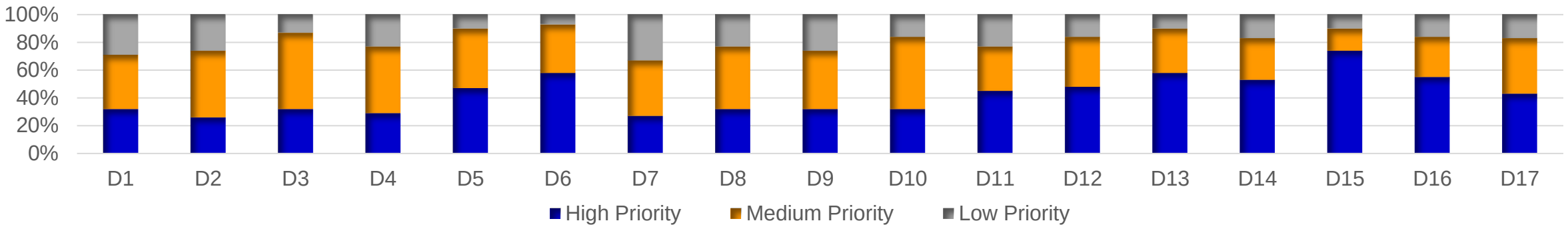
A1	Open-source CAD tools for security verification
A2	Creating metrics for security verification and validation coverage analysis
A3	Developing test chips for cross validation security metrics
A4	Using formal methods to create security and trust proofs
A5	Vulnerability assessment of High-level synthesis flow
A6	Analysis of unintentional security vulnerabilities introduced by EDA tool
A7	Security IP development



All Rights Reserved

Digital and Programmable Devices

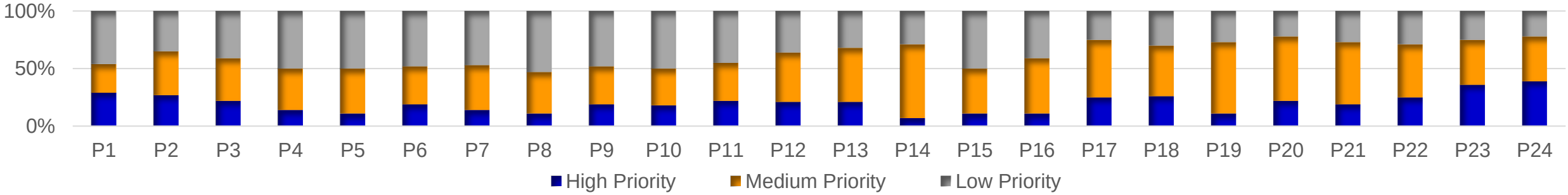
D1	Trojan/Malware insertion
D2	Cloning and Overbuilding
D3	Reverse engineering
D4	FPGA tool chain security (opensource vs proprietary tools)
D5 **D6** **D7** **D8**	Side-Channel attacks on FPGAs (DPA, EMI, FA) Security policies and assets management (key management, HW-RoT, encrypted memory) Over-the-air FPGA programming Security in cloud-based FPGAs
D9	Counterfeited FPGAs
D10	eFPGA implications on the SoCs security (security policy, access rights, testing/programing ports vulnerabilities)
D11 **D12**	Speculative attacks (Meltdown, Spectre, etc.) Side-Channel attacks in processors
D13 **D14** **D15** **D16**	HW security (information leakage, side-channel attacks) in special purpose processors and accelerators: GPUs DSPs Crypto-accelerators AI accelerators
D17	HW-Security and Chain-of-Trust in PLC and SCADA systems (infrastructure monitoring and control, industrial control)



All Rights Reserved

Physical Inspection

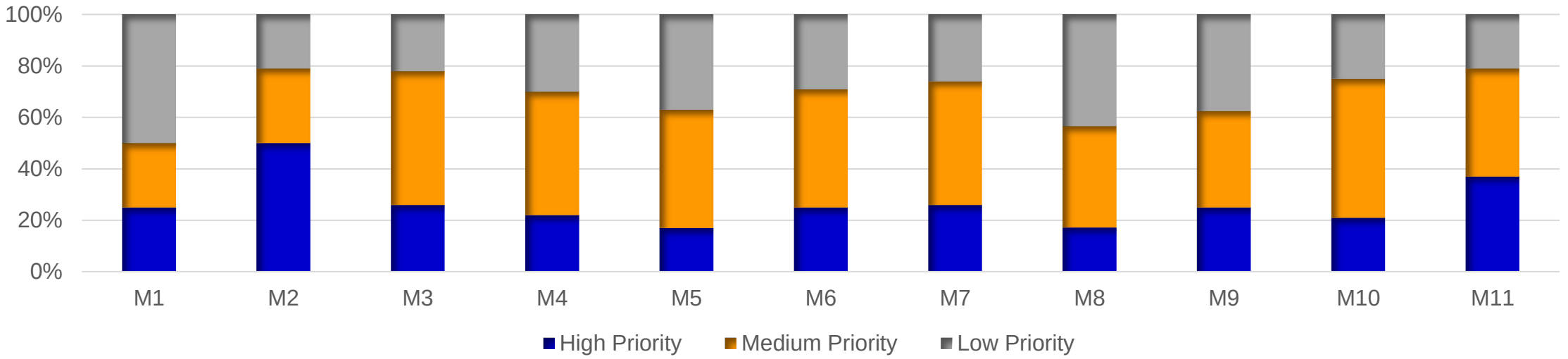
P1 **P2**	• Bill of material extraction • Defect detection
P3	Optical Inspection for components defect inspection
P4 **P5**	2D X-ray for PCB board internal structure inspection 2D X-ray for PCB surface mounted components inspection
P6 **P7**	3D X-ray for PCB board internal structure inspection 3D X-ray for PCB surface mounted components inspection
P8	Destructive PCB reverse engineering
P9	2D and 3D X-ray for die level inspection
P10	Acoustic imaging for components package integrity
P11	Electro Optical probing and imaging for data extraction
P12	IR and Thermal imaging for IC inspection
P13	Scanning Electron Microscopy (SEM) for IC decomposition or Trojan detection
P14	He Ion imaging for IC decomposition or Trojan detection
P15	THz imaging and spectroscopy for PCB reverse engineering
P16	THz imaging and spectroscopy for components fingerprinting
P17	Focused Ion Beam (FIB) for circuit edit, reroute and asset extraction
P18	Micro/Nano/Pico Probing for asset extraction
P19	Scanning Microwave Impedance Microscopy (sMIM) for asset extraction (floating gates)
P20	Electron Beam Probing for asset extraction (cache activity)
P21	Fault injection using laser/X-ray beam/Electron beam
P22	Packaging encapsulant security and reliability
P23	Packaging interposer security and reliability
P24	3D package structure security and reliability



All Rights Reserved

Analog/Mixed-Signal

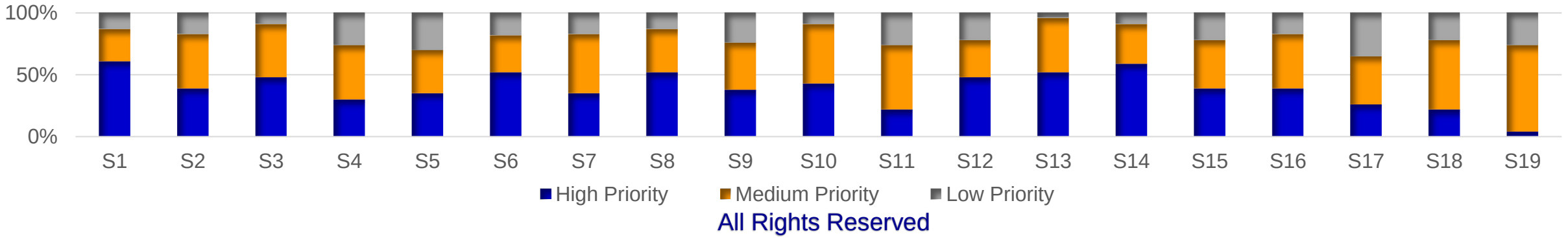
M1	Circuit level reverse engineering and IP piracy
M2	Analog enhanced security IPs including PUFs, CDIR, TRNG, etc.
M3	Side-Channel protection of wireline and wireless receivers
M4	Functional probing and tampering of RF and Mixed-Signal
M5	Camouflaged Analog/RF/Mixed-Signal circuits and systems
M6	Tamper-proof circuits (detection of imaging such as X-RAY, SEM, etc to disable active operation)
M7	Analog signaling and encryption (i.e., modulation analog signal via key or sequences)
M8	Layout-centric IP reverse engineering protection (metallization, dummy circuits, etc)
M9	Post fabrication processing for IP protection
M10	Lifetime/aging analysis for counterfeit detection
M11	Interface security



All Rights Reserved

System Security

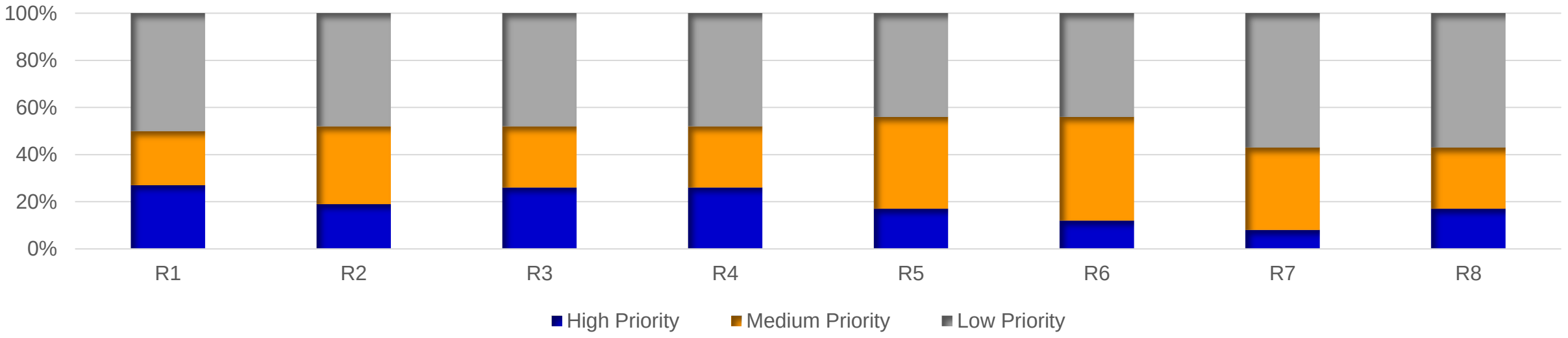
S1 **S2** **S3**	**Security and assurance as a design constraint on system level:** Quantification metrics of security and assurance CAD for security (assessment and countermeasures implementation) End-to-end security and assurance framework (from specification to deployment and retirement)
S4 **S5**	**3PIP security and assurance:** Trojan detection IP protection, overproduction, reverse engineering
S6 **S7** **S8** **S9** **S10** **S11** **S12**	**Security on the SoC level:** Security policies, asset management, and access control Secure enclaves and encrypted/secure memories Integration of untrusted IPs Test structure vulnerabilities and countermeasures Information leakage through SoC interfaces (JTAG, SPI, UART, GPIO, etc) Reverse engineering and IP piracy System stability and fault tolerance
S13 **S14** **S15** **S16**	**SoC HW/SW stack integration:** Hardware Root-of-Trust (HW RoT), and Chain-of-Trust Secure Boot Formally verified secure operating systems Over-the-Air SW updates/patches
S17 **S18** **S19**	**Board level security:** PCB side-channel leakage (EMI and near field information leakage) Supply-chain assurance and malicious components (big-hack like threats) RF/AMS modules security



All Rights Reserved

Reliability

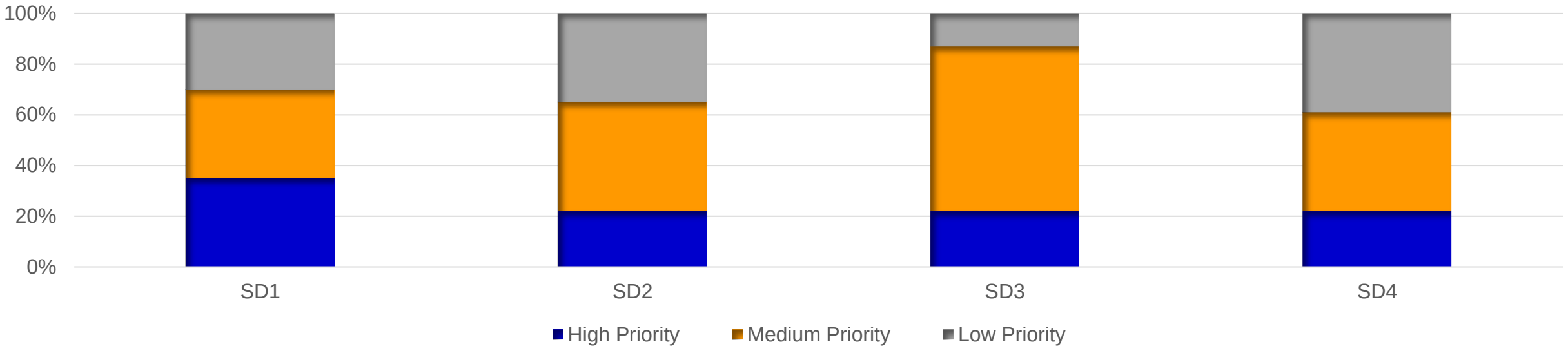
R1	System resiliency and self calibration (ABB and ASV)
R2	Performance degradation and analysis & efficient guardbanding
R3	In-field system repair
R4	Lifetime degradation analysis (MTTF)
R5	Soft-error mitigation
R6	Analyzing reliability challenges in lower technology nodes (TDDB, Electromigration, BTI, and HCI)
R7	Reliable storage that allows proofs of retrievability
R8	ESD analysis and protection



All Rights Reserved

Standard Development

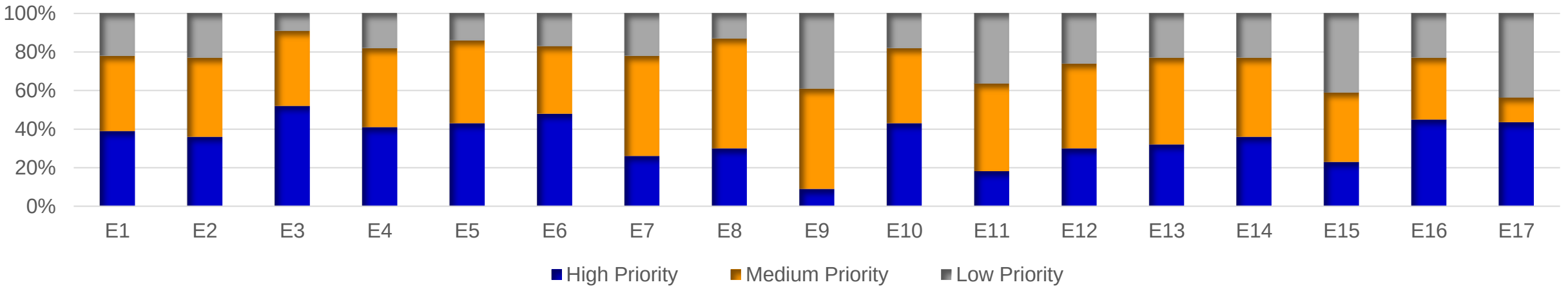
SD1	Development of standard tests or design methods to detect or prevent IC tampering. (Hardware Trojans; Reverse engineering; Side-channel attack; Probing)
SD2	Development of standard for counterfeit IC detection and avoidance.(Technology readiness and cost analysis; Cost/benefit analysis for counterfeit detection using existing techniques;…
SD3	Hardware security auditing
SD4	Development of standards for preventing ICs cloning. (Unique reliable chip ID; Active hardware; metering; Application of DNA marking/Nano rods/Nano particles)



All Rights Reserved

Emerging Threats

E1	Monitoring trends in counterfeiting
E2	New counterfeit types
E3	Automotive security
E4	Introducing new attack vectors
E5	Attacks security features through machine learning and AI
E6	New side-channel attacks (e.g., Cache)
E7	Attacking virtual rootkits
E8	Corrupting devices
E9	Backside imaging techniques without decapping
E10	Security analysis of Post-quantum crypto modules
E11	Neuromorphic Computing
E12	Privacy preserving computing
E13	Homomorphic encryption
E14	Security concerns created by AI accelerators
E15	Blockchain for checking the authenticity of microelectronics and FPGA designs
E16	Digital Twin for secure microelectronics
E17	Secure packaging



All Rights Reserved