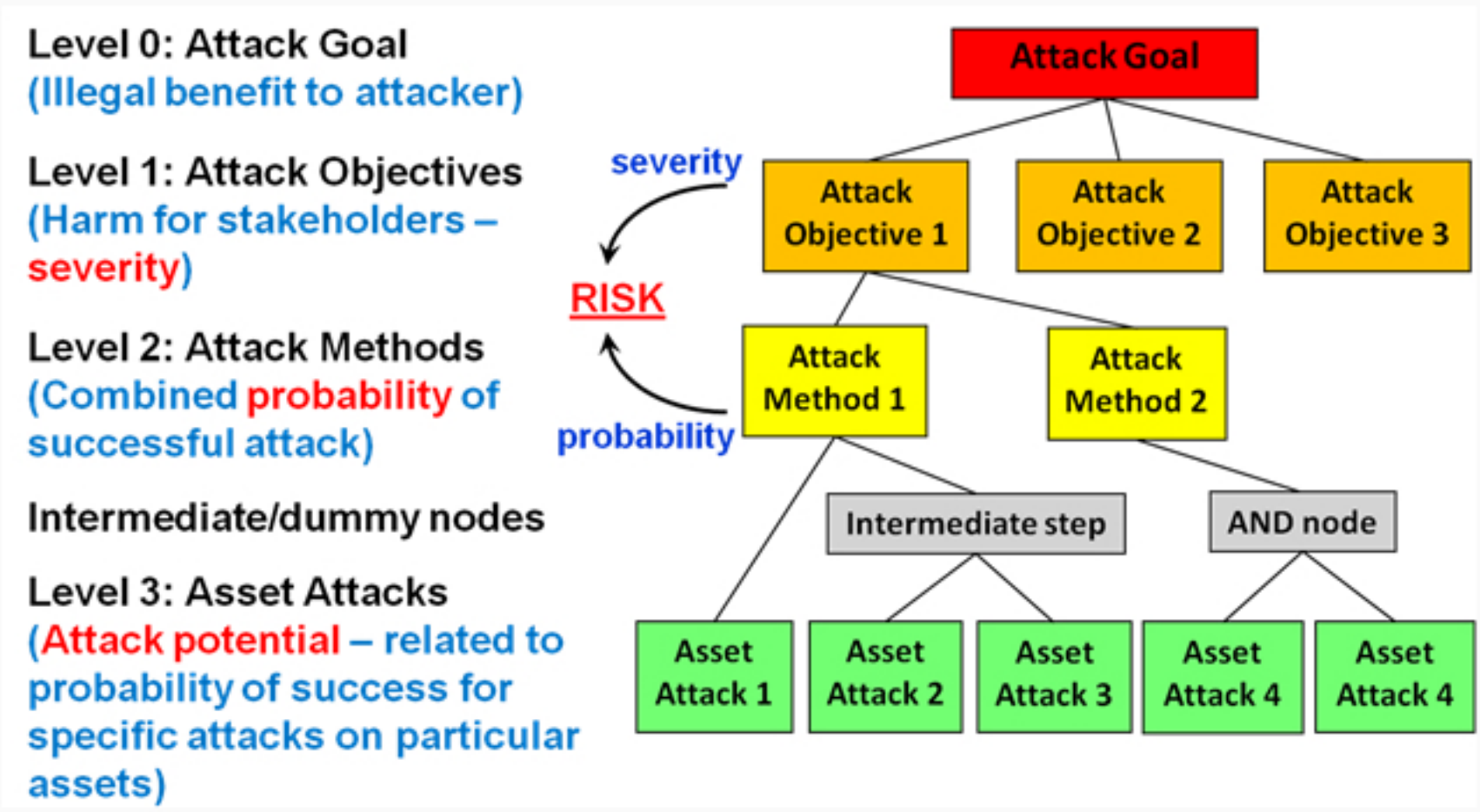
Automotive Cybersecurity - TARA

“Cyber-physical vehicle system은 허가되지 않은 접근 또는 악의적인 공격으로 부터 시스템을 보호하기 위해 잠재적인 사이버 보안 위협을 식별하고 식별된 보안 위협과 관련된 위험성을 평가하는 활동 (Threat Analysis and Risk Assessment, TARA)이 요구됩니다.”

TARA를 수행하는 방법으로는 E-Safety Vehicle Intrusion Protected Applications (EVITA), Threat, Vulnerabilities, and implementation Risks Analysis (TVRA), Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) 등이 있습니다.

TARA를 수행하기 위해서는 우선 잠재적인 공격 위협 (Attack Potential)을 도출해야 하는데, 이때 가장 많이 사용되는 방법이 공격 트리 (Attack Tree) 입니다. 공격 트리는 아래 그림처럼 공격자가 대상 시스템으로 부터 이득을 얻고자 하는 Attack Goal에서 부터 출발하여, Attack Objectives □ Attack Methods □ Asset Attacks 으로 구체화하는 과정을 거치게 됩니다.

■ Attack Tree 구성



TARA 수행 방법 중 EVITA 에서는 보안 목적으로 Safety, Privacy, Financial, Operational의 4가지를 고려하고 있으며, 도출된 잠재 위협에 대한 위험성 평가를 위해 Severity, Probability, Controllability 분류 상세 기준을 제시하고 있습니다. 특히 보안 위협에 의해 기능 안전 (Safety)이 실패하는 경우에 대한 위험도는 아래와 같이 평가됩니다.

■ 안전 관련 보안 위협에 대한 위험도

Controllability (C)	Safety-related Severity (S_S)	Combined Attack Probability (A)				
		A=1	A=2	A=3	A=4	A=5
C=1	S_S = 1	R0	R0	R1	R2	R3
	S_S = 2	R0	R1	R2	R3	R4
	S_S = 3	R1	R2	R3	R4	R5
	S_S = 4	R2	R3	R4	R5	R6
C=2	S_S = 1	R0	R1	R2	R3	R4
	S_S = 2	R1	R2	R3	R4	R5
	S_S = 3	R2	R3	R4	R5	R6
	S_S = 4	R3	R4	R5	R6	R7
C=3	S_S = 1	R1	R2	R3	R4	R5
	S_S = 2	R2	R3	R4	R5	R6
	S_S = 3	R3	R4	R5	R6	R7
	S_S = 4	R4	R5	R6	R7	R7+
C=4	S_S = 1	R2	R3	R4	R5	R6
	S_S = 2	R3	R4	R5	R6	R7
	S_S = 3	R4	R5	R6	R7	R7+
	S_S = 4	R5	R6	R7	R7+	R7+

(출처 : SAE J3061, Cybersecurity Guidebook for Cyber-Physical Vehicle Systems)